grass valley
A BELDEN BRAND

GV STRATUS®

VIDEO PRODUCTION & CONTENT MANAGEMENT SYSTEM

Topic Library

Version 6.8

2019-03-18

www.grassvalley.com

FCC Compliance

In order to comply with FCC/CFR47: Part 15 regulations, it is necessary to use Mini HDMI to HDMI high-quality triple-screened cable assemblies with integrated ferrite suppression at both ends.

Patent Information

This product may be protected by one or more patents.

For further information, please visit: www.grassvalley.com/patents/

Copyright and Trademark Notice

Copyright © 2019, Grass Valley Canada. All rights reserved.

Belden, Belden Sending All The Right Signals, and the Belden logo are trademarks or registered trademarks of Belden Inc. or its affiliated companies in the United States and other jurisdictions. Grass Valley, GV STRATUS are trademarks or registered trademarks of Grass Valley Canada. Belden Inc., Grass Valley Canada, and other parties may also have trademark rights in other terms used herein.

Terms and Conditions

Please read the following terms and conditions carefully. By using Product Name documentation, you agree to the following terms and conditions.

Grass Valley hereby grants permission and license to owners of Product Name to use their product manuals for their own internal business use. Manuals for Grass Valley products may not be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose unless specifically authorized in writing by Grass Valley.

A Grass Valley manual may have been revised to reflect changes made to the product during its manufacturing life. Thus, different versions of a manual may exist for any given product. Care should be taken to ensure that one obtains the proper manual version for a specific product serial number.

Information in this document is subject to change without notice and does not represent a commitment on the part of Grass Valley.

Warranty information is available from the Legal Terms and Conditions section of Grass Valley's website (www.grassvalley.com).

Title	GV STRATUS Topic Library
Version	6.8
Revision	2019-03-18, 01:49

This version of the GV STRATUS Topic Library is provided for download. Once downloaded, this version is uncontrolled and is not tracked for updates. For the most current and up-to-date information refer to the online Topic Library at http://wwwapps.grassvalley.com/gv_stratusmanual

Contents

Release Notes....15
GV STRATUS Version 6.8....15
Not supported in this GV STRATUS release....15
Changes and features in previous releases....16
GV STRATUS Version 6.5....16
GV STRATUS Version 6.0....17
GV STRATUS Version 5.7....18
GV STRATUS Version 5.5 (SP3)....19
GV STRATUS Version 5.5 (SP1)....19
GV STRATUS Version 5.5....20
GV STRATUS Version 5.0 (SP2)....20
GV STRATUS Version 5.0 (SP1)....21
GV STRATUS Version 5.0....21
GV STRATUS Version 4.8 (SP4)....22
GV STRATUS Version 4.8 (SP2)....22
GV STRATUS Version 4.8 (SP1)....22
GV STRATUS Version 4.8....23
GV STRATUS Version 4.5.2....24
GV STRATUS Version 4.5....24
GV STRATUS Version 4.0.8....25
GV STRATUS Version 4.0.7....26
GV STRATUS Version 4.0.6....26
GV STRATUS Version 4.0.5....27
GV STRATUS Version 4.0.4....27
GV STRATUS Version 4.0.3....28
GV STRATUS Version 4.0.1....28
GV STRATUS Version 4.0....29
GV STRATUS Version 3.5.1....29
GV STRATUS Version 3.5....30
GV STRATUS Version 3.1....32
GV STRATUS Version 3.0....32
GV STRATUS Rundown Version 8.2....33
GV STRATUS Rundown Version 8.1....34
GV STRATUS Rundown Version 8.0....34
GV STRATUS VTR Ingest Version 9.5....34
GV STRATUS VTR Ingest Version 8.5.0.29....35
Additional notes....35
Topic Library replaces PDF manuals....35
About groups and users on a GV STRATUS system....37
GV STRATUS roles matrix....37
Grass Valley Recommended Deployment and Monitoring Solutions....40
Passwords and security on Grass Valley systems....41
Disabling User Account Control for GV STRATUS Rundown on Windows 7 clients....43
Setting up AMP control for GV STRATUS Rundown on a K2 Client....43
Installing GV STRATUS Rundown software manually....43
Setting up ENPS for GV STRATUS Rundown....44
Setting up iNEWS for GV STRATUS Rundown....46
Setting up Octopus for GV STRATUS Rundown....47
GV STRATUS Operation considerations....50
GV STRATUS Rundown Operation considerations....51
GV STRATUS VTR Ingest Operation considerations....51
GV STRATUS Version compatibility....52

System requirements for GV STRATUS client PC 52
Compatible GV STRATUS components....54
Grass Valley products compatible with GV STRATUS....56
Third party products compatible with GV STRATUS....57
GV STRATUS archive support....58
GV STRATUS Rundown Version compatibility....58
GV STRATUS Rundown System specifications....59
Grass Valley products compatible with GV STRATUS Rundown....59
Third party products compatible with GV STRATUS Rundown....60
GV STRATUS VTR Ingest Version compatibility....61
GV STRATUS VTR Ingest system specifications....61
Licensing GV STRATUS products....61
Licensing a GV STRATUS system....61
About GV STRATUS Rundown software licensing....62
GV STRATUS Rundown licenses....62
GV STRATUS VTR Ingest licenses....63
Licensing EDIUS....63
Requesting a license....63
Adding a license....64
Deleting licenses....64
Archiving licenses....64
GV STRATUS Known Problems....65
GV STRATUS Rundown Known Problems....71
GV STRATUS VTR Ingest Known Problems....73

GV STRATUS Upgrade....74
Upgrading GV STRATUS systems....74
Upgrading to GV STRATUS version 6.8 and K2 Summit version 10.1.1....74
Upgrading GV STRATUS from version 6.5 to version 6.8 with K2 Summit version 9.8.7....101
Upgrading GV STRATUS from version 6.0 to version 6.8 with K2 Summit version 9.8.7....124
Upgrade GV Render Engine server software and EDIUS client software....148
Upgrade Workflow Server, license, configure Rules....170
Upgrading GV STRATUS Rundown systems....173
Upgrading GV STRATUS Rundown devices with SiteConfig....173
Installing and Upgrading GV STRATUS VTR Ingest/GV STRATUS VTR Controller....181
About installing GV STRATUS VTR Ingest/GV STRATUS VTR Controller devices with SiteConfig..181
Prepare for install....182
Prepare SiteConfig for software deployment....182
Install Important Windows updates (recommended)....182
Upgrade K2 systems....183
Install Grass Valley Prerequisite Files on the SiteConfig PC....183
Installing GV STRATUS VTR Ingest/GV STRATUS VTR Controller with SiteConfig....184
Additional Topics....194
Complete listing of device types, roles, and software packages for GV STRATUS devices....194
GV STRATUS roles matrix....204
About Auto Logout....207
Summary of previous GV STRATUS upgrades....208

GV STRATUS Installation and Service....220
Overview of the GV STRATUS System....220
GV STRATUS system and server variants....220
Small (Express) system description: Proxy on Core Services server....221
Medium (A1) system description: Proxy on K2 Summit SAN....222
Large (B1, C1) system description: Proxy on dedicated Proxy Storage system....224
Proxy and live streaming workflow overview....225
HTTP server overview....226
Proxy encoding overview....226
Functional descriptions....227

Preparing for installation....229
About installing the GV STRATUS system....229
Commissioning process....230
Complete system installation process....230
Commissioning a system....231
Commissioning process....231
Rack, cable, and power on process....232
Test system setup and configuration process....246
Customer network, licenses, and roles process....250
Client PC set up process....253
Reference to GV STRATUS Control Panel settings....296
Reference to settings: Required and optional....296
STRATUS Core Services settings....296
MDI Configuration settings....302
Metadata settings....318
Engines settings....328
K2 Storage settings....338
Proxy Config settings....343
Resource Management settings....352
Search Index Config settings....353
Audio Tag Management settings....354
Channels settings....358
Format Configuration settings....362
License Management settings....365
Rules settings....368
Locations Config settings....370
Web Monitor settings....377
EDIUS Settings....378
Ingest settings....380
Rundown Configuration settings....390
RMI settings....396
Router Configuration settings....397
TX Scheduler settings....400
Segmentation settings....403
The Dashboard tool....403
The Send Message tool....409
The Help tool....411
Understanding system concepts....411
Understanding networks....411
About GV STRATUS client PCs....416
About the GV STRATUS Assets view....417
About GV STRATUS system databases....418
About redundant K2 SANs....419
About GV STRATUS markers, Dyno markers, and the K2 database....419
About loop modes in K2, Dyno, and GV STRATUS....422
About custom fields....422
About timecode source and clock synchronization....422
About advanced query syntax, advanced searches and custom expressions....423
Understanding credentials....425
Understanding virus and security policies....427
Understanding system configuration tools....428
Proxy/live streaming technical details....441
MDI and Encoder logical names convention....442
About archive MDIs....442
About roles....443
Asset copies and deletions....443
Devices components: Roles, cab files, services, and licenses....444

GV STRATUS roles matrix....462
Administering and maintaining the GV STRATUS system....469
Configuring the GV STRATUS system....469
Remote and multiple site configuration....473
Security....475
Working with SiteConfig....485
Licensing a GV STRATUS system....498
Working with GV Log Viewer....500
Working with K2Config....522
Working with GV STRATUS servers....524
Configuring a Router....545
Set up RMI PC access to high-resolution assets....557
Working with GVRE Transcoder....558
Configuring Rules....577
Publishing content to Social Media platforms....656
Setting up GV STRATUS in ENPS....660
Setting up Avid workstations with GV STRATUS....661
Configure iNews for Monitor On....684
Configuring custom metadata for House Number List....686
Database planning and maintenance strategies....686
Changing passwords....710
Ports and services mapping....715
Embedded Security modes and policies....718
Complete system set up and configuration....721
Complete system installation process....721
Express/Core server set up process....724
Proxy Server/Storage set up process....738
Render Engine Server set up process....768
Social Media Engine Server set up process....802
External Media Engine Server set up process....819
Standalone Database Server set up process....829
GV STRATUS Control Panel system configuration process....839
SiteConfig software deployment process....857
Archive system set up process....874
Workflow Server set up process....898
Proxy Streaming Server set up process....907
Fully qualified domain configuration....913
Grass Valley SMB Storage configuration....927
K2 Central Storage configuration....934
Troubleshooting the GV STRATUS system....944
Troubleshooting tools....944
If you have trouble launching EDIUS XS....944
Troubleshooting tips....945
Test proxy media generation....946
About application status....947
Viewing and copying version and status information....949
Commissioning checklist....950
Commissioning checklist....950

GV STRATUS Operation....952
Overview of the GV STRATUS application....952
About the GV STRATUS product....952
Logging on....953
About the GV STRATUS application....954
The Navigator panel....955
The Asset List panel....956
The Inspector panel....958
About GV STRATUS tools....960

The Send Message tool....961
The Web Monitor....963
The Dashboard tool....964
About customizing the application workspace....970
Arranging control tray buttons....971
Focusing on a tool....973
Focusing on a viewer in a tool....973
Previewing a live streaming video....975
Managing assets....975
Using the Explore section....975
About the GV STRATUS Assets view....975
Browsing assets....976
Browsing camera angles....977
Asset indicators....977
Adding a favorite 979
Removing or deleting a favorite....979
Managing Asset Lists....979
Searching assets....988
Creating and modifying bins and groups....995
Asset copies and deletions....996
Viewing a video asset....996
Using the Audio Overlay....1002
Adding or modifying audio tags of an asset....1005
Sending video asset to the next display monitor....1007
Access to multiple GV STRATUS sites....1008
Changing the thumbnail of an asset....1010
Importing image file as thumbnail of an asset....1010
Adding or modifying metadata....1012
Adding metadata to assets with angles....1014
Copying asset metadata....1016
Printing asset metadata....1017
Using custom metadata in Inspector....1018
Viewing relationships....1020
Viewing the properties of an item....1020
Verifying proxy association....1021
Regenerating proxy....1022
Ingesting assets....1022
The Scheduler tool....1022
The RMI tool....1058
Working with GV STRATUS Channels....1070
The Channel Panel tool....1070
Configuring K2 Channels User Preferences....1073
Creating a Channel Panel....1075
Launching and closing a Channel Panel....1076
Modifying a Channel Panel while in use....1078
Resizing channels and gangs....1080
Modifying a Channel Panel configuration....1080
Copying a Channel Panel configuration....1080
About recording clips in a Channel Panel....1081
About playing clips in a Channel Panel....1085
Controlling an individual channel in a gang....1090
Locating a loaded clip or playlist....1091
About salvos....1091
Configure router settings in Channel Panel....1093
About keyboard shortcuts and input focus in a Channel Panel....1093
Modifying the clip name in a Channel Panel....1094
Loading an asset into the Inspector from a Channel Panel....1094

Using the scrub bar to navigate through a clip....1095
Identifying and selecting the timecode type....1095
Selecting timecode type to navigate and mark clips....1096
Channel panel markers....1096
Hiding transport controls....1097
Managing Channel Panel configurations....1097
Channel Panel ganging limitations....1097
Channel status indicators....1098
Reconnecting channels....1098
The Playlist Editor tool....1098
Importing, Exporting, and Transferring....1104
About importing, exporting, and transferring....1104
Creating an export share....1104
Importing files to a Grass Valley system 1104
Exporting assets from a K2 Summit system 1105
Transferring between bins using drag and drop....1106
Transferring assets between bins using the context menu....1107
Transferring using Send Destination....1108
Transferring an asset from a remote site....1110
Transferring an asset to a remote site....1111
Sending assets for playout....1112
Monitoring imports, exports, or transfers....1115
Conforming a complex asset to a simple clip....1118
About archiving assets....1122
About restoring assets....1124
The Scheduled Transfer tool....1127
Editing....1137
The Storyboard Editor tool....1137
The Source Viewer....1138
Using mark-in and mark-out points....1145
Adding markers....1146
Adding keywords....1148
Navigating to keywords or markers in an asset....1150
Deleting a marker....1150
Create a subclip....1151
Create subclips from keywords....1152
Trimming a clip in Inspector....1153
The Storyboard....1153
The Sequence Viewer....1155
Creating a sequence 1158
Editing an event....1158
Splitting an event....1158
Configuring Storyboard Editor User Preferences....1159
Using keywords and markers to add an event to a sequence....1159
Adding and removing transitions....1159
Rearranging or deleting events in a sequence....1160
Playing a sequence....1160
Launching a sequence in the EDIUS application....1162
Viewing the properties of an item....1163
Using EDIUS for GV STRATUS application....1164
Using the GV STRATUS application in Adobe Premiere Pro CC 1201
Using the GV STRATUS application with Avid....1227
Installing K2 Avid Connect....1235
Using GV Connect with Final Cut Pro....1275
Logging assets....1284
The Advanced Logging tool....1284
The Button Panel....1286

The Marker Panel....1287
The Segmentation Panel....1287
Adding a Logging Suite....1289
Adding a Segmentation panel....1292
Assigning segments to assets....1294
Adding Button Panels....1296
Creating and adding logging buttons....1299
Customizing of Logging Panels and Buttons using Design Mode....1303
Pinning logging buttons....1304
Adding markers using logging buttons....1305
Logging assets in Live Mode....1306
Using a keyword or marker to add an event to a sequence....1308
Modifying Logging Suites and Button Panels....1309
Modifying logging buttons of the Button Panel....1310
Deleting logging buttons from a Button Panel....1310
Changing Advanced Logging user preferences....1311
Modifying markers and keywords....1311
Viewing logging history of markers....1315
Importing Logging Suite....1316
Using the Assignment List....1316
The Assignment List tool....1316
Story status colors....1318
Changing ALP User Preferences....1319
Adding placeholders....1324
Modifying a placeholder....1326
Deleting a placeholder....1326
Adding a new sequence....1328
Checking missing clips....1328
Viewing placeholder properties....1330
Viewing and modifying metadata of linked placeholders....1332
Creating a new sequence in the EDIUS application....1335
Using the GV STRATUS application in a Newsroom Computer System....1337
Using the GV STRATUS application in GV STRATUS Rundown....1369
Integrating assets with traffic system and K2 Edge....1371
Integration with traffic system and playout automation....1371
The Segmentation tool....1371
The House Number panel....1384
Configuring the GV STRATUS application....1387
Configuring User Preferences....1387
Configuring Affinity User Preferences....1390
Installing a GV STRATUS language pack....1392
Customizing the application workspace....1392
Troubleshooting the GV STRATUS application....1399
About application status....1399
Viewing and copying version and status information....1401
If you have trouble launching EDIUS XS....1402
Troubleshooting tips....1403
Keyboard shortcuts....1403
Inspector keyboard shortcuts....1403
Channel Panel keyboard shortcuts....1407
Playlist Editor keyboard shortcuts....1408
Scheduler keyboard shortcuts....1408
Segmentation keyboard shortcuts....1409
Sequence Viewer keyboard shortcuts....1409
Source Viewer keyboard shortcuts....1410
Storyboard keyboard shortcuts....1413
All keyboard shortcuts....1414

Specifications....1418
System requirements for GV STRATUS client PC....1418
4K (QFHD) and 1080p supported formats....1420
K2 system specifications....1422

GV STRATUS Web Client....1437
Using the GV STRATUS Web Client....1437
Logging on to the GV STRATUS Web Client....1439
The Navigator panel....1441
The Asset List panel....1443
The Inspector panel....1444
Browsing assets....1446
Viewing assets....1448
Searching assets....1455
Creating a subclip....1457
Archiving an asset....1458
Restoring archived assets....1460
Applying rules via the GV STRATUS UI....1461
Transferring assets using Send Destination....1463
The Dashboards....1465
Monitoring imports, exports, or transfers....1468
The Assignment List....1469
Viewing placeholder properties....1471
Checking missing clips....1472
Linking clip to a placeholder....1474
The Segmentation tool....1475
Adding a Segmentation panel....1478
Assigning segments to assets....1480
Protecting a segment....1481
Renaming a segment....1481
Editing segments....1482
Deleting a segment....1483
The Simple Editor tool....1484
The Source Viewer....1486
The Sequence Viewer....1487
Viewer buttons....1488
The Timeline....1489
Timeline buttons....1489
Creating an EDL....1490
Editing an event....1491
Rearranging or deleting events....1492
Splitting an event....1492
Playing an EDL....1492

GV STRATUS Rundown Operation....1494
Introducing GV STRATUS Rundown....1494
About GV STRATUS Rundown....1494
Terms You Should Know....1495
Overview of GV STRATUS Rundown....1495
Using GV STRATUS Rundown....1496
Overview of the Assignment List Manager....1498
Overview of the Simple Database (SDB) Server....1499
Overview of the XMOS Server....1500
Installing GV STRATUS Rundown hardware....1500
Hardware installation checklist....1500
Installing GV STRATUS Rundown Hardware....1501
Cabling the GV STRATUS Rundown computer....1501
Connecting the RDU 1510 Under Monitor Display....1502

Installing the Sealevel SeaI/O-410E GPIO Controller....1503
Installing the X-keys Jog/Shuttle Controller....1506
Configuring GV STRATUS Rundown....1507
Configuring GV STRATUS Rundown....1507
Configuring the GV STRATUS Rundown application....1508
Configuring the Simple Database (SDB) Server....1528
Configuring the XMOS Server....1534
Configuring the standalone Assignment List Manager....1537
Setting up your NCS for GV STRATUS Rundown....1538
Setting Up Your NCS for GV STRATUS Rundown....1538
Setting up ENPS for GV STRATUS Rundown....1539
Setting up iNEWS for GV STRATUS Rundown....1541
Setting up Octopus for GV STRATUS Rundown....1542
Using NCS Rundowns and GV STRATUS Rundown....1545
Using NCS rundowns and GV STRATUS Rundown....1545
Using the Assignment List in GV STRATUS ActiveX Plug-in....1546
The Assignment List tool....1546
Adding placeholders....1548
Modifying a placeholder....1550
Deleting a placeholder....1550
Adding a new sequence....1552
Checking missing clips....1552
Viewing and modifying metadata of linked placeholders....1553
Editing and GV STRATUS Rundown....1556
Editing and GV STRATUS Rundown....1556
Using the Assignment List Manager....1557
Receiving Editing Assignments....1558
Additional features of Assignment List Manager....1558
Using the GV STRATUS application in GV STRATUS Rundown....1561
Playing clips to air....1564
Playing Clips to Air....1564
About GV STRATUS Rundown Toolbar....1565
About the Playlist....1567
About Playout channels....1568
About Rundowns....1570
About the Clip Browser....1571
About the Playlist overview....1572
Creating a Playlist....1573
Cueing Clips....1577
Playing clips....1579
Archiving Clips....1579
Customizing playlist for broadcast....1580
GV STRATUS Rundown Appendix....1583
Sample of MOS Gateway configuration file....1583

GV STRATUS VTR Ingest Operation....1587
Configuring GV STRATUS VTR Ingest....1587
Configuring GV STRATUS VTR Ingest application....1587
Using GV STRATUS VTR Ingest....1590
Opening the GV STRATUS VTR Ingest application....1590
Overview of the GV STRATUS VTR Ingest window....1591
Recording with GV STRATUS VTR Ingest....1594
Scanning tape with broken timecodes....1597
Importing an EDL....1598
Exporting an EDL....1598
Software licenses....1599
cmemdc....1599
cping....1599

CSizingToolBar....1599
MIT....1600
mozilla....1601
resizeable lib....1609

GV STRATUS VTR Controller Operation....1611
Installing GV STRATUS VTR Controller Hardware....1611
Installing RS-422 card for GV STRATUS VTR Controller....1611
Configuring GV STRATUS VTR Controller....1612
Configuring GV STRATUS VTR Controller Application....1612
Using GV STRATUS VTR Controller....1614
Using GV STRATUS VTR Controller....1614
Overview of the GV STRATUS VTR Controller Window....1614
Viewing VTR Properties....1615
Accessing GV STRATUS VTR Controller....1615
Software licenses....1616
Software Licenses....1616

GV I/O Live Ingest and Playback....1630
About the GV I/O Live Ingest and Playback Server....1630
Introduction....1630
Standard features....1630
Product component summary....1631
Front view....1631
Rear view components....1631
Cabling GV I/O Live Ingest and Playback Server....1632
Rack mounting....1632
Cabling GV I/O server: Dell R640....1634
Installing GV I/O Live Ingest and Playback Server....1634
BIOS startup....1635
Preparing for GV I/O installation....1635
SiteConfig placeholder setup for GV I/O....1636
Adding GV I/O to the control network with SiteConfig....1638
Configuring deployment groups....1638
Adding software roles to a GV I/O Client....1640
Installing software into a GV I/O Live Ingest and Playback Server....1640
About the Grass Valley AppService....1642
Shutting down the Grass Valley AppService....1642
Licensing GV I/O Live Ingest and Playback server....1643
SabreTooth GV I/O license process....1643
Verifying the GV I/O configuration....1643
Setting backup and recovery of the GV I/O Live Ingest and Playback Server....1645
About the recovery image process....1645
Creating a recovery disk image....1645
Restoring from a system-specific recovery image....1647

Fault Tolerant Server....1649
About the FT Server....1649
Introduction....1649
Standard features....1649
Product component summary....1650
Front view....1650
Rear view components....1651
FT Server Installation Information....1652
Installation overview....1652
Unpacking....1652
Rack types....1653
Install chassis in rack....1660
Install CPU/IO modules....1664

2.5 inch hard disk drives....1666
Cable connections....1666
STRATUS-CS-FT server: Core (B1, C1)....1668
Power up....1669
CPU/IO module status....1671
POST check....1672
Front panel LEDs....1675
Install or remove front bezel....1676
Power off....1677
Configuring the FT Server....1678
Configuration overview....1678
Service Program configuration....1678
Confirming control software version....1679
Disk operations....1679
Dual disk configuration overview....1679
Build dynamic disk....1693
Duplex LAN configuration overview....1694
Servicing the FT Server....1699
Checking status with LEDs....1699
Diagnostics, logs and error messages....1705
Backup and recovery strategies....1708
Replacing failed components....1727
Specifications....1734
Storage device specifications....1734
Mechanical specifications....1734
Power supply specifications....1734
Environmental specifications....1735

Grass Valley Ports....1736

Glossary....1744

Grass Valley Knowledge Base....1752

Safety Summary....1753
Safety Summary....1753
Safety terms and symbols....1753
Warnings....1754
Cautions....1754
Sicherheit – Überblick....1755
Sicherheit – Begriffe und Symbole....1755
Warnungen....1756
Vorsicht....1757
Consignes de sécurité....1758
Consignes et symboles de sécurité....1758
Avertissements....1759
Mises en garde....1760
Certifications and compliances....1761
Laser compliance....1761
Safety certification....1762
ESD Protection....1762
Recommended ESD Guidelines....1762
Sources of ESD and Risks....1763
Grounding Requirements for Personnel....1763

Trademarks and Agreements....1765
Trademarks....1765
Patent Information....1765
JPEG acknowledgment....1765

Release Notes

GV STRATUS Version 6.8

- **Password encryption** — GV STRATUS supports secure password via encryption in any database in the system, and in any other persistent store, such as configuration files and registry settings. The Key Upgrade Utility must be run on the GV STRATUS Core server to support password encryption. For more info, refer to *Upgrade GV STRATUS system with the Key Upgrade Utility* on page 90.
- **GV STRATUS Web Client enhancements** — GV STRATUS Web Client is now enhanced with the Assignment List and Segmentation tool which were previously supported via desktop applications only. For more info, refer to *The Assignment List* on page 1469 and *The Segmentation tool* on page 1475.
- **GV I/O Live Ingest and Playback Server** — The GV I/O Live Ingest and Playback Server now supports playback of simple clips on SDI channels in addition to ingests via SDI, SMPTE 2022-6, SMPTE 2110, and HTTP source. The GV I/O server can be configured as a standalone device with local storage, or a shared storage client with Dell EMC Isilon network-attached storage system in this release. For more info, refer to *GV I/O Live Ingest and Playback* on page 1630.
- **DIVA Archive category enhancement** — GV STRATUS supports multiple DIVA archive categories when only one category was supported previously. The Diva Category Update Utility must be run on the GV STRATUS Core server after the software deployment. For more info, refer to *DIVA Categories Add/Modify Field settings* on page 310 and *Upgrade GV STRATUS system with the DIVA Category Update Utility* on page 99.
- **Rename of Summit MDI** — Summit MDI has been renamed to **Grass Valley Media Server** MDI type in the MDI Configuration settings of GV STRATUS Control Panel. MDI settings for all K2 Summit Standalone, K2 SAN, K2 Central, GV I/O, and Third Party Storage systems must be reconfigured in this release. For more details, refer to *Grass Valley Media Server MDI standalone settings* on page 304, *Grass Valley Media Server MDI SAN settings* on page 306, *GV STRATUS Control Panel configuration for K2 Central* on page 937, and *GV STRATUS Control Panel configuration for SMB storage* on page 930.
- **Requirement of Microsoft .NET 4.7.1 and Microsoft Visual C++ Redistributable for VS 2017** — GV STRATUS requires the installation of Microsoft .NET 4.7.1 and Microsoft Visual C++ Redistributable for Visual Studio 2017. For more details, refer to *Upgrade Microsoft .NET* on page 79 and *Upgrade Microsoft Visual C++ Redistributable for VS 2017* on page 78.

Not supported in this GV STRATUS release

The following devices and functionality are not supported with this version of GV STRATUS software. Check with your Grass Valley representative regarding availability.

- **Missing Material List role** — This role in GV STRATUS Control Panel License Management settings is for use by Grass Valley personnel for testing purposes only. Do not assign this role to users or groups.
- **ProRes format** — GV STRATUS does not support the media workflow of assets in ProRes format for this release.
- **Quota for K2 Summit standalone systems** — Quota limit on K2 Summit system is only applicable for the K2 SAN media folders.
- **Quota for EDIUS** — Quota limit on K2 Summit system is only applicable for the K2 SAN media folders.

- **Archive/Restore for assets with 64 audio tracks** — Archive/Restore and partial file restore operations are not supported for assets with 64 audio tracks for these archive vendors:
  - FlashNet
  - Masstech (for GXF format)
- **Windows Server 2008** — GV STRATUS does not support Windows Server 2008 in this release. Only Windows Server 2012 R2 and Windows Server 2016 are supported for GV STRATUS servers.
- **Digital Media Platform (DMP) workflow** — GV STRATUS does not support the DMP workflow with Ignite in this release.

Changes and features in previous releases

The following sections describe changes and features in past releases.

GV STRATUS Version 6.5

- **4K (QFHD) and 1080p support** — GV STRATUS now supports 4K QFHD (single essence – file only) and 1080p formats. STRATUS-QFHD license is required to enable GV STRATUS operations with 4K (QFHD) assets. For more info, refer to *4K (QFHD) and 1080p supported formats* on page 1420.
- **The Simple Editor tool on GV STRATUS Web Client** — The GV STRATUS Web Client is enhanced with a simple editing tool that is accessible anywhere from desktops, tablets, and mobile phones. For more info, refer to *The Simple Editor tool* on page 1484.
- **GV I/O Ingest Appliance enhancement** — The GV I/O Ingest Appliance now supports ingests via the IP network. Configurations of IP Ingest channels can be done via Control Panel and Channel Panel. For more info, refer to *GV I/O Record Channel settings* on page 359 and *Modifying a Channel Panel while in use* on page 1078.
- **GV STRATUS External Media Engine** — GV STRATUS introduces the new GV STRATUS External Media Engine on the GV STRATUS Core server, Workflow Server, or a separate server, to publish content and metadata to popular social media networks (such as Facebook, Twitter, and YouTube) via Social Media CMS-Systems. For more info, refer to *Publishing content to Social Media platforms* on page 656 and *External Media Engine Server set up process* on page 819.
- **Support of Verizon CMS System** — GV STRATUS supports publishing of assets to popular social media networks via the Verizon CMS system with the GV STRATUS application. For more info, refer to *External Media Locations Configuration Add/Modify settings* on page 376 and *Configure and authenticate Verizon location* on page 825.
- **Rename of Social Media rules** — Both Social Media rules have been renamed to - "Publish External Media Network rule" and "Media Network Counts rule" to support both Social Media and External Media workflows. For more info, refer to *Adding a publish external media network rule* on page 621 and *Adding a media network counts rule* on page 629.
- **GV STRATUS Proxy Streaming Server** — GV STRATUS introduces the Proxy Streaming Server which supports frame accurate playback of proxy files in GV STRATUS Web Clients within an HTML5 standard browser. For more details, refer to *Proxy Streaming Server set up process* on page 907.

- **EDIUS Project deletions** — GV STRATUS application supports permanent deletion of EDIUS Projects and associated assets from the GV STRATUS database and EDIUS project location. For more details, refer to *Deleting EDIUS Projects* on page 1192 and *Deleting assets* on page 985.
- **Affinity settings** — GV STRATUS adds the Affinity tab in User Preferences settings to allow users to limit the display of Assets Locations and Associations to specific storage or device locations. For more info, refer to *Configuring Affinity User Preferences* on page 1390.
- **K2 software version 10.1 compatibility** — GV STRATUS inherits the latest features and functionality from K2 family products. You have the option to upgrade your K2 systems either to version 9.8.5 or 10.1 for compatibility with this GV STRATUS version. You can upgrade K2 systems with the typical software upgrade from the current version 9.8.x to version 9.8.5. However for the upgrade to K2 version 10.1, you must reimage and upgrade hardware in the K2 Summit systems. SNFS (StoreNext File System) version 6.0.6 is required to work with K2 Summit version 10.1. Refer to *Upgrading to GV STRATUS version 6.5 and K2 Summit version 10.1* for upgrade information.
- **Requirement of Microsoft .NET 4.7.1 and Microsoft Visual C++ Redistributable for VS 2017** — GV STRATUS requires the installation of Microsoft .NET 4.7.1 and Microsoft Visual C++ Redistributable for Visual Studio 2017. For more details, refer to *Upgrade Microsoft .NET* on page 79 and *Upgrade Microsoft Visual C++ Redistributable for VS 2017* on page 78.
- **Windows 10 support** — GV STRATUS supports the Windows 10 operating system for GV STRATUS low-res clients and EDIUS XS workstations. GV STRATUS high-res clients and EDIUS Workgroup workstations are also supported if SNFS 6.0.6 is installed. For more info, refer to *System requirements for GV STRATUS client PC* on page 52.
- **Windows Server 2016 support** — GV STRATUS supports Windows Server 2016 for Express, Core, Workflow, GV Render Engine, Proxy and FSM servers with this latest software release.
- **SQL 2017 support** — GV STRATUS supports SQL Server 2017 on Windows Server 2016 systems with the upgrade to this version of GV STRATUS software.

GV STRATUS Version 6.0

- **GV STRATUS Social Media Engine** — GV STRATUS introduces the new GV STRATUS Social Media Engine on the GV STRATUS Core server, Workflow Server, or a separate server, to publish content and metadata to popular social media networks (such as Facebook, Twitter, and YouTube). For more info, refer to *Publishing content to Social Media platforms* on page 656 and *Social Media Engine Server set up process* on page 802.
- **GVRE Transcoder** — GV Render Engine is enhanced with a new function as a generic transcoder for import and export rules. The STRATUS-TRANSCODE license must be installed to enable transcode functionality on the Render Engine server. For more info, refer to *Working with GVRE Transcoder* on page 558.
- **GV I/O Ingest Appliance** — GV STRATUS introduces a commodity hardware solution to support Ingests without the need for Replay in a fast-paced production and editing environment. The GV I/O Ingest Appliance has up to four Recorder channels with the baseband HD-SDI support via an on-board video card. A software only version is also available for users to deploy the solution on standard IT hardware in their production systems. For more info, refer to *GV I/O Live Ingest and Playback* on page 1630.
- **GV STRATUS Web Client enhancements** — The GV STRATUS Web Client is enhanced with transfer, archive, advanced search options, send destinations, and job monitoring features that are accessible anywhere from desktops, tablets, and mobile phones. For more info, refer to *GV STRATUS Web Client* on page 1437.

- **GV STRATUS Proxy Streaming Service** — The addition of GV STRATUS Proxy Streaming Service allows frame accurate playback of proxy files in GV STRATUS Web Client within an HTML5 standard browser. For more details, refer to *Express server components* on page 444 and *Core Server components* on page 448.
- **Dashboard enhancement** — The Dashboard tool supports a new tab to display data in graphical form for statistical information of all Social Media platforms. Additional roles are added to manage user access of each tab in the Dashboard tool. For more info, refer to *The Dashboard tool* on page 403.
- **Social Media rules** — GV STRATUS introduces 2 new rules - "Publish Social Media" and "Social Media Counts" to support the Social Media Management workflow. For more info, refer to *Adding a publish external media network rule* on page 621 and *Adding a media network counts rule* on page 629.
- **Rename Asset Rights** — Introduction of a new role in GV STRATUS to limit renaming of assets to approved users only. Existing users and groups that do not have this role must be assigned with the Rename Asset Rights role in GV STRATUS Control Panel if needed. For more info, refer to *Authorization Manager settings* on page 366.
- **Scavenge Priority** — GV STRATUS supports the customization of proxy scavenge workflow. For more info, refer to *Scavenge Priority settings* on page 348 and *Scavenge Priority Add/Modify settings* on page 349.
- **Mono/Stereo Audio Mode Shortcuts** — Enhancements of GV STRATUS keyboard shortcuts to support the toggle of Mono/Stereo audio mode in the Source Viewer and Inspector. For more info, refer to *Using the Audio Overlay* on page 1002, *Inspector keyboard shortcuts* on page 1403, and *Source Viewer keyboard shortcuts* on page 1410.
- **Protection of Segments** — Enhancement in the Segmentation tool to protect individual segments from modification and deletion. For more info, refer to *Protecting a segment* on page 1379.
- **Segment Preview enhancement** — The Segmentation tool allows users to play clip after the mark-out point, as long as the loop mode is off. For more info, refer to *Previewing a segment* on page 1377 and *Editing segments* on page 1376.
- **Setting of recording location in the same device** — The Scheduler tool supports the option to only display recording locations in the same recording device when scheduling an ingest. For more info, refer to *Ingest Location Setup settings* on page 386 and *Adding an event* on page 1034.
- **Setting of date/time fields to local time for Avid exports** — GV STRATUS supports the setting of date/time fields to local time when exporting assets into Avid. For more info, refer to *Configure Avid Media Composer send destinations* on page 666, *Configure Avid Interplay send destinations* on page 671, and *Configure Avid ISIS send destinations* on page 668.

GV STRATUS Version 5.7

- **GV STRATUS Web Client** — GV STRATUS introduces a web client–server architecture in which GV STRATUS applications run via web browsers. For more info, refer to *Using the GV STRATUS Web Client* on page 1437 and *Logging on to the GV STRATUS Web Client* on page 1439.
- **Audio Tags Management** — GV STRATUS supports the customization of audio tags in asset workflows. For more info, refer to *Audio Tag Management settings* on page 354, *Audio Tags settings* on page 356, and *Adding or modifying audio tags of an asset* on page 1005.
- **Extended Player Focus Shortcuts** — Enhancements of GV STRATUS keyboard shortcuts to support extended player focus and timecode navigation. For more info, refer to *Focusing on a tool* on page 973, *Focusing on a viewer in a tool* on page 973, and *Modifying timecode to navigate asset playback* on page 998.

- **Support of the Aspera Server on Linux** — GV STRATUS supports the export rule workflow with Aspera Server running on the Linux operating system. Previously, only Aspera servers running on the Windows operating system are supported. For more info, refer to *Data Mover engine settings* on page 331.
- **Bug fixes** — This release consists of bug fixes to improve the reliability and performance of the GV STRATUS application.
- **Documentation** — The following changes have been updated to the GV STRATUS 5.7 Topic Library:
  - Updates to GV STRATUS compatibility tables in the "Release Notes" section. For more details, refer to *GV STRATUS Version compatibility* on page 52.
  - Updates to GV STRATUS list of known problems. For more details, refer to *GV STRATUS Known Problems* on page 65.

GV STRATUS Version 5.5 (SP3)

- **Bug fixes** — This release consists of bug fixes to improve the reliability and performance of the GV STRATUS system.
- **Documentation** — The following changes have been updated to the GV STRATUS 5.5 Topic Library:
  - Updates to GV STRATUS compatibility tables in the Release Notes section. For more details, refer to *GV STRATUS Version compatibility* on page 52.
  - Created a new topic for SMS7000 configuration and added to the Configuring a Router section. For more details, refer to *Configuring Router Windows Service (for SMS7000 protocol only)* on page 556.
  - Updates to the Workflow Server upgrade section. For more details, refer to *Upgrade Workflow Server, license, configure Rules* on page 170.
  - Updates to the GV STRATUS ports section. For more details, refer to these topics:
    - *GV STRATUS application ports* on page 257
    - *GV STRATUS Control Panel application ports* on page 259
    - *Ports and services mapping* on page 715
    - *Grass Valley Ports* on page 1736

GV STRATUS Version 5.5 (SP1)

- **Bug fixes** — This release consists of bug fixes to improve the reliability and performance of the GV STRATUS system.
- **Documentation** — The following changes have been updated to the GV STRATUS 5.5 Topic Library:
  - Updates to GV STRATUS compatibility tables in the Release Notes section. For more details, refer to *GV STRATUS Version compatibility* on page 52.
  - Updates to Backup and Restore procedures in the Fault Tolerant Server section. For more details, refer to *Backup and recovery strategies* on page 1708.

GV STRATUS Version 5.5

- **Audio Tags in Rules workflows** — GV STRATUS supports the use of predefined audio mapping profiles in Rules workflows. For more info, refer to *Profiles settings* on page 354 and *Adding an export rule* on page 580.
- **Segmentation Panel in Advanced Logging Suite** — An option to include segmentation panels in the Advanced Logging Tool for users assigned with the Segmentation role. For more info, refer to *The Advanced Logging tool* on page 1284 and *Adding a Logging Suite* on page 1289.
- **Custom Metadata in Scheduler Event Templates** — Addition of custom metadata in Scheduler Event Templates provides the capability to specify custom fields on event templates across GV STRATUS systems. For more info, refer to *Saving event as a template* on page 1052. To enable the Custom Metadata Feature on Scheduler Event Templates after a new install, refer to *Setting Custom Metadata in the Ingest Database* on page 688.
- **Site ID upgrade** — An upgrade of GV STRATUS Site ID from DEFAULTDOMAIN to unique Site IDs. For more info, refer to *Upgrade GV STRATUS Site ID*.
- **Support of the standalone GV STRATUS Database Server** — GV STRATUS supports the installation of databases into a standalone Database Server, if needed. For more details, refer to *Standalone Database Server set up process* on page 829.
- **Requirement of Microsoft .NET 4.6.2 and Visual Studio 2015** — GV STRATUS requires the installation of Microsoft .NET 4.6.2 and Visual Studio 2015 Update 3. For more details, refer to *Upgrade Microsoft .NET* and *Upgrade Microsoft Visual C++ Redistributable for VS 2015 Update 3*.
- **Bug fixes** — This release consists of bug fixes to improve the reliability and performance of the GV STRATUS application.
- **Documentation** — The following changes have been updated to the GV STRATUS 5.5 Topic Library:
  - Updates to GV STRATUS compatibility tables in the "Release Notes" section. For more details, refer to *GV STRATUS Version compatibility* on page 52.
  - Updates to GV STRATUS list of known problems. For more details, refer to *GV STRATUS Known Problems* on page 65.

GV STRATUS Version 5.0 (SP2)

- **Bug fixes** — This release consists of bug fixes to improve the reliability and performance of the GV STRATUS application.
- **Documentation** — The following changes have been updated to the GV STRATUS 5.0 Topic Library:
  - Updates to GV STRATUS compatibility tables in the Release Notes section. For more details, refer to *GV STRATUS Version compatibility* on page 52.
  - Updates for Conform workflow in the GV STRATUS Operation section. For more details, refer to *Considerations for conforming assets* on page 1120.
  - Updates for Backup and Restore procedures in the Fault Tolerant Server section. For more details, refer to *Backup and recovery strategies* on page 1708.

GV STRATUS Version 5.0 (SP1)

- **Bug fixes** — This release consists of bug fixes to improve the reliability and performance of the GV STRATUS application.
- **Documentation** — The following changes have been updated to the GV STRATUS 5.0 Topic Library:
  - Updates to GV STRATUS compatibility tables in the "Release Notes" section. For more details, refer to *GV STRATUS Version compatibility* on page 52.
  - Updates to GV STRATUS list of known problems. For more details, refer to *GV STRATUS Known Problems* on page 65.
  - Updates for MOS Redirection workflow in GV STRATUS Operation section. For more details, refer to *Using GV STRATUS with ENPS* on page 1338 and *Configuring MOS Redirection workflow with ENPS* on page 1345.
  - Updates to GV STRATUS Control Panel settings reference section. For more details, refer to *Profiles settings* on page 354.

GV STRATUS Version 5.0

- **Quotas** — GV STRATUS supports the ability to view disk space quotas that had been reserved for specific K2 bins. For more details, refer to *The Dashboard tool* on page 403 and *About application status* on page 947.
- **Live Advanced Logging** — Add markers instantly to still recording assets via Live Mode in the Advanced Logging tool. For more info, refer to *Logging assets in Live Mode* on page 1306.
- **64 channels Audio Support** — GV STRATUS supports the media workflow of assets up to 64 audio tracks on high resolution clients. For more info, refer to *Using the Audio Overlay* on page 1002.
- **Audio Tags and scalable Audio Meters** — The display of audio tags and audio meters can be configured and customized for the GV STRATUS system. For more info, refer to *Mapping audio channels* and *Configuring Player User Preferences* on page 1008.
- **Copy of metadata** — GV STRATUS supports the copy of asset's metadata for users assigned with the Copy Metadata role. For more info, refer to *Copying asset metadata* on page 1016.
- **Import of Thumbnails** — GV STRATUS supports the import of thumbnails for assets. For more info, refer to *Importing image file as thumbnail of an asset* on page 1010.
- **Assignable High Resolution Thumbnails** — High resolution thumbnails can be assigned to assets in the GV STRATUS application. For more info, refer to *Changing the thumbnail of an asset* on page 1010.
- **Restore assets from keywords** —GV STRATUS supports the restore of archived assets from keywords. For more info, refer to *Restoring assets from keywords* on page 1125.
- **GV Log Viewer** — A new Grass Valley log monitoring application with the capability to view and monitor all GV STRATUS machines. For more info, refer to *Working with GV Log Viewer* on page 500.
- **Move growing files** — GV STRATUS supports the move of growing files between K2 Summit bins. For more info, refer to *Transferring between bins using drag and drop* on page 1106.
- **Export EDIUS Markers and Keywords** — EDIUS supports the ability to export markers and keywords into GV STRATUS. For more details, refer to *Sending EDIUS sequences with markers and keywords to GV STRATUS* on page 1186.

- **Restore of archived asset in EDIUS Workgroup** — EDIUS Workgroup supports the ability to restore archived assets from GV STRATUS system. For more details, refer to *Restoring archived assets in EDIUS* on page 1183.
- **Custom metadata for Markers and Keywords** — GV STRATUS supports custom metadata for markers and keywords in the GV STRATUS plug-in for Adobe® Premiere® Pro CC . For more details, refer to *Viewing asset metadata* on page 1221.
- **Bug fixes** — This release consists of bug fixes to improve the reliability and performance of the GV STRATUS application.
- **Documentation** — The following changes have been updated to the GV STRATUS 5.0 Topic Library:
  - Updates to GV STRATUS compatibility tables in the "Release Notes" section. For more details, refer to *GV STRATUS Version compatibility* on page 52.
  - Updates to GV STRATUS list of known problems. For more details, refer to *GV STRATUS Known Problems* on page 65.

GV STRATUS Version 4.8 (SP4)

- **Bug fixes** — This release consists of bug fixes to improve the reliability and performance of the GV STRATUS application.
- **Documentation** — The following changes have been updated to the GV STRATUS 4.8 Topic Library:
  - Updates to GV STRATUS compatibility tables in the "Release Notes" section. For more details, refer to *GV STRATUS Version compatibility* on page 52.
  - Updates to GV STRATUS list of known problems. For more details, refer to *GV STRATUS Known Problems* on page 65.
  - Updates to renaming core/express servers topic. For more details, refer to *Renaming a GV STRATUS Core/Express server* on page 545.
  - Updates to GV STRATUS Control Panel Permissions setting topic. For more details, refer to *Permissions Modify Field settings* on page 322.

GV STRATUS Version 4.8 (SP2)

- **Bug fixes** — This release consists of bug fixes to improve the reliability and performance of the GV STRATUS application.
- **Documentation** — The following changes have been updated to the GV STRATUS 4.8 Topic Library:
  - Updates to GV STRATUS compatibility tables in the "Release Notes" section. For more details, refer to *GV STRATUS Version compatibility* on page 52.

GV STRATUS Version 4.8 (SP1)

- **RMI support of XDCAM XAVC format** — GV STRATUS supports the ability to ingest assets in XDCAM XAVC format via the RMI tool. For more details, refer to *RMI format specifications* on page 1059.
- **Audio mapping with K2 Summit 9.6** — GV STRATUS supports audio mapping of K2 Summit channels via the AppCenter. For more details, refer to *Mapping audio channels*.

- **Support for .NET 4.6 and Visual Studio 2015** — GV STRATUS requires the installation of .NET 4.6 and Visual Studio 2015. For more details, refer to *Upgrade .NET* and *Upgrade Microsoft Visual C++ Redistributable for VS 2015*.
- **Bug fixes** — This release consists of bug fixes to improve the reliability and performance of the GV STRATUS application.
- **Documentation** — The following changes have been updated to the GV STRATUS 4.8 Topic Library:
  - Updates to GV STRATUS compatibility tables in the "Release Notes" section. For more details, refer to *GV STRATUS Version compatibility* on page 52.
  - Updates to install and upgrade topics of GV STRATUS plug-in for Adobe Premiere Pro application. The **Extension Manager Command Line** tool must be used to install GV STRATUS plug-in for Adobe Premiere Pro version 9.0 and above. For more details, refer to *Installing Adobe Premiere Pro CC and GV STRATUS plug-in* on page 1203 and *Upgrading Adobe Premiere Pro CC and GV STRATUS plug-in* on page 1210.

GV STRATUS Version 4.8

- **Metadata Access Control** — GV STRATUS supports Metadata Access Control with this release. For more details, refer to *Permissions settings* on page 321.
- **Security enhancement for Markers and Segments** — GV STRATUS supports enhanced access control on markers and segments. Full permissions are needed to create, update, or delete markers and segments. For more details, refer to *Setting security in Inspector* on page 477.
- **EDIUS Field Editing enhancement** — The **STRATUS Send for WAN Editing** option is available in EDIUS to enhance field editing operation. For more details, refer to *Sending the field EDIUS project to the home GV STRATUS system* on page 1197.
- **Common RESTful Archive MDI** — GV STRATUS supports the Common RESTful Archive sytem with this release. You can configure up to 2 Common RESTful Archive MDIs in the GV STRATUS Control Panel. For more details, refer to *Common RESTful Archive MDI settings* on page 316.
- **K2 Central configuration enhancement** — K2 Central system deployment and configuration are enhanced with this release. For more details, refer to *K2 Central Storage configuration* on page 934.
- **GV SMB Storage configuration enhancement** — Grass Valley SMB Storage system deployment and configuration are enhanced with this release. For more details, refer to *GV STRATUS Control Panel configuration for SMB storage* on page 930.
- **Proxy Configuration** — GV STRATUS supports the ability to define custom proxy configuration. For more details, refer to *Proxy Quality settings* on page 347.
- **Custom metadata for Markers and Keywords** — GV STRATUS supports the configuration of custom metadata for markers and keywords. Only users assigned with the Media Manager role are allowed to create the custom metadata. For more details, refer to *Custom Metadata settings* on page 318.
- **Support for .NET 4.6 and Visual Studio 2015** — GV STRATUS requires the installation of .NET 4.6 and Visual Studio 2015. For more details, refer to *Upgrade .NET* and *Upgrade Microsoft Visual C++ Redistributable for VS 2015*.
- **Bug fixes** — This release consists of bug fixes to improve the reliability and performance of the GV STRATUS application.

- **Documentation** — The following changes have been updated to the GV STRATUS 4.8 Topic Library:
  - Updates to GV STRATUS compatibility tables in the "Release Notes" section. For more details, refer to *GV STRATUS Version compatibility* on page 52.
  - Updates to GV STRATUS list of known problems. For more details, refer to *GV STRATUS Known Problems* on page 65.

GV STRATUS Version 4.5.2

- **K2 Central TX Shared Storage support** — GV STRATUS supports K2 Central TX Shared Storage with this release. For more details, refer to *K2 Central Storage configuration* on page 934.
- **K2 Summit 9.6 support** — GV STRATUS supports K2 Summit version 9.6 with this release. For more details, refer to *Grass Valley products compatible with GV STRATUS* on page 56.
- **EDIUS Project Migration tool** — The EDIUS Project Migration tool is required to migrate existing EDIUS projects created before your upgrade to the GV STRATUS 4.5 system. For more details, refer to *Using the EDIUS Project Migration tool* on page 166.
- **New location of EDIUS cab file** — The EDIUS cab file is now included in the GrassValley_STRATUSClient cab file. For more details, refer to *Add software package to deployment group for EDIUS clients and Render Engine server* on page 149 and *Installing EDIUS software with SiteConfig* on page 281.
- **Audio track mapping on import and export to Avid** — GV STRATUS supports audio track mapping on import and export to Avid with this release. For more details, refer to *Adding an Avid import rule* on page 676, *Configure Avid Media Composer send destinations* on page 666, *Configure Avid ISIS send destinations* on page 668, and *Configure Avid Interplay send destinations* on page 671.
- **Adobe Premiere Pro 9.2 support** — For GV STRATUS plug-in to work in the Adobe Premiere Pro 9.2 application, the self-signed GV STRATUS security certificate must be manually installed. For more details, refer to *Installing the self-signed GV STRATUS security certificate for Adobe Premiere Pro* on page 1205.
- **Bug fixes** — This release consists of bug fixes to improve the reliability and performance of the GV STRATUS application.
- **Documentation** — The following changes have been updated to the GV STRATUS 4.5 Topic Library:
  - Updates to GV STRATUS compatibility tables in the "Release Notes" section. For more details, refer to *GV STRATUS Version compatibility* on page 52.
  - Updates to *Adding an archive rule* on page 605 topic to support partial transfers in the archive rule.

GV STRATUS Version 4.5

- **Render Engine replaces Proxy Encoder** — The GV Render Engine now supports Proxy Encoder functionality.
  - H.264 proxy supported.
  - Proxy quality can be configured with low, medium, and high resolution.
  - Systems with existing Proxy Encoder servers must convert to Render Engine servers.

- **Scheduled Transfer** — The new tool in GV STRATUS application to schedule asset transfers into a repository.
- **Resource Management** — The new utility in GV STRATUS Control Panel to monitor and manage available resources.
- **MEWS Service enhancements**:
  - Support for multiple MEWS engines, each of them providing 3 simultaneous transfer streams.
  - Using the GV STRATUS rules engine, transfer of growing files from GV STRATUS / K2 into Avid, and edit-while-transfer.
  - MEWS transcoding of media files upon transfer from GV STRATUS to Avid or export from Avid to GV STRATUS. This is a licensed option.
  - Send from GV STRATUS / K2 into Avid ISIS / Interplay, checking asset and all pre-configured metadata (including custom metadata fields) into Interplay.
- **EDIUS Project Management** — Addition of EDIUS Projects directory in the GV STRATUS application and STRATUS Browser to ease project management and workflow in EDIUS.
- **EDIUS Workgroup** — The EDIUS Elite product has been rebranded and renamed as the EDIUS Workgroup.
- **User interface enhancements**:
  - Revamp of the whole GV STRATUS user interface with new look and feel.
  - Movable overlay controls in Inspector and Source Viewer.
  - Scrub Bar Zoom to navigate and zoom in Inspector and other Viewers.
- **ENPS workflow enhancements** — The MOS item workflow by inserting assets directly as MOS items into ENPS scripts.
- **Dyno workflow enhancements** — Browse camera angles in Asset Lists.
- **K2 Summit 9.5 support** — GV STRATUS supports K2 Summit version 9.5 with this release. SNFS (StoreNext File System) version 4.7.2 is required. For more details, refer to *Compatible K2 Summit/Solo components* and the "Upgrading K2 systems" section of the K2 Topic Library.
- **K2 Dyno 3.5 support** — GV STRATUS supports K2 Dyno S Replay Controller version 3.5 with this release. For more details, refer to *K2 Dyno S 3.5 Topic Library*.

GV STRATUS Version 4.0.8

- **K2 Summit 9.5 support** — GV STRATUS supports K2 Summit version 9.5 with this release. SNFS (StoreNext File System) version 4.7.2 is required. For more details, refer to *Compatible K2 Summit/Solo components* and the "Upgrading K2 systems" section of the K2 Topic Library.
- **K2 Dyno 3.5 support** — GV STRATUS supports K2 Dyno S Replay Controller version 3.5 with this release. For more details, refer to *K2 Dyno S 3.5 Topic Library*.
- **Important Windows Updates required** — GV STRATUS requires the installation of Important Windows Updates on all GV STRATUS client and server devices. For more details, refer to *Install Important Windows updates (required)* on page 106.
- **Bug fixes** — This release consists of bug fixes to improve the reliability and performance of the GV STRATUS application.

- **Documentation** — The following additional changes have been made to the GV STRATUS 4.0 Topic Library:
  - Updates to GV STRATUS compatibility tables in the "Release Notes" section. For more details, refer to *GV STRATUS Version compatibility* on page 52.
  - Updates to GV STRATUS list of known problems. For more details, refer to *GV STRATUS Known Problems* on page 65.
  - Updates to *Printing asset metadata* on page 1017 and *Modifying an event* on page 1048 topics in the "GV STRATUS Operation" section.
  - Updates to *GV STRATUS VTR applications client PC components* on page 462 topic in the "GV STRATUS Installation and Service" section.

GV STRATUS Version 4.0.7

- **Important Windows Updates required** — GV STRATUS requires the installation of Important Windows Updates on all GV STRATUS client and server devices. For more details, refer to *Install Important Windows updates (required)* on page 106.
- **Ingest Database setting required** — The Auto Close feature must be disabled if upgrading the Ingest Database. For more details, refer to *Disabling the Auto Close feature in Ingest Database* on page 689.
- **Bug fixes** — This release consists of bug fixes to improve the reliability and performance of the GV STRATUS application.
- **Documentation** — The following additional changes have been made to the GV STRATUS 4.0 Topic Library:
  - Updates to GV STRATUS compatibility tables in the "Release Notes" section. For more details, refer to *GV STRATUS Version compatibility* on page 52.
  - Updates to GV STRATUS list of known problems. For more details, refer to *GV STRATUS Known Problems* on page 65.
  - Updated *Summary of upgrade from version 3.5 to version 4.0* on page 218 in the "GV STRATUS Upgrade" section.
  - Updated *GV STRATUS Operation considerations* on page 50 in the "Release Notes" section.
  - Updated *Browsing assets* on page 976 in the "GV STRATUS Operation" section.

GV STRATUS Version 4.0.6

- **Important Windows Updates required** — GV STRATUS requires the installation of Important Windows Updates on all GV STRATUS client and server devices. For more details, refer to *Install Important Windows updates (required)* on page 106.
- **Bug fixes** — This release consists of bug fixes to improve the reliability and performance of the GV STRATUS application.

- **Documentation** — The following additional changes have been made to the GV STRATUS 4.0 Topic Library:
  - Updates to GV STRATUS compatibility tables in the "Release Notes" section. For more details, refer to *GV STRATUS Version compatibility* on page 52.
  - Updates to GV STRATUS list of known problems. For more details, refer to *GV STRATUS Known Problems* on page 65.
  - Added *Set firewall for application ports* on page 257 in the "Client PC set up process" section.
  - Updated *Summary of upgrade from version 3.1 to version 4.0* on page 217 in the "GV STRATUS Upgrade" section.
  - Updates to Octopus configuration topics. For more details, refer to *Configuring the MOS Device for Octopus* on page 48 and *Creating an ActiveX Device for Octopus* on page 50.
  - Updates to Adobe Premiere Pro topics. For more details, refer to *Exporting Adobe Premiere sequences to GV STRATUS* on page 1225 and *Upgrading Adobe Premiere Pro CC and GV STRATUS plug-in* on page 1210.

GV STRATUS Version 4.0.5

- **Important Windows Updates required** — GV STRATUS version 4.0.5 requires the installation of Important Windows Updates on all GV STRATUS client and server devices. For more details, refer to *Install Important Windows updates (required)* on page 106.
- **Bug fixes** — This release consists of bug fixes to improve the reliability and performance of the GV STRATUS application.
- **Documentation** — The following additional changes have been made to the GV STRATUS 4.0 Topic Library:
  - Updates to GV STRATUS compatibility tables in the "Release Notes" section. For more details, refer to *GV STRATUS Version compatibility* on page 52.
  - Updates to GV STRATUS list of known problems. For more details, refer to *GV STRATUS Known Problems* on page 65.
  - Updated "Using EDIUS with GV STRATUS application" section with this new topic — *Applying User Settings to multiple EDIUS users* on page 1167
  - Republished GV STRATUS 4.0 Topic Library on 20150813.

GV STRATUS Version 4.0.4

- **Important Windows Updates required** — GV STRATUS version 4.0.4 requires the installation of Important Windows Updates on all GV STRATUS client and server devices. For more details, refer to *Install Important Windows updates (required)* on page 106.
- **Bug fixes** — This release consists of bug fixes to improve reliability and performance of the GV STRATUS application.
- **Documentation** — The following additional changes have been made to the GV STRATUS 4.0 Topic Library:
  - Updates to GV STRATUS compatibility tables in the "Release Notes" section. For more details, refer to *GV STRATUS Version compatibility* on page 52.
  - Updates to the *Access K2 storage from a Windows workstation* on page 1213 topic for the GV STRATUS integration with Adobe Premiere Pro.
  - Republished GV STRATUS 4.0 Topic Library on 20150723.

GV STRATUS Version 4.0.3

- **Scheduler tool enhancement** — Optimization of Scheduler's reliability and performance.
- **Send workflow** — Support of transactional copy to GV STRATUS remote destinations. For more details, refer to *Transferring an asset to a remote site* on page 1111.
- **Dashboard role** — Dashboard role is available in all licenses except for Newsroom Basic. It is recommended that a maximum of 5 users assigned to the Dashboard role. For more details, refer to *Old GV STRATUS roles matrix*.
- **Thumbnail extraction** — Thumbnails can now be extracted via the Export rule. An export thumbnail is defined by a **tn** marker on the asset. For more details, refer to *Adding a thumbnail marker* on page 643.
- **SQL server memory setting** — To prevent low memory issues, the SQL server memory limit can be set on the GV STRATUS Core server. For more details, refer to *Setting the SQL server memory limit* on page 687.
- **Conformed asset timecode setting** — For all conform jobs, the start timecode of the resultant simple clip is based on EDIUS XS Start Timecode setting in the GV STRATUS Control Panel. For more details, refer to *EDIUS Settings* on page 159.
- **EDIUS lock enhancement** — When an EDIUS project is being edited, the project and its included sequences and clips are locked in the GV STRATUS application. For more details, refer to *Adding GV STRATUS assets to EDIUS timeline* on page 1181.
- **Documentation** — The following additional changes have been made to the GV STRATUS 4.0 Topic Library:
  - Updates to GV STRATUS compatibility tables in "Release Notes" section.
  - Information added on High Priority Windows Updates for EDIUS and GV Render Engine server. For more details, refer to *Install Important Windows updates for EDIUS* on page 148.
  - Republished GV STRATUS 4.0 Topic Library on 20150604.

GV STRATUS Version 4.0.1

- **Avid/MEWS workflow enhancements**:
  - Locations configuration to support Avid ISIS.
- **Import and export rules enhancements**
- **User interface enhancements**:
  - Show/hide detailed transcode jobs in Jobs Monitor.
- **Documentation** — The following additional changes have been made to the GV STRATUS 4.0 Topic Library:
  - "About This Release" section renamed "Release Notes" and moved to top of Topic Library.
  - Updates to topics in "Fully qualified domain configuration" section.
  - Information added about K2 Summit system QuickTime FTP support.

GV STRATUS Version 4.0

- **Security** — When GV STRATUS Security is enforced, the Security Manager role allows you to set access permissions and assign ownership to assets and bins. Also, a security certificate installed on the GV STRATUS Core server enhances the security of the GV STRATUS system.
- GV STRATUS software installation automatically creates and installs a security certificate on the GV STRATUS Core server. No manual steps are required.
- **Metadata Mapping** — For material imported with the RMI tool, metadata can be mapped to GV STRATUS metadata.
- **Send Message** — Advanced Logging Tool panels can be sent via the Send Message tool.
- **Camera angles** — Angles can be selected in Inspector and Channel Panel, for clips that are a part of a K2 Dyno camera angle set or a GV STRATUS gang record set.
- **Conform and clean** — When deleting an asset, options are available to conform associated lists and subclips.
- **EDIUS for GV STRATUS** — EDIUS Elite and EDIUS XS launch mode combined.
- **Ingest Schedule Monitor** — The schedule can be displayed on a large screen for viewing by a group of people.
- **Workflow Engine** — Aspera Server supported in GV STRATUS Rules.
- **Documentation** — The following organization and structural changes have been made to the GV STRATUS Topic Library:
  - Release note and upgrade sections for GV STRATUS Rundown and GV STRATUS VTR Ingest consolidated with sections for GV STRATUS.
  - Added master list of Grass Valley ports.
  - Added sections for fully qualified domain and SMB storage.
  - Removed Director tool sections.

GV STRATUS Version 3.5.1

- **Wide Area News field editing integration with EDIUS Elite** — Grass Valley's Wide Area News toolset has been created to provide news operations the utmost flexibility in allocating resources between field and newsroom operations. Wide Area News removes the distance barrier, giving field personnel an editing experience identical to the one they would enjoy in the newsroom with the same access to central newsroom content. By mixing newsroom proxy with locally shot full resolution clips the field user can create finished product with no missing scenes of "black holes". There is no need to transfer full resolution content to the field since a smart conform server at the home base will automatically find the full resolution content for any shots covered by proxy in the field.

  The following specific GV STRATUS 3.5 enhancements enable Grass Valley Wide Area News:

  - Support for mixed full resolution/proxy timeline in EDIUS Elite in the field to support mixing local full resolution content in timeline with "home base" proxies
  - New "Home/Field" project setting in EDIUS Elite
  - Send partially rendered project to home base for final render where proxies are replaced with full resolution

GV STRATUS Version 3.5

- **GV STRATUS Digital Media Platform (DMP)** — GV STRATUS DMP is the industry's most highly integrated and powerful toolset for content delivery to the full spectrum of digital destinations. In a shift from a technology-centric approach to business-driven workflows, users can create a set of properties that accompany content throughout the production and preparation processes, and new properties can be created at each stage. These properties eventually determine to which media the content is sent, how it must be transcoded or reformatted to be suitable to those destinations, special instructions for content embargoes depending on the specific destination medium, and content replacement instructions for both files and live streams added either manually or automatically via an Ignite Production Automation system.

  The following specific GV STRATUS 3.5 enhancements enable the GV STRATUS Digital Media Platform:

  - New custom metadata type
  - Metadata categories (Tabs)
  - Segmentation tool improvements
  - Segment template metadata back to NRCS for markup
  - Search for segments
  - Online Video Platform (Brightcove) interface
  - Additional live encoding and file transcoding interface - Elemental Technologies
  - Rules Engine enhancements
    - Export support for multiple transcode profiles in one rule
    - Force metadata value on export
    - Force lower or UPPER case extension on export
    - E-mail notifications on export failure/success
    - Elemental file encoder support
    - Faster and better CC extraction with K2 Summit for SCC and TTML

      NOTE: Rules based CC extraction through 3rd party transcode products is no longer supported.

- **Rule-based Import of content and metadata** — Import Rules provide broad ability for importing virtually all file types including user generated content, syndicated "store and forward" file delivery systems, and still images.
  - Configure rules in GV STRATUS Control Panel
  - Rules will act on combinations of folder locations and file extensions
  - Accompanying metatada can be mapped to GV STRATUS database and imported
- **Enhanced K2 Dyno integration with support for scheduled multicam recording** — Consistent with the K2 Dyno environment, with GV STRATUS you can now access and work with multicam angle assets in same way as standard clips.

- **Various other significant capabilities** — Numerous additional enhancements in version 3.5 are applicable to the GV STRATUS Digital Media Platform and/or add new functionality to existing GV STRATUS workflows:
  - Support for Evoxe NIS5 newsroom computer system
  - GV STRATUS Render Engine replaces GV STRATUS Conform and GV STRATUS XRE
  - GV STRATUS VTR Ingest application (GV STRATUS enabled version of Aurora VTR Ingest)
  - GV STRATUS VTR Controller application (GV STRATUS enabled version of Aurora VTR Controller)
  - Subclips preserve original clip metadata including markers when in range
  - User roles:
    - Move - to enable/disable users to move assets
    - Rename bin - to enable/disable users to rename bin
    - Queue management - to enable/disable users to manage job queues (cancel etc.)
    - Force delete assets for media manager - bypass protection by association
  - F11 send dialog box enhancements
    - You can now add a description on send
    - Description is added to placeholder when saved
    - Description is added to clip when "Send" is done
  - Partial file transfer from remote to local site.
  - Search enhancements
    - Search for segments
    - Use "quotes" in search to search for characters like _-+*/= and for exact match searches
  - EDIUS enhancements:
    - You can do audio mapping including AC3 and Dolby E
    - Audio mixer available on sources
    - Audio monitoring setting (mono/stereo/custom)

    Refer to EDIUS product documentation for more information.
  - Adobe® Premiere® Pro CC enhancements
    - Support for Mac OS
    - F11 send dialog export box including link to NRCS placeholders
    - Advanced searches
    - Sorting
  - Avid transfers without DHM and without Avid Transfer Manager powered by Marquis MEWS API services
  - GV STRATUS User Interface enhancements
    - Scroll dates by year and months in calendar views
    - New color scheme with choices of 4 different themes with purple or green highlights
    - ALP displays creation date for placeholder
    - "Favorite" enhancements: Now you can add anything in Favorites, including segment templates

- **Documentation** — PDF manuals are replaced by an online HTML format Topic Library. Refer to *Topic Library replaces PDF manuals* on page 35.
- **About product naming** — Effective with GV STRATUS 3.5 version and as part of the introduction of cloud enabled GV STRATUS Playout for play-to-air workflows, two existing applications have been adapted for use in GV STRATUS installations:
  - Version of Aurora Playout application modified for GV STRATUS environment is introduced under the name of GV STRATUS Rundown. No new nomenclature or ordering information is associated with this introduction as the product remains activated by GV STRATUS Elite licenses.
  - Version of Aurora VTR Ingest modified for GV STRATUS environment is introduced under the name of GV STRATUS VTR Ingest, with new nomenclature STRATUS-VTR-ING. Other than an updated GUI color scheme, the GV STRATUS VTR Ingest application has identical specifications as the Aurora VTR Ingest product.

  Both Aurora Playout and Aurora VTR Ingest applications are still available for deployments in non-GV STRATUS installations, such as in standalone configurations or with Aurora Suite.

GV STRATUS Version 3.1

- **Search** — Enhanced search features provide an advanced query syntax for searching one or more words and for using boolean operators. This changes the behavior of a simple search. Previously, a simple search of multiple words, with no syntax, was a phrase search only. Now you must use the advanced query syntax to specify a phrase search.
- **Internal system account** — You can change the internal system account from the default GVAdmin account to a different account, if required by your site's policies.

  NOTE: Do not change internal system account except under the supervision of qualified Grass Valley Support personnel. Extensive system configuration is required to achieve a working GV STRATUS system.
- **Rules** — Support for Harmonic® Workflow System (WFS™), conform, priority, and other enhancements.
- **Adobe® Premiere® Pro CC** — A GV STRATUS plug-in to Adobe® Premiere® Pro CC provides edit-in-place and enhanced workflow.
- **Documentation** — Use K2/STRATUS Documentation Set 071-8910-02 December 2013. The following manuals have been revised:
  - "GV STRATUS Installation and Service Manual" 071-8814-07
  - "FT Server Instruction Manual" 071-8852-03

  The following manual has been revised to support the GV STRATUS plug-in to Adobe® Premiere® Pro CC . Use this version of the manual rather than the version on K2/STRATUS Documentation Set 071-8910-02.
  - "GV STRATUS User Manual" 071-8813-08

  In addition to the documentation listed above, use these release notes and "GV STRATUS Upgrade Instructions" 071-8853-09.

GV STRATUS Version 3.0

- **Multisite** — Enables remote browsing of proxy media and transfer of media across distributed facilities or from field locations.

- **HTTP server** — Provides access to proxy media, replacing the SMB mount access in previous versions.
- **Search indexing service** — Enables faster search across assets.
- **Rules enhancements** — Includes the following:
  - Archive rule
  - Restore rule
  - Export rule exports metadata only
  - Export SCC close captioning when using 3rd party transcoders
  - Thumbnail export
  - Integration with Telestream® Vantage™ 3rd party transcoding engine
- **DataMover Engine** — Supports transfers between devices outside the GV STRATUS system.
- **Full Screen** — Provides full screen playback and timecode selection.
- **Playback ganged clips** — Clips recorded as a gang are associated for playback.
- **Inspector improvements** — Simplified tabs and the ability to reorder properties provide improved access to information.
- **OpenMedia News Room Computer System** — Support for MOS integration with the Annova OpenMedia NRCS.
- **Trim Rights** — Restricts the trim operation to designated user accounts.
- **Metadata** — Reordering of metadata and printing of metadata report card.
- **Event Viewer** — An improved GV Event Viewer application provides easier access to system information.
- **Documentation** — Use K2/STRATUS Documentation Set 071-8910-01 September 2013. The following manuals have been revised:
  - "GV STRATUS User Manual" 071-8813-06
  - "GV STRATUS Installation and Service Manual" 071-8814-06
  - "FT Server Instruction Manual" 071-8852-02

  In addition to the manuals on the Documentation Set, use these release notes and "GV STRATUS Upgrade Instructions" 071-8853-08.

GV STRATUS Rundown Version 8.2

- **Aurora Playout name change to GV STRATUS Rundown** — The Aurora Playout product is rebranded as GV STRATUS Rundown to reflect its workflow in the news environment with the GV STRATUS 3.5 application.
- **Audible countdown before a playback** — Support for audible countdown setting before the start of a playback. The audible countdown audio file can be selected in the Playback setting of the GV STRATUS Rundown application. Refer to *Setting Playback options* on page 1510 for more information about this setting.
- **NIS5 NRCS support** — Support for Evoxe NIS5 newsroom computer system.
- **GV STRATUS 3.5 support** — The GV STRATUS Rundown application supports the workflow with GV STRATUS 3.5 Media Workflow Application Framework.
- **Documentation** — PDF manuals are replaced by an online HTML format Topic Library. Refer to *Topic Library replaces PDF manuals* on page 35.

GV STRATUS Rundown Version 8.1

- **Sealevel GPIO 8004e PCI Express card support** — Support for the Sealevel GPIO 8004e PCI Express card to connect and control the GV STRATUS Rundown application. The card is compatible with Windows 7, Vista, and XP operating systems.
- **Sealevel GPIO SeaI/O-410E Ethernet support** — Support for the Sealevel GPIO SeaI/O-410E device to connect and control the GV STRATUS Rundown application. The device is compatible with Windows 7, Vista, and XP operating systems.
- **GPO command for Embargo status** — Support for Embargo status that can be set to stories in Avid iNEWS newsroom computer system. This is to ensure that stories with Embargo status are to be played on-air only, while stories without the Embargo status can be played to air and streamed via other media options. The GPO command can be configured in the GPIO Configuration tab in the GV STRATUS Rundown application.
- **GV STRATUS 3.1 support** — The GV STRATUS Rundown application supports the workflow with GV STRATUS 3.1 Media Workflow Application Framework.
- **Documentation for this release** — In addition to these release notes, use the following document for this release of GV STRATUS Rundown software:

  - GV STRATUS Rundown User Manual v8.1 — 071-8516-08 — December, 2013

  You can search for the document at *http://www.grassvalley.com/docs*.

GV STRATUS Rundown Version 8.0

- **OpenMedia NRCS support** — Support for MOS integration with the Annova OpenMedia News Room Computer System.
- **New setting in Cue and Chain options** — With the new **Prevent Auto Recue above first cued item** setting in the GV STRATUS Rundown application, you can avoid automatic recue of clips above the first cued clip in the playlist. However, clips can still be cued manually above the first cued item by operators. Refer to the this Topic Library for more information about this setting.
- **GV STRATUS ActiveX Plug-in** — GV STRATUS ActiveX Plug-in is available within the GV STRATUS Rundown application. With the plug-in, playback operators can search, add, edit assets for broadcast, and preview assets via the Source Viewer or the Inspector without taking up a channel on the playout server. In order to use GV STRATUS within GV STRATUS Rundown, the STRATUS-ELITE license is needed on the GV STRATUS Core Services server.
- **New GV STRATUS Database setting in SDB Server** — With this new setting, GV STRATUS database can be accessed via the GV STRATUS ActiveX Plug-in within GV STRATUS Rundown, and proxy paths of assets are available to the newsroom computer system.
- **Documentation for this release** — In addition to these release notes, use the following document for this release of GV STRATUS Rundown software:

  - GV STRATUS Rundown User Manual v8.0 — 071-8516-07 — April, 2013

  You can search for the document at *http://www.grassvalley.com/docs*.

GV STRATUS VTR Ingest Version 9.5

- **Security** — Support for GV STRATUS security.

GV STRATUS VTR Ingest Version 8.5.0.29

- **Aurora VTR Ingest name change to GV STRATUS VTR Ingest** — The name change is to reflect the revamping of Aurora VTR Ingest application into the GV STRATUS workflow.
- **GV STRATUS 3.5 support** — The GV STRATUS VTR Ingest application supports the workflow with GV STRATUS 3.5 Media Workflow Application Framework.
- **Video capture device support** — The GV STRATUS VTR Ingest application supports the following video capture devices:
  - Hauppauge! WinTV-HVR-1150
  - BlackMagic DeckLink SDI 4K
  - BlackMagic UltraStudio SDI
- **Documentation** — PDF manuals are replaced by an online HTML format Topic Library. Refer to *Topic Library replaces PDF manuals* on page 35.

Additional notes

The following sections contain additional information about this release.

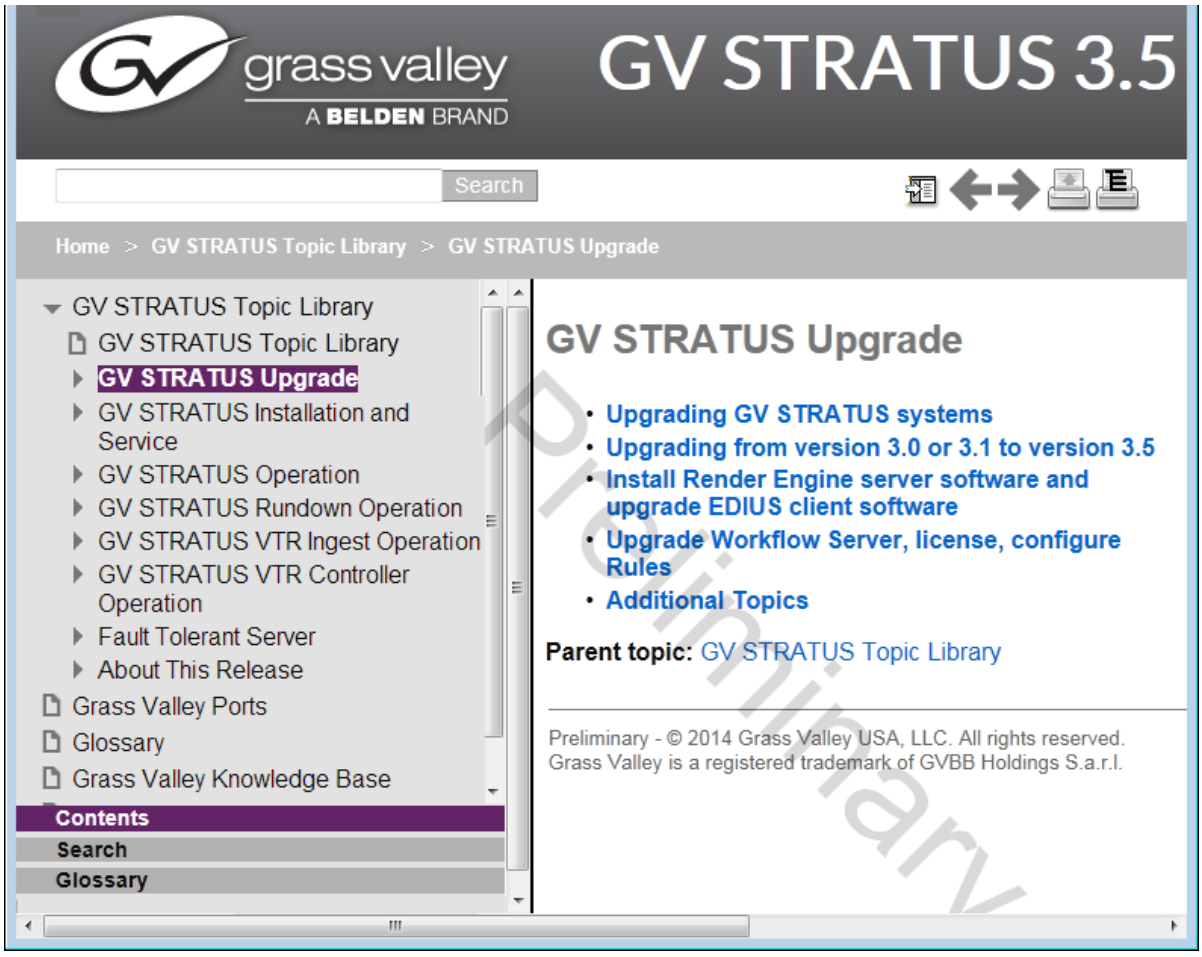
Topic Library replaces PDF manuals

Customer documentation for select Grass Valley products is now delivered as an online HTML format Topic Library, rather than as PDF manuals, with the following benefits:

- A unified search tool finds information anywhere in a product's documentation set. It is no longer necessary to search multiple PDF manuals.
- Extended workflows can be linked, even when the scope crosses multiple installation and operational scenarios. It is no longer necessary to jump between PDF manuals to follow the complete workflow.
- Other usability enhancements.

Information previously found in PDF manuals is now found in the Topic Library. The content of a PDF manual is an expandable section in the Topic Library tree-view.

For example, the content of the "GV STRATUS Upgrade Instructions" PDF manual is in the Topic Library section highlighted in the following illustration.



For the GV STRATUS product, find information as follows:

Information from this PDF manual...	Is in this Topic Library section:
"GV STRATUS Upgrade Instructions"	GV STRATUS Upgrade
"GV STRATUS Release Notes", "Aurora Playout Release Notes", "Aurora Ingest Release Notes"	Release Notes
"GV STRATUS Installation and Service Manual"	GV STRATUS Installation and Service
"GV STRATUS User Manual"	GV STRATUS Operation
"Aurora Playout User Manual"	GV STRATUS Rundown Operation
"Aurora Ingest System Guide" Using VTR Ingest	GV STRATUS VTR Ingest Operation
"Aurora Ingest System Guide" Using VTR Controller	GV STRATUS VTR Controller Operation
"FT Server Instruction Manual"	Fault Tolerant Server

A Topic Library is hosted online on the Grass Valley website. Access to a Topic Library is available at the same location as PDF manuals. For example, if a reader is accustomed to downloading PDF

manuals on the Grass Valley website from a Product Software Download page or from a Product Documentation Library page, a link to the Topic Library is provided on the same page.

A Topic Library provides several options for accessing information offline, as follows:

- Print a single topic or a group of topics with **Print topic** or **Print topic and sub-topics** toolbar buttons. If your printer options support creating a PDF file, you can create a PDF file rather than printing.

About groups and users on a GV STRATUS system

If your GV STRATUS system is on a domain, all servers and client PCs on that system that have any interaction with Grass Valley components must be logged on to Windows with a domain user account. Do not use a local user account.

GV STRATUS licensing and roles are applied to Windows operating system groups and users. Any groups or users to which you assign GV STRATUS licenses or roles must be available for authentication on the GV STRATUS server with role of Common Services, which is typically the GV STRATUS Core server, and on all K2 devices that are part of your GV STRATUS system. This includes the following devices:

- GV STRATUS servers
- K2 Summit standalone systems
- K2 Summit SAN-attached systems
- K2 Media Servers

Groups and/or user accounts are not authorized on the GV STRATUS client PC itself. When you log on to an application from a client PC, you are authorized against the roles assigned to the accounts available on the GV STRATUS Core server as follows:

- GV STRATUS application — If you are using a domain, the log on accounts are on the domain server and are managed by the domain so the GV STRATUS Core server must be on the domain. If you are using a workgroup, the log on accounts must be a part of the workgroup on the GV STRATUS Core server.
- GV STRATUS Control Panel application — You must log on with Windows administrator credentials in order to have access to all the configuration settings in the GV STRATUS Control Panel application. The log on account must be a part of the local Windows administrator account on the GV STRATUS Core server. This is required whether you are using a domain or a workgroup. If you are using a domain, you can additionally add the log on account to the domain administrators group.

  If on a network Workgroup, to configure Authorization Manager settings, you must be running GV STRATUS Control Panel on the GV STRATUS Core server.

GV STRATUS roles matrix

Key:

- AA = Automatically Added for a User or Group with that license (except during version upgrades).
- P = Possible to add for a User or Group with that license.

- X = Not available to be added for a User or Group with that license.

	News room Basic	Express	Flex	Pro	Elite	Enables a Group or User:
Advanced Editor	X	X	AA	AA	AA	Enables a Group or User: Access to Go! Web Client Editor.
Advanced Logging	X	X	X	AA	AA	Access to Advanced Logging tool.
Archive Rights	X	AA	AA	AA	AA	Ability to archive Assets.
Assignment List	AA	AA	AA	AA	AA	Access to Assignment List tool.
Auto Logout	AA	AA	AA	AA	AA	To be automatically logged off as part of Auto Logout scope.
Bin Creation Rights	AA	AA	AA	AA	AA	Ability to create Bins.
Change Thumbnail Rights	AA	AA	AA	AA	AA	Ability to upload, set, and delete Thumbnails.
Channel Panel	X	X	X	AA	AA	Access to Channel Panel tool.
Copy Metadata	AA	AA	AA	AA	AA	Ability to copy and paste Metadata.
Dashboard	X	P	P	P	P	Access to Dashboard node.
Dashboard - Channel Status	X	X	P	P	P	Access to Channel Status Dashboard (Dashboard Role Also Required).
Dashboard - Quotas	X	P	P	P	P	Access to Quota Dashboard (Dashboard Role Also Required).
Dashboard - Social Media	X	P	P	P	P	Access to Social Media Dashboard (Dashboard Role Also Required).
Dashboard - Statistics	X	P	P	P	P	Access to Statistics Dashboard (Dashboard Role Also Required).
Dashboard - Storage	X	P	P	P	P	Access to Storage Dashboard (Dashboard Role Also Required)
Delete Rights	AA	AA	AA	AA	AA	Ability to delete Bins, Assets, and Associations.

Edius Project Management	X	P	P	P	P	Access to EDIUS Projects node.
Edius XS	X	X	AA	AA	AA	Ability to launch Assets into EDIUS XS.
Export Rights	AA	AA	AA	AA	AA	Ability to export Assets.
Media Manager	X	P	P	P	P	See note below.
Missing Material List	P	P	P	P	P	GV Developer Use Only.
Move Rights	AA	AA	AA	AA	AA	Ability to move Assets (Locations and Groups) (Delete Rights Role Also Required).
Multisite Access	X	AA	AA	AA	AA	Access and search for remote Assets.
Playlist Editor	X	X	X	AA	AA	Access to Playlist Editor tool.
Queue Management	X	AA	AA	AA	AA	Ability to set job priority within Job Monitor.
Rename Asset Rights	AA	AA	AA	AA	AA	Ability to rename Assets.
Rename Bin Rights	AA	AA	AA	AA	AA	Ability to rename Bins in Locations node.
Restore Rights	X	AA	AA	AA	AA	Ability to restore Assets as copy.
RMI	X	X	X	AA	AA	Access to RMI tool.
Schedule Monitor	X	AA	AA	AA	AA	Access to Schedule Monitor under Monitors node.
Scheduled Transfer	X	X	X	X	P	Access to Scheduled Transfer tool.
Scheduler	X	X	X	X	AA	Access to Scheduler tool.
Scheduler (Read Only)	X	AA	AA	AA	P	Access to Read-Only Scheduler tool.
Security Manager	X	P	P	P	P	Bypass security/permissions, modify any Bin, Group, or Asset permissions, owner, and owner hint, plus all Media Manager functionality.
Segmentation	X	AA	AA	AA	AA	Access to Segmentation tool and House Number tool. Ability to make Segments in Web Client.

Send Message	X	AA	AA	AA	AA	Access to Send Message tool.
Simple Editor	X	AA	AA	AA	AA	Access to Simple Editor tool and Lost and Found group.
Source Viewer	X	AA	AA	AA	AA	Access to Source Viewer tool.
Storyboard Editor	X	AA	AA	AA	AA	Access to Storyboard Editor tool.
Trim Rights	AA	AA	AA	AA	AA	Ability to Trim and Untrim Assets.
Web Monitor	X	AA	AA	AA	AA	Access to Web Monitor tool for web pages.
Web Access	AA	AA	AA	AA	AA	Access to GV STRATUS Web Client shortcut nodes.

Notes:

Media Manager Role:

- Enables Archive Rights
- Enables Restore Rights as copy and also as move
- Enables Extended Delete Type Options (Delete Rights Role Also Required)
- Enables the ability to save Public Searches
- Enables access to the Lost and Found group
- Enables access to the Archives in Devices node
- Enables the ability to copy and paste Metadata even if Denied
- Enables an API account to create Custom Metadata for Markers and Keywords

The Deny Role option disables a role's functionality or tool(s) for a specific User or Group.

Example: Enable Delete Rights for Group X members, then Deny Delete Rights for User Y of Group X.

Related Topics

If you have trouble launching EDIUS XS on page 169

Grass Valley Recommended Deployment and Monitoring Solutions

To maximize up-time, a maintenance strategy must provide the ability to easily identify the root cause of an unanticipated hardware or software failure and to quickly compile failure data. The ability to proactively predict failures and to quickly notify those who can rectify them makes the maintenance strategy even more powerful. Grass Valley has a long history of building the necessary functionality into critical broadcast products. With Grass Valley's next generation tool, GV GUARDIAN, remote monitoring and proactive predictive failure analysis are important contributors to Grass Valley system solutions. GV GUARDIAN runs on commercial off-the-shelf server PCs, such as the K2 system control point PC, and is also available as an all-in-one turnkey product. Grass Valley and 3rd party devices report status via Window Messaging, Simple Network Management Protocol (SNMP), or syslog to GV GUARDIAN. The tool provides easy to use, fully autonomous

remote monitoring to predict errors, provide proactive notifications, and centrally consolidate error logs and hardware failure information. With GV GUARDIAN you can maximize your up-time with less manpower, as compared to manual system monitoring. Watching for indicator lights, physically scanning logs, and other manual monitoring is far more time consuming, more error-prone, and much less accurate. Grass Valley recommends using GV GUARDIAN as your remote monitoring tool.

Passwords and security on Grass Valley systems

To provide a basic level of security, Grass Valley systems recognize three different security levels based on Windows users and groups, and the systems ship from the factory with accounts pre-configured accordingly. To access the system you must log on with the user name and password for one of the pre-configured accounts.

The following table shows the different types of users and their privileges.

	Windows administrator	Grass Valley product administrator	K2 product administrator	Grass Valley product user
User name	Administrator	GVAdmin	K2Admin	GVUser
AppCenter Configuration Manager	Full access	Full access	Full access	Can view
AppCenter	Full access	Full access	Full access	Full access; requires an account on the K2 Summit system
Storage Utility	Full access	Full access	Full access	Can’t access
K2Config	Full access	Full access	Full access	Can’t access
Server Control Panel	Full access	Full access	Can view	Can view
Windows Operating System	Full access	Full access	Limited access (based on Windows user account privileges).	Limited access (based on Windows user account privileges)

To support legacy FTP and security features, K2 systems also have *movie*, *mxfmovie*, *mpgmovie*, and *video_fs* accounts. Do not use these accounts to log in to the Windows operating system on K2 systems.

Related Topics

About credentials in SiteConfig on page 42
Set credentials on page 266
Changing passwords on page 710
GV STRATUS servers logon account on page 245

About application security on the K2 SAN

The K2Config application and the Storage Utility application both require that you be logged in to the application with administrator privileges in order to modify any settings. These privileges are based on the Windows account that you use when you log in to the K2Config application. When you open Storage Utility from within the K2Config application, the account information is passed to Storage Utility, so you do not need to log in separately to Storage Utility.

In SiteConfig you configure global and/or device-type credentials for device access. These credentials are likewise based on Windows accounts.

You must use a Windows account that has local administrator privileges on the machine to be configured. For example, when you are on a control point PC and you run the K2Config application for the purpose of configuring a K2 Media Server, the account with which you log in to the K2Config application must be present on the K2 Media Server and must have administrator privileges on the K2 Media Server.

For initial setup and configuration, you can use the default Windows Administrator username and password to log in to applications and machines as you work on your K2 SAN. However, for ongoing security you should change the username/password and/or create unique accounts with similar privileges. When you do this, you must ensure that the accounts are present locally on all K2 SAN machines, including control point PCs, K2 Media Servers, K2 Media Clients, K2 Summit Production Clients, and other iSCSI clients.

Grass Valley recommends mapping the SNMP manager administrator with product administrator accounts for your K2 and other Grass Valley products. This allows you to log on to the SNMP manager as administrator using the product administrator logon.

Refer to related topics about Grass Valley recommended deployment and monitoring solutions in the "Release Notes" section of the K2 Topic Library.

About credentials in SiteConfig

SiteConfig requires administrative privileges on devices in order to perform most of the network configuration and deployment tasks. For known devices types, SiteConfig has a default administrator account and password. These default credentials depend on the SiteConfig version, so check your SiteConfig Release Notes for any changes. When you add a device based on a known device type, SiteConfig references the default administrator account and password. Then, when you use remote desktop or perform software deployment to the device, SiteConfig automatically uses these credentials. These credentials are called "global" credentials for the device since the same credentials are used on all devices of that type in the system.

You can choose to override the default credentials for a given device type. For example, if you have specified a different administrator account or a different password on the devices when commissioning the system, then you want SiteConfig to use these modified credentials.

It is possible to also override the default credentials for a single device.

Related Topics

Understanding credentials on page 425
Changing passwords on page 710

Disabling User Account Control for GV STRATUS Rundown on Windows 7 clients

You need to disable the User Account Control on Windows 7 in order to configure **Tools | Options** settings in GV STRATUS Rundown.

1. Go to **Start | Control Panel | User Accounts**.
2. Click on the **Change User Account Control settings** link.
3. Drag the slider bar to the lowest value that shows **Never notify**.
4. Click **OK**.
5. Restart your computer for the change to take effect.

Setting up AMP control for GV STRATUS Rundown on a K2 Client

K2 Media Client and K2 Summit Production Client are controlled via AMP Protocol over Ethernet.

To set up AMP control of a K2 Client:

1. On AppCenter of the client, click the **Options** button for the desired panel.
2. Set the Control setting to either **Remote Only** or **Remote and Local** and the Protocol setting to **AMP**. Repeat this step for each panel that will be controlled remotely.
3. In the SDB Server application, go to **Tools | Options | Media**, click the Add button to add the media server and add the name of the client.
4. In the GV STRATUS Rundown application, go to **Tools | Options | Channel Configuration** and select channel from the dropdown list. To configure the channel, add the channel name, media server and channel server name.

   NOTE: Each K2/Summit channel should be connected to either Aurora Ingest or* GV STRATUS Rundown *only. Connecting to both applications at the same time will cause channel conflicts.

Installing GV STRATUS Rundown software manually

Because you must configure some components with the locations of other components, you should plan your overall installation before you begin.

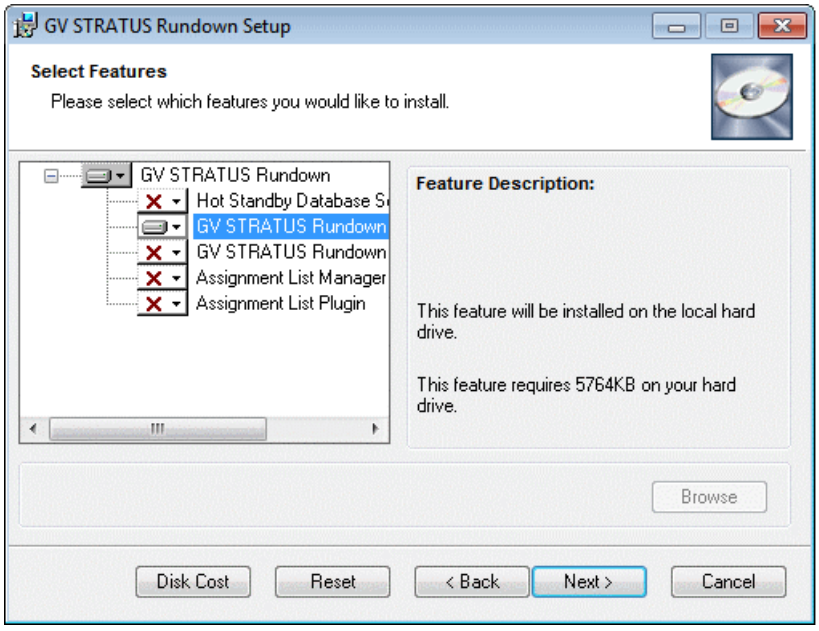
If you don't have SiteConfig within your operation, you can install GV STRATUS Rundown software using the GV STRATUS Rundown installation file that you received from Grass Valley.

The various GV STRATUS Rundown components reside on multiple computers. Using the GV STRATUS Rundown installer, you can choose which component to install on a particular computer.

Component	Machine where you install it...
GV STRATUS Rundown application	GV STRATUS Rundown computer. ***NOTE: It is recommended that* GV STRATUS Rundown *is run at a display resolution of 1280 x 1024.***
GV STRATUS Rundown Server Components: XMOS Server / SDB Server	Recommend installing on a separate computer even though they are allowed to be on GV STRATUS Rundown computer. ***NOTE: The* GV STRATUS Control Panel *application must be installed in the SDB Server / XMOS Server.***

Component	Machine where you install it...
Assignment List Manager (standalone version)	Non-NCS computers, usually used by Newsroom Producers.
Assignment List Plug-in	All NCS client computers.
Hot Standby Database Server	Optional; install on a PC on the same network as the GV STRATUS Rundown computer.

1. Navigate to and double-click **Setup.exe**.
2. Click **Next** until you reach the Select Features screen.



3. At the Select Features screen, select the component(s) that you want to install.
4. Click **Next** to start the installation.
5. Click **Finish** at the Installation Complete screen.

Setting up ENPS for GV STRATUS Rundown

To set up ENPS for use with GV STRATUS Rundown, you need to modify your ENPS configuration.

1. On the ENPS server, find the *enps.ini* file and add the following to the **[ENPS]** section:

```
QTMediaExtensions=.mov,.mp4
```

2. On an ENPS client, log on as the administrator and start up ENPS.
3. From the ENPS folder, select **System Maintenance | Groups | New** and create a new group with these parameters:

ID	KXYZGVG
Description	GV Clips
Server	Select the name of your ENPS server from the drop-down list

4. Click **Save** and close ENPS on the workstation.
5. Close the News Object Manager and it should restart automatically. After the NOM has started, restart the ENPS client.
6. From the ENPS folder, select **System Maintenance | MOS Configuration | New** and create a new MOS entry with these parameters:

ID	The MOS ID; this value is case sensitive and must match the MOS ID configured in the XMOS Server Options. The recommended format is <family>.<machine>.<location>.<enterprise>.mos. Standard practice is to use station call letters for location and station group abbreviation for enterprise.
Description	GV STRATUS - for operation with GV STRATUS.
	GV Assignment List - for GV STRATUS Rundown operation only.
IP	The IP address or host name of the machine hosting the SDB Server and the XMOS Server.
ActiveX	GV.STRATUS.1 - for operation with GV STRATUS.
	GVG.XMOSCtrl.1 - for GV STRATUS Rundown operation only.
Default Settings	Leave blank. These settings are configured during installation.
Program	The group ID you configured in step 3.
MOS Version	2.6 or 2.8.2
Local DragDrop	Off
Auto Create	On
Story Send	On

7. From the ENPS folder, select **System Maintenance | Global Configuration Options**, add a new property named `AddMOSObjDuration` and set its value to **1**.

   NOTE: `AddMOSObjDuration` is the optional setting that allows the duration of clips to be automatically included in the rundown timing. If you prefer to manually enter the duration of your story and clips, do not activate this setting.

8. Add **mp4** to the `MOSBrowseMediaExtensions` property, as can be seen below:

   ```
   MOSBrowseMediaExtensions=bmp,jpg,jpeg,mp4,3gp,wmv,wav,sdp,ts
   ```

9. Restart the ENPS client application.

Related Topics

Setting Up Your NCS for GV STRATUS Rundown on page 1538

Setting ENPS MOS ready to air

If you want producers to have the ability to indicate to the GV STRATUS Rundown operation when a rundown is ready, use the ENPS MOS Ready to Air feature.

To set the feature:

- Set the ENPS rundown property “Ready to air” to ON.

A corresponding READY flag is set to ON in the GV STRATUS Rundown rundown window Status column.

Setting up iNEWS for GV STRATUS Rundown

To set up iNEWS for use with GV STRATUS Rundown, you need to add a new MOS device to the iNEWS configuration file:

1. On the MOS gateway machine, open the file C:\Program Files\Avid\MOSGateway\mosconfig.xml.
2. Modify the following lines of the file, adding values for your location:

Value	Description
ncs id	Your Newsroom Computer System name; this value is case sensitive and must match the NCS ID configuration in the XMOS Server options.
host	The hostname of the iNEWS server.
mos	Your MOS ID; this value is case sensitive and must match the MOS ID configuration in the XMOS Server options.
amcp	The tag displayed in iNEWS scripts for placeholders embedded in scripts. This value should match the device name that appears in the iNEWS SYSTEM.MAP file.
network	The hostname of the machine running the XMOS Server.

NOTE: With iNEWS, <handlesRoItemLevelCommands> default setting could cause stories to drop to the bottom of the playlist when they are newly inserted, or when their channel assignment is changed. Therefore, <handlesRoItemLevelCommands> value should be set to NO in the mosconfig.xml file.

Related Topics

Setting Up Your NCS for GV STRATUS Rundown on page 1538

Configuring status translations for iNEWS

To ensure correct status reporting between GV STRATUS Rundown and iNEWS server, you need to edit the status translation table in the iNEWS configuration file.

- The status translation table within the mosconfig.xml file should appear as below:

```
<statusTranslations>
   <statusUnavailable>NOT READY</statusUnavailable>
   <statusCueing>CUEING</statusCueing>
   <statusAvailable>READY</statusAvailable>
   <statusCued>STAND BY</statusCued>
   <statusPlaying>PLAY</statusPlaying>
   <statusPaused>STOPPED</statusPaused>
   <statusStopped>END</statusStopped>
   <statusUnknown>DISCONNECTED</statusUnknown>
</statusTranslations>
```

- On the iNEWS server, your MCS dictionary (located at /site/dict/mcs) would typically contain these lines:

```
A_EVERR                    /5ERROR
A_CAFRZ                    /END
A_CATREL                   /2STANDBY
A_CATHRD                   /THREAD
A_CACUING                  /2CUEING
A_CACUED                   /2CUED
A_CANOTAPE                 /4NOT READY
A_CABIN                    /READY
A_CAPLAY                   /3PLAY
A_CAPAUSE                  /3STOPPED
A_CAREW                    /REWIND
A_CAEJECT                  /EJECT
A_CAINCMPLT                /TRANSFER
```

NOTE: Since the statuses that appear in this dictionary can be customized, the values shown in the right column of your MCS dictionary may vary slightly from the ones shown here.

To ensure correct configuration with iNEWS, a sample of the mosconfig.xml file is provided in the appendix section.

Setting up Octopus for GV STRATUS Rundown

In order to use Octopus with GV STRATUS Rundown, you need to configure it first.

To configure Octopus for GV STRATUS Rundown, you need to create an ActiveX device, and modify the MOS Devices configuration.

Related Topics

Setting Up Your NCS for GV STRATUS Rundown on page 1538

Configuring the MOS Device for Octopus

You need to configure the MOS Device before using Octopus with GV STRATUS.

1. Launch the Octopus client, and click the **Devices** button.

   The **Devices** page opens.

2. Click the **New** button on the toolbar.

   The **Device** window opens.

3. Configure the Basic tab as follows:

mosID	These values must match those set for the XMOS Server.
ncsID	
Version	This value must match with the version set for the XMOS Server.
Disabled	Unchecked
Media host	Name or IP address of machine hosting the SDB Server.
Media port	SDB Server port (normally won't change from default setting)
Rundown host	Name or IP address of machine hosting the XMOS Server.
Rundown port	XMOS Server port (normally won't change from default setting)

4. Configure the Stories tab as follows:

Option	Setting
Send empty stories	✓
Send production requirements	✓
Send story custom fields	✓
Use standard ed times	✓

5. Configure the Rundowns tab as follows:

Refresh method	roReplace
Send roMetadataReplace	✓
Send broadcast channel name in roChannel	✓
roSlug pattern	%TYPE% %START%

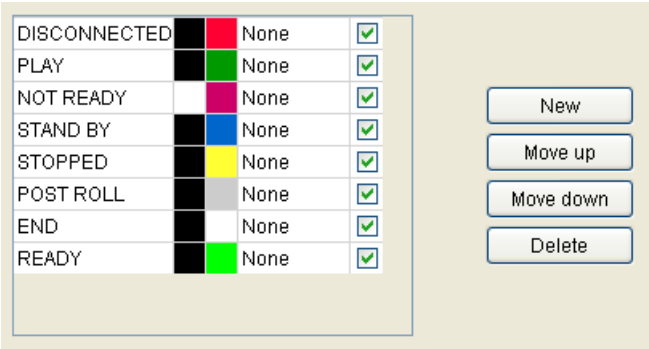
6. Configure the Prompting tab as follows:

Send story text	✓
Keep sending roStoryReplace or roElementAction	✓

7. Configure the Status tab as follows:

Accepts on-air status	✓
Accept status for slugs in not-ready rundowns	✓

a) Create these status categories (these are the suggested names and order):



8. Configure the MOS Objects tab as follows:

Update private objects	✓
Translate redirected IDs	✓
Supports mosListAll	✓
Display name instead of jobID	✓

9. Configure the Placeholders tab as follows:

Allow MOS object creation	✓
Default MOS object creation device	✓
Allow automatic MOS object creation	✓
Use the <mosObjCreate> message	✓
Default duration of created MOS objects	00:00:00:00
Naming pattern of created MOS objects	%NAME

10. On the Other tab, configure as follows:

Send and receive times in UTC	✓

11. Click **OK**.

Creating an ActiveX Device for Octopus

You need to create an ActiveX device before using Octopus with GV STRATUS.

1. Launch the Octopus client, and click the **Devices** button.

   The **Devices** page opens.
2. Highlight the MOS ID for GV STRATUS.
3. Click the **Edit** button on the toolbar.

   The **Device** window opens.
4. Select the **Plugins** tab, and click **Add**.

   The **Plugin** window opens.
5. Configure the device as follows:

Option	Setting
Short Name	User preference (e.g., GV Plug-in)
Long Name	User preference (e.g., GV STRATUS Plug-in)
Size	800 width x 600 height
Type	Player (ActiveX)
Version	1.0 ENPS
Platform	ActiveX
Placement	Modeless
Implementation	GV.STRATUS.1

6. Click **OK** twice.

GV STRATUS Operation considerations

- On the K2/STRATUS system do not exceed the following maximum amounts:
  - Maximum bin depth: 9
  - Maximum number of markers per asset: 100
  - Maximum number of assets per page: 2500 in the 32-bit application, 10000 in the 64-bit application
  - Maximum number of search results: 2000 in the 32-bit application, 5000 in the 64-bit application
  - Maximum number of jobs monitored: 2000 in the 32-bit application, 5000 in the 64-bit application
  - Maximum number of placeholders for optimal performance: 2000
  - Maximum K2 database size: 80 MB

- If a Dell server that is a GV STRATUS "Engine" server is on a redundant K2 SAN, Grass Valley recommends two media network (iSCSI) connections on the server, one to the A side of the K2 SAN and one to the B side of the K2 SAN. If such a server is connected to just one side of a redundant K2 SAN and a failover occurs on the K2 SAN, you must shut down the server if it is on the "failed" side of the K2 SAN.
- The Render Engine generates proxy media for high-resolution clips with one video track. Clips with more than one video track are not supported.
- Rename bins with careful considerations. A bin containing a large number of assets can consume system resources for an extended period of time while the rename operation is applied. To rename bins, you must be assigned **Rename Bin Rights** in GV STRATUS Control Panel. If GV STRATUS security settings are enforced, you must have adequate permissions. If not, menu selections are disabled. Rename bin operation also cannot be completed if assets in the bin are locked or in-use.
- 4K is not supported on K2 SAN systems with clients that are connected via iSCSI. A 4K client must be connected via fibre channel.
- K2 SAN clients with iSCSI connections can only support a maximum of two 1080p records per client.

GV STRATUS Rundown Operation considerations

- For GV STRATUS Rundown to work in Windows 7, you need to disable the User Account Control in your machine. Refer to *Disabling User Account Control for GV STRATUS Rundown on Windows 7 clients* on page 43 for more information in these release notes.
- For GV STRATUS Control Panel to successfully configure SDB and XMOS servers, the GV STRATUS Control Panel application must be installed on SDB / XMOS machines.
- The graphics workflow with Orad's Maestro On Air Graphics System and Aurora Edit is only supported in GV STRATUS Rundown (formerly known as Aurora Playout) version 7.1.1 and below.
- Windows 2000 that was supported in previous versions of GV STRATUS Rundown software is no longer supported.

GV STRATUS VTR Ingest Operation considerations

- If multiple clients are pointed to the same VTR, each client will report a successful connection. When operating the VTRs, however, the multiple clients may interfere with each other. It is important to allocate VTRs properly so collisions of this nature do not occur.
- Records have a frame accuracy recording window of +/- 3 frames for the GV STRATUS VTR Ingest with K2.
- When controlling a VTR that is in 720p mode, transport commands, such as single frame and ten frame advances may not be frame accurate.

GV STRATUS Version compatibility

Versions qualified for compatibility with this version of GV STRATUS software are summarized in the following sections.

System requirements for GV STRATUS client PC

All systems require one or more GV STRATUS client PCs. Verify that all GV STRATUS client PCs meet system requirements.

Virtual Machines, Remote Desktop, and other modes of remote access are not supported. Lack of robust video/graphic support can cause video display problems.

It is also recommended not to run multiple GV STRATUS desktop clients at a time logged in as the same user.

GV STRATUS Web client

These minimum requirements apply to a device running the following:

- The GV STRATUS Web Client

Characteristic	Specification
Web Browser	Recommended: Google Chrome
Frame accurate Streaming	Browser must support webRTC GV STRATUS system must be licensed with GV STRATUS Streaming Server.

GV STRATUS Laptop, and low-resolution Client workstation

These minimum requirements apply to a PC running one or more of the following:

- The GV STRATUS application with a proxy media workflow.
- The GV STRATUS Control Panel application.
- The SiteConfig application.

Characteristic	Specification
Processor	Minimum: Intel Core i3 mid-range processors and above Recommended: Intel Core i5 processor and above
Memory	Minimum: 4GB RAM Recommended: 8GB RAM (Especially when shared with 3rd party applications)
Graphics	Direct 3D 9+ support
System drive	Minimum: 80GB 7200RPM hard drive

Characteristic	Specification
Network	Single Ethernet 1000 Base-T network interface
Operating system	Microsoft Windows 7 SP1 32-bit (supported) or 64-bit (preferred) Microsoft Windows 10 64 bit
Microsoft .NET Framework	Version 4.7.1
Web Browser	Recommended: Google Chrome
Other support	DirectX 9 compatible

GV STRATUS/EDIUS XS Laptop, and low-resolution Client workstation

These minimum requirements apply to a PC running the following:

- The GV STRATUS application and the EDIUS XS application, with a proxy media workflow.

Characteristic	Specification
Processor	Intel Core i5 4 core processor and above
Memory	8GB RAM
Graphics	Integrated or discrete graphics with Direct 3D 9 or better
System drive	Minimum: 80GB 7200RPM hard drive Recommended: 128GB SSD drive or larger
Network	Single Ethernet 1000 Base-T network interface
Operating system	Microsoft Windows 7 SP1 32-bit (supported) or 64-bit (preferred) Microsoft Windows 10 64-bit ***NOTE: 64-bit required for EDIUS XS***
Microsoft .NET Framework	Version 4.7.1
Web Browser	Recommended: Google Chrome
Other support	DirectX 9 compatible

GV STRATUS high-resolution workstation

These requirements apply to a PC running the following:

- The GV STRATUS application with a high-resolution media workflow. This requires access to high-resolution assets.
- The EDIUS Workgroup application with a high-resolution media workflow. This requires access to high-resolution assets.

Characteristic	Specification
Processor	Recommended: Intel Core i7 4 Core 4GHz (For desktop grade machines) OR Recommended: Intel Xeon E5-2630 Quad Core 2.4 GHz (For workstation grade machines)
Memory	Minimum: 8GB RAM Recommended: 16GB RAM
Graphics	Integrated or discrete graphics with Direct 3D 9 or better
System drive	256GB SSD drive recommended OR 1TB 7200RPM hard drive (if SSD not available)
Network	Dual Ethernet 1000 Base-T network interface
Operating system	Microsoft Windows 7 SP1 64-bit. Windows 7 must be used for workstations connecting to existing K2 SAN systems running SNFS 4.7. Microsoft Windows 10 64-bit (on systems with SNFS 6.0.6 installed). Windows 10 must be used for workstations connecting to new K2 SAN systems delivered (from late 2018) running SNFS 6.x. ***NOTE: 64-bit required for EDIUS Workgroup.***
Microsoft .NET Framework	Version 4.7.1
Other support	DirectX 9 compatible

Compatible GV STRATUS components

The following components are part of GV STRATUS products. Components are compatible with this release of GV STRATUS software as listed in the following table. Compatible versions are pre-installed on GV STRATUS Servers when you receive them new from Grass Valley.

Component	6.8 Compatible	Comments
GV STRATUS Application	6.8.0.179	—
GV STRATUS Control Panel	6.8.0.201	—
GV STRATUS Control Panel Service	6.8.0.233	—
GV STRATUS Databases	6.8.0.154	—
Common Services	6.8.0.256	—
Ingest Services	6.8.0.4997	—
GV STRATUS Traffic Gateway Service	6.8.0.3717	—

Component	6.8 Compatible	Comments
GV STRATUS HTTP Proxy Server	6.8.0.194	—
Core Services	6.8.0.256	—
GV STRATUS Summit Services	6.8.0.210	—
Summit, Generic FTP, FlashNet, DIVA,Masstech, CRArchive, and Proxy MDI	6.8.0.209	—
GV STRATUS Render Engine	9.3.1.4457	—
GV STRATUS Mediaflow Engine	6.8.0.4361	—
GV STRATUS Rules Engine	6.8.0.4124	—
GV STRATUS Transcode Engine	6.8.0.4082	—
GV STRATUS DataMover Engine	6.8.0.4069	—
GV STRATUS ProxyStreamingService	6.8.0.255	—
GV STRATUS Scheduled Transfer Engine	6.8.0.2727	—
GV STRATUS ExternalMedia	6.8.0.171	—
GV STRATUS SocialMedia	6.8.0.171	—
GV STRATUS WebApps	6.8.0.245	—
GV STRATUS WebClient	6.8.0.287	—
GV DeviceKeyService	6.8.0.227	—
GV Log Manager	6.8.0.236	—
GV Log Viewer	6.8.0.203	—
GV Embedded Security Manager	1.0.0.24	—
GrassValley_STRATUSClient cab file	6.8.0.172	Contains compatible software install cab files for GV STRATUS client PCs
GrassValley_CoreServer cab file	6.8.0.172	Contains compatible software install cab files for GV STRATUS servers
GrassValley_K2system cab file	6.8.0.172	Contains compatible software install cab files for K2 systems version 9.8.7.2606
GrassValley_K2Plus cab file	6.8.0.172	Contains compatible software install cab files for K2 systems version 10.1.1.2652

Component	6.8 Compatible	Comments
GrassValley_GVIO cab file	6.8.0.172	Contains compatible software install cab files for GV I/O Live Ingest and Playback Server version 2.4.5.232

Grass Valley products compatible with GV STRATUS

Grass Valley products are compatible with this release of GV STRATUS software as follows:

Product	6.8 Compatibility	Comments
K2 Summit/SAN system software	9.8.7.2606	Compatible with SNFS version 4.7.2.b50774
K2 Summit 3G Plus system software	10.1.1.2652	Compatible with SNFS version 6.0.6.b75382-14
GV STRATUS Rundown	11.8.0.58	—
GV STRATUS VTR Ingest	11.8.0.64	—
EDIUS	9.3.1.4457	—
K2 FCP Connect	2.3.0.71	—
SiteConfig	2.2.0.663	—
SiteConfig Discovery Agent	2.2.0.215	—
Grass Valley Prerequisite Files	2.0	Required by SiteConfig to support software installation of GV STRATUS Rundown.
Grass Valley Embedded Security Manager	1.0.0.24	—
K2 Dyno S Replay Controller	3.8.7.542	Compatible with K2 Summit/SAN system software
K2 Dyno S3 Replay Controller	4.1.1.549	Compatible with K2 Summit 3G Plus system software
SabreTooth	2.7.1.33	—
K2 Avid	7.3.5.251	With Interplay Engine v3.5
Adobe® Premiere® Pro CC plug-in extension	6.8.0.0 with Adobe® Premiere® Pro CC (2018)	—
Aurora To GV STRATUS Migration Utility	6.8.0.256	—
EDIUS Project Migration Utility	9.3.1.4457	—

Third party products compatible with GV STRATUS

Products by manufacturers other than Grass Valley are compatible with this release of software as follows:

Product	6.8 Compatibility	Comments
ENPS Server	8.2.3.3054	—
ENPS Client	8.2.3.3054	—
iNEWS Server/Client/MOS Gateway	7.0.0.108 / 7.0.0.36 / 4.5.05	—
Octopus	8.1.18451.66	—
NIS Web client	5.6.6	—
OpenMedia Server/Client	4.3.2129	—
Netia	8.2	—
Inception	11.0	—
MOS	2.8.2	—
Oracle Digital DIVArchive software	7.6	Check with your Grass Valley representative.
FlashNet	6.8.06.27	—
Masstech	8.1.2.3	—
Generic FTP	0.9.60	Generic FTP archive with FileZilla and a nearline K2 SAN is supported. Other generic FTP archive configurations are not supported.
Aspera Enterprise Server	3.7.4.147264	With Windows Operating System
	3.7.4.147133	With Linux Operating System
Harmonic ProMedia™ Carbon (formerly Carbon Coder™)	3.24.0.48292	—
Telestream Vantage™	7.1	—
Harmonic WFS	2.2.0.6	—
Elemental	2.2.1.22	—
MEWS	4.0.0.196	With Avid Interplay Production 3.6.x and 3.7.x
Avid Media Composer	8.7.2	—
Final Cut Pro	7.0.3 with Mac OS X 10.9.5	—

Product	6.8 Compatibility	Comments
Adobe® Premiere® Pro CC (2018)	12.1.2 with Windows and Mac OS X 10.13.6 Check with your Grass Valley representative for updates.	To install the GV STRATUS security certificate, please refer to: *Installing GV STRATUS security certificate for Adobe Premiere Pro*
Encore	1.8.2	—
Jupiter (AccuSwitch)	8.0.1	—
Microsoft Visual C++ 2017 Redistributable	14.12.25810.0	—
Microsoft .NET Framework	4.7.1	—
Microsoft SQL	2017, 2014 SP2	—

GV STRATUS archive support

Features and formats supported for integration with archive systems are as follows:

Table 1: Partial file restore

Supported	FlashNet	Oracle Digital DIVA	Masstech	Generic FTP
GXF	Yes	Yes	No	No
MXF	Yes	Yes ***NOTE: 64 audio tracks are not supported for partial file restore of MXF on 720p format for DIVA.***	Yes. Check with your Grass Valley representative for supported video codecs. Partial file restore is not supported for XAVC format. ***NOTE: Audio tags are not supported for partial file restore in MXF format for Masstech.***	No

NOTE: Audio tags are not supported for partial file restore in GXF format for all archive vendors.

GV STRATUS Rundown Version compatibility

Versions qualified for compatibility with this release of software are summarized in the following sections.

GV STRATUS Rundown System specifications

This section describes the hardware requirements that customers should use when purchasing equipment for this release. The minimum spec describes the bare minimum requirement for running GV STRATUS Rundown, which may reduce the quality of user experience, depending on the task. The expected lifespan of minimum spec equipment is also less than that of recommended spec equipment, since it lacks head room for future growth.

NOTE: Minimum specs for SD configurations are provided only for existing SD customers upgrading to this release. New customers should use HD configurations.

GV STRATUS Rundown

	MINIMUM Spec	RECOMMENDED Spec
Processor	Intel Core 2 Dual Core 2.3 GHz	Intel Core i5 processor and above
Memory	1 GB (for 32-bit OS) 2 GB (for 64-bit OS)	4 GB (for 32-bit OS) 8 GB (for 64-bit OS)
Graphics	Integrated or discrete graphics with Direct3D 9 and above	Discrete graphics with Direct3D 9 and above
System Drive	80 GB 7200 RPM SATA	100 GB 7200 RPM SATA
Optical Drive	CD/DVD	CD/DVD
Network	Gigabit Ethernet (2)	Gigabit Ethernet (2)
Operating System	Microsoft Windows 7 SP1 (32/64-bit)	Microsoft Windows 7 SP1 (64-bit) Microsoft Windows 10 (64-bit)
Notes	It is the customer's responsibility to ensure that the system has sufficient number and type of expansion slots to meet the intended use. GV STRATUS Rundown requires one free PCI slot for each Comtrol 422 and Sealevel GPIO board. GV STRATUS Rundown supports: • Sealevel GPIO 8004e PCI Express card • Sealevel GPIO SeaI/O-410E Ethernet module	

Grass Valley products compatible with GV STRATUS Rundown

Grass Valley products are compatible with this release of software as follows:

Product	Compatibility with GV STRATUS 6.8	Comments
EDIUS	9.3.1.4457	—

Product	Compatibility with GV STRATUS 6.8	Comments
Generic iSCSI Installer	3.3.2.1401 or 7.4.3.x or 8.1.9.x or 9.8.7.2606 or 10.1.1.2652	—
GVG_MLib Installer	3.3.2.1401 or 7.4.3.x or 8.1.9.x or 9.8.7.2606 or 10.1.1.2652	—
K2 system software	3.3.2.1401 for K2 Media Client	With compatible version of SNFS.
	7.4.3.x for K2 Summit Production Client	
	8.1.9.x for K2 Summit Production Client	
	9.8.7.2606 for K2 Summit 3G Production Client	
	10.1.1.2652 for K2 Summit 3G+ Production Client	
GV STRATUS application	6.8.0.179	—
SiteConfig application	2.2.0.663	—
SiteConfig Discovery Agent	2.2.0.215	—
Grass Valley Prerequisite Files	2.0	Required by SiteConfig to support software installation of GV STRATUS Rundown.

Third party products compatible with GV STRATUS Rundown

Products by manufacturers other than Grass Valley are compatible with this release of software as follows:

Product	Compatibility with GV STRATUS	Comments
ENPS Server	8.2.3.3054	—
ENPS Client	8.2.3.3054	—
iNEWS Server/Client/MOS Gateway	7.0.0.108 / 7.0.0.36 / 4.5.05	—
Netia	8.2	—
Octopus	8.1.18451.66	—
Inception	11.0	—
NIS Web client	5.6.6	—
OpenMedia Server/Client	4.3.2129	—
MOS	2.8.2	—

GV STRATUS VTR Ingest Version compatibility

For compatible Grass Valley products and third party products, refer to related topics in this Topic Library.

GV STRATUS VTR Ingest system specifications

This section describes the hardware requirements that customers should use when purchasing equipment for this release. The minimum spec describes the bare minimum requirement for running GV STRATUS VTR Ingest and GV STRATUS VTR Controller, which may reduce the quality of user experience, depending on the task. The expected lifespan of minimum spec equipment is also less than that of recommended spec equipment, since it lacks head room for future growth.

NOTE: Minimum specs for SD configurations are provided only for existing SD customers upgrading to this release. New customers should use HD configurations.

GV STRATUS VTR Ingest and GV STRATUS VTR Controller

	MINIMUM Spec	RECOMMENDED Spec
Processor	Intel Core i3-2120 3.3GHz	Intel Core i5 processor and above
Memory	4GB RAM	8GB RAM
Graphics	Integrated or discrete graphics with Direct 3D 9 or better	Integrated or discrete graphics with Direct 3D 9 or better
System Drive	80GB 7200RPM hard drive	100GB 7200RPM hard drive
Optical Drive	CD-ROM drive	CD-ROM drive
Network	Single Ethernet 1000 Base-T network interface	Dual Ethernet 1000 Base-T network interface
OS	Microsoft Windows 7 32-bit or 64-bit	Microsoft Windows 7 64-bit Microsoft Windows 10 64-bit
Other support	DirectX 9 compatible	DirectX 9 compatible

Licensing GV STRATUS products

The following sections contain instructions for managing GV STRATUS product licenses.

Licensing a GV STRATUS system

Licenses are requested through email and managed through the SabreTooth License Manager, which is installed on the Grass Valley product with the Grass Valley software. The SabreTooth License Manager must be located on the Grass Valley product.

License information is stored in XML files that you can manage just like any other file on your system. Node-locked licenses are unique to the system for which they are requested and cannot be used on any other machine. A floating license can be used on multiple machines, one at a time. You should back up the license text files to a separate drive or as part of a recovery image.

Licenses are based on your system's unique identifier, which is partially derived from your system's Media Access Control (MAC) address. If you change your system's MAC address by performing operations such as changing the System Processor card, you must obtain a new license based on the new MAC address.

To license a GV STRATUS system, one or more licenses must be installed on the GV STRATUS server with role of Common Services. If the system has a server that does proxy encoding, one or more licenses for proxy encoding must be installed on that server as well.

Related Topics

Devices components: Roles, cab files, services, and licenses on page 444

About GV STRATUS Rundown software licensing

If you want to use GV STRATUS Rundown, you need to install the STRATUS-ELITE license on the GV STRATUS Core Services server. The GV STRATUS Rundown application checks for the STRATUS-ELITE license in order for you to operate in GV STRATUS environments.

Licenses are requested through email and managed through the SabreTooth License Manager, which is installed on the Grass Valley product with the Grass Valley software. The SabreTooth License Manager must be located on the Grass Valley product.

Due to the fix to Meltdown and Spectre vulnerabilities, GV STRATUS Rundown no longer supports connecting to a remote SabreTooth License Manager if you are not connected to the GV STRATUS Core server. GV STRATUS Rundown users with remote licensing should procure the license and install it in the local SabreTooth License Manager.

License information is stored in XML files that you can manage just like any other file on your system. Node-locked licenses are unique to the system for which they are requested and cannot be used on any other machine. A floating license can be used on multiple machines, one at a time. You should back up the license text files to a separate drive or as part of a recovery image.

Licenses are based on your system's unique identifier, which is partially derived from your system's Media Access Control (MAC) address. If you change your system's MAC address by performing operations such as changing the System Processor card, you must obtain a new license based on the new MAC address.

GV STRATUS Rundown licenses

The Grass Valley licenses available at the time of this writing that can be installed on GV STRATUS Rundown are as follows. Contact your Grass Valley representative for more information about licenses.

GV STRATUS Rundown licenses

License	License type
Aurora GFX	SabreTooth

License	License type
STRATUS-ELITE	SabreTooth

GV STRATUS VTR Ingest licenses

The Grass Valley licenses available at the time of this writing that can be installed on GV STRATUS VTR Ingest are as follows. Contact your Grass Valley representative for more information about licenses.

GV STRATUS VTR Ingest licenses

License	License type
STRATUS-VTR-ING	SabreTooth

NOTE: The licensing is based on per concurrent user. A single license permits the use of GV STRATUS VTR Ingest application by a single user at a time. For multiple concurrent sessions, you must purchase multiple licenses.

Licensing EDIUS

If using EDIUS XS or EDIUS Workgroup with GV STRATUS, you must ensure the appropriate licenses are in place, as follows:

- EDIUS XS: This license is installed on GV STRATUS Core server and managed by GV STRATUS Sabretooth license management. The GV STRATUS system must have a Flex, Pro, or Elite license.
- EDIUS Workgroup: Three licenses are required to be installed on the client PC that hosts the GV STRATUS and EDIUS Workgroup applications. These licenses are managed by EDIUS license management, rather than GV STRATUS Sabretooth license management.
    - EDIUS Workgroup license
    - EDIUS K2 Option license
    - EDIUS STRATUS Option license

On client PCs, only one EDIUS license type is supported. Do not install both EDIUS XS and EDIUS Workgroup on the same PC.

Requesting a license

Features for your GV STRATUS system are enabled by SabreTooth licenses. For each server you are licensing, you must provide a generated unique ID to Grass Valley. Grass Valley uses the ID to create your unique license.

1. Refer to the license sheet that you received with your GV STRATUS license. The license sheet has the Sales Order number that you need.

2. Generate a unique ID of the device where you will install software, as follows:
   a) Double click on the License Manager icon on the Windows Desktop.
      The SabreTooth License Manager opens.
   b) Choose **File | Generate Unique Id** the License Manager.
   c) Click **Copy to clipboard** to copy the generated ID, and **OK** to exit.
3. Prepare an email that includes the following information:
   - Customer Name
   - Customer Email
   - Sales Order Number
   - Unique ID of the device where you will install software.
   - The license types you are requesting.
4. Send the email to GrassValleyLicensing@grassvalley.com.

The SabreTooth license number will be emailed to the email address you specified.

Next add the license to the SabreTooth License Manager.

Adding a license

Your software license, *Licenses_<SalesNumber>.txt*, is provided as a text file. Use the License Manager to add this file to your system and enable the desired feature.

1. Double click on the License Manager icon on the Windows Desktop.
   The SabreTooth License Manager opens.
2. Do one of the following:
   - Choose **File | Import License** and navigate to the file location to open the text file.
   - Drag and drop the text file onto the License Manager.

   You will now see the permanent license in SabreTooth, as well as any other licenses, permanent or temporary, that have been installed on this machine.

You should archive the permanent license to a backup system.

Deleting licenses

Deleting a license disables the feature that it enabled. You might want to delete a temporary license prior to its expiry if you have decided not to purchase the feature. You can delete a temporary license after the permanent license has been installed without disabling the licensed product.

1. Select the license in the SabreTooth License Manager.
2. Use the Delete key on your keyboard or right click with your mouse and select **Delete**.

Archiving licenses

You can archive your licenses to a secure external location. This allows you to quickly re-install a license should it be deleted or should you have to downgrade and then re-license the software. You can archive multiple licenses at the same time.

NOTE: If you downgrade to an earlier version of the licensed software, make sure to archive the licenses first.

1. In the SabreTooth License Manager, select the license or licenses.
2. Choose **File | Export License** to open the Save As dialog box.
3. Assign a meaningful name to the file, and save it to the desired location. Grass Valley recommends saving the license file to a USB drive or other external location.

GV STRATUS Known Problems

The following limitations are present in this release of software. If you wish to obtain more information about these limitations, please mention the reference numbers.

DE487 ncb00038625 STR-6425	Description:	An undocked panel, when located on a GV STRATUS client PC's secondary monitor, does not remain maximized if the GV STRATUS application is minimized then restored.
	Workaround:	After minimizing/restoring the GV STRATUS application, adjust undocked panels on secondary monitors.
DE543 ncb00061357 STR-6373	Description:	In the GV STRATUS application there is no indicator that identifies a clip as a Super Slo-Mo clip.
	Workaround:	View clips in the K2 AppCenter application to identify Super Slo-Mo clips.
DE550 ncb00061426 STR-6366	Description:	In a list details mode, applying a column filter can make scroll bars disappear, resulting in the inability to scroll to the desired location in the list. This occurs if the list is large enough to require scroll bars and then scrolling to the right to apply a column filter. If the filter yields an empty list that does not require scroll bars, there is no scroll bar available to scroll back to the left.
	Workaround:	Right-click the list, select **Filters**, and in the dialog box that opens modify the filters.
DE1281 ncb00074834 STR-5771	Description:	Proxy media does not load after regenerating proxy if the asset remains open in Inspector.
	Workaround:	1. Load an asset into Inspector that does not have proxy media. 2. Regenerate proxy for that asset. 3. Load a different asset into Inspector. 4. Load the asset for which you regenerated proxy. Now the proxy media loads.
DE1323 ncb00074846 STR-5731	Description:	Renaming a bin removes the bin from the Favorites node.
	Workaround:	Add the renamed bin to the Favorites node again.

DE1878 ncb00075564 STR-5259	Description:	Assets deleted on K2 Dyno appear in the GV STRATUS Lost and Found bin.
	Workaround:	Delete the assets from the GV STRATUS Lost and Found bin.
DE2709 ncb00076221 STR-4693	Description:	Wrong Mark In/Out display on Asset List for the merged import of trimmed clips via the RMI tool.
	Workaround:	Drag the imported clip into the Inspector and select **Relationships | Markers** tab to view the correct Mark In/Out display in the Inspector panel.
DE2998 ncb00076113 STR-4462	Description:	The new name is not displayed in GV STRATUS Control Panel Authorization Manager when renaming a group or user.
	Workaround:	Restart the GV STRATUS Control Panel application.
DE3542 ncb00076390 STR-4158	Description:	A custom metadata field appears in an Asset List and cannot be removed. This occurs when a custom metadata field is added that has the same name as a field that was previously deleted.
	Workaround:	Before deleting a custom metadata field, rename it to a name that you will not use again.
DE3571 ncb00076391 STR-4141	Description:	GV STRATUS is unable to play legacy proxy that has 44.1kHz audio.
	Workaround:	To get audio, the video should be restored from archive and the proxy should be regenerated..
DE3811 ncb00076395 STR-4005	Description:	MXF and QuickTime export fails when exporting a list created in Storyboard Editor. This occurs if one or more clips in the list have no ancillary data track and fewer than four audio tracks, which creates empty tracks that are not compatible with the export format.
	Workaround:	Ensure clips have an ancillary data track and four or more audio tracks.
DE3853 ncb00076397 STR-3988	Description:	Removing channels in Ingest configuration with auto-assigned events still scheduled on that channel will cause the events to start recording on other channels during the event start time.
	Workaround:	Remove all events that have been set to Auto-Assign before removing the channel.
DE4389 ncb00076566 STR-3786	Description:	An asset cannot be added to a Storyboard list, conformed, or used to generate proxy. This occurs if the clip has one or more video, audio, or data track modified in K2 AppCenter. This can change the clip to a "Sequence" asset in the GV STRATUS application and limit its use.
	Workaround:	Use EDIUS to modify asset tracks.

DE4576 ncb00076634 STR-3687	Description:	When deleting an asset from a location, if the asset has multiple high-resolution associations, all high-resolution associations in all locations are deleted. For more information refer to the related topic about asset copies and deletions in this Topic Library.
	Workaround:	To delete a high-resolution association, do the following: 1. Load the asset into the Inspector. 2. Click on the **Associations** tab. 3. Select and delete the desired high-resolution association from the tab.
DE4577 ncb00076634 STR-3686	Description:	Copying assets back and forth between the same locations on different K2 storage systems results in unexpected behavior. Automatic rename and overwrite features do not produce the expected asset names and associations.
	Workaround:	Once an asset is copied to a different K2 storage location, do not copy it back to its original location.
DE5183 ncb00076807 STR-3367	Description:	Transfers and sends between local and remote GV STRATUS sites have unexpected results if a transferred asset already exists at the destination. The destination asset is overwritten with no warning. This applies to transfer and to Send Destination.
	Workaround:	Delete or rename assets so that assets to be transferred or sent do not exist at the destination.
DE5250 ncb00076805 STR-3324	Description:	A playlist has no thumbnail and is empty. This occurs if the playlist was created, then deleted, on a connected K2 Dyno Replay Controller.
	Workaround:	In the GV STRATUS application, delete the playlist.
DE5301 ncb00076803 STR-3290	Description:	"Video Playback Is Not Available" displays in Inspector when attempting to play a subclip with no proxy association. This can occur when using a high-resolution workflow to create subclips, such as on high-resolution GV STRATUS client, editor, or a K2 Dyno Reply Controller, and the parent clip has no proxy association.
	Workaround:	Make sure the high-resolution parent clip has a proxy association by using a clip recorded on a K2 Summit channel that immediately creates proxy files, or by waiting until a GV STRATUS Render Engine generates proxy files for the high-resolution parent clip.
DE5394 ncb00076829 STR-3229	Description:	Local proxy video is missing and cannot be generated for an asset transferred from a remote site to the local site. This occurs if the asset is not of type "Clip", such as a subclip or a list.
	Workaround:	Export/import MXF or MOV formats rather than remote transfer. Or, once transferred, conform the asset. Both of these workarounds result an asset of type "Clip".

DE6605 ncb00077068 STR-2729	Description:	When the Conform Engine renders a complex MPEG2 asset, the resulting simple clip is in a higher video format (bitrate) than that specified in GV STRATUS Control Panel Format settings.
	Workaround:	This is as designed. The bitrate is increased to the minimum required to avoid encoding issues.
DE10959 STR-385	Description:	When recording in Scheduler with a set duration, the resultant clip is shorter than the duration set. This occurs after changing the NTSC/PAL reference standard in GV STRATUS Control Panel **General | Format | Formats**.
	Workaround:	After changing the reference standard, restart the Core/Express server to recalibrate the record duration setting.
DE11592 KT-48	Description:	MOV imports are failing randomly but very often on GV STRATUS ISILON system.
	Workaround:	Use MXF/GXF imports or transcode during import using rules.
STR-40993	Description:	Assets could not be loaded when a Summit MDI is deleted with the "Delete MDI Only" option selected, and then re-added with a different port number.
	Workaround:	Configure the new Summit MDI to use the same port number as the deleted Summit MDI.
STR-42062	Description:	If a Summit MDI is renamed, then all rules configured to that Summit MDI stopped working.
	Workaround:	Change every rule associated with the renamed Summit MDI to point to the new Summit MDI name.
STR-46958	Description:	The GV STRATUS application is unable to open after an upgrade if registry entries for RSA/SHA512 and ECDSA/SHA512 are missing.
	Workaround:	Install the following Windows updates on the core server: • KB2975719 OR • KB2919355 ***NOTE: Always install the required Microsoft Visual C++ redistributable update before installing the latest Windows Important Updates.***
STR-49479	Description:	GV Embedded Security Manager fails to uninstall version 1.0.0.16, which is part of the K2 Summit image.
	Workaround:	Check Software via SiteConfig on each K2 Summit after the failure. The uninstall task of version 1.0.0.16 comes back and works on a second try.
STR-49672	Description:	K2 Central displays as "Unable to connect" on Core | Proxy Config | Test Connections tab of the GV STRATUS Control Panel.
	Workaround:	Start the GV STRATUS K2 Configuration Service on the K2 Central manually.

STR-50980	Description:	Playback fails for XDCAM-EX and XDCAM-HD422 assets after the drag and drop operation from K2-Avid Explorer into an Avid bin.
	Workaround:	Import via AMA link to playback those XDCAM-EX and XDCAM-HD422 assets.
STR-53128	Description:	Deleting a logical group that contains assets is not supported, but the logical group will be moved into the Lost and Found bin.
	Workaround:	None
STR-67687	Description:	GV I/O channel fails to record after switching the video format.
	Workaround:	When changing a video feed on the GV I/O appliance, the signal feed on the SDI input of the AJA card must be set first. Then in GV STRATUS Control Panel, change the **Channel Format** in **General | Channels | GV I/O** settings to match the format of the new video feed.
STR-67999	Description:	GV I/O channel fails to cue and playout a clip that has both 16-bit and 24-bit audio tracks.
	Workaround:	Make sure that all audio tracks in the clip are of the same type.
STR-68244	Description:	When upgrading a GV STRATUS 6.5 system with SNFS 6.0 via SiteConfig, the previous version of SNFS does NOT get automatically uninstalled, but the newer version is installed.
	Workaround:	Using SiteConfig, do the following: 1. Remove and re-add all SNFS devices to the deployment group(s) and then Check Software again. 2. Re-deploy SNFS to capture the latest software version.

STR-68352	Description:	• If the default GVAdmin account does not exist in the GV STRATUS Core server after a clean install, users are not allowed to log into GV STRATUS Control Panel. • If the system delegate credentials are modified in the workgroup/domain prior to being reconfigured in GV STRATUS Control Panel, users are not allowed to log into GV STRATUS Control Panel.

	Workaround:	• When performing a clean install of GV STRATUS version 6.8, the default GVAdmin account credentials must exist and be valid for the GV STRATUS Core server.
		• If altering credentials:
		  • If changing the delegate credentials password without changing the username, reconfigure the password within GV STRATUS Control Panel *before* altering the password within the workgroup/domain. If the password has already been changed and GV STRATUS Control Panel is unusable, restore the password to its previous value, then reconfigure in GV STRATUS Control Panel.
		  • If changing both username and password, the order of operations is unimportant and GV STRATUS Control Panel will not be negatively impacted as long as the credentials are valid.

STR-68445	Description:	GV I/O channel's Record and Playout-specific options do not update in the Channel Panel tool after changing them in the GV STRATUS Control Panel.
	Workaround:	The GV STRATUS desktop application needs to be restarted after changing a GV I/O channel from Playout to Record or from Record to Playout in order to see updated configuration options in the Channel Panel tool.
STR-68640	Description:	When launching the GV STRATUS Control Panel application, the splash screen displays 'The connection type for (machine name) could not be resolved" message.
	Workaround:	None. It does not affect the GV STRATUS Control Panel application and will be fixed in the next release.
STR-69326	Description:	Protected assets will not transfer from a remote site to a local site.
	Workaround:	Disable the Protected status of the asset before transferring from remote site to the local site. ***NOTE: Protected assets can be transferred from local site to a remote site, but not the other way around.***
STR-69574	Description:	When setting mark in/out for a 720p XDCAM Long GOP asset using a GV I/O channel, the marks will be forced to the nearest even video frame.
	Workaround:	None.

STR-69697	Description:	Conforming an EDL from GV STRATUS Web Client's Simple Editor fails while working with growing assets.
	Workaround:	Make sure asset recordings have been completed or stopped before conforming an EDL.
STR-69723	Description:	Changing a GV I/O channel input to **SMPTE 2110** from either SDI, SMPTE 2022-6, or Web Stream, after previously saving a different SMPTE 2110 channel allows saving the channel configuration without uploading a new SDP file.
	Workaround:	Set the SDP file for the particular channel before saving your settings. If not, the channel will be configured with an incorrect SDP file from another **SMPTE 2110** channel.

GV STRATUS Rundown Known Problems

The following limitations are present in this release of software. If you wish to obtain more information about these limitations, please mention the reference numbers.

GV STRATUS Rundown

CR42885	Description:	If GV STRATUS Rundown doesn't play all the way through your playlist when using the Archive Play feature, there may be a problem with the black clip that is used as filler between clips.
	Workaround:	Make sure that you have a clip called “BLACK” (all uppercase) in the same bin on the Media Server where you send stories for playout (normally the “default” bin). One way to create this clip is to insert 10 seconds of filler into an otherwise empty EDIUS sequence and send it to the playout bin.
CR68152	Description:	A K2 version 3.2 playout system supports a maximum of only eight channeless AMP connections at one time (this is separate from the channeled connections that are used for playback).
	Workaround:	Make sure only eight channeless AMP connections are activated at a time.
CR68611	Description:	Problems with updating the Ready status of clips.
	Workaround:	More than one GV STRATUS Rundown system should not be configured to connect to the same channel on a K2 as this can cause problems with updating the Ready status of clips.
PR20458	Description:	When installing GV STRATUS Rundown on Windows 7 clients, a pending SiteConfig dialog can be missed.

	Workaround:	When a dialog is pending, a blinking icon displays on the Windows 7 task bar. Clicking on this indicator brings up the dialog that takes you to the isolated session. If you are logged in via remote desktop, the interactive services detection service sends a notification about the pending dialog. If the notification has been missed, go into Windows Services and stop and restart the Interactive Services Detection Service. This causes the service to send an immediate notification about the pending dialog.
ncb00077242	Description:	Placeholder status in ALP updates slowly or does not update at all.
	Workaround:	1. Do not put the shortcut into “all users” startup with the installer. 2. Do not put the database in the Programs directory. 3. Do not allow multiple instances of XMOS and SDB servers to launch.

Newsroom Computer System (NCS)

CR34585	Description:	When working with iNEWS rundowns, the Rundown Bar window in GV STRATUS Rundown will always display "NOT READY" in the Status column.
	Workaround:	This column is designed to work with the "MOS Ready to air" property that is available with ENPS rundowns. Since this feature is not applicable with iNEWS rundowns, you may wish to resize the Status column to its minimum size when connected to an iNEWS system.
CR35882	Description:	The connection between iNEWS rundowns is lost and then re-established (such as by rebooting the iNEWS server).
	Workaround:	Re-monitor your rundowns through iNEWS before they will be available in GV STRATUS Rundown's dropdown list.
CR35932	Description:	When connected to a Newsroom Computer System, channel assignment or status changes that were made through the GV STRATUS Rundown interface will be reset if the item's rundown position is changed on the NCS.
	Workaround:	This is by design. If you wish to keep manual channel assignments when reordering items, you can assign channels through the NCS, rather than through GV STRATUS Rundown.
CR44269	Description:	In ENPS client, the Actual column couldn’t be updated with the Editorial Duration set for the GV STRATUS Rundown placeholder.
	Workaround:	In the ENPS client, the script window for a story must be closed before the Actual column will be updated with the Editorial Duration set for the GV STRATUS Rundown placeholder.

CR44677	Description:	When media is sent to a placeholder that is embedded in an iNEWS story, the Clip Duration column in the iNEWS client will not update. This problem is no longer applicable to iNEWS version 4.0 and above, with GV STRATUS Rundown version 8.2 and above.
	Workaround:	The duration will update if the media is first sent to the placeholder and then added to the iNEWS story.
CR49674	Description:	Differences in MOS status reporting could lead to Octopus not operating correctly with GV STRATUS Rundown.
	Workaround:	Octopus users need to make these following changes to the Statuses tab within **Admin | MOS | Devices** of the Octopus application: 1. Change **CUED** status to **STAND BY**. 2. Change **PLAYED** status to **END**.
CR63446	Description:	Trimming a clip in a GV STRATUS Rundown channel will not affect the duration that displays on a Newsroom Computer System.
	Workaround:	None.
CR69097	Description:	Status translation table in mosconfig.xml on the iNEWS MOS Gateway system did not operate correctly with GV STRATUS Rundown.
	Workaround:	iNEWS users may need to make the following changes to the status translation table in mosconfig.xml on the iNEWS MOS Gateway system in order to make statuses operate correctly with GV STRATUS Rundown: 1. Change **<statusCued>CUED</statusCued>** to **<statusCued>STAND BY</statusCued>**. 2. Change **<statusStopped>PLAYED</statusStopped>** to **<statusStopped>END</statusStopped>**.

GV STRATUS VTR Ingest Known Problems

The following limitations are present in this release of software. If you wish to obtain more information about these limitations, please mention the reference numbers.

GV STRATUS VTR Ingest

DE6608 KT-479	Description:	In the K2 AppCenter, the recorded clip that showed the mark in and mark out do not match with the embedded LTC in the clip.
	Workaround:	None.

GV STRATUS Upgrade

Upgrading GV STRATUS systems

This section contains the tasks necessary for upgrading to this release of GV STRATUS software using the SiteConfig application. Work through the tasks sequentially to complete the upgrade.

NOTE: These upgrade instructions assume that current software is at version 6.0 or version 6.5. If you have a lower version of software, first follow the upgrade instructions for lower versions of software as appropriate to upgrade to version 6.0 or 6.5. Then upgrade to this release of GV STRATUS software.

⚠ ***CAUTION: If you upgrade a server and then decide you do not want to stay with this version of software, you must use the recovery disk image process to downgrade to your previous version.***

With the installation instructions in this section, you use SiteConfig from a network connected control point PC and remotely install/upgrade software simultaneously on your system devices. This is the recommended process for software installation and upgrades. When installing the GV STRATUS application or the GV STRATUS Control Panel application, if SiteConfig installation is not possible, you may install manually on the local PC. You must uninstall before installing.

The upgrade instructions in this document apply to the following devices:

- GV STRATUS client PC connected on the corporate LAN for low-resolution (proxy) workflow
- GV STRATUS client PC connected on the media (iSCSI) network for high-resolution workflow
- GV STRATUS servers as follows:
    - Express server
    - Core server
    - Database server
    - Proxy server (A1)
    - Proxy Storage file system server (B1, C1)
    - Workflow Server
    - Render Engine Server

The following installation tasks provide information specifically for the upgrade to this version of software. Read the information in these sections carefully before attempting any upgrade to software.

Upgrading to GV STRATUS version 6.8 and K2 Summit version 10.1.1

Follow the topics in the section sequentially to perform the upgrade.

Upgrading K2 systems' hardware

GV STRATUS version 6.8 supports K2 Summit version 10.1.1 and SNFS 6.0 for K2 Summit Standalone(s) and redundant K2 SAN systems.

In order to preserve assets and metadata when upgrading from K2 Summit 9.x/SNFS 4.7 to K2 Summit 10.1.1/SNFS 6.0 for redundant K2 SANs and K2 Summit Standalone(s), the Server Migration and OS upgrade tools must be used.

K2 Summit 10.1.1 systems require the following:

- 64 GB flash or mSATA cards installed on all K2 Summits
- AIC 2208 RAID controller installed on K2 Summit Standalone(s)
- SNFS version 6.0.6.b75382-14 installed
- The latest Windows 10 OS image installed on all K2 Summits
- The latest Windows 2016 OS image installed on all Dell servers (for FSMs, FTP servers, GVREs, WFEs, Core servers, etc.)

***NOTE: K2 Centrals are currently not supported and must remain at K2 Summit version 9.8 to work with* GV STRATUS.**

K2 software downgrade is supported only via the recovery image process. If you must downgrade and you do not have a recovery image at the desired software version, obtain a recovery image from Grass Valley Support.

Prepare for K2 Summit hardware upgrade

Before upgrading, do the following:

- Procure the Acronis 8179 W10 image on the USB Recovery Flash Drive(s) of 32 GB or greater via the appropriate distribution method.
- Procure the 64 GB flash or mSATA cards required to upgrade your K2 Summit hardware.
- On K2 Summit Standalone(s), verify that you have the AIC 2208 RAID controller installed. Procure the AIC 2208 RAID controller if you do not have it in your system.

  NOTE: The LSI controller does not support K2 Summit software version 10 and above.
- Stop all media access on the devices you are upgrading.
- Shut down all applications on the devices you are upgrading.

Creating a recovery image

Before creating a recovery image, determine the storage location for the image. Grass Valley recommends that you store the recovery image on the Recovery Flash Drive that you received, and this task provides instructions for that location. If you use a different location, such as a network connected drive or another connected USB drive, alter the steps in this task as appropriate.

1. Make sure that media access is stopped and that the system on which you are working is not being used.
2. If you have not already done so, connect keyboard, monitor, and mouse.
3. Do the following:
   a) Insert the Recovery Flash Drive into a USB port.
   b) Restart the machine, or power on if currently shut down.

      The machine boots from the Recovery Flash Drive, into a version of Windows stored on the drive.

      A MS-DOS command window opens.
   c) Press the **F11** key to enter Boot options.
   d) When prompted with a list of options, select the Acronis option and then press **Enter**.

   The Acronis program loads.

4. In the Acronis main window, click **Backup**.

   The Create Backup Wizard opens.

5. On the Welcome page, click **Next**.
6. On the Partitions Selection page, do the following:
   a) Select the **(C:)** partition and then click **Next**.

      NOTE: Verify capacity to make sure you select the boot media card (CompactFlash or mSATA) and not a media drive. The boot media has a much smaller capacity.

      If a "…choose full backup mode…" message appears, click **OK**.

7. On the Backup Archive Location page, do the following:
   a) in the tree view select **Removable Disk (D:)** and enter the name of the image file you are creating.

      Create the file name using the machine hostname and the date. Name the file with the .tib extension.

      For example, if the hostname is MySystem1, in the File name field you enter `A:\MySystem1_20180827.tib`.

   b) Click **Next**.
8. On the Select Backup Mode page, select **Create a new full backup archive** and then click **Next**.
9. On the Backup Options page, do not change any settings. Click **Next**.
10. On the Archive Comment page, if desired, enter image comments such as the date, time, and software versions contained in the image you are creating. Click **Next**.
11. On the "…ready to proceed…" page, do the following:
    a) Verify that you are creating an image from the C: drive and writing to the D:\ drive, then click **Proceed**.

       If a "...insert next volume..." message appears, click **OK**.

12. On the Operation Progress page, observe the progress report.
13. When a message appears indicating a successful backup, click **OK**.
14. Click **Operations | Exit** to exit the Acronis True Image program.

    The machine restarts automatically.

15. Remove the recovery media while the machine is shutting down.

Replace the CompactFlash or mSATA Card

Before upgrading to K2 Summit system version 10.1 and above, verify that your flash or mSATA card is 64 GB or greater.

Make sure you already created the recovery image for K2 Summit and save the backup on your USB Recovery Flash Drive.

Do not do this task if you have:

- A K2 Summit system with CompactFlash or mSATA system drive of 64 GB or greater.

Do this task if you have:

- A K2 Summit system with CompactFlash or mSATA system drive of 32 GB.

1. Replace the 32-GB flash or mSATA card with a 64-GB card or greater.
2. Restore the K2 Summit image using Acronis according to the procedure in *Restoring from a generic image* on page 77.

   NOTE: A reboot will be required after the first boot in order to see the new card, but no other configurations should be required.
3. Before upgrading the software, verify that your K2 Summit system is working normally with the old OS/software and new hardware.

Restoring from a generic image

This task provides instructions for accessing an image on the USB Recovery Flash Drive. If you access an image from a different location, such as a network connected drive or another connected USB drive, alter the steps in this task as appropriate.

NOTE: This procedure restores the* K2 Summit system *to its factory default condition. Passwords and other site-specific configurations are reset to factory defaults.

1. Make sure that media access is stopped and that the system on which you are working is not being used.
2. If you have not already done so, connect keyboard, monitor, and mouse.
3. Do the following:
   a) Insert the Recovery Flash Drive into a USB port.
   b) Restart the machine, or power on if currently shut down.

      The machine boots from the Recovery Flash Drive, into a version of Windows stored on the drive.

      A MS-DOS command window opens.
   c) Press the **F11** key to enter Boot options.
   d) When prompted with a list of options, select the Acronis option and then press **Enter**.
4. In the Acronis main window, click **Recovery**.

   The Restore Data Wizard opens.
5. On the Welcome page, click **Next**.
6. On the Backup Archive Selection page, in the tree view expand the node for **Removable Disk (D:)** and select the image file, then click **Next**.
7. On the Restoration Type Selection page, select **Restore disks or partitions** and then click **Next**.
8. On the Partition or Disk to Restore page, select **MBR and Track 0** and then click **Next**.
9. On the Disk Selection page, select **Disk 1** and then click **Next**.

   NOTE: Verify capacity to make sure you select the boot media card (CompactFlash or mSATA) and not a media drive. The boot media has a much smaller capacity and has an interface identified as "IDE (0) Primary Master".
10. On the Next Selection page, select **Yes, I want to restore another partition or hard disk drive** and then click **Next**.

11. On the Partition or Disk to Restore page, select **(C:)** and then click **Next**.
12. On the Restored Partitions Resizing page, select **Yes, I want to resize partitions** and then click **Next**.
13. On the Restored Location page, select **(C:)** and then click **Next**.

    Verify capacity to make sure you select the boot media card (CompactFlash or mSATA) and not a media drive. The boot media has a much smaller capacity and has an interface identified as "IDE (0) Primary Master".
14. On the Restored Partition Type page, select **Active** and then click **Next**.
15. Do one of the following:

    - If the Restored Partition Size page does not appear. Skip ahead to the Next Selection page.
    - If the Restored Partition Size page appears. Continue with the next step.

16. On the Restored Partition Size page, do one of the following:

    - If **Free space after** reports 0 bytes, leave settings as they are. Click **Next**.
    - If **Free space after** does not report 0 bytes, increase **Partition size** until **Free space after** reports 0 bytes. Click **Next**.

17. On the Next Selection page, select **No, I do not** and then click **Next**.
18. On the Restoration Options page, do not make any selections. Click **Next**.
19. On the "…ready to proceed…" page, verify that you are restoring the correct image to the correct location. Click **Proceed**.
20. On the Operation Progress page, observe the progress report.
21. When a message appears indicating a successful recovery, click **OK**.
22. Click **Operations | Exit** to exit the Acronis True Image program.

    The machine restarts automatically.
23. Remove the USB Recovery Flash Drive while the machine is shutting down.
24. Upon startup, wait for initialization processes to complete. This can take several minutes, during which time USB keyboard/mouse input is not operational. The system might automatically restart. Do not attempt to shutdown or otherwise interfere with initialization processes.
25. When prompted, enter the K2 Summit system machine name.

    Make sure the name is identical to the name it previously had.

    After start up, one or more device discovery windows can open. Allow processes to complete without interference.
26. Verify that the K2 Summit system is functioning normally.
27. Next, launch the Embedded Security Manager and put every server in Update mode.

Upgrade Microsoft Visual C++ Redistributable for VS 2017

This task applies to the following:

- All types/roles of GV STRATUS servers.

- Client PCs hosting one or more of the following:
  - GV STRATUS
  - GV STRATUS Control Panel
  - EDIUS XS
  - EDIUS Workgroup

This task does not apply to the following:

- K2 Summit systems, as they should have only Microsoft Visual C++ Redistributable for VS 2015 installed

1. From the Windows Start menu navigate to **Control Panel | Programs and Features** and check for the following:

   Microsoft Visual C++ Redistributable for VS 2017

   - If Microsoft Visual C++ Redistributable for VS 2017 is already installed, do not do the remainder of this task.
   - If Microsoft Visual C++ Redistributable for VS 2017 is not installed, continue with this procedure.

2. Procure the **Microsoft Visual C++ Redistributable for VS 2017** installation file from the *Microsoft software download page* or the Grass Valley FTP site.
3. Select the installation file(s) as follows:
   - For servers and Windows 64-bit OS client PCs, select the following:
     - vc_redist.x64.exe
     - vc_redist.x86.exe
   - For Windows 32-bit OS client PCs, select the following:
     - vc_redist.x86.exe
4. Run the installation file and install as directed by the installation wizard.

Upgrade Microsoft .NET

Do not do this task if:

- The system has Microsoft .NET Framework 4.7.1 installed

Do this task if:

- The system does not have Microsoft .NET Framework 4.7.1 installed

This task applies to the following:

- K2 Summit systems

- All types/roles of GV STRATUS servers

1. On the computer, check Windows Control Panel **Programs and Features** for currently installed .NET version(s), then proceed as follows:
   - If Microsoft .NET 4.7.1 is installed, skip this task.
   - If Microsoft .NET 4.7.1 is not installed, continue with this procedure.
2. Procure the Microsoft .NET 4.7.1 installation file from the *Microsoft software download page* or the Grass Valley FTP site.
3. Run the installation file and install Microsoft .NET 4.7.1 as directed by the installation wizard.

Prepare for upgrade via SiteConfig

Before upgrading, do the following:

- Procure the software installation files for this release via the appropriate distribution method, such as download, network drive, or external drive.
- Export all configured rules to avoid recreating them from scratch after the upgrade.
- Disable all rules on the GV STRATUS Control Panel.
- Stop all media access on the devices you are upgrading.
- Shut down all applications on the devices you are upgrading. This includes the SDB Server if you have GV STRATUS Rundown in your operation.
- Terminate all users' sessions using the GV STRATUS Control Panel.
- Put every server in **Update mode** — this is required to upgrade the Embedded Security Manager.

Prepare SiteConfig for software deployment

If a newer version of SiteConfig is available, you must upgrade to the latest version. For more info, refer to *Grass Valley products compatible with GV STRATUS* on page 56.

Do the following to prepare SiteConfig for the software upgrade.

1. If a newer version of SiteConfig is available for upgrade and you have not yet upgraded SiteConfig, do the following:
   a) From Windows **Programs and Features**, uninstall the current version of SiteConfig from the control point PC.
   b) Install the new version of SiteConfig on the control point PC.
2. After the installation is complete, click **Finish** and launch the SiteConfig application.
3. Next, configure the deployment group.

Configuring deployment groups

- The device must be assigned in the SiteConfig system description and network connectivity must be present.

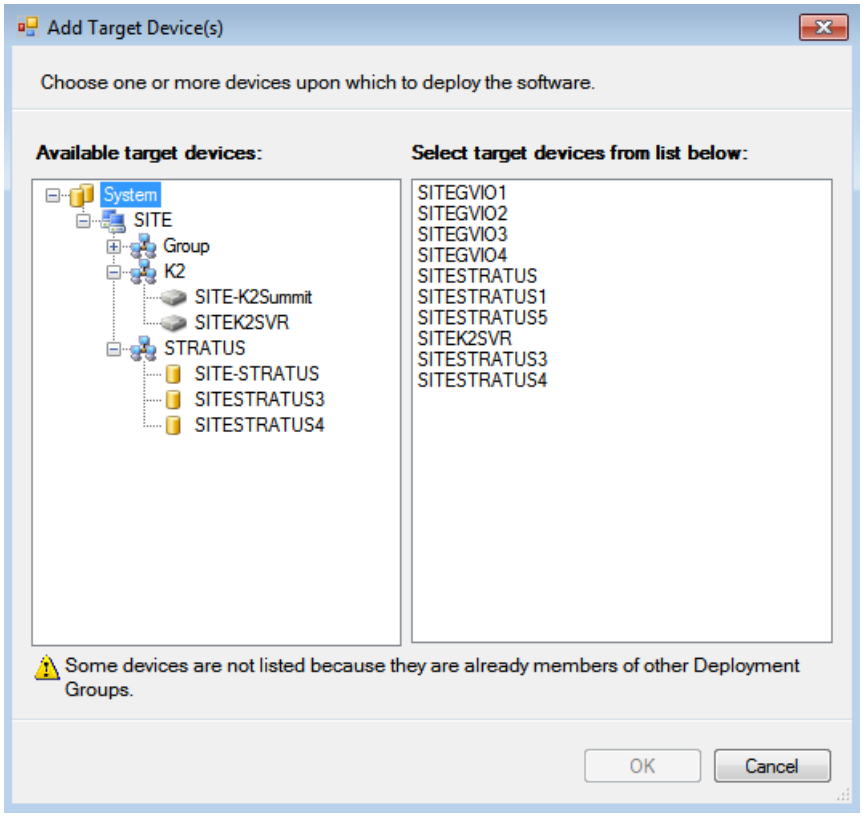
- GV STRATUS systems containing mixed K2 Summit versions of 9.8 and 10.1 will require at least two separate deployment groups, one for K2 Summit 9.8.x system and one for K2 Summit 10.x system.

1. In the **Software Deployment | Deployment Groups** tree view, right-click the top node and select **Add Deployment Group**.

   A deployment group appears in the tree view.

2. Right-click the deployment group, select **Rename**, and enter a name for the deployment group.
3. Right-click the deployment group and select **Add Target Device**.

   The Add Target Device(s) wizard opens.



4. In the Available Target Devices tree view, select the node that displays the devices that you are combining as a deployment group.
5. In the right-hand pane, select the devices that you are combining as a deployment group.

   To select multiple devices, you can drag through the devices, use Ctrl + Click, or use Shift + Click.

6. Click **OK**.

The devices appear in the Deployment Groups tree view under the deployment group. Before you perform a software deployment, you must check software on the devices that will be receiving new software. If you have already added packages to the group, on the Deployment Groups tab you will also see deployment tasks generated for every device with roles that match the package contents.

Upgrading the Discovery Agent

If a newer version of SiteConfig Discovery Agent is available, you must upgrade to the latest version. For more info, refer to *Grass Valley products compatible with GV STRATUS* on page 56.

1. On the device you plan to manage with SiteConfig, open the Windows Services Control Panel and look for the following required item:
   - SiteConfig Discovery Agent
2. Check the version number of the SiteConfig Discovery Agent.
   - If the latest version is installed, skip this task.
   - If the latest version is not installed, continue with this procedure.
3. In order to upgrade Discovery Agent on all your devices, add only the DiscoveryAgent cab to your deployment group(s).
4. Click the **Start Deployment** button.

   Deployment tasks run and software is uninstalled. Progress is reported and next steps are indicated in both the Status and Details columns.
5. When the Uninstall task completes, set Restart to Complete when the **Restart required** option displays on SiteConfig.

   NOTE: This is to prevent Siteconfig from losing its connection with any of your devices during the Uninstall/Install process. If the connection is lost, you will need to install Discovery Agent manually and perform a check software on the device(s) in order to sync them up with Siteconfig.
6. Once the DiscoveryAgent cab is installed, click the "Restart required" option to restart the server.

Add software roles for upgrade to version 6.8

Before doing this task, make sure devices are added to the SiteConfig system description with the correct family and device type. Refer to *Complete listing of device types, roles, and software packages for GV STRATUS devices* on page 194.

For your K2 Summit systems, make sure you have separate deployment groups for the upgrade to version 9.8.x and version 10.1.x if you have both versions in your operation.

NOTE: If upgrading to K2 Summit version 10.1.x, you cannot use Siteconfig to directly upgrade from SNFS 4.7 to SNFS 6.0 on FSMs and K2 Standalone Summits. Refer to Upgrading to SNFS 6.0 on page 87 before proceeding, if applicable.

These SiteConfig roles are new or require special consideration with this software upgrade. Verify and add roles if necessary.

1. As appropriate for your system design and licensing, in your SiteConfig system description, configure as follows:
   - For your GV STRATUS Express Server, or Core Server, add the new device as follows:
     - GV STRATUS Proxy Streaming Server (optional)

       These new roles will be automatically added:

       - GV STRATUS Proxy Streaming Service
       - GV Embedded Security Manager
       - GV Log Manager
   - For your GV STRATUS Express Server, Core Server, Workflow Server or a separate server, add the new role as follows:
     - GV STRATUS ExternalMedia Engine (optional)
   - For your GV I/O Client - Standalone device, add the new device as follows:
     - GV I/O Standalone Device

       These new roles will be automatically added as follows:

       - GV STRATUS IO Appliance
       - GV Embedded Security Manager
       - GV STRATUS Summit Service
   - For your GV I/O Client - Shared Storage device, add the new device to Isilon system deployment group as follows:
     - GV I/O Client (SMB)

       These new roles will be automatically added as follows:

       - GV STRATUS IO Appliance
       - GV Embedded Security Manager

   NOTE: GVEngine and MPIcore must be manually installed on any GV I/O device(s). The installation files can be procured from the Grass Valley FTP site.

2. Save SiteConfig and verify in `C:\ProgramData\Grass Valley\ConfigurationDataFiles\SiteConfig` that .scsd and .config files are saved to the Core server.

If you want to verify all your currently configured SiteConfig roles, refer to the complete list of roles and software packages.

Add software package to deployment group for GV STRATUS and other devices

- The GV STRATUS devices to which you are deploying software must have their SiteConfig roles correctly configured.
- The GV STRATUS devices to which you are deploying software must be in a deployment group.
- The following software upgrade system cab files apply to all deployment groups.
  - *GrassValley_STRATUSClient_X.X.X.XXX.cab*
  - *GrassValley_CoreServer_X.X.X.XXX.cab*
- The following software upgrade system cab file apply to K2 Summit 10.x devices. For each deployment group, choose the one that applies.
  - *GrassValley_K2Plus_X.X.X.XXX.cab*
- The following software upgrade system cab file apply to K2 Summit 9.8.x devices. For each deployment group, choose the one that applies.
  - *GrassValley_K2system_X.X.X.XXX.cab*
- The following software upgrade system cab files apply to GV I/O devices, if already added as a standalone device or a shared storage client with Dell EMC Isilon network-attached storage system.
  - *GrassValley_GVIO_X.X.X.XXX.cab*

    NOTE: Next, you must manually run the GVEngineInstaller-x.x.x.xxx_xxxxx_xxx.exe and MPIcore on each GV I/O device in your operation. The installation files can be procured from the Grass Valley FTP site.

1. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.
2. Click the **Add** button.

   The Add Package(s) dialog box opens.
3. Do one of the following to select the software package:
   - Select from the list of packages then click **OK**.
   - Click **Browse**, browse to and select the package, then click **Open**.
4. If one or more EULAs are displayed, accept them to proceed. If you do not accept a EULA, the associated software is not assigned to the deployment group.

   SiteConfig adds the package to the deployment group.

The package appears in the Managed Packages list for the selected deployment group. SiteConfig creates new software deployment tasks for the package and displays them in the Tasks list view.

Setting deployment options

- A software package must be assigned to the deployment group and applicable deployment tasks must be displayed in the Tasks area.

1. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.

2. In the Tasks list view, view tasks and determine if you must set deployment options.

   Tasks that need to have deployment options set display in the Details column a message stating "Deployment options required."

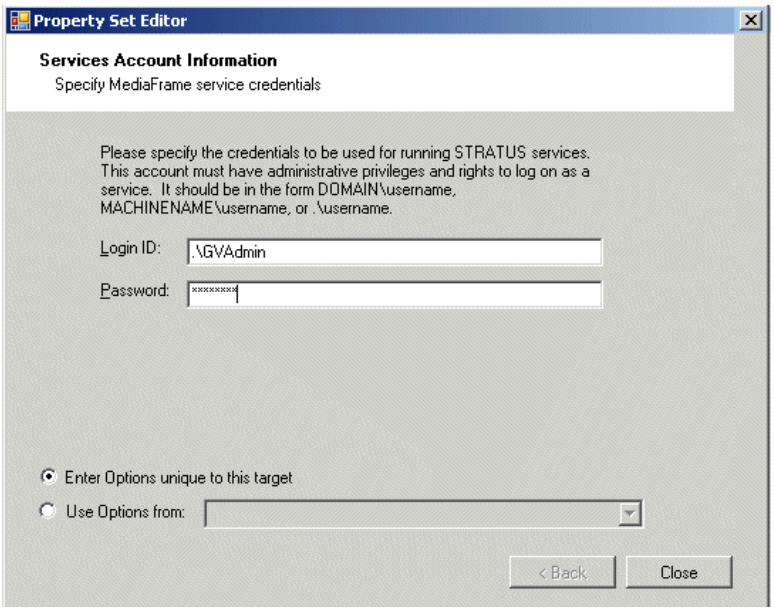
   If you select a task that needs to have its deployment options set, the Start Deployment button is disabled and the message is displayed next to the button.

3. Do one of the following to set deployment options:

   - Double-click the task.
   - Select the task and click the **Options** button.

   A wizard opens.

4. Work through wizards and set deployment options for GV STRATUS software as follows:

Software	Deployment options
GrassValley_STRATUS_CommonServices GrassValley_STRATUS_ControlPanelService GrassValley_STRATUS_CoreServices GrassValley_STRATUS_CRArchive_MDI GrassValley_STRATUS_Databases GrassValley_STRATUS_DataMover GrassValley_STRATUS_DIVA_MDI GrassValley_STRATUS_ExternalMedia GrassValley_STRATUS_FlashNet_MDI GrassValley_STRATUS_GFTP_MDI GrassValley_STRATUS_HttpProxyServer GrassValley_STRATUS_IngestServices GrassValley_STRATUS_Masstech_MDI GrassValley_STRATUS_MediaFlow GrassValley_STRATUS_MEWS GrassValley_STRATUS_Proxy_MDI GrassValley_STRATUS_ProxyStreamingService GrassValley_STRATUS_RenderEngine GrassValley_STRATUS_Rules GrassValley_STRATUS_ScheduledTransferEngine GrassValley_STRATUS_SocialMedia GrassValley_STRATUS_Summit_MDI GrassValley_STRATUS_TrafficGateway GrassValley_STRATUS_Transcode GrassValley_STRATUS_WebApps GrassValley_STRATUS_WebClient GrassValley_DeviceKeyService GrassValley_LogManager GrassValley_LogViewer	 Use the local system account if your system is on a workgroup or if it's on a domain but uses the local system account in SQL. Use a domain\admin account if the account was previously mapped in SQL to the MediaFrame, MediaFlow, RulesEngine and WFPersistence databases. Entering account credentials allows you to use the **Use options from** feature for all other devices of the same type. Once you enter the account credentials this way on the first device, it becomes the template from which options for other devices are copied.

5. If you have multiple devices of the same type, you can enter deployment options for one of them using the wizard. Then, when you bring up the same wizard on every device, you can choose the **Use options from** radio button and select the first device for which you set options.

   SiteConfig copies the options you set for the first device and fills in the blanks on the wizard.

Upgrading to SNFS 6.0

Before deploying systemcabs to upgrade to K2 Summit 10.1 systems and above, you must upgrade the SNFS from version 4.7 to version 6.0 on your K2 SAN's K2 Media Server (FSMs) and K2 Summit Standalone(s) using the following script: **SNFS_6.0.6upgrade-vXXXXXXXX.zip**

NOTE: K2 Summit 10.1 systems and above require all servers to be upgraded to Windows 2016 OS and all K2 Summit clients to be upgraded to Windows 10 OS.

Verify the following before doing this task:

- K2 SAN is not in service and all servers are in Update Mode
- Only one gvfs_*.cfg file exists in the D:\SNFS\config folder on the FSMs
- Only one gvfs_*.cfg file exists in the C:\SNFS\config on K2 Summit Standalone(s)

1. Copy the **SNFS_6.0.6upgrade-vXXXXXXXX.zip** file to your FSMs, B1 proxy servers and K2 Standalone desktops.
2. Extract the zip file.
3. Run the appropriate batch file for each device:
   - **gvSnfsSetupK2.bat** (For FSMs)
   - **gvSnfsSetupSummit.bat** (For K2 Summit Standalone)
4. Delete the zip and extracted files.
5. Run a Check Software on all your devices in Siteconfig and verify that those FSMs and K2 Summit Standalone(s) show SNFS 6.0 is installed.

   NOTE: If upgrading from a GV STRATUS 6.5 system already installed with SNFS 6.0, the previous version of SNFS does NOT get automatically uninstalled but the newer version is still installed. You must remove and re-add the devices to the deployment group(s) and then Check Software again. Then, re-deploy SNFS to capture the latest version.

Upgrade software with SiteConfig

- The devices that you are upgrading must be in a deployment group.
- For the software you are upgrading, a newer version of that managed software package must be added to the deployment group.
- A SiteConfig "Check Software" operation must be performed on the devices you are upgrading.
- All servers have been set to **Update mode** in the Embedded Security Manager.

NOTE: K2 Summit 10.1 systems and above require all servers to be upgraded to Windows 2016 OS and all K2 Summit clients to be upgraded to Windows 10 OS.

If you are upgrading multiple software components for which there is a required sequence, you must check and uncheck tasks and run multiple deployment sessions to control the sequence. For some software components, SiteConfig aids you by enforcing dependencies. For each individual software component, SiteConfig enforces an uninstall of the current version of software before installing the

upgrade version. SiteConfig provides uninstall deployment tasks and install deployment tasks to indicate the taskflow. SiteConfig can do the uninstall/install in a single deployment session.

1. In the **Software Deployment | Deployment Groups** tree view, select the device or the group of devices to which you are deploying software.

   The corresponding software deployment tasks are displayed in the Tasks list view.

2. For the software you are deploying, do the following:

   a) Select the **Deploy** check box in the row for the uninstall task.

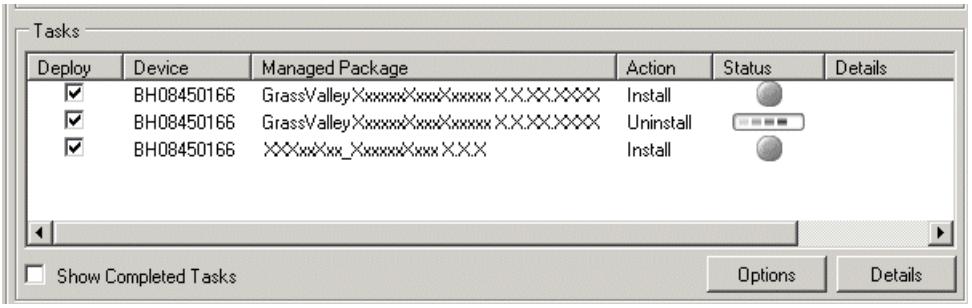
   b) Select the **Deploy** check box in the row for the install task.

   If a WFRegMon install task appears, install it as well. It is required to support Grass Valley software installers. There is no uninstall task.

3. Check the area next to the Start Deployment button for a message.

   If a message instructs you to upgrade the Discovery Agent, on the control point PC go to the directory to which SiteConfig is installed, find the `DiscoveryAgent_x.x.x.x.cab` file, add it to the deployment group, and deploy the Discovery Agent software as well.

4. Click the **Start Deployment** button.



   Deployment tasks run and software is uninstalled. Progress is reported and next steps are indicated in both the Status and Details columns. If an error appears regarding prerequisite software, install the Grass Valley Prerequisite Files on the control point PC and then repeat this step.

   SiteConfig uninstalls/install software in the proper sequence.

5. When the Status or Details columns indicate next steps, identify the software in the row, then do one of the following:

   - If Details displays a **Restart required** link (but not "Visible dialog pending..."), click the link and when prompted "...are you sure...", click **Yes**.
   - If Details does not display any indication of additional steps required, proceed with the next step in this task.

6. Monitor progress as indicated by both the Status and Details column. When finished, the Status column indicates complete.
7. Shutdown the entire GV STRATUS/K2 Summit system and power up the servers in the correct order, starting the required services as needed.
8. Set all servers back to **Enabled mode** in the Embedded Security Manager.
9. If you deployed the MEWS Service, after deployment is complete, start the MEWS Service.

Upgrade GV STRATUS Database

This task applies to the following:

- The GV STRATUS server with the role of GV STRATUS Database.

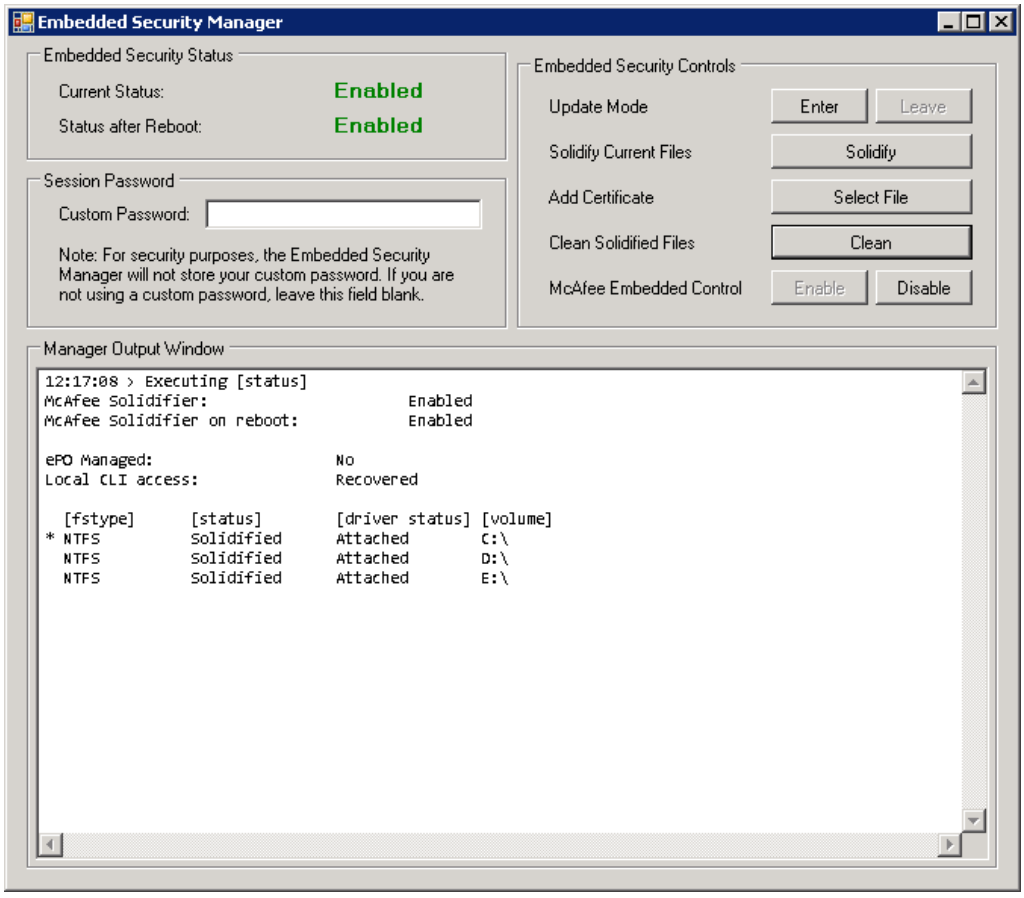
Before doing this task, do the following:

- Upgrade software on the GV STRATUS server.

This task upgrades the GV STRATUS database.

1. Log on to the GV STRATUS server as Administrator.
2. From the Windows desktop, click **Start | All Programs | Grass Valley | Embedded Security Manager**.

   Embedded Security Manager opens.



3. If Current Status is **Enabled**, click **Enter** in the Embedded Security Controls section to put it in **Update Mode**.

4. Locate the following file:

   `C:\Program Files\Grass Valley\STRATUS Databases\MediaFrameDbUpgrade.exe`

   This file is copied to the GV STRATUS server along with the software upgrade.
5. Double-click `MediaFrameDbUpgrade.exe` to upgrade the database.
6. Reboot the GV STRATUS server.

A "The database upgrade completed successfully" message displays.

Related Topics

Standalone Database Server set up process on page 829

Upgrade GV STRATUS system with the Key Upgrade Utility

This task applies to the following:

- The GV STRATUS Core server

Before upgrading, do the following:

- Disable any currently active rules on the GV STRATUS Control Panel.
- Make sure there are no currently processing or running workflows on the GV STRATUS system.

Before running the utility, do the following:

- Upgrade GV STRATUS software on the GV STRATUS Core server.
- Upgrade the GV STRATUS database.
- Restart the GV STRATUS Core server.

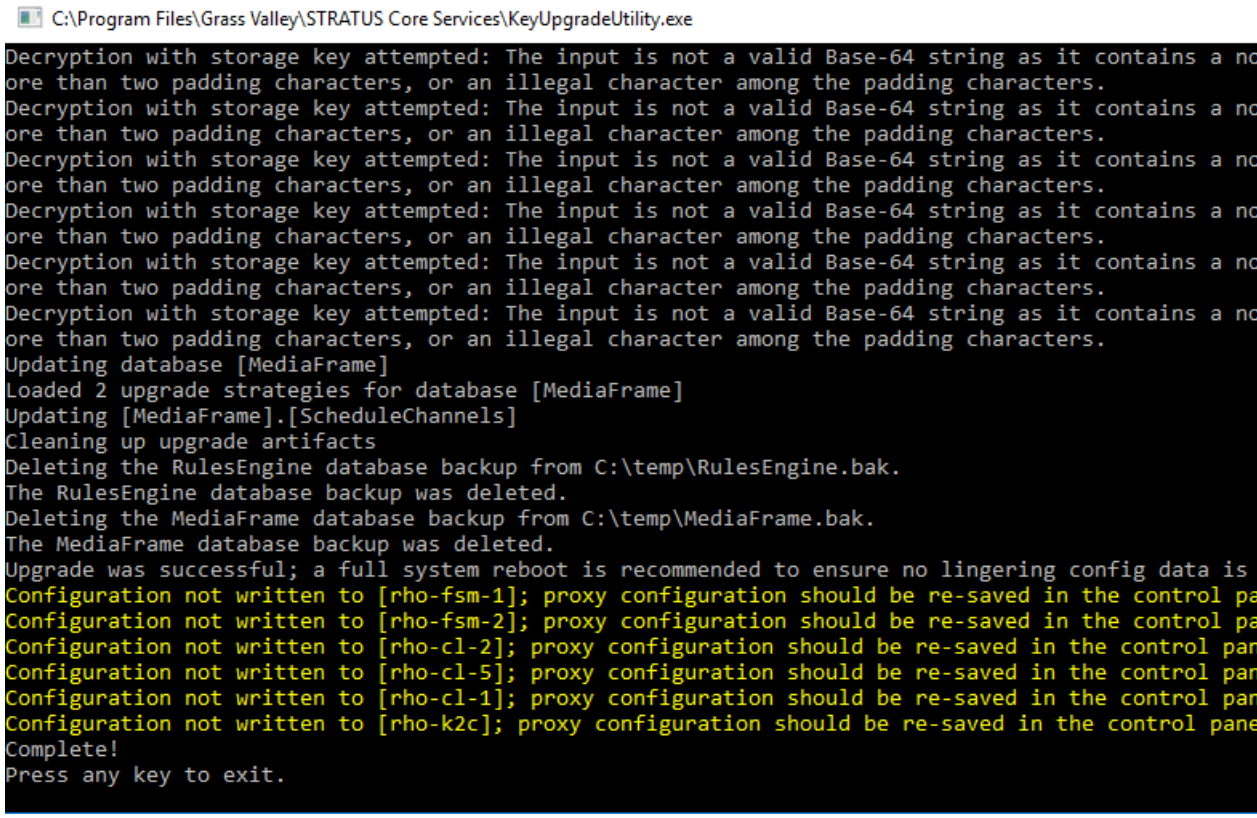
1. Log on to the GV STRATUS Core server as an Administrator.
2. Locate the following file:

   `C:\Program Files\Grass Valley\STRATUS Core Services\KeyUpgradeUtility.exe`

   This file is copied to the GV STRATUS Core server along with the software upgrade.

3. Run the *KeyUpgradeUtility.exe* to upgrade the encryption keys on your GV STRATUS Core server.

   Note any yellow messages in the output and take the requested action; these will occur at the end of the utility execution.



   The process is successful when the **Complete!** message displays at the end of the output.

4. In the **Proxy Config | Proxy Settings** tab in GV STRATUS Control Panel, re-check the **Enable Proxy Creation** setting and click **Save**.

   Verify all pop-ups succeed before continuing.

5. Reboot the GV STRATUS Core server.
6. Re-enable any rules that were disabled earlier.
7. Procure and run the *EngineConfig_6_8.cmd* file where any of the following engines are installed and running:

   - DataMover Engine
   - Transcode Engine
   - Workflow Engine
   - Rules Engine
   - Social Media Engine
   - External Media Engine

Upgrade K2 Summit OS from Windows 7 to Windows 10 on K2 Summit 10.1 systems

1. Back up the configurations of all K2 Summits on Windows 7 operating system by doing the following:
   a) Copy the **OSupgrade-vXXXXXXXX.zip** file to the `C:\temp` directory on each Windows 7 Summit.
   b) Extract the zip file.
   c) Move the **OSupgrade** folder to the `C:\temp` directory.
   d) Run the **ConfigBackup.bat** file.
   e) Zip up the OSupgrade and GVBACKUP folders together and copy the zip file to an external device.
2. Update and verify that the BIOS is updated to the latest version to ensure that you have the Meltdown & Spectre patches.
3. Using the **20180716-SUM-W10.tib** image (or later), reimage the Windows 7 Summits to Windows 10.
4. On each reimaged K2 Summit:
   a) Reconfigure the network.
   b) Re-share the V: drives for K2 Summit MDI and GV Render Engine purposes.
   c) Manually install Discovery Agent 2.2.0.215 or later.
5. Launch the SiteConfig application and do the following:
   a) From the Devices tab, remove all the Summit devices that were reimaged.
   b) Re-add all the K2 Summit devices in the Devices tab, and add them back to the desired deployment group(s)—(only to those deployment groups containing the K2 Plus systemcab).
   c) For K2 Summit Standalone(s), re-add the GV STRATUS Summit Services role.
   d) Perform a Check Software on all the newly added devices.
   e) Re-deploy GV STRATUS 6.8 systemcabs.
6. License your reimaged K2 Summits.
7. Restore the configurations on your K2 Summit SAN clients and Standalone(s) by doing the following:
   a) Copy the zip files of K2 Summit configurations to the local `C:\temp` folders on all reimaged K2 Summits.
   b) Extract the zip file and copy the OSupgrade and GVBACKUP folder to the `C:\temp` directory on each K2 Summit.
   c) Run the **ConfigRestore.bat** file. This should restore all your K2Config/SAN settings and channel settings.

Upgrade GV STRATUS server OS from Windows 2008/2012 to Windows 2016

The purpose of this upgrade is to provide GV STRATUS servers the use of the latest images/OS/SQL on new servers.

You must follow and apply upgrade steps in this section sequentially to upgrade your GV STRATUS system. These upgrade instructions apply to Core servers, Workflow servers, FSMs, FTP servers and GV Render Engine servers.

NOTE: The GV STRATUS system must be already upgraded to version 6.8 before replacing the core server, and that the user has basic knowledge of Microsoft SQL and Windows.

Prepare for upgrade to Windows 2016

Before upgrading, do the following:

- Procure the latest ServerMigration-xxxxxxxx.zip file for this release via the appropriate distribution method, such as download, network drive, or external drive. This contains the scripts you will need to backup the SQL databases and the required Grass Valley directories and registry keys.
- If you are replacing an Express Core server, you will need to backup the **F | proxy** folder manually.
- Record down all the **shared folders**, such as the Workflow engine/Xcode Control Working directory, the proxy share (express cores only), the Thumbnails folder in the GV STRATUS Rundown directory, etc. These will need to be recreated/re-shared on the new server.
- Record down the **licensed GV STRATUS users/groups**. You will need to recreate the users/groups local to the server.
- You must obtain new **Sabretooth and SQL licenses** for the new Core server.
- Verify that the BIOS is updated to the latest version to ensure that you have the Meltdown & Spectre patches.

Create backup for the upgrade to Windows 2016

1. Launch the Embedded Security Manager and put the server in Update mode.
2. **For Express Core server only**: Copy the entire Proxy folder from the F: drive to an external thumb/hard drive.

   NOTE: Make sure the system is not in use or creating new assets during this time.

3. Copy the Server Migration zip file to the D: drive of the server.
4. Extract the file on the D: drive, keeping the default name.
5. Move the ServerMigration folder within the extracted folder to the root of the D: drive.
6. Open the folder and run the **ConfigBackup.bat** file. This saves the required Grass Valley directories, the registry keys and the SQL databases to the **GVBACKUP** folder.
7. Zip the entire ServerMigration folder, giving it a unique name, such as **YYYY-MM-DD_serverName_ServerMigration.zip**.
8. Copy the zip file to an external thumbdrive or hard drive.

For Core server only: Make a list of the **users/groups** that you will need to recreate on the new Core server.

For Core/Workflow/GV Render Engine servers: Review the GV Control Panel configuration in order to determine the **shared folders** you will need to setup on the new server(s). You must verify the GV STRATUS Control Panel configurations after the new server(s) are setup.

Once you have all the required information/files backed up from the old server, do the following:

- Remove the old server from the domain.
- Remove the Control network and FTP network IP addresses from the network adapters, if applicable.
- Shut down the old server. It should not have to be turned on again from this point forward.

Upgrading GV STRATUS server OS from Windows 2008/2012 to Windows 2016

1. Using the **20180726-740-w2016.tib** image (or later), reimage the Windows 2008/2012 servers to Windows 2016.
2. On each re-imaged server, do the following:
   a) Configure the new server with the same name, IP addresses and drives as the previous server.
   b) **For Fibre-connected devices**: Install ATTO drivers. (These are already installed in the 20180726-740-w2016 image, or later)
   c) **For Failover clients**: Install MPIOs. (These are already installed in the Windows 10 Summit/K2Plus images.)
   d) Add the server to the domain, if applicable.
   e) **For Core servers only**:
      1. Install SQL by double-clicking the **Install_SQL_2017.bat** file located in **C | Grass Valley** and follow the UI pop-up dialogs.
      2. License the SQL.
      3. Set the SQL limit based on the RAM: 16 GB RAM -> 8,192 limit; 32 GB -> 18,432 limit; 48 GB -> 32,768 limit; 64 GB -> 47,104 limit;
      4. Recreate the desired local users/groups that were on the previous core server.
   f) Manually install Discovery Agent 2.2.0.215 or later.
   g) Reboot the server.
3. Reorder network adapters by running the **ConfigureW2016NetworkAdapters-PerUserInput.ps1** script on the re-imaged server.

   The specified order is as follows:

1) Control Connection
2) FTP Connection
3) iSCSI A or SMB Connection (if either apply)
4) iSCSI B Connection (if applicable)

   NOTE: If connections 3 and 4 are Unused, the script still requires the user to input their names.

4. Launch the SiteConfig application on the ControlPoint PC, and do the following:
   a) On the **Network Configuration | Devices** tab, remove all devices that were reimaged.
   b) Re-add all devices in the Devices tab.
   c) In the **Software Deployment | Deployment Groups** tab, add the devices back to the deployment group and include all the original roles.
   d) Perform a Check Software on all the newly added devices.
   e) Deploy GV STRATUS 6.8 systemcabs.
   f) Reboot the server after all systemcabs have been installed successfully.

5. Restore the files and configuration settings by doing the following:
   a) **For Express Core servers only**: Copy back the Proxy folder to the **F: drive**.
   b) Reconfigure the shared folders that were shared on the previous server(s), if any.
   c) Obtain and install new Sabretooth licenses, if applicable.
   d) If you have a separate WFE or DMEs, make sure they are shut off before running the .bat file on a core server, or vice versa.
   e) Copy the zip file from your external hard drive to the root of the D: drive and extract it at that location.
   f) Move the **ServerMigration** folder from the extracted folder to the root of the **D: drive**.
   g) Open the folder and run the **ConfigRestore.bat** file.

      NOTE: If this fails, verify that all GV services were stopped. Then, review the C | Temp | GV*.log files.

   h) Put the server in Enabled mode and reboot.
   i) **For FSMs only**: In K2Config, expand the FSM, select the iSCSI Bridge, and click the Check button. If all the check marks are green proceed to the next step. Otherwise, click the View Target Drives… button, click Close, and re-click the Check button—they should be all green now.
6. In GV STRATUS Control Panel, do the following:
   a) Verify the previous Control Panel settings in each tab.

      NOTE: No settings should be lost.

   b) Resave the **Proxy Config** tab, to verify that the proxy share is setup correctly. (Add the domain/gvadmin permissions manually on fully domain-integrated systems.)
   c) **For Core servers only**: Reset Index under **Core | Search Index Config**. This may take two to four hours, depending on the size of your system.

      While the system is re-indexing, verify that the Navigator, Inspector, Send/Conform Destinations, Transfers, Rules, etc. are working in the GV STRATUS application.

Configuring permissions for proxy folder

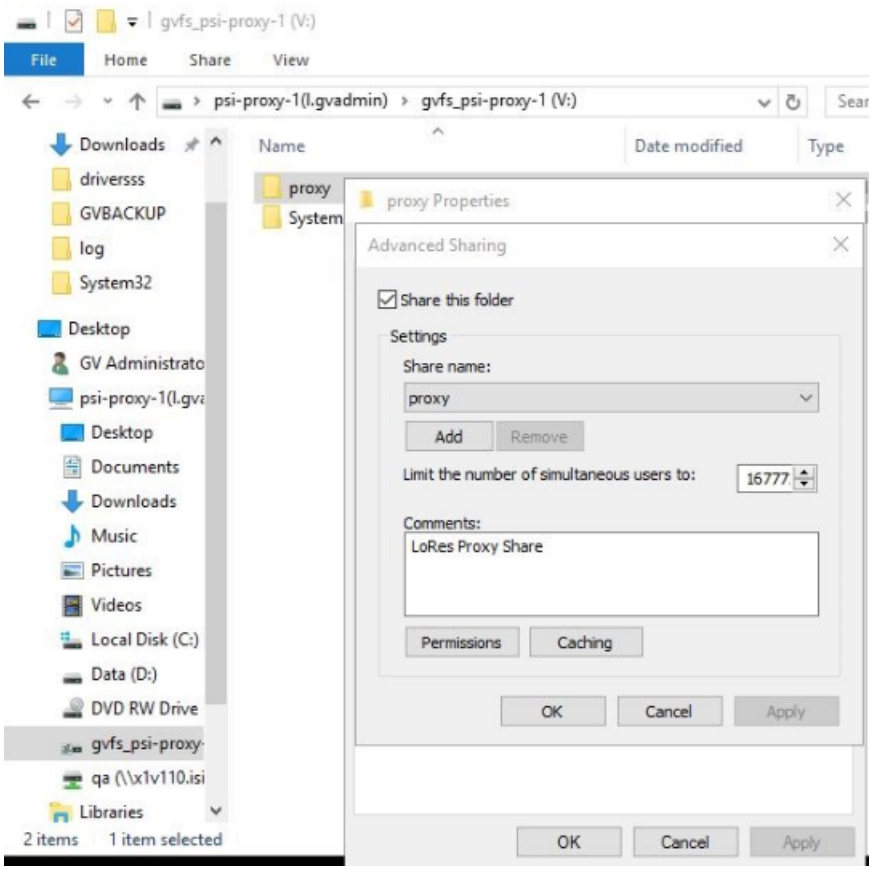
This is only applicable to fully domain-integrated systems. If the gvadmin account used is part of the domain such as gvservice\gvadmin, you must add the domain\gvadmin account and apply permissions to enable proxy access.

1. Launch the GV STRATUS Control Panel, go to **Proxy Config | Proxy Settings** tab and re-save the proxy settings.
2. In Windows Explorer, right-click on the proxy folder and select **Properties**.

   The proxy properties window opens.

3. Select the **Sharing** tab and click the **Advanced Sharing** button.

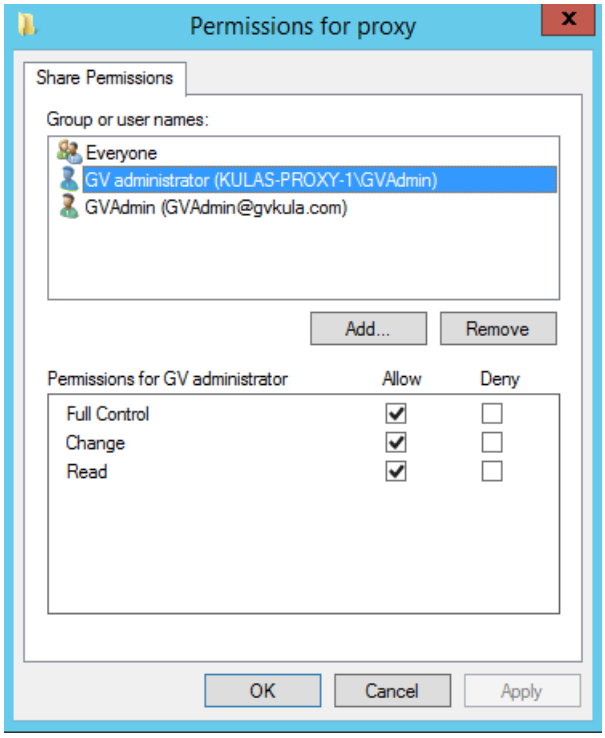
   The Advanced Sharing window opens.



4. Select the **Share this folder** check-box.

5. Click the **Permissions** button.

   The Permissions window opens.



6. Select the domain\gvadmin account under group or user names.
7. Select the **Allow** check-box for all items to grant full access to the proxy folder.
8. Click **OK**.

Verify that devices are configured properly

After all software, hardware and OS upgrades are complete, do the following to verify systems and tools are ready for configuration:

- Reboot your GV STRATUS system in the correct order.
- Put all servers running Embedded Security Manager in Enable Mode.
- On the Core server, open SQL and go to **Databases | ISDB | Properties | Options**. Verify that **AutoClose** is set to **False**.

- Grass Valley recommends the GV STRATUS Control Panel is only configured on the Core server. In the GV STRATUS Control Panel, do the following:
  - Re-save the Proxy settings.
  - In each Grass Valley Media Server MDI, do the following:
    - Verify the UNC path to the V: drive exists. (This is required for GV Render Engines to work.)
    - Verify all K2 SANs, K2 Centrals, and Third Party Storage systems have a primary and secondary devices entered (usually set as the first and second K2 Summit clients).
    - Re-save the Grass Valley Media Server MDI. (This is required for GV I/Os to work, if any have been added.)
  - In Engines settings, do the following:
    - Verify that all engines are running.
    - Select and reconfigure the Xcode Control Engine, if you have the Telestream Vantage transcoder in your operation.
    - Select and configure the new External Media engine, if you have the Verizon-CMS system in your operation.
  - If your system has a K2 SAN, click **Core | K2 Storage | K2 SAN Storage** and verify that the information for the K2 SAN is the same information that is in K2Config. If the information is the same, it means that the Control Panel application is correctly reading the information from the K2Config application.
  - If your system has a GV I/O Live Ingest and Playback Server, configure the GV I/O channel formats in **General | Channels | GV I/O** to the desired formats configured in the **General | Format | Formats** settings, if you added one or more GV I/O Live Ingest and Playback Servers to your operation.
- From each machine in the GV STRATUS system, verify that you can ping all the devices that the GV STRATUS server needs to communicate with over the control network.
- For the machines that need to communicate with a Proxy server, verify you can log in to that Proxy server using the credentials that the system will be using.
- Verify that GV Render Engines are configured correctly. Mapped V: drives for non-iSCSI connection to K2 Summits are no longer needed. You may need to delete the Servers in the **XREAdminConsole | Plug-in | Importer/Exporter | K2 (SAN) | Server** window and re-select the "Configure automatically" check-box, then verify these Server settings:
  - FSMs will get the server names.
  - K2Centrals, SMB Storage SANs, and K2 Summit Standalone(s) will get the Grass Valley Media Server MDI names.
- If you exported an XML file backup of your GV STRATUS Rules before the upgrade, those rules cannot be used anymore once you upgrade to version 6.8 due to the new encryption support. You must import the XML file backup into GV STRATUS system after the upgrade. Then, export your rules again and re-import them to enable the encryption.
- The GV STRATUS database is automatically indexed to support enhanced search features. During this time, Search features and Rules are not fully functional. In GV STRATUS Control Panel, click **Core | Search Index Config** to view indexing progress.
- Begin by configuring STRATUS Core Services settings and move on to other settings.

After automatic re-index completes, reboot system in the correct order and verify that the GV STRATUS-EDIUS system is working.

NOTE: If prompted for a Java update, upgrade to the latest version of Java software to ensure you have the latest security updates.

Upgrade GV STRATUS system with the DIVA Category Update Utility

- The GV STRATUS software must have been upgraded on the GV STRATUS Core server.
- There are no currently processing or running archive/restore workflows between DIVA archive and the GV STRATUS system.

This task applies to the following:

- The GV STRATUS Core server

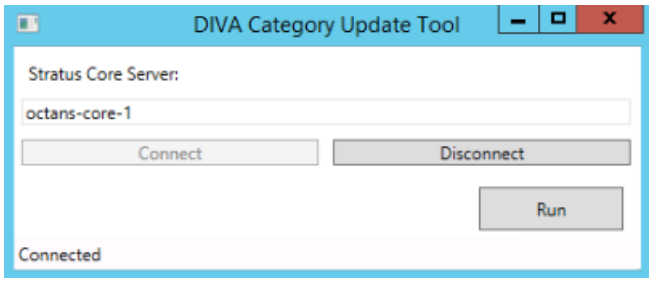
The `DivaCategoryUpdateUtility.exe` must be run on the GV STRATUS Core server after upgrading GV STRATUS software if you have DIVA archive in your system. Running the tool ensures existing GV STRATUS assets' associations paths are updated with the newly supported multiple DIVA categories.

1. Log on to the GV STRATUS Core server as an Administrator.
2. Locate the following file:

   `C:\Program Files\Grass Valley\STRATUS MDI DIVA\DivaCategoryUpdateUtility.exe`

   This file is copied to the GV STRATUS Core server during software deployment.
3. Run the `DivaCategoryUpdateUtility.exe` to update DIVA categories to assets' association paths in your GV STRATUS system.

   The **DIVA Category Update Tool** opens.
4. Enter the name of the GV STRATUS Core server and click **Connect**.

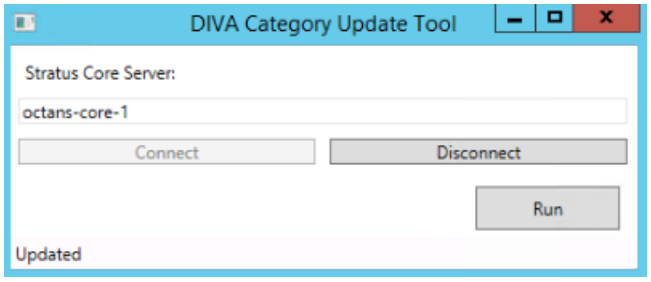


   If there are any conflicts, the **Resolve Conflict** section will be displayed.
5. Ensure the Name, Metadata ID (URN), and Category columns are shown (in that order), with a drop-down list in the Category column for users to select a DIVA category.

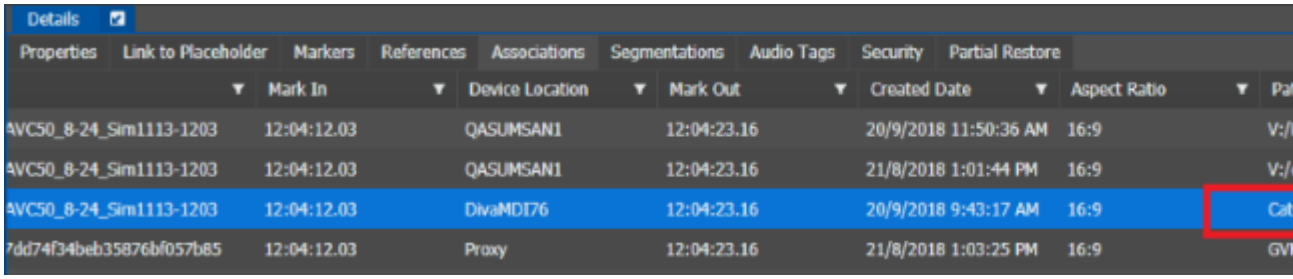
6. Do one of the following:

   - Resolve any conflicts by assigning the correct DIVA category to assets. Then click **Run**.
   - If there are no conflicts, just click **Run**.

   The process is completed when the status changes to **Updated** in the DIVA Category Update Tool.



With a successful run of the DIVA Category Update Utility, the DIVA Category and Disk Array name will be displayed in the **Path** column of the Associations tab when you load a DIVA archived asset into the Inspector.



Upgrade GV STRATUS Rundown and VTR Ingest systems

- K2 systems must be upgraded to the compatible version of K2 system software.
- GV STRATUS systems must be upgraded to the compatible versions of software.
- Grass Valley Prerequisite Files must be installed on the control point PC.

Upgrade your GV STRATUS Rundown and GV STRATUS VTR Ingest systems to the compatible versions of software. Refer to related topics in GV STRATUS Rundown and GV STRATUS VTR Ingest upgrade procedures.

Related Topics

Upgrading GV STRATUS Rundown systems on page 173
Installing and Upgrading GV STRATUS VTR Ingest/GV STRATUS VTR Controller on page 181

Make recovery images of servers

After you have upgraded software as instructed in these procedures and verified that your system is working properly, you should always make a recovery image of each of your upgraded computers. Use a sequence of tasks similar to those you followed for upgrading software so that as you take systems offline you manage redundancy, servers, and clients, as appropriate for your system.

Refer to the Grass Valley product's *Service Manual* for recovery image procedures.

Upgrading GV STRATUS from version 6.5 to version 6.8 with K2 Summit version 9.8.7

Follow the topics in the section sequentially to perform the upgrade.

Summary of upgrade from version 6.5 to version 6.8

Several upgrade tasks are new or require special consideration with this upgrade. Apply upgrade tasks as appropriate for your system design, as follows:

- All systems:
  - SiteConfig: Before upgrading GV STRATUS, upgrade your SiteConfig application and Discovery Agent to the latest version. For more info, refer to *Grass Valley products compatible with GV STRATUS* on page 56.
  - Password encryption: To enable password encryption in GV STRATUS system after the software upgrade, you must run the Key Upgrade Utility on the GV STRATUS Core server. For more info, refer to *Upgrade GV STRATUS system with the Key Upgrade Utility* on page 90.
  - Summit MDIs: Summit MDI has been renamed to **Grass Valley Media Server** MDI type in the MDI Configuration settings of GV STRATUS Control Panel. You must reconfigure MDI settings for all K2 Summit Standalone, K2 SAN, K2 Central, and Third Party Storage systems in this release. For more details, refer to *Grass Valley Media Server MDI standalone settings* on page 304, *Grass Valley Media Server MDI SAN settings* on page 306, *GV STRATUS Control Panel configuration for K2 Central* on page 937, and *GV STRATUS Control Panel configuration for SMB storage* on page 930.
  - GV I/O Live Ingest and Playback Server SiteConfig roles: These new SiteConfig roles for Standalone or SMB third party storage client must be assigned to GV I/O Live Ingest and Playback Server before upgrading the GV STRATUS system, if applicable. For more details, refer to *Add software roles for upgrade to version 6.8* on page 82.
  - Advanced Editor: After the upgrade, existing users and groups do not have this role assigned in GV STRATUS Control Panel, so you must assign the role if needed. If you create new users and groups, the new role must be added or removed if appropriate. For more info, refer to *GV STRATUS roles matrix* on page 37.
  - DIVA Archive categories: GV STRATUS supports multiple DIVA archive categories with this release. The Diva Category Update Utility must be run on the GV STRATUS Core server after the software deployment. For more info, refer to *DIVA Categories Add/Modify Field settings* on page 310 and *Upgrade GV STRATUS system with the DIVA Category Update Utility* on page 99.
  - GV STRATUS Rules Backup: If you exported an XML file backup of your actual rules before the upgrade, those rules cannot be used anymore once you upgrade to version 6.8 due to the new encryption support. You must import the XML file backup into GV STRATUS system after the upgrade. Then, export your rules again and re-import them to enable the encryption. For more info, refer to *Exporting rules* on page 641 and *Importing rules* on page 642.
  - Internal system account: If the internal system account for your GV STRATUS system is on a fully qualified domain or is not the default GVAdmin account, configure settings at GV STRATUS Control Panel **Core | STRATUS Core Services | Primary Site** as appropriate for your system.
- Systems with Windows 2008 servers:
  - Requires an upgrade to Windows 2012 or Windows 2016 operating system. For more details, refer to *Upgrade GV STRATUS server OS from Windows 2008/2012 to Windows 2016* on page 92.

Make recovery images of servers

Do not do this task if:

- You previously made a recovery image at the current software version for each computer you are upgrading.

Do this task if:

- You do not have a recovery image at the current software version for one or more of the computers you are upgrading.

The recommended procedure is to make a recovery image immediately after a software upgrade. If you neglected to do this when you last upgraded software you should make the recovery image now, before upgrading to the new version.

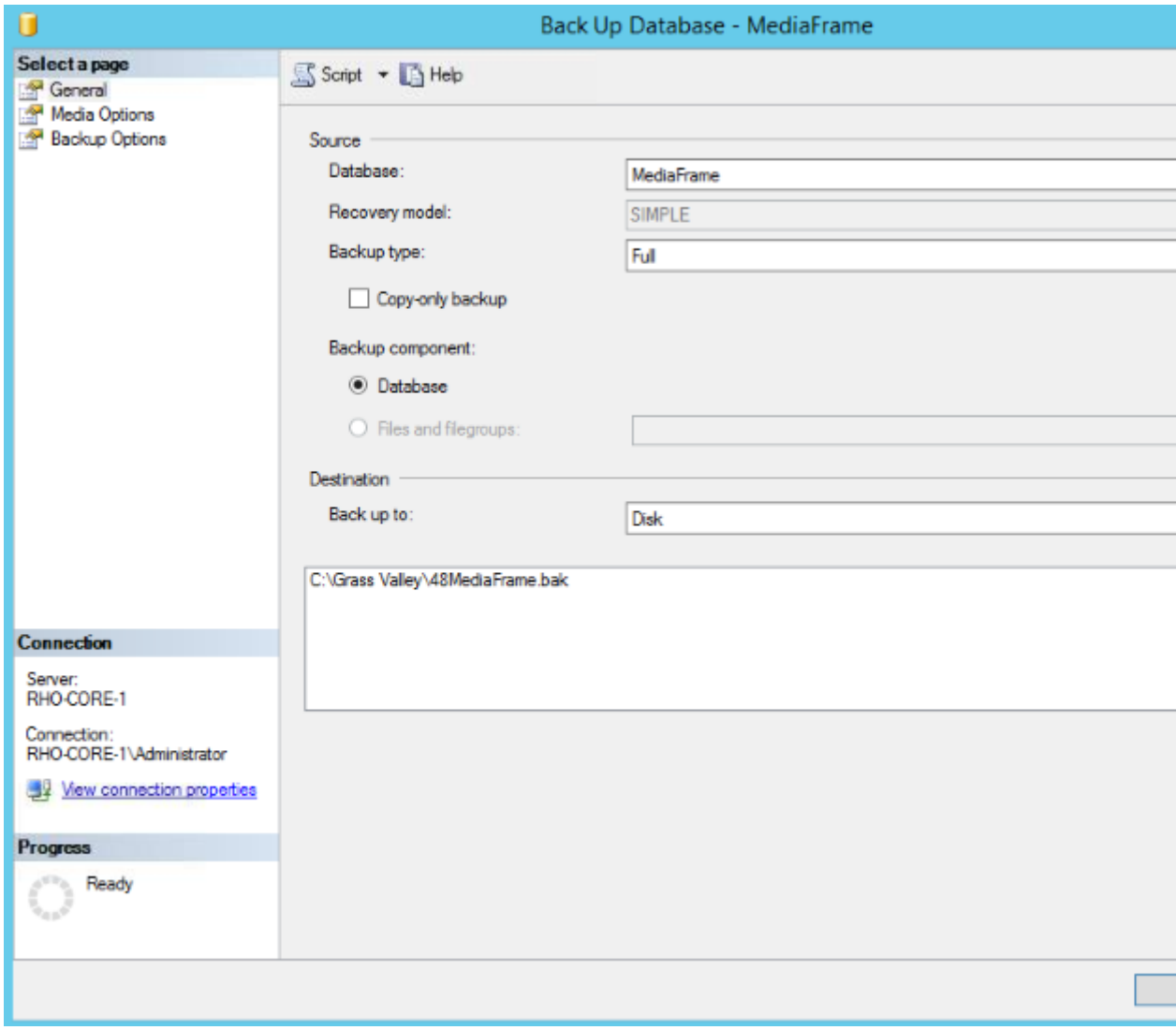
⚠ ***CAUTION: If you upgrade and then decide you do not want to stay with this version of software, you must use the recovery disk image process to downgrade to your previous version.***

Backing up a database

Grass Valley recommends that you back up all the databases of the GV STRATUS system before upgrading to the latest version of the software or before moving your databases from the GV STRATUS Core server to a standalone Database Server. With a database backup, you can avoid any lost of feed schedules and the need to key in everything again in case of a system crash. The backup could also be placed on another machine or an external drive for extra precaution.

1. Open and log in to Microsoft SQL Server Management Studio.
2. In the tree-view expand the **Databases** node and identify the databases of the GV STRATUS system to backup, which are the following:
   - ISDB
   - MediaFlow
   - MediaFrame
   - RulesEngine
   - WfPersistence

3. Right-click on a database and select **Tasks | Back Up**.



4. On the General page, select a database to be backed up from the **Database** drop-down list.
5. Select **Full** on the **Backup type** drop-down list.
6. In the Destination section, click **Add** and select the backup destination.
7. On the Media Options page, select **Back up to the existing media set** and **Overwrite all existing backup sets**.
8. On the Backup Options page, enter the name of the backup database.
9. Click **OK**.
10. Repeat for other databases of the GV STRATUS system that you are backing up.

Replace the CompactFlash Card

K2 Summit clients and K2 Standalone servers must be either 3G or have the 32 GB Flash card installed before installing Windows updates.

Do not do this task if you have:

- A K2 Summit 3G system with mSATA system drive.

Do this task if you have:

- A K2 Summit system with CompactFlash system drive.

1. Backup the K2 Summit using Acronis.
2. Replace the 16-GB flash card with a 32-GB flash card.
3. Restore the K2 Summit image using Acronis and verify that the C: drive is over 27 GB in size.

Upgrade Microsoft Visual C++ Redistributable for VS 2017

This task applies to the following:

- All types/roles of GV STRATUS servers.
- Client PCs hosting one or more of the following:
  - GV STRATUS
  - GV STRATUS Control Panel
  - EDIUS XS
  - EDIUS Workgroup

This task does not apply to the following:

- K2 Summit systems, as they should have only Microsoft Visual C++ Redistributable for VS 2015 installed

1. From the Windows Start menu navigate to **Control Panel | Programs and Features** and check for the following:

   Microsoft Visual C++ Redistributable for VS 2017

   - If Microsoft Visual C++ Redistributable for VS 2017 is already installed, do not do the remainder of this task.
   - If Microsoft Visual C++ Redistributable for VS 2017 is not installed, continue with this procedure.

2. Procure the **Microsoft Visual C++ Redistributable for VS 2017** installation file from the *Microsoft software download page* or the Grass Valley FTP site.
3. Select the installation file(s) as follows:
   - For servers and Windows 64-bit OS client PCs, select the following:
     - vc_redist.x64.exe
     - vc_redist.x86.exe
   - For Windows 32-bit OS client PCs, select the following:
     - vc_redist.x86.exe
4. Run the installation file and install as directed by the installation wizard.

Upgrade Microsoft .NET

Do not do this task if:

- The system has Microsoft .NET Framework 4.7.1 installed

Do this task if:

- The system does not have Microsoft .NET Framework 4.7.1 installed

This task applies to the following:

- K2 Summit systems
- All types/roles of GV STRATUS servers

1. On the computer, check Windows Control Panel **Programs and Features** for currently installed .NET version(s), then proceed as follows:
   - If Microsoft .NET 4.7.1 is installed, skip this task.
   - If Microsoft .NET 4.7.1 is not installed, continue with this procedure.
2. Procure the Microsoft .NET 4.7.1 installation file from the *Microsoft software download page* or the Grass Valley FTP site.
3. Run the installation file and install Microsoft .NET 4.7.1 as directed by the installation wizard.

Install Important Windows updates (required)

Grass Valley requires the installation of all Microsoft Windows Important updates on all GV STRATUS client and server devices, except as specifically instructed otherwise by Grass Valley.

If a computer does not have the Grass Valley Embedded Security solution one-time initial deployment process applied, do not install any Windows updates. Apply the one-time process before installing Windows updates.

⚠ ***CAUTION: Only "Important Updates" should be installed. Do not install other Windows or driver updates unless specifically directed by product documentation or by Grass Valley Support.***

Prerequisite: Always install the required Microsoft Visual C++ redistributable update before installing the latest Windows Important Updates.

1. Go to **Start | Control Panel | Windows Updates | Check for updates**.
2. If these updates appear, right-click on them and select **Hide update**.

3. Install other "Important Updates".
4. Reboot all GV STRATUS client and server devices after installing those Windows updates.

Related Topics

Deploy Embedded Security solution - One-time process

Prepare for upgrade

Before upgrading, do the following:

- Procure the software installation files for this release via the appropriate distribution method, such as download, network drive, or external drive.
- Export all configured rules to avoid recreating them from scratch after the upgrade.
- Stop all media access on the devices you are upgrading.
- Shut down all applications on the devices you are upgrading. This includes the SDB Server if you have GV STRATUS Rundown in your operation.
- Terminate all users' sessions using the GV STRATUS Control Panel.

Prepare SiteConfig for software deployment

If a newer version of SiteConfig is available, you must upgrade to the latest version. For more info, refer to *Grass Valley products compatible with GV STRATUS* on page 56.

Do the following to prepare SiteConfig for the software upgrade.

1. If a newer version of SiteConfig is available for upgrade and you have not yet upgraded SiteConfig, do the following:
   a) From Windows **Programs and Features**, uninstall the current version of SiteConfig from the control point PC.
   b) Install the new version of SiteConfig on the control point PC.
2. After the installation is complete, click **Finish** and launch the SiteConfig application.
3. Next, configure the deployment group.

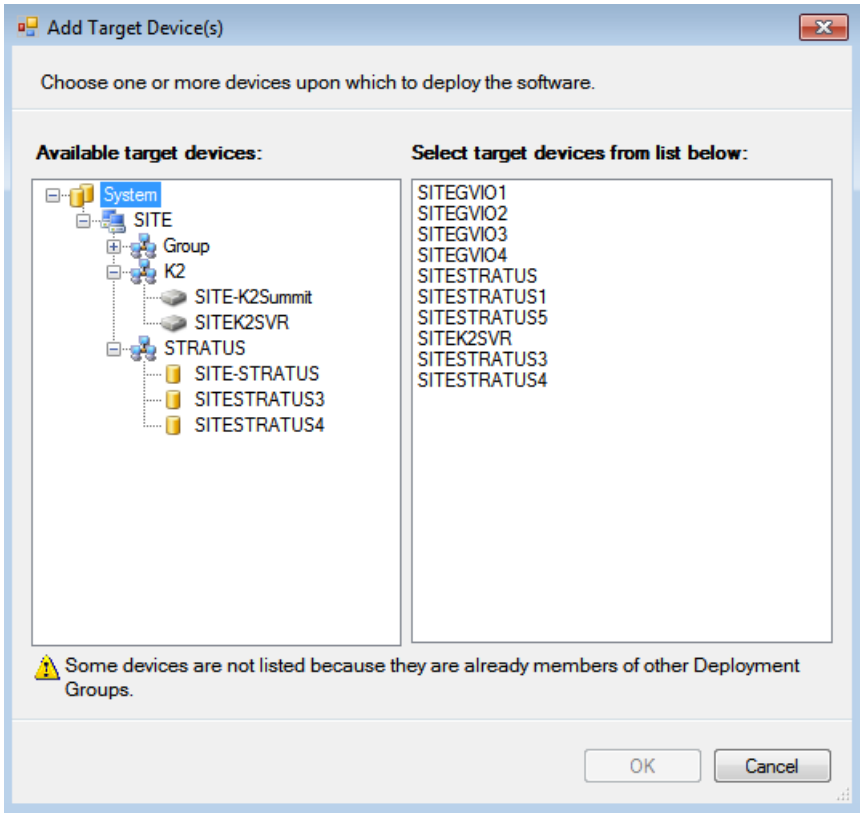
Configuring deployment groups

- The device must be assigned in the SiteConfig system description and network connectivity must be present.
- GV STRATUS systems containing mixed K2 Summit versions of 9.8 and 10.1 will require at least two separate deployment groups, one for K2 Summit 9.8.x system and one for K2 Summit 10.x system.

1. In the **Software Deployment | Deployment Groups** tree view, right-click the top node and select **Add Deployment Group**.
   A deployment group appears in the tree view.
2. Right-click the deployment group, select **Rename**, and enter a name for the deployment group.

3. Right-click the deployment group and select **Add Target Device**.

   The Add Target Device(s) wizard opens.



4. In the Available Target Devices tree view, select the node that displays the devices that you are combining as a deployment group.
5. In the right-hand pane, select the devices that you are combining as a deployment group.

   To select multiple devices, you can drag through the devices, use Ctrl + Click, or use Shift + Click.
6. Click **OK**.

The devices appear in the Deployment Groups tree view under the deployment group. Before you perform a software deployment, you must check software on the devices that will be receiving new software. If you have already added packages to the group, on the Deployment Groups tab you will also see deployment tasks generated for every device with roles that match the package contents.

Upgrading the Discovery Agent

If a newer version of SiteConfig Discovery Agent is available, you must upgrade to the latest version. For more info, refer to *Grass Valley products compatible with GV STRATUS* on page 56.

1. On the device you plan to manage with SiteConfig, open the Windows Services Control Panel and look for the following required item:
   - SiteConfig Discovery Agent

2. Check the version number of the SiteConfig Discovery Agent.
   - If the latest version is installed, skip this task.
   - If the latest version is not installed, continue with this procedure.
3. In order to upgrade Discovery Agent on all your devices, add only the DiscoveryAgent cab to your deployment group(s).
4. Click the **Start Deployment** button.

   Deployment tasks run and software is uninstalled. Progress is reported and next steps are indicated in both the Status and Details columns.
5. When the Uninstall task completes, set Restart to Complete when the **Restart required** option displays on SiteConfig.

   NOTE: This is to prevent Siteconfig from losing its connection with any of your devices during the Uninstall/Install process. If the connection is lost, you will need to install Discovery Agent manually and perform a check software on the device(s) in order to sync them up with Siteconfig.
6. Once the DiscoveryAgent cab is installed, click the "Restart required" option to restart the server.

Add software roles for upgrade to version 6.8

Before doing this task, make sure devices are added to the SiteConfig system description with the correct family and device type. Refer to *Complete listing of device types, roles, and software packages for GV STRATUS devices* on page 194.

For your K2 Summit systems, make sure you have separate deployment groups for the upgrade to version 9.8.x and version 10.1.x if you have both versions in your operation.

NOTE: If upgrading to K2 Summit version 10.1.x, you cannot use Siteconfig to directly upgrade from SNFS 4.7 to SNFS 6.0 on FSMs and K2 Standalone Summits. Refer to Upgrading to SNFS 6.0 on page 87 before proceeding, if applicable.

These SiteConfig roles are new or require special consideration with this software upgrade. Verify and add roles if necessary.

1. As appropriate for your system design and licensing, in your SiteConfig system description, configure as follows:
   - For your GV STRATUS Express Server, or Core Server, add the new device as follows:
     - GV STRATUS Proxy Streaming Server (optional)

       These new roles will be automatically added:

       - GV STRATUS Proxy Streaming Service
       - GV Embedded Security Manager
       - GV Log Manager
   - For your GV STRATUS Express Server, Core Server, Workflow Server or a separate server, add the new role as follows:
     - GV STRATUS ExternalMedia Engine (optional)
   - For your GV I/O Client - Standalone device, add the new device as follows:
     - GV I/O Standalone Device

       These new roles will be automatically added as follows:

       - GV STRATUS IO Appliance
       - GV Embedded Security Manager
       - GV STRATUS Summit Service
   - For your GV I/O Client - Shared Storage device, add the new device to Isilon system deployment group as follows:
     - GV I/O Client (SMB)

       These new roles will be automatically added as follows:

       - GV STRATUS IO Appliance
       - GV Embedded Security Manager

   NOTE: GVEngine and MPIcore must be manually installed on any GV I/O device(s). The installation files can be procured from the Grass Valley FTP site.

2. Save SiteConfig and verify in `C:\ProgramData\Grass Valley\ConfigurationDataFiles\SiteConfig` that .scsd and .config files are saved to the Core server.

If you want to verify all your currently configured SiteConfig roles, refer to the complete list of roles and software packages.

Add software package to deployment group for GV STRATUS and other devices

- The GV STRATUS devices to which you are deploying software must have their SiteConfig roles correctly configured.
- The GV STRATUS devices to which you are deploying software must be in a deployment group.
- The following software upgrade system cab files apply to all deployment groups.
  - *GrassValley_STRATUSClient_X.X.X.XXX.cab*
  - *GrassValley_CoreServer_X.X.X.XXX.cab*
- The following software upgrade system cab files apply to K2 Summit 9.8.x devices. For each deployment group, choose the one that applies.
  - *GrassValley_K2system_X.X.X.XXX.cab*
- The following software upgrade system cab file apply to K2 Summit 10.x devices. For each deployment group, choose the one that applies.
  - *GrassValley_K2Plus_X.X.X.XXX.cab*
- The following software upgrade system cab files apply to GV I/O devices, if already added as a standalone device or a shared storage client with Dell EMC Isilon network-attached storage system.
  - *GrassValley_GVIO_X.X.X.XXX.cab*

  NOTE: Next, you must manually run the GVEngineInstaller-x.x.x.xxx_xxxxx_xxx.exe and MPIcore on each GV I/O device in your operation. The installation files can be procured from the Grass Valley FTP site.

1. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.
2. Click the **Add** button.

   The Add Package(s) dialog box opens.
3. Do one of the following to select the software package:
   - Select from the list of packages then click **OK**.
   - Click **Browse**, browse to and select the package, then click **Open**.
4. If one or more EULAs are displayed, accept them to proceed. If you do not accept a EULA, the associated software is not assigned to the deployment group.

   SiteConfig adds the package to the deployment group.

The package appears in the Managed Packages list for the selected deployment group. SiteConfig creates new software deployment tasks for the package and displays them in the Tasks list view.

Related Topics

Complete listing of device types, roles, and software packages for GV STRATUS devices on page 194

Complete listing of device types, roles, and software packages for GV STRATUS devices on page 194

Setting deployment options

- A software package must be assigned to the deployment group and applicable deployment tasks must be displayed in the Tasks area.

1. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.
2. In the Tasks list view, view tasks and determine if you must set deployment options.

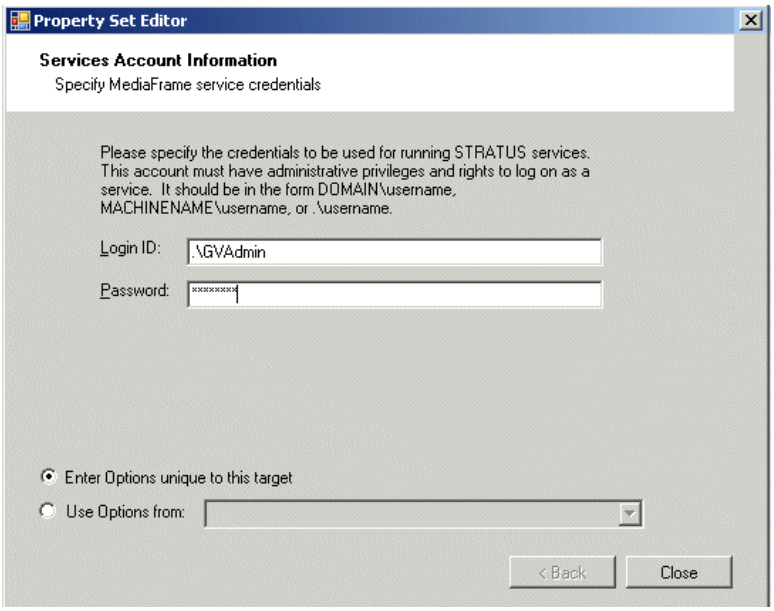
   Tasks that need to have deployment options set display in the Details column a message stating "Deployment options required."

   If you select a task that needs to have its deployment options set, the Start Deployment button is disabled and the message is displayed next to the button.
3. Do one of the following to set deployment options:

   - Double-click the task.
   - Select the task and click the **Options** button.

   A wizard opens.

4. Work through wizards and set deployment options for GV STRATUS software as follows:

Software	Deployment options
GrassValley_STRATUS_CommonServices GrassValley_STRATUS_ControlPanelService GrassValley_STRATUS_CoreServices GrassValley_STRATUS_CRArchive_MDI GrassValley_STRATUS_Databases GrassValley_STRATUS_DataMover GrassValley_STRATUS_DIVA_MDI GrassValley_STRATUS_ExternalMedia GrassValley_STRATUS_FlashNet_MDI GrassValley_STRATUS_GFTP_MDI GrassValley_STRATUS_HttpProxyServer GrassValley_STRATUS_IngestServices GrassValley_STRATUS_Masstech_MDI GrassValley_STRATUS_MediaFlow GrassValley_STRATUS_MEWS GrassValley_STRATUS_Proxy_MDI GrassValley_STRATUS_ProxyStreamingService GrassValley_STRATUS_RenderEngine GrassValley_STRATUS_Rules GrassValley_STRATUS_ScheduledTransferEngine GrassValley_STRATUS_SocialMedia GrassValley_STRATUS_Summit_MDI GrassValley_STRATUS_TrafficGateway GrassValley_STRATUS_Transcode GrassValley_STRATUS_WebApps GrassValley_STRATUS_WebClient GrassValley_DeviceKeyService GrassValley_LogManager GrassValley_LogViewer	 Use the local system account if your system is on a workgroup or if it's on a domain but uses the local system account in SQL. Use a domain\admin account if the account was previously mapped in SQL to the MediaFrame, MediaFlow, RulesEngine and WFPersistence databases. Entering account credentials allows you to use the **Use options from** feature for all other devices of the same type. Once you enter the account credentials this way on the first device, it becomes the template from which options for other devices are copied.

5. If you have multiple devices of the same type, you can enter deployment options for one of them using the wizard. Then, when you bring up the same wizard on every device, you can choose the **Use options from** radio button and select the first device for which you set options.

   SiteConfig copies the options you set for the first device and fills in the blanks on the wizard.

Upgrade software on GV STRATUS devices

- The devices that you are upgrading must be in a deployment group.
- For the software you are upgrading, a newer version of that managed software package must be added to the deployment group.
- A SiteConfig "Check Software" operation must be performed on the devices you are upgrading.
- All servers have been set to **Update mode** in the Embedded Security Manager.

If you are upgrading multiple software components for which there is a required sequence, you must check and uncheck tasks and run multiple deployment sessions to control the sequence. For some software components, SiteConfig aids you by enforcing dependencies. For each individual software component, SiteConfig enforces an uninstall of the current version of software before installing the upgrade version. SiteConfig provides uninstall deployment tasks and install deployment tasks to indicate the taskflow. SiteConfig can do the uninstall/install in a single deployment session.

1. In the **Software Deployment | Deployment Groups** tree view, select the device or the group of devices to which you are deploying software.

   The corresponding software deployment tasks are displayed in the Tasks list view.

2. For the software you are deploying, do the following:

   a) Select the **Deploy** check box in the row for the uninstall task.

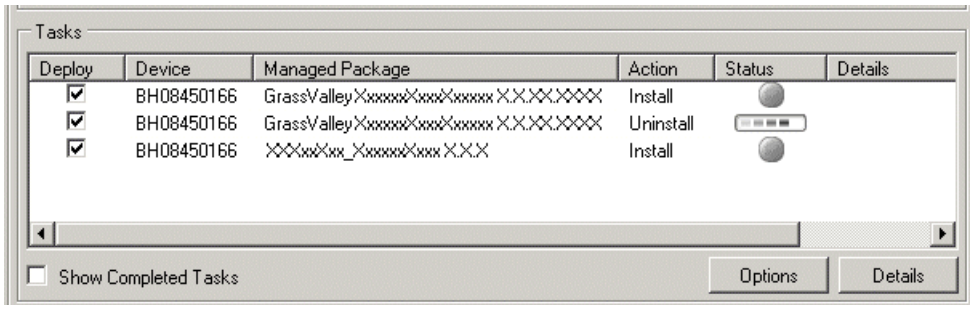
   b) Select the **Deploy** check box in the row for the install task.

   If a WFRegMon install task appears, install it as well. It is required to support Grass Valley software installers. There is no uninstall task.

3. Check the area next to the Start Deployment button for a message.

   If a message instructs you to upgrade the Discovery Agent, on the control point PC go to the directory to which SiteConfig is installed, find the `DiscoveryAgent_x.x.x.x.cab` file, add it to the deployment group, and deploy the Discovery Agent software as well.

4. Click the **Start Deployment** button.



Deployment tasks run and software is uninstalled. Progress is reported and next steps are indicated in both the Status and Details columns. If an error appears regarding prerequisite software, install the Grass Valley Prerequisite Files on the control point PC and then repeat this step.

SiteConfig uninstalls/install software in the proper sequence.

5. When the Status or Details columns indicate next steps, identify the software in the row, then do one of the following:
   - If Details displays a **Restart required** link (but not "Visible dialog pending..."), click the link and when prompted "...are you sure...", click **Yes**.
   - If Details does not display any indication of additional steps required, proceed with the next step in this task.
6. Monitor progress as indicated by both the Status and Details column. When finished, the Status column indicates complete.
7. Shutdown the entire GV STRATUS/K2 Summit system and power up the servers in the correct order, starting the required services as needed.
8. Set all servers back to **Enabled mode** in the Embedded Security Manager.
9. If you deployed the MEWS Service, after deployment is complete, start the MEWS Service.

Related Topics

Upgrade GV Render Engine server software and EDIUS client software on page 148

Upgrade K2/Summit/SAN systems that are accessed by the GV STRATUS system

- You have procured the necessary software and documentation for the upgrade. Go to *Grass Valley products compatible with GV STRATUS* on page 56 and determine the compatible software versions required.
- All standalone K2 Summit systems must be offline (all media access stopped) and shut down. The power must be off for a few seconds before switching it on again.
- If upgrading a K2 SAN, all SAN clients must be offline (all media access stopped) and shut down. The power must be off for a few seconds before switching it on again. Depending on your system design, this could include devices such as SAN-attached K2 Summit systems, GV STRATUS servers, and GV STRATUS Client PCs.

NOTE: When upgrading from a K2 software version lower than 9.x to a K2 software version at 9.x or higher, you must reimage each* K2 Summit system*. Hardware upgrades might also be required on a* K2 Summit system*.

1. Upgrade your K2 systems to the compatible version of K2 system software. This includes K2 SAN systems and stand-alone K2 Summit systems.

   When upgrading for compatibility with GV STRATUS, use `GrassValley_K2system_x.x.x.cab` file, which contains the required `GrassValley_STRATUS_SummitServices_x.x.x.cab` file.
2. On systems running Embedded Security, do the one-time initial deployment process for the Embedded Security solution, if you have not already done so.
3. Update K2 Summit licenses.

About deploying software for the K2 SAN

You must control the sequence of software deployment tasks and device restarts as you upgrade software across the K2 SAN. The general sequence is to upgrade K2 Media Servers first then the SAN-attached K2 systems. The exact steps can vary from software version to version. Make sure you follow the task flow in the *K2 Release Notes* for the version of software to which you are upgrading.

Related Topics

Installing GV STRATUS application with SiteConfig on page 280

Upgrade GV STRATUS Database

This task applies to the following:

- The GV STRATUS server with the role of GV STRATUS Database.

Before doing this task, do the following:

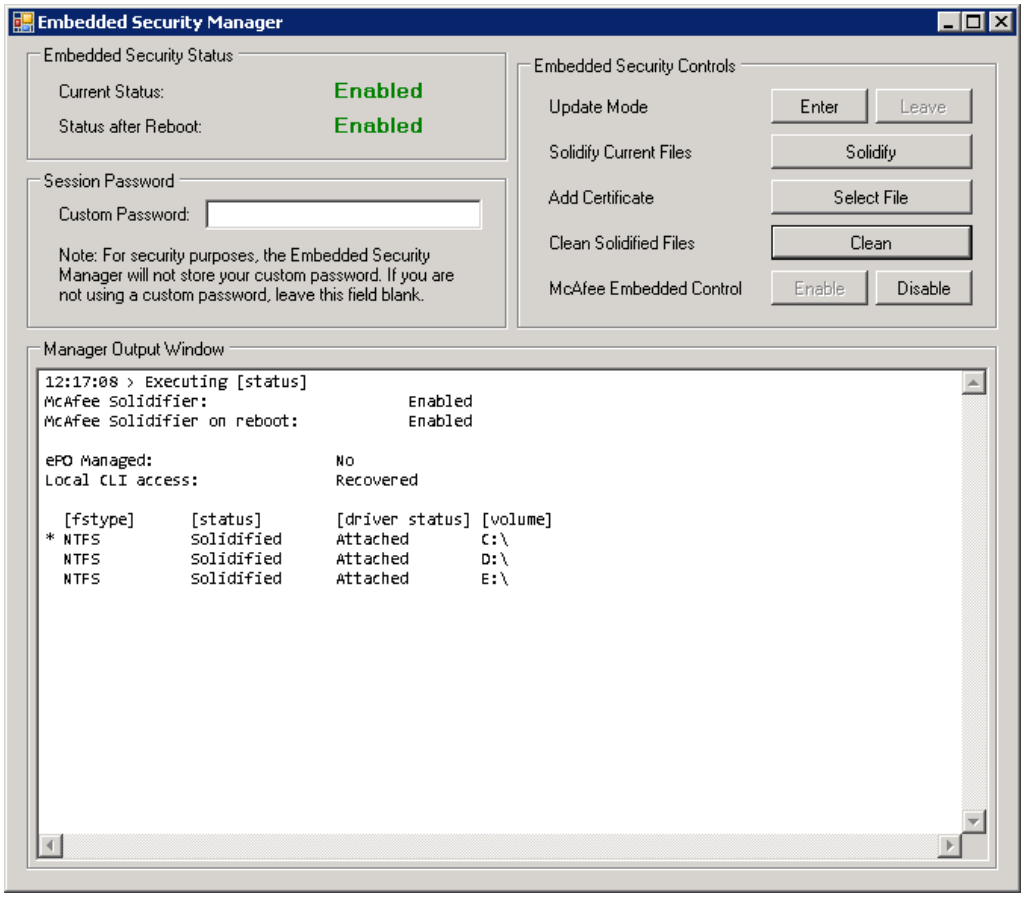
- Upgrade software on the GV STRATUS server.

This task upgrades the GV STRATUS database.

1. Log on to the GV STRATUS server as Administrator.

2. From the Windows desktop, click **Start | All Programs | Grass Valley | Embedded Security Manager**.

   Embedded Security Manager opens.



3. If Current Status is **Enabled**, click **Enter** in the Embedded Security Controls section to put it in **Update Mode**.
4. Locate the following file:

   `C:\Program Files\Grass Valley\STRATUS Databases\MediaFrameDbUpgrade.exe`

   This file is copied to the GV STRATUS server along with the software upgrade.
5. Double-click `MediaFrameDbUpgrade.exe` to upgrade the database.
6. Reboot the GV STRATUS server.

A "The database upgrade completed successfully" message displays.

Related Topics

Standalone Database Server set up process on page 829

Upgrade GV STRATUS system with the Key Upgrade Utility

This task applies to the following:

- The GV STRATUS Core server

Before upgrading, do the following:

- Disable any currently active rules on the GV STRATUS Control Panel.
- Make sure there are no currently processing or running workflows on the GV STRATUS system.

Before running the utility, do the following:

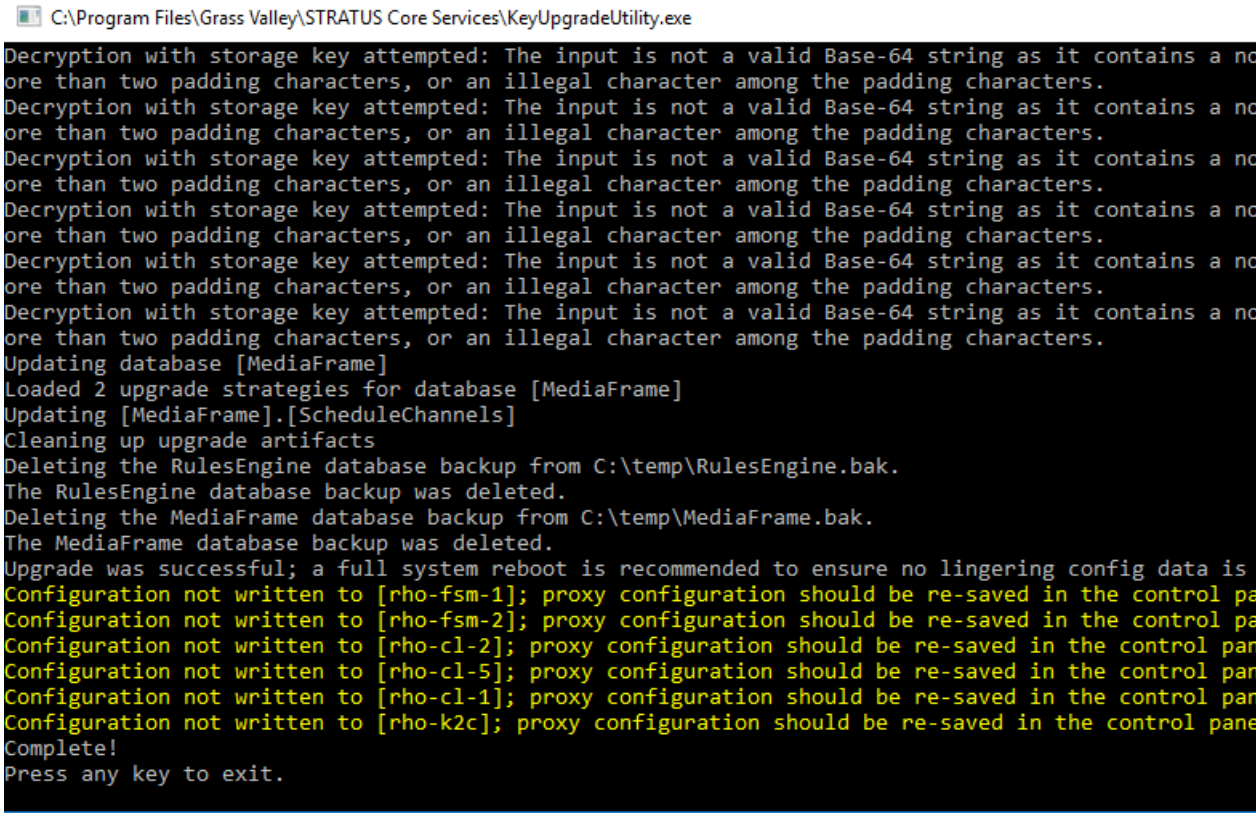
- Upgrade GV STRATUS software on the GV STRATUS Core server.
- Upgrade the GV STRATUS database.
- Restart the GV STRATUS Core server.

1. Log on to the GV STRATUS Core server as an Administrator.
2. Locate the following file:

   `C:\Program Files\Grass Valley\STRATUS Core Services\KeyUpgradeUtility.exe`

   This file is copied to the GV STRATUS Core server along with the software upgrade.
3. Run the `KeyUpgradeUtility.exe` to upgrade the encryption keys on your GV STRATUS Core server.

   Note any yellow messages in the output and take the requested action; these will occur at the end of the utility execution.



   The process is successful when the **Complete!** message displays at the end of the output.
4. In the **Proxy Config | Proxy Settings** tab in GV STRATUS Control Panel, re-check the **Enable Proxy Creation** setting and click **Save**.

   Verify all pop-ups succeed before continuing.

5. Reboot the GV STRATUS Core server.
6. Re-enable any rules that were disabled earlier.
7. Procure and run the *EngineConfig_6_8.cmd* file where any of the following engines are installed and running:
   - DataMover Engine
   - Transcode Engine
   - Workflow Engine
   - Rules Engine
   - Social Media Engine
   - External Media Engine

SabreTooth license process

GV STRATUS licenses are installed on the GV STRATUS server with role of Common Services. Typically the GV STRATUS Core server has the role of Common Services.

1. Refer to the license sheet that you received with your GV STRATUS license. The license sheet has the Sales Order number that you need.
2. On the GV STRATUS server with role of Common Services, run the SabreTooth License Manager, generate a unique ID, and send the email to Grass Valley requesting your license or licenses.

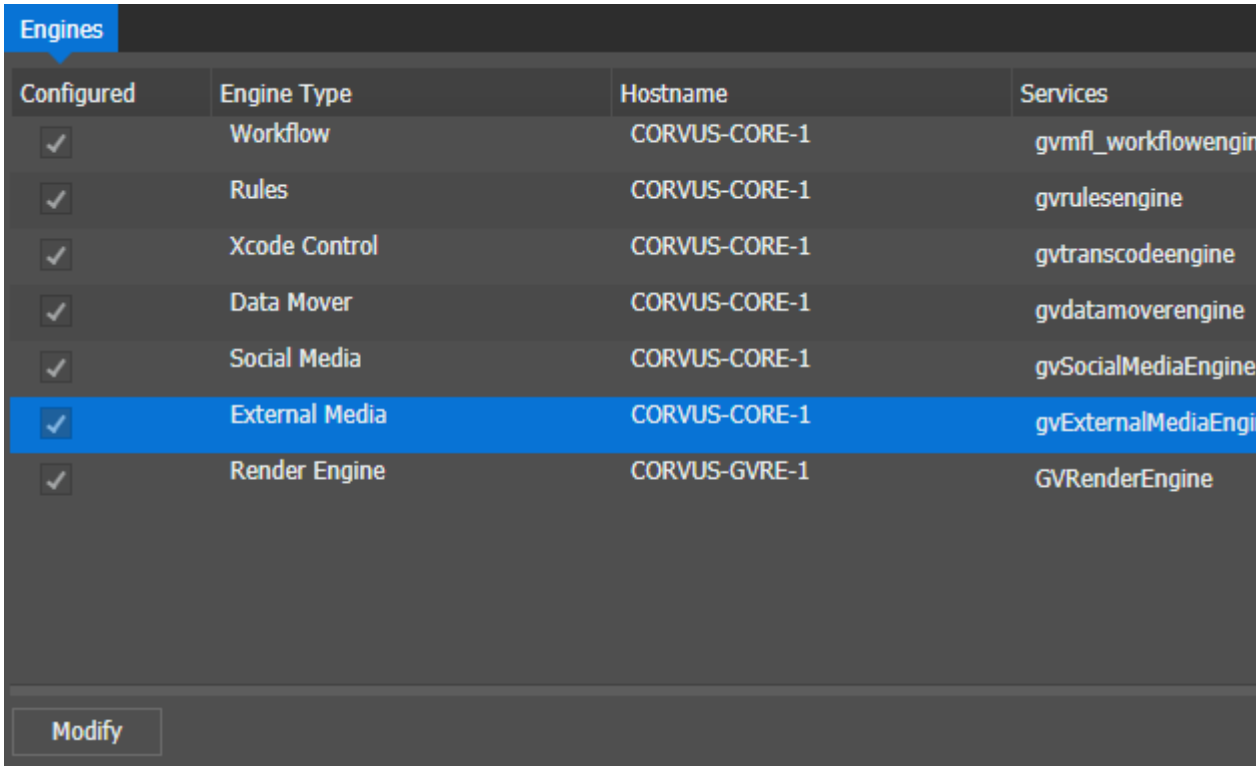
   Refer to this Topic Library for detailed licensing procedures.
3. When you receive your license file, use SabreTooth License Manager and install it on the server.
4. Repeat steps as appropriate to install licenses on other devices.

Verify GV STRATUS Engines are running

After upgrading software, make sure the GV STRATUS Engine services are running. This is especially important if you added a SiteConfig role that installs a type of Engine software or otherwise made a change that could affect Engine software as part of the upgrade.

1. In GV STRATUS Control Panel, click **Core | Engines.**

   Engine settings open.



2. Make sure that in the **Configured** column the Engine is selected.
3. Make sure that in the **Action** column the **Stop** icon is displayed.

   This indicates the Engine service is playing.
4. Make sure that the **Status** column reports **Running**.
5. Verify that GV STRATUS servers with role of Render Engine are listed, and that those servers are set to Engine Type **Render Engine**.
6. In the **Configured** column, select each server with role of Render Engine, with Engine Type **Render Engine**.

   You must save settings at initial install/config and any time a GV STRATUS server with an Engine Type role is added, removed, or modified in SiteConfig.
7. Click **Save**.

   Settings are saved to the selected GV STRATUS servers.

Verify that devices are configured properly

Within the Control Panel application, do the following to verify systems and tools are ready for configuration. Grass Valley recommends the GV STRATUS Control Panel is only configured on the Core server:

- In the GV STRATUS Control Panel, do one or both of the following:
  - If your system has a K2 SAN, click **Core | K2 Storage | K2 SAN Storage** and verify that the information for the K2 SAN is the same information that is in K2Config. If the information is the same, it means that the Control Panel application is correctly reading the information from the K2Config application.
  - If your system has a standalone K2 Summit system, K2 SAN, K2 Central or Third Party Storage system, you must reconfigure MDI settings of all K2 Summit Standalone, K2 SAN, K2 Central, and Third Party Storage systems in this release. The Summit MDI Type has been renamed to **Grass Valley Media Server** in the MDI Configuration settings within GV STRATUS Control Panel.
  - If your system has a K2 SAN, K2 Central or Third Party Storage system, you must enter the Secondary Device in the MDI configuration. For optimum system performance it is recommended that if there are K2 Summit Clients, use them for the primary and secondary device. If there is only one client, use the client as the primary device and the FSM/Storage Manager as the secondary device. If it is shared storage with no attached K2 Summit clients, configure the primary FSM or Storage Manager as the primary device and the secondary FSM (if exists) or FTP Server as the secondary device.
  - If your system has a standalone K2 Summit system, verify the UNC Path in the standalone Grass Valley Media Server MDI configuration in **Core | MDI Configuration | Managed Devices**. Then, click **Core | K2 Storage | K2 Standalone Storage** and verify that the information for the K2 Summit system is the same information that is in SiteConfig. If the information is the same, it means that the Control Panel application is correctly reading the information from the SiteConfig application.
  - If your system has a GV I/O Live Ingest and Playback Server, configure the GV I/O channel formats in **General | Channels | GV I/O** to the desired formats configured in the **General | Format | Formats** settings.
- From each machine in the GV STRATUS system, verify that you can ping all the devices that the GV STRATUS server needs to communicate with over the control network.
- For the machines that need to communicate with a Proxy server, verify you can log in to that Proxy server using the credentials that the system will be using.
- If you exported an XML file backup of your GV STRATUS Rules before the upgrade, those rules cannot be used anymore once you upgrade to version 6.8 due to the new encryption support. You must import the XML file backup into GV STRATUS system after the upgrade. Then, export your rules again and re-import them to enable the encryption.
- The GV STRATUS database is automatically indexed to support enhanced search features. During this time, Search features and Rules are not fully functional. In GV STRATUS Control Panel, click **Core | Search Index Config** to view indexing progress.
- Begin by configuring STRATUS Core Services settings and move on to other settings.

After automatic re-index completes, reboot system in the correct order and verify that the GV STRATUS-EDIUS system is working.

NOTE: If prompted for a Java update, upgrade to the latest version of Java software to ensure you have the latest security updates.

Related Topics

About Control Panel, SiteConfig, and K2Config settings on page 433

Upgrade GV STRATUS system with the DIVA Category Update Utility

- The GV STRATUS software must have been upgraded on the GV STRATUS Core server.
- There are no currently processing or running archive/restore workflows between DIVA archive and the GV STRATUS system.

This task applies to the following:

- The GV STRATUS Core server

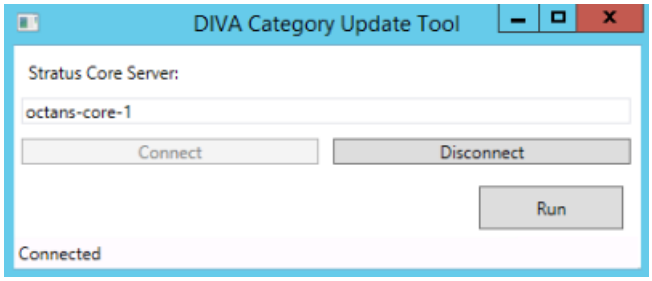
The `DivaCategoryUpdateUtility.exe` must be run on the GV STRATUS Core server after upgrading GV STRATUS software if you have DIVA archive in your system. Running the tool ensures existing GV STRATUS assets' associations paths are updated with the newly supported multiple DIVA categories.

1. Log on to the GV STRATUS Core server as an Administrator.
2. Locate the following file:

   `C:\Program Files\Grass Valley\STRATUS MDI DIVA\DivaCategoryUpdateUtility.exe`

   This file is copied to the GV STRATUS Core server during software deployment.
3. Run the `DivaCategoryUpdateUtility.exe` to update DIVA categories to assets' association paths in your GV STRATUS system.

   The **DIVA Category Update Tool** opens.
4. Enter the name of the GV STRATUS Core server and click **Connect**.

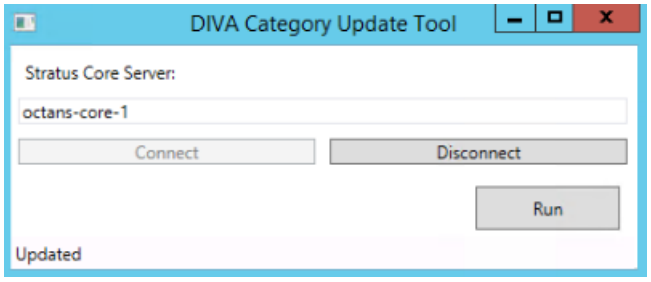


   If there are any conflicts, the **Resolve Conflict** section will be displayed.
5. Ensure the Name, Metadata ID (URN), and Category columns are shown (in that order), with a drop-down list in the Category column for users to select a DIVA category.

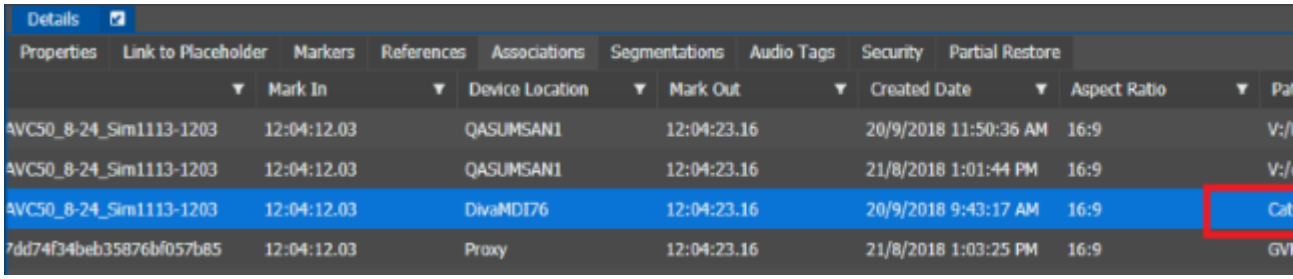
6. Do one of the following:

   - Resolve any conflicts by assigning the correct DIVA category to assets. Then click **Run**.
   - If there are no conflicts, just click **Run**.

   The process is completed when the status changes to **Updated** in the DIVA Category Update Tool.



With a successful run of the DIVA Category Update Utility, the DIVA Category and Disk Array name will be displayed in the **Path** column of the Associations tab when you load a DIVA archived asset into the Inspector.



Upgrade GV STRATUS Rundown and VTR Ingest systems

- K2 systems must be upgraded to the compatible version of K2 system software.
- GV STRATUS systems must be upgraded to the compatible versions of software.
- Grass Valley Prerequisite Files must be installed on the control point PC.

Upgrade your GV STRATUS Rundown and GV STRATUS VTR Ingest systems to the compatible versions of software. Refer to related topics in GV STRATUS Rundown and GV STRATUS VTR Ingest upgrade procedures.

Related Topics

Upgrading GV STRATUS Rundown systems on page 173
Installing and Upgrading GV STRATUS VTR Ingest/GV STRATUS VTR Controller on page 181

Make recovery images of servers

After you have upgraded software as instructed in these procedures and verified that your system is working properly, you should always make a recovery image of each of your upgraded computers. Use a sequence of tasks similar to those you followed for upgrading software so that as you take systems offline you manage redundancy, servers, and clients, as appropriate for your system.

Refer to the Grass Valley product's *Service Manual* for recovery image procedures.

Upgrading GV STRATUS from version 6.0 to version 6.8 with K2 Summit version 9.8.7

Follow the topics in the section sequentially to perform the upgrade.

Summary of upgrade from version 6.0 to version 6.8

Several upgrade tasks are new or require special consideration with this upgrade. Apply upgrade tasks as appropriate for your system design, as follows:

- All systems:
  - SiteConfig: Before upgrading GV STRATUS, upgrade your SiteConfig application and Discovery Agent to the latest version. For more info, refer to *Grass Valley products compatible with GV STRATUS* on page 56.
  - Password encryption: To enable password encryption in GV STRATUS system after the software upgrade, you must run the Key Upgrade Utility on the GV STRATUS Core server. For more info, refer to *Upgrade GV STRATUS system with the Key Upgrade Utility* on page 90.
  - Summit MDIs: Summit MDI has been renamed to **Grass Valley Media Server** MDI type in the MDI Configuration settings of GV STRATUS Control Panel. You must reconfigure MDI settings for all K2 Summit Standalone, K2 SAN, K2 Central, and Third Party Storage systems in this release. For more details, refer to *Grass Valley Media Server MDI standalone settings* on page 304, *Grass Valley Media Server MDI SAN settings* on page 306, *GV STRATUS Control Panel configuration for K2 Central* on page 937, and *GV STRATUS Control Panel configuration for SMB storage* on page 930.
  - GV STRATUS Proxy Streaming Server, GV STRATUS External Media Engine, and GV I/O Live Ingest and Playback Server SiteConfig roles: These new SiteConfig roles must be assigned to Express/Core server before upgrading the GV STRATUS system, if applicable. For more details, refer to *Add software roles for upgrade to version 6.8* on page 82, *SiteConfig Proxy Streaming Server software install* on page 909, and *SiteConfig External Media Engine software install* on page 820.
  - Simple Editor and Advanced Editor: After the upgrade, existing users and groups do not have these roles assigned in GV STRATUS Control Panel, so you must assign the role if needed. If you create new users and groups, the new role must be added or removed if appropriate. For more info, refer to *GV STRATUS roles matrix* on page 37.
  - GV STRATUS External Media Engine: GV STRATUS supports the deployment of External Media Engine on the GV STRATUS Core server, Workflow Server, or a separate server, to publish content and metadata to popular social media networks (such as Facebook, Twitter, and YouTube) via Social Media CMS-Systems. For more info, refer to *External Media Engine Server set up process* on page 819.
  - GV STRATUS Proxy Streaming Server: GV STRATUS introduces the Proxy Streaming Server which supports frame accurate playback of proxy files in GV STRATUS Web Clients within an HTML5 standard browser. For more info, refer to *Proxy Streaming Server set up process* on page 907.
  - GV I/O Live Ingest and Playback Server: GV STRATUS introduces the GV I/O Live Ingest and Playback Server, a commodity hardware solution to support record and playback with up to four Recorder/Player channels, and baseband HD-SDI support via an on-board video card on standard IT hardware. For more info, refer to *Installing GV I/O Live Ingest and Playback Server* on page 1634.
  - DIVA Archive categories: GV STRATUS supports multiple DIVA archive categories with this release. The Diva Category Update Utility must be run on the GV STRATUS Core server after the software deployment. For more info, refer to *DIVA Categories Add/Modify Field settings* on page 310 and *Upgrade GV STRATUS system with the DIVA Category Update Utility* on page 99.
  - GV STRATUS Rules Backup: If you exported an XML file backup of your actual rules before the upgrade, those rules cannot be used anymore once you upgrade to version 6.8 due to the new encryption support. You must import the XML file backup into GV STRATUS system

after the upgrade. Then, export your rules again and re-import them to enable the encryption. For more info, refer to *Exporting rules* on page 641 and *Importing rules* on page 642.

- Microsoft Visual C++ Redistributable for VS 2017 install: All GV STRATUS servers, K2 Summit systems, and all client PCs hosting GV STRATUS application and/or EDIUS applications must install Microsoft Visual C++ Redistributable for VS 2017. For more details, refer to *Upgrade Microsoft Visual C++ Redistributable for VS 2017* on page 78.
- Microsoft .NET upgrade: All GV STRATUS servers, K2 Summit systems, and K2 Media servers must upgrade to .NET 4.7.1, if that version of .NET is not already installed. For more details, refer to *Upgrade Microsoft .NET* on page 79.
- Internal system account: If the internal system account for your GV STRATUS system is on a fully qualified domain or is not the default GVAdmin account, configure settings at GV STRATUS Control Panel **Core | STRATUS Core Services | Primary Site** as appropriate for your system.

- Systems with Windows 2008 servers:
  - Requires an upgrade to Windows 2012 or Windows 2016 operating system. For more details, refer to *Upgrade GV STRATUS server OS from Windows 2008/2012 to Windows 2016* on page 92.

Make recovery images of servers

Do not do this task if:

- You previously made a recovery image at the current software version for each computer you are upgrading.

Do this task if:

- You do not have a recovery image at the current software version for one or more of the computers you are upgrading.

The recommended procedure is to make a recovery image immediately after a software upgrade. If you neglected to do this when you last upgraded software you should make the recovery image now, before upgrading to the new version.

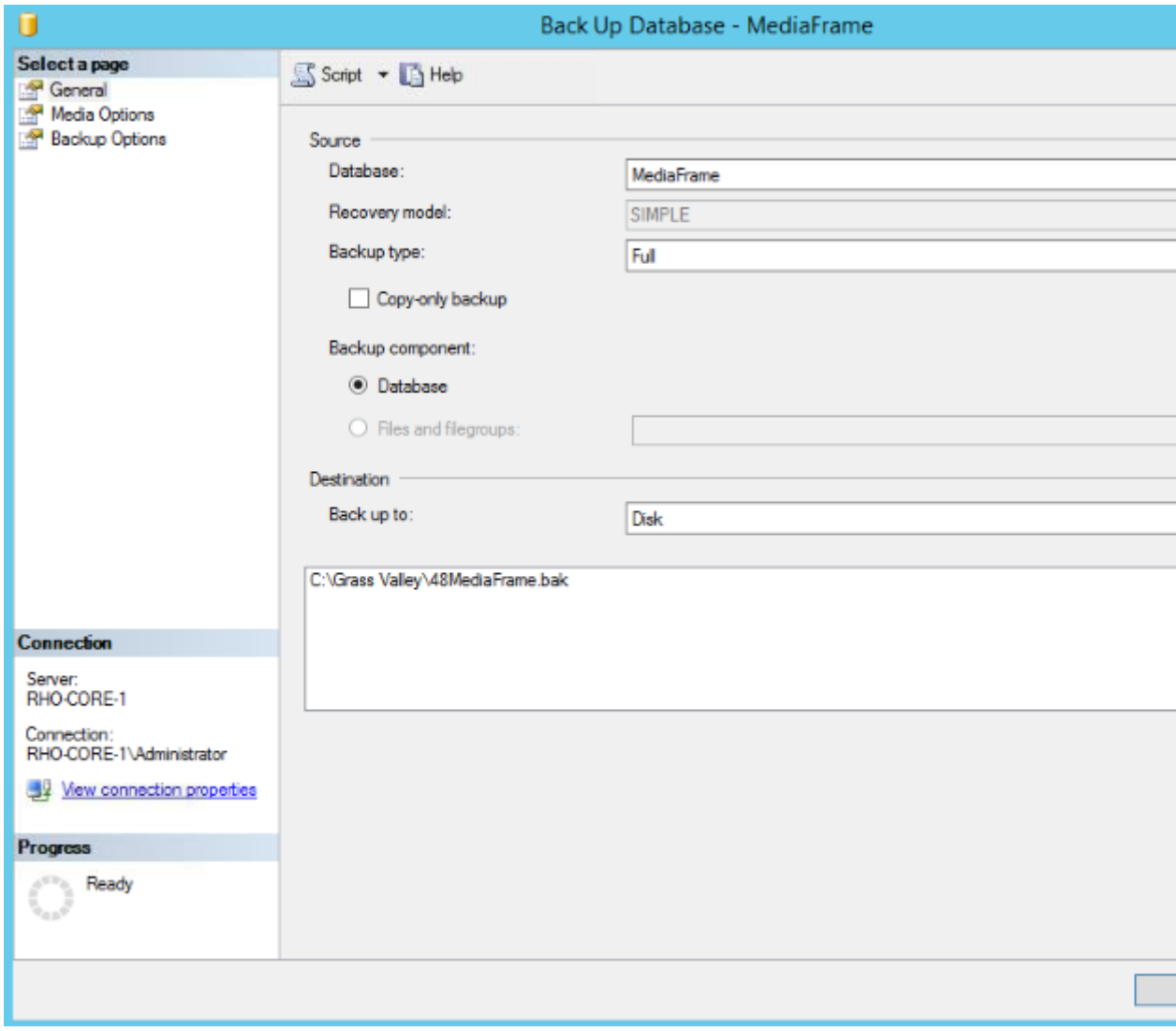
⚠ ***CAUTION: If you upgrade and then decide you do not want to stay with this version of software, you must use the recovery disk image process to downgrade to your previous version.***

Backing up a database

Grass Valley recommends that you back up all the databases of the GV STRATUS system before upgrading to the latest version of the software or before moving your databases from the GV STRATUS Core server to a standalone Database Server. With a database backup, you can avoid any lost of feed schedules and the need to key in everything again in case of a system crash. The backup could also be placed on another machine or an external drive for extra precaution.

1. Open and log in to Microsoft SQL Server Management Studio.

2. In the tree-view expand the **Databases** node and identify the databases of the GV STRATUS system to backup, which are the following:
   - ISDB
   - MediaFlow
   - MediaFrame
   - RulesEngine
   - WfPersistence
3. Right-click on a database and select **Tasks | Back Up**.



4. On the General page, select a database to be backed up from the **Database** drop-down list.
5. Select **Full** on the **Backup type** drop-down list.
6. In the Destination section, click **Add** and select the backup destination.
7. On the Media Options page, select **Back up to the existing media set** and **Overwrite all existing backup sets**.
8. On the Backup Options page, enter the name of the backup database.

9. Click **OK**.
10. Repeat for other databases of the GV STRATUS system that you are backing up.

Replace the CompactFlash Card

K2 Summit clients and K2 Standalone servers must be either 3G or have the 32 GB Flash card installed before installing Windows updates.

Do not do this task if you have:

- A K2 Summit 3G system with mSATA system drive.

Do this task if you have:

- A K2 Summit system with CompactFlash system drive.

1. Backup the K2 Summit using Acronis.
2. Replace the 16-GB flash card with a 32-GB flash card.
3. Restore the K2 Summit image using Acronis and verify that the C: drive is over 27 GB in size.

Upgrade Microsoft Visual C++ Redistributable for VS 2017

This task applies to the following:

- All types/roles of GV STRATUS servers.
- Client PCs hosting one or more of the following:
  - GV STRATUS
  - GV STRATUS Control Panel
  - EDIUS XS
  - EDIUS Workgroup

This task does not apply to the following:

- K2 Summit systems, as they should have only Microsoft Visual C++ Redistributable for VS 2015 installed

1. From the Windows Start menu navigate to **Control Panel | Programs and Features** and check for the following:

   Microsoft Visual C++ Redistributable for VS 2017

   - If Microsoft Visual C++ Redistributable for VS 2017 is already installed, do not do the remainder of this task.
   - If Microsoft Visual C++ Redistributable for VS 2017 is not installed, continue with this procedure.

2. Procure the **Microsoft Visual C++ Redistributable for VS 2017** installation file from the *Microsoft software download page* or the Grass Valley FTP site.

3. Select the installation file(s) as follows:
   - For servers and Windows 64-bit OS client PCs, select the following:
     - vc_redist.x64.exe
     - vc_redist.x86.exe
   - For Windows 32-bit OS client PCs, select the following:
     - vc_redist.x86.exe
4. Run the installation file and install as directed by the installation wizard.

Upgrade Microsoft .NET

Do not do this task if:

- The system has Microsoft .NET Framework 4.7.1 installed

Do this task if:

- The system does not have Microsoft .NET Framework 4.7.1 installed

This task applies to the following:

- K2 Summit systems
- All types/roles of GV STRATUS servers

1. On the computer, check Windows Control Panel **Programs and Features** for currently installed .NET version(s), then proceed as follows:
   - If Microsoft .NET 4.7.1 is installed, skip this task.
   - If Microsoft .NET 4.7.1 is not installed, continue with this procedure.
2. Procure the Microsoft .NET 4.7.1 installation file from the *Microsoft software download page* or the Grass Valley FTP site.
3. Run the installation file and install Microsoft .NET 4.7.1 as directed by the installation wizard.

Install Important Windows updates (required)

Grass Valley requires the installation of all Microsoft Windows Important updates on all GV STRATUS client and server devices, except as specifically instructed otherwise by Grass Valley.

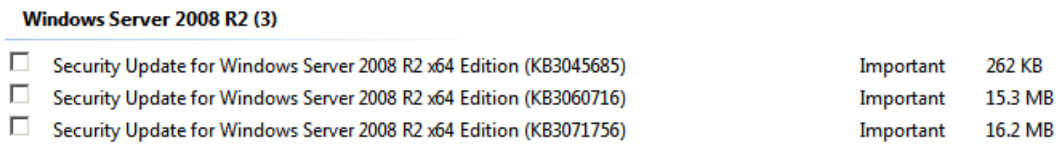
If a computer does not have the Grass Valley Embedded Security solution one-time initial deployment process applied, do not install any Windows updates. Apply the one-time process before installing Windows updates.

⚠ ***CAUTION: Only "Important Updates" should be installed. Do not install other Windows or driver updates unless specifically directed by product documentation or by Grass Valley Support.***

Prerequisite: Always install the required Microsoft Visual C++ redistributable update before installing the latest Windows Important Updates.

1. Go to **Start | Control Panel | Windows Updates | Check for updates**.

2. If these updates appear, right-click on them and select **Hide update**.



3. Install other “Important Updates”.
4. Reboot all GV STRATUS client and server devices after installing those Windows updates.

Related Topics

Deploy Embedded Security solution - One-time process

Prepare for upgrade

Before upgrading, do the following:

- Procure the software installation files for this release via the appropriate distribution method, such as download, network drive, or external drive.
- Export all configured rules to avoid recreating them from scratch after the upgrade.
- Stop all media access on the devices you are upgrading.
- Shut down all applications on the devices you are upgrading. This includes the SDB Server if you have GV STRATUS Rundown in your operation.
- Terminate all users’ sessions using the GV STRATUS Control Panel.

Prepare SiteConfig for software deployment

If a newer version of SiteConfig is available, you must upgrade to the latest version. For more info, refer to *Grass Valley products compatible with GV STRATUS* on page 56.

Do the following to prepare SiteConfig for the software upgrade.

1. If a newer version of SiteConfig is available for upgrade and you have not yet upgraded SiteConfig, do the following:
   a) From Windows **Programs and Features**, uninstall the current version of SiteConfig from the control point PC.
   b) Install the new version of SiteConfig on the control point PC.
2. After the installation is complete, click **Finish** and launch the SiteConfig application.
3. Next, configure the deployment group.

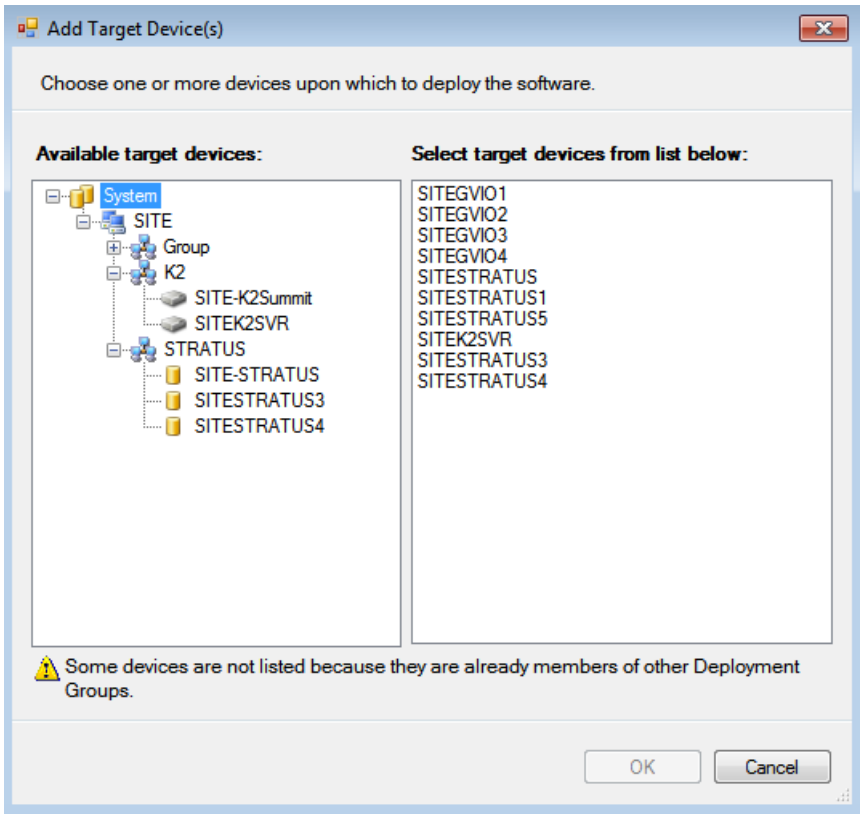
Configuring deployment groups

- The device must be assigned in the SiteConfig system description and network connectivity must be present.
- GV STRATUS systems containing mixed K2 Summit versions of 9.8 and 10.1 will require at least two separate deployment groups, one for K2 Summit 9.8.x system and one for K2 Summit 10.x system.

1. In the **Software Deployment | Deployment Groups** tree view, right-click the top node and select **Add Deployment Group**.

   A deployment group appears in the tree view.

2. Right-click the deployment group, select **Rename**, and enter a name for the deployment group.
3. Right-click the deployment group and select **Add Target Device**.
   The Add Target Device(s) wizard opens.



4. In the Available Target Devices tree view, select the node that displays the devices that you are combining as a deployment group.
5. In the right-hand pane, select the devices that you are combining as a deployment group.
   To select multiple devices, you can drag through the devices, use Ctrl + Click, or use Shift + Click.
6. Click **OK**.

The devices appear in the Deployment Groups tree view under the deployment group. Before you perform a software deployment, you must check software on the devices that will be receiving new software. If you have already added packages to the group, on the Deployment Groups tab you will also see deployment tasks generated for every device with roles that match the package contents.

Upgrading the Discovery Agent

If a newer version of SiteConfig Discovery Agent is available, you must upgrade to the latest version. For more info, refer to *Grass Valley products compatible with GV STRATUS* on page 56.

1. On the device you plan to manage with SiteConfig, open the Windows Services Control Panel and look for the following required item:
   - SiteConfig Discovery Agent

2. Check the version number of the SiteConfig Discovery Agent.
   - If the latest version is installed, skip this task.
   - If the latest version is not installed, continue with this procedure.
3. In order to upgrade Discovery Agent on all your devices, add only the DiscoveryAgent cab to your deployment group(s).
4. Click the **Start Deployment** button.

   Deployment tasks run and software is uninstalled. Progress is reported and next steps are indicated in both the Status and Details columns.
5. When the Uninstall task completes, set Restart to Complete when the **Restart required** option displays on SiteConfig.

   NOTE: This is to prevent Siteconfig from losing its connection with any of your devices during the Uninstall/Install process. If the connection is lost, you will need to install Discovery Agent manually and perform a check software on the device(s) in order to sync them up with Siteconfig.
6. Once the DiscoveryAgent cab is installed, click the "Restart required" option to restart the server.

Add software roles for upgrade to version 6.8

Before doing this task, make sure devices are added to the SiteConfig system description with the correct family and device type. Refer to *Complete listing of device types, roles, and software packages for GV STRATUS devices* on page 194.

For your K2 Summit systems, make sure you have separate deployment groups for the upgrade to version 9.8.x and version 10.1.x if you have both versions in your operation.

NOTE: If upgrading to K2 Summit version 10.1.x, you cannot use Siteconfig to directly upgrade from SNFS 4.7 to SNFS 6.0 on FSMs and K2 Standalone Summits. Refer to Upgrading to SNFS 6.0 on page 87 before proceeding, if applicable.

These SiteConfig roles are new or require special consideration with this software upgrade. Verify and add roles if necessary.

1. As appropriate for your system design and licensing, in your SiteConfig system description, configure as follows:
   - For your GV STRATUS Express Server, or Core Server, add the new device as follows:
     - GV STRATUS Proxy Streaming Server (optional)

       These new roles will be automatically added:

       - GV STRATUS Proxy Streaming Service
       - GV Embedded Security Manager
       - GV Log Manager
   - For your GV STRATUS Express Server, Core Server, Workflow Server or a separate server, add the new role as follows:
     - GV STRATUS ExternalMedia Engine (optional)
   - For your GV I/O Client - Standalone device, add the new device as follows:
     - GV I/O Standalone Device

       These new roles will be automatically added as follows:

       - GV STRATUS IO Appliance
       - GV Embedded Security Manager
       - GV STRATUS Summit Service
   - For your GV I/O Client - Shared Storage device, add the new device to Isilon system deployment group as follows:
     - GV I/O Client (SMB)

       These new roles will be automatically added as follows:

       - GV STRATUS IO Appliance
       - GV Embedded Security Manager

   NOTE: GVEngine and MPIcore must be manually installed on any GV I/O device(s). The installation files can be procured from the Grass Valley FTP site.

2. Save SiteConfig and verify in `C:\ProgramData\Grass Valley\ConfigurationDataFiles\SiteConfig` that .scsd and .config files are saved to the Core server.

If you want to verify all your currently configured SiteConfig roles, refer to the complete list of roles and software packages.

Add software package to deployment group for GV STRATUS and other devices

- The GV STRATUS devices to which you are deploying software must have their SiteConfig roles correctly configured.
- The GV STRATUS devices to which you are deploying software must be in a deployment group.
- The following software upgrade system cab files apply to all deployment groups.
  - *GrassValley_STRATUSClient_X.X.X.XXX.cab*
  - *GrassValley_CoreServer_X.X.X.XXX.cab*
- The following software upgrade system cab files apply to K2 Summit 9.8.x devices. For each deployment group, choose the one that applies.
  - *GrassValley_K2system_X.X.X.XXX.cab*
- The following software upgrade system cab file apply to K2 Summit 10.x devices. For each deployment group, choose the one that applies.
  - *GrassValley_K2Plus_X.X.X.XXX.cab*
- The following software upgrade system cab files apply to GV I/O devices, if already added as a standalone device or a shared storage client with Dell EMC Isilon network-attached storage system.
  - *GrassValley_GVIO_X.X.X.XXX.cab*

  NOTE: Next, you must manually run the GVEngineInstaller-x.x.x.xxx_xxxxx_xxx.exe and MPIcore on each GV I/O device in your operation. The installation files can be procured from the Grass Valley FTP site.

1. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.
2. Click the **Add** button.

   The Add Package(s) dialog box opens.
3. Do one of the following to select the software package:
   - Select from the list of packages then click **OK**.
   - Click **Browse**, browse to and select the package, then click **Open**.
4. If one or more EULAs are displayed, accept them to proceed. If you do not accept a EULA, the associated software is not assigned to the deployment group.

   SiteConfig adds the package to the deployment group.

The package appears in the Managed Packages list for the selected deployment group. SiteConfig creates new software deployment tasks for the package and displays them in the Tasks list view.

Related Topics

Complete listing of device types, roles, and software packages for GV STRATUS devices on page 194

Complete listing of device types, roles, and software packages for GV STRATUS devices on page 194

Setting deployment options

- A software package must be assigned to the deployment group and applicable deployment tasks must be displayed in the Tasks area.

1. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.
2. In the Tasks list view, view tasks and determine if you must set deployment options.

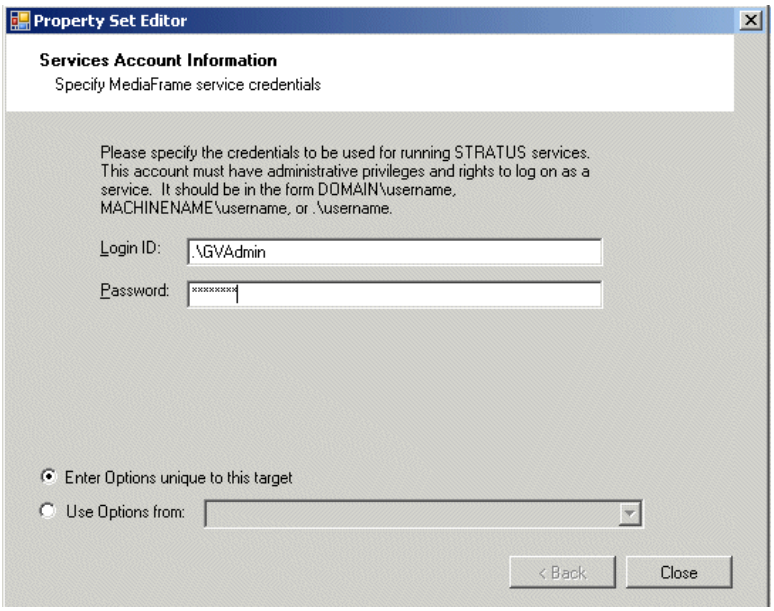
   Tasks that need to have deployment options set display in the Details column a message stating "Deployment options required."

   If you select a task that needs to have its deployment options set, the Start Deployment button is disabled and the message is displayed next to the button.
3. Do one of the following to set deployment options:

   - Double-click the task.
   - Select the task and click the **Options** button.

   A wizard opens.

4. Work through wizards and set deployment options for GV STRATUS software as follows:

Software	Deployment options
GrassValley_STRATUS_CommonServices GrassValley_STRATUS_ControlPanelService GrassValley_STRATUS_CoreServices GrassValley_STRATUS_CRArchive_MDI GrassValley_STRATUS_Databases GrassValley_STRATUS_DataMover GrassValley_STRATUS_DIVA_MDI GrassValley_STRATUS_ExternalMedia GrassValley_STRATUS_FlashNet_MDI GrassValley_STRATUS_GFTP_MDI GrassValley_STRATUS_HttpProxyServer GrassValley_STRATUS_IngestServices GrassValley_STRATUS_Masstech_MDI GrassValley_STRATUS_MediaFlow GrassValley_STRATUS_MEWS GrassValley_STRATUS_Proxy_MDI GrassValley_STRATUS_ProxyStreamingService GrassValley_STRATUS_RenderEngine GrassValley_STRATUS_Rules GrassValley_STRATUS_ScheduledTransferEngine GrassValley_STRATUS_SocialMedia GrassValley_STRATUS_Summit_MDI GrassValley_STRATUS_TrafficGateway GrassValley_STRATUS_Transcode GrassValley_STRATUS_WebApps GrassValley_STRATUS_WebClient GrassValley_DeviceKeyService GrassValley_LogManager GrassValley_LogViewer	 Use the local system account if your system is on a workgroup or if it's on a domain but uses the local system account in SQL. Use a domain\admin account if the account was previously mapped in SQL to the MediaFrame, MediaFlow, RulesEngine and WFPersistence databases. Entering account credentials allows you to use the **Use options from** feature for all other devices of the same type. Once you enter the account credentials this way on the first device, it becomes the template from which options for other devices are copied.

5. If you have multiple devices of the same type, you can enter deployment options for one of them using the wizard. Then, when you bring up the same wizard on every device, you can choose the **Use options from** radio button and select the first device for which you set options.

   SiteConfig copies the options you set for the first device and fills in the blanks on the wizard.

Upgrade software on GV STRATUS devices

- The devices that you are upgrading must be in a deployment group.
- For the software you are upgrading, a newer version of that managed software package must be added to the deployment group.
- A SiteConfig "Check Software" operation must be performed on the devices you are upgrading.
- All servers have been set to **Update mode** in the Embedded Security Manager.

If you are upgrading multiple software components for which there is a required sequence, you must check and uncheck tasks and run multiple deployment sessions to control the sequence. For some software components, SiteConfig aids you by enforcing dependencies. For each individual software component, SiteConfig enforces an uninstall of the current version of software before installing the upgrade version. SiteConfig provides uninstall deployment tasks and install deployment tasks to indicate the taskflow. SiteConfig can do the uninstall/install in a single deployment session.

1. In the **Software Deployment | Deployment Groups** tree view, select the device or the group of devices to which you are deploying software.

   The corresponding software deployment tasks are displayed in the Tasks list view.

2. For the software you are deploying, do the following:

   a) Select the **Deploy** check box in the row for the uninstall task.

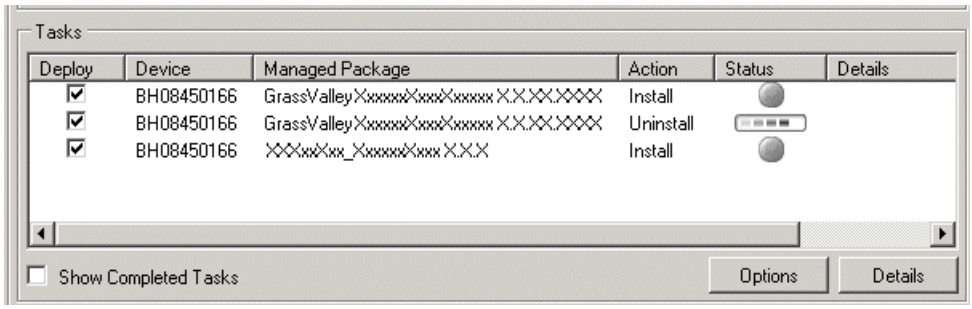
   b) Select the **Deploy** check box in the row for the install task.

   If a WFRegMon install task appears, install it as well. It is required to support Grass Valley software installers. There is no uninstall task.

3. Check the area next to the Start Deployment button for a message.

   If a message instructs you to upgrade the Discovery Agent, on the control point PC go to the directory to which SiteConfig is installed, find the `DiscoveryAgent_x.x.x.x.cab` file, add it to the deployment group, and deploy the Discovery Agent software as well.

4. Click the **Start Deployment** button.



Deployment tasks run and software is uninstalled. Progress is reported and next steps are indicated in both the Status and Details columns. If an error appears regarding prerequisite software, install the Grass Valley Prerequisite Files on the control point PC and then repeat this step.

SiteConfig uninstalls/install software in the proper sequence.

5. When the Status or Details columns indicate next steps, identify the software in the row, then do one of the following:
   - If Details displays a **Restart required** link (but not "Visible dialog pending..."), click the link and when prompted "...are you sure...", click **Yes**.
   - If Details does not display any indication of additional steps required, proceed with the next step in this task.
6. Monitor progress as indicated by both the Status and Details column. When finished, the Status column indicates complete.
7. Shutdown the entire GV STRATUS/K2 Summit system and power up the servers in the correct order, starting the required services as needed.
8. Set all servers back to **Enabled mode** in the Embedded Security Manager.
9. If you deployed the MEWS Service, after deployment is complete, start the MEWS Service.

Related Topics

Upgrade GV Render Engine server software and EDIUS client software on page 148

Upgrade K2/Summit/SAN systems that are accessed by the GV STRATUS system

- You have procured the necessary software and documentation for the upgrade. Go to *Grass Valley products compatible with GV STRATUS* on page 56 and determine the compatible software versions required.
- All standalone K2 Summit systems must be offline (all media access stopped) and shut down. The power must be off for a few seconds before switching it on again.
- If upgrading a K2 SAN, all SAN clients must be offline (all media access stopped) and shut down. The power must be off for a few seconds before switching it on again. Depending on your system design, this could include devices such as SAN-attached K2 Summit systems, GV STRATUS servers, and GV STRATUS Client PCs.

NOTE: When upgrading from a K2 software version lower than 9.x to a K2 software version at 9.x or higher, you must reimage each* K2 Summit system*. Hardware upgrades might also be required on a* K2 Summit system*.

1. Upgrade your K2 systems to the compatible version of K2 system software. This includes K2 SAN systems and stand-alone K2 Summit systems.

   When upgrading for compatibility with GV STRATUS, use `GrassValley_K2system_x.x.x.cab` file, which contains the required `GrassValley_STRATUS_SummitServices_x.x.x.cab` file.
2. On systems running Embedded Security, do the one-time initial deployment process for the Embedded Security solution, if you have not already done so.
3. Update K2 Summit licenses.

About deploying software for the K2 SAN

You must control the sequence of software deployment tasks and device restarts as you upgrade software across the K2 SAN. The general sequence is to upgrade K2 Media Servers first then the SAN-attached K2 systems. The exact steps can vary from software version to version. Make sure you follow the task flow in the *K2 Release Notes* for the version of software to which you are upgrading.

Related Topics

Installing GV STRATUS application with SiteConfig on page 280

Upgrade GV STRATUS Database

This task applies to the following:

- The GV STRATUS server with the role of GV STRATUS Database.

Before doing this task, do the following:

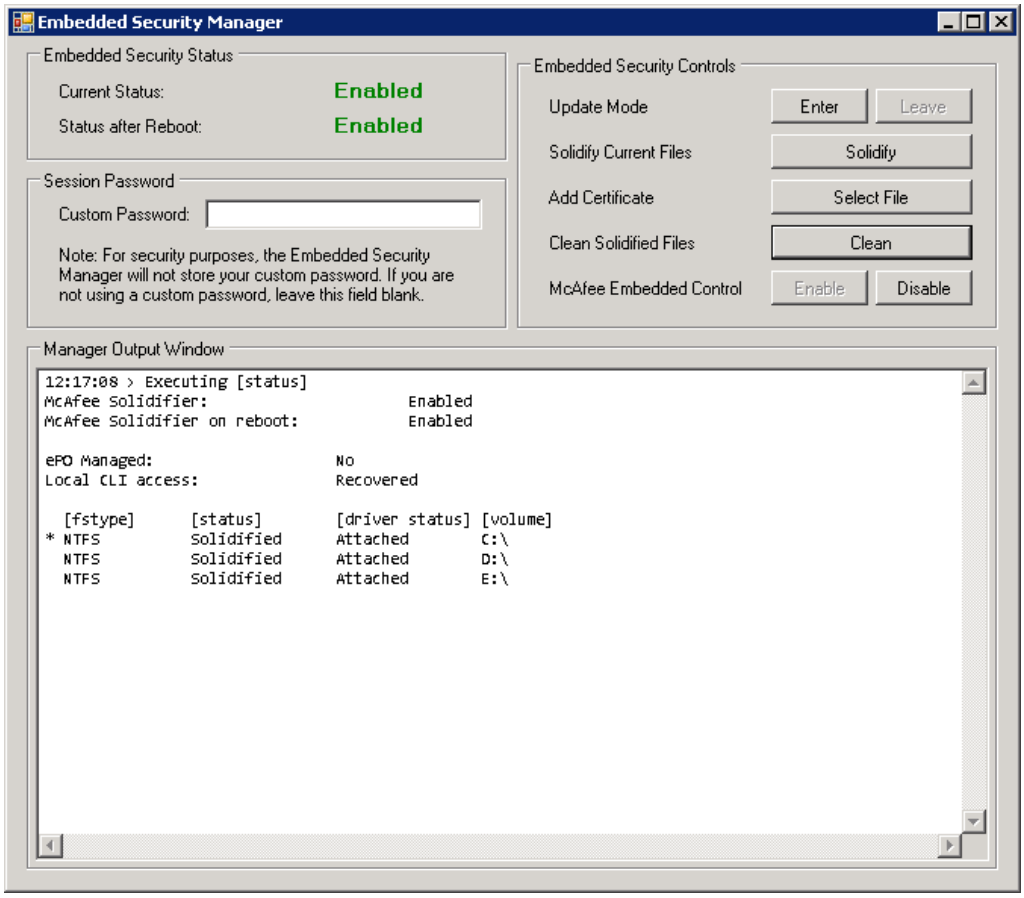
- Upgrade software on the GV STRATUS server.

This task upgrades the GV STRATUS database.

1. Log on to the GV STRATUS server as Administrator.

2. From the Windows desktop, click **Start | All Programs | Grass Valley | Embedded Security Manager**.

   Embedded Security Manager opens.



3. If Current Status is **Enabled**, click **Enter** in the Embedded Security Controls section to put it in **Update Mode**.
4. Locate the following file:

   `C:\Program Files\Grass Valley\STRATUS Databases\MediaFrameDbUpgrade.exe`

   This file is copied to the GV STRATUS server along with the software upgrade.
5. Double-click `MediaFrameDbUpgrade.exe` to upgrade the database.
6. Reboot the GV STRATUS server.

A "The database upgrade completed successfully" message displays.

Related Topics

Standalone Database Server set up process on page 829

Upgrade GV STRATUS system with the Key Upgrade Utility

This task applies to the following:

- The GV STRATUS Core server

Before upgrading, do the following:

- Disable any currently active rules on the GV STRATUS Control Panel.
- Make sure there are no currently processing or running workflows on the GV STRATUS system.

Before running the utility, do the following:

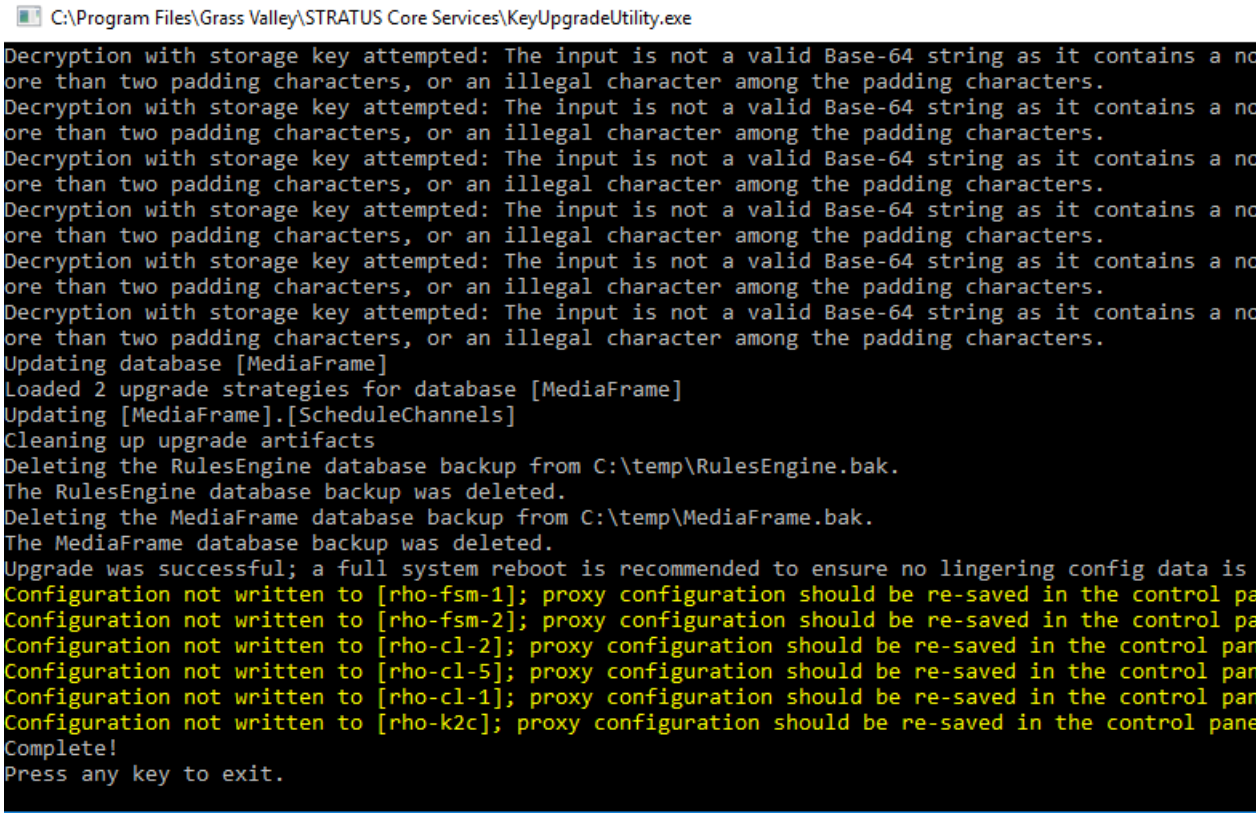
- Upgrade GV STRATUS software on the GV STRATUS Core server.
- Upgrade the GV STRATUS database.
- Restart the GV STRATUS Core server.

1. Log on to the GV STRATUS Core server as an Administrator.
2. Locate the following file:

   `C:\Program Files\Grass Valley\STRATUS Core Services\KeyUpgradeUtility.exe`

   This file is copied to the GV STRATUS Core server along with the software upgrade.
3. Run the `KeyUpgradeUtility.exe` to upgrade the encryption keys on your GV STRATUS Core server.

   Note any yellow messages in the output and take the requested action; these will occur at the end of the utility execution.



   The process is successful when the **Complete!** message displays at the end of the output.
4. In the **Proxy Config | Proxy Settings** tab in GV STRATUS Control Panel, re-check the **Enable Proxy Creation** setting and click **Save**.

   Verify all pop-ups succeed before continuing.

5. Reboot the GV STRATUS Core server.
6. Re-enable any rules that were disabled earlier.
7. Procure and run the *EngineConfig_6_8.cmd* file where any of the following engines are installed and running:
   - DataMover Engine
   - Transcode Engine
   - Workflow Engine
   - Rules Engine
   - Social Media Engine
   - External Media Engine

SabreTooth license process

GV STRATUS licenses are installed on the GV STRATUS server with role of Common Services. Typically the GV STRATUS Core server has the role of Common Services.

1. Refer to the license sheet that you received with your GV STRATUS license. The license sheet has the Sales Order number that you need.
2. On the GV STRATUS server with role of Common Services, run the SabreTooth License Manager, generate a unique ID, and send the email to Grass Valley requesting your license or licenses.

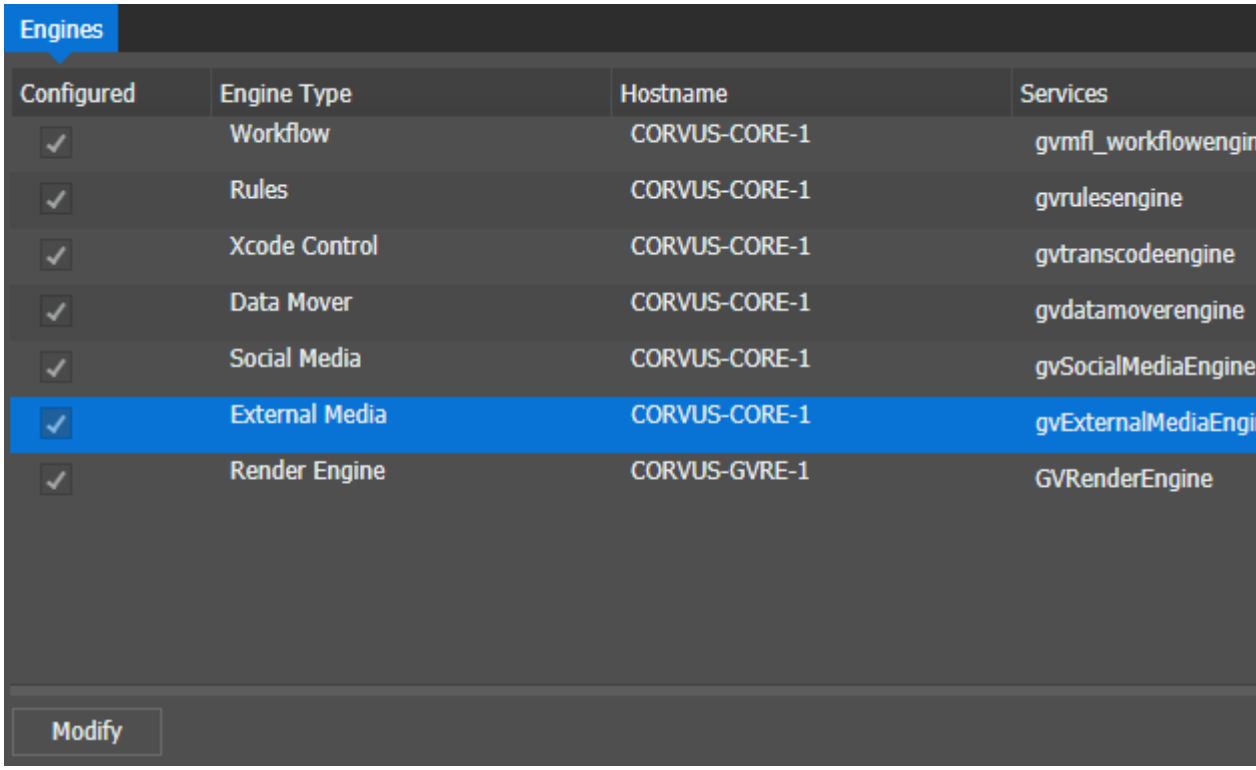
   Refer to this Topic Library for detailed licensing procedures.
3. When you receive your license file, use SabreTooth License Manager and install it on the server.
4. Repeat steps as appropriate to install licenses on other devices.

Verify GV STRATUS Engines are running

After upgrading software, make sure the GV STRATUS Engine services are running. This is especially important if you added a SiteConfig role that installs a type of Engine software or otherwise made a change that could affect Engine software as part of the upgrade.

1. In GV STRATUS Control Panel, click **Core | Engines.**

   Engine settings open.



2. Make sure that in the **Configured** column the Engine is selected.
3. Make sure that in the **Action** column the **Stop** icon is displayed.

   This indicates the Engine service is playing.
4. Make sure that the **Status** column reports **Running**.
5. Verify that GV STRATUS servers with role of Render Engine are listed, and that those servers are set to Engine Type **Render Engine**.
6. In the **Configured** column, select each server with role of Render Engine, with Engine Type **Render Engine**.

   You must save settings at initial install/config and any time a GV STRATUS server with an Engine Type role is added, removed, or modified in SiteConfig.
7. Click **Save**.

   Settings are saved to the selected GV STRATUS servers.

Verify that devices are configured properly

Within the Control Panel application, do the following to verify systems and tools are ready for configuration. Grass Valley recommends the GV STRATUS Control Panel is only configured on the Core server:

- In the GV STRATUS Control Panel, do one or both of the following:
  - If your system has a K2 SAN, click **Core | K2 Storage | K2 SAN Storage** and verify that the information for the K2 SAN is the same information that is in K2Config. If the information is the same, it means that the Control Panel application is correctly reading the information from the K2Config application.
  - If your system has a standalone K2 Summit system, K2 SAN, K2 Central or Third Party Storage system, you must reconfigure MDI settings of all K2 Summit Standalone, K2 SAN, K2 Central, and Third Party Storage systems in this release. The Summit MDI Type has been renamed to **Grass Valley Media Server** in the MDI Configuration settings within GV STRATUS Control Panel.
  - If your system has a K2 SAN, K2 Central or Third Party Storage system, you must enter the Secondary Device in the MDI configuration. For optimum system performance it is recommended that if there are K2 Summit Clients, use them for the primary and secondary device. If there is only one client, use the client as the primary device and the FSM/Storage Manager as the secondary device. If it is shared storage with no attached K2 Summit clients, configure the primary FSM or Storage Manager as the primary device and the secondary FSM (if exists) or FTP Server as the secondary device.
  - If your system has a standalone K2 Summit system, verify the UNC Path in the standalone Grass Valley Media Server MDI configuration in **Core | MDI Configuration | Managed Devices**. Then, click **Core | K2 Storage | K2 Standalone Storage** and verify that the information for the K2 Summit system is the same information that is in SiteConfig. If the information is the same, it means that the Control Panel application is correctly reading the information from the SiteConfig application.
  - If your system has a GV I/O Live Ingest and Playback Server, configure the GV I/O channel formats in **General | Channels | GV I/O** to the desired formats configured in the **General | Format | Formats** settings.
- From each machine in the GV STRATUS system, verify that you can ping all the devices that the GV STRATUS server needs to communicate with over the control network.
- For the machines that need to communicate with a Proxy server, verify you can log in to that Proxy server using the credentials that the system will be using.
- If you exported an XML file backup of your GV STRATUS Rules before the upgrade, those rules cannot be used anymore once you upgrade to version 6.8 due to the new encryption support. You must import the XML file backup into GV STRATUS system after the upgrade. Then, export your rules again and re-import them to enable the encryption.
- The GV STRATUS database is automatically indexed to support enhanced search features. During this time, Search features and Rules are not fully functional. In GV STRATUS Control Panel, click **Core | Search Index Config** to view indexing progress.
- Begin by configuring STRATUS Core Services settings and move on to other settings.

After automatic re-index completes, reboot system in the correct order and verify that the GV STRATUS-EDIUS system is working.

NOTE: If prompted for a Java update, upgrade to the latest version of Java software to ensure you have the latest security updates.

Related Topics

About Control Panel, SiteConfig, and K2Config settings on page 433

Upgrade GV STRATUS system with the DIVA Category Update Utility

- The GV STRATUS software must have been upgraded on the GV STRATUS Core server.
- There are no currently processing or running archive/restore workflows between DIVA archive and the GV STRATUS system.

This task applies to the following:

- The GV STRATUS Core server

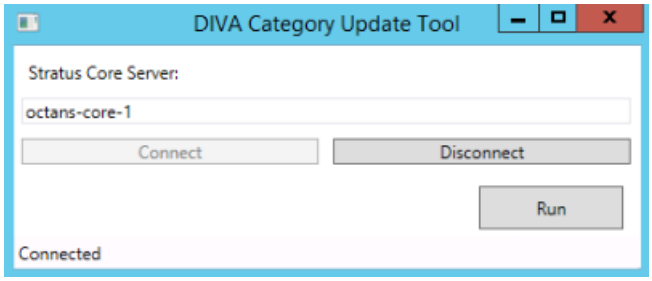
The `DivaCategoryUpdateUtility.exe` must be run on the GV STRATUS Core server after upgrading GV STRATUS software if you have DIVA archive in your system. Running the tool ensures existing GV STRATUS assets' associations paths are updated with the newly supported multiple DIVA categories.

1. Log on to the GV STRATUS Core server as an Administrator.
2. Locate the following file:

   `C:\Program Files\Grass Valley\STRATUS MDI DIVA\DivaCategoryUpdateUtility.exe`

   This file is copied to the GV STRATUS Core server during software deployment.
3. Run the `DivaCategoryUpdateUtility.exe` to update DIVA categories to assets' association paths in your GV STRATUS system.

   The **DIVA Category Update Tool** opens.
4. Enter the name of the GV STRATUS Core server and click **Connect**.

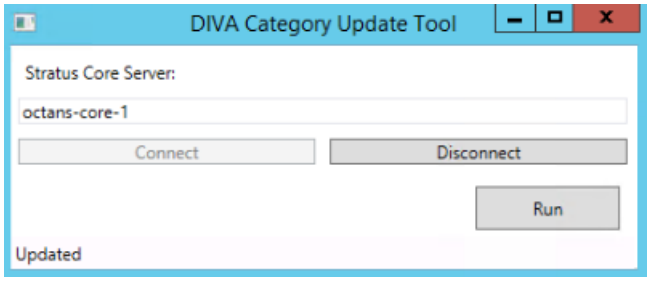


   If there are any conflicts, the **Resolve Conflict** section will be displayed.
5. Ensure the Name, Metadata ID (URN), and Category columns are shown (in that order), with a drop-down list in the Category column for users to select a DIVA category.

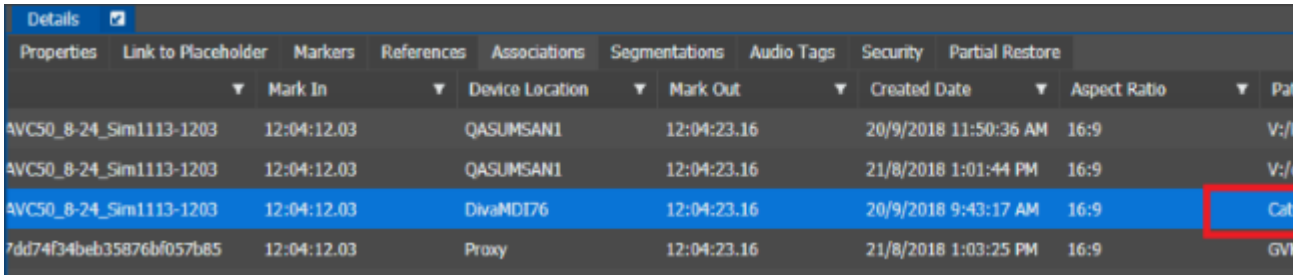
6. Do one of the following:

   - Resolve any conflicts by assigning the correct DIVA category to assets. Then click **Run**.
   - If there are no conflicts, just click **Run**.

   The process is completed when the status changes to **Updated** in the DIVA Category Update Tool.



With a successful run of the DIVA Category Update Utility, the DIVA Category and Disk Array name will be displayed in the **Path** column of the Associations tab when you load a DIVA archived asset into the Inspector.



Upgrade GV STRATUS Rundown and VTR Ingest systems

- K2 systems must be upgraded to the compatible version of K2 system software.
- GV STRATUS systems must be upgraded to the compatible versions of software.
- Grass Valley Prerequisite Files must be installed on the control point PC.

Upgrade your GV STRATUS Rundown and GV STRATUS VTR Ingest systems to the compatible versions of software. Refer to related topics in GV STRATUS Rundown and GV STRATUS VTR Ingest upgrade procedures.

Related Topics

Upgrading GV STRATUS Rundown systems on page 173
Installing and Upgrading GV STRATUS VTR Ingest/GV STRATUS VTR Controller on page 181

Make recovery images of servers

After you have upgraded software as instructed in these procedures and verified that your system is working properly, you should always make a recovery image of each of your upgraded computers. Use a sequence of tasks similar to those you followed for upgrading software so that as you take systems offline you manage redundancy, servers, and clients, as appropriate for your system.

Refer to the Grass Valley product's *Service Manual* for recovery image procedures.

Upgrade GV Render Engine server software and EDIUS client software

Follow the topics in this section for Render Engine and EDIUS components in your system.

Uninstall EDIUS Workgroup and supporting software

If you have an EDIUS Workgroup client PC on which you have previously installed EDIUS manually (not with SiteConfig), you must do this task before attempting to install software with SiteConfig. Failure to do so results in problems that can require a reimage of the client PC.

Do not attempt to convert an EDIUS Workgroup PC to an EDIUS XS PC. This conversion is not supported.

1. Uninstall the following software from the PC.

   NOTE: You must uninstall manually. Do not attempt to use SiteConfig to uninstall.

   - K2 EDIUS CONNECT
   - EDIUS
   - GV STRATUS application
   - Generic iSCSI
   - StorNext File System
   - SiteConfig Discovery Agent
   - GV LicenseManager

2. Restart the PC.

Install Important Windows updates for EDIUS

- For systems running on EDIUS hardware, Important Windows updates may be required. If your EDIUS I/O hardware driver is not working properly, please check whether these security updates have been installed:

  1. *Security Update for Windows (KB3035131)*
  2. *Security Update for Windows (KB3033929)*

  If you encounter problems to install these security updates, please install the latest Windows roll up package instead.

Verify Render Engine and EDIUS software roles

Before doing this task, make sure devices are added to the SiteConfig system description with the correct family and device type. Refer to *Complete listing of device types, roles, and software packages for GV STRATUS devices* on page 194.

NOTE: GV STRATUS/EDIUS client PC must be in GV STRATUS family, not EDIUS family.

For upgrading components, verify SiteConfig roles on devices as follows:

- EDIUS XS client, installed on a GV STRATUS client PC
  - GV STRATUS Application
  - EDIUS (Required for EDIUS XS)
- EDIUS Workgroup client, installed on a SAN-attached GV STRATUS client PC
  - GV STRATUS Application
  - StorNext File System Client (non K2 only)
  - Generic iSCSI Client (non K2 only)

    NOTE: First install StorNext File System Client, then install Generic iSCSI Client via SiteConfig for the following:

    - ***First installation of GV STRATUS application into a system.***
    - ***When there is an upgrade of the StorNext File System Client.***
  - EDIUS (Required for EDIUS Workgroup)
- Render Engine server
  - GV STRATUS Control Panel
  - GV Log Manager
  - StorNext File System Client
  - GV Embedded Security Manager
  - GV STRATUS Render Engine

Related Topics

Complete listing of device types, roles, and software packages for GV STRATUS devices on page 194

Add software package to deployment group for EDIUS clients and Render Engine server

1. Do a SiteConfig **Check Software** operation on all the devices to which you are deploying software.

   NOTE: If an "Unable to copy ... to target" error appears for a device that has the Grass Valley Embedded Security solution, apply the* Embedded Security *solution one-time initial deployment process to the device. After the one-time process is complete the error does not appear and it is no longer necessary to put* Embedded Security *in Update mode.
2. Refer to release notes to verify software upgrade version information.

3. Add software packages to SiteConfig deployment groups as follows:

   The following software upgrade cab files apply to GV STRATUS/EDIUS XS client PCs.

   - *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:
     - *GrassValley_STRATUS_Application_x.x.x.cab*
     - *EDIUS_x.x.x.cab* (Required for EDIUS XS)

   The following software upgrade cab files apply to GV STRATUS/EDIUS Workgroup (iSCSI SAN-attached) client PCs.

   - *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:
     - *GrassValley_STRATUS_Application_x.x.x.cab*
     - *GenericISCSI_x64_ x.x.x.cab*
     - *SNFS_nonK2_x64_x.x.x.cab*
     - *EDIUS_x.x.x.cab* (Required for EDIUS Workgroup).

   The following software upgrade cab files apply to Render Engine servers.

   - *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
     - *GrassValley_STRATUS_RenderEngine_x.x.x.cab*
     - *GVEmbeddedSecurityManager_x.x.x.cab*
     - *GrassValley_Sabretooth_Application_x.x.x.cab*
     - *GrassValley_LogManager_x.x.x.cab*
   - For K2 9.8.x systems; use *GrassValley_K2system_x.x.x.cab*, which contains the following cab files that apply to this device:
     - *GrassValleyK2Server_x64_9.8.x.x.cab*
     - *SNFS_x64_4.7.x.xxx.cab*
   - For K2 10.x systems; use *GrassValley_K2Plus_x.x.x.cab*, which contains the following cab files that apply to this device:
     - *GrassValleyK2Server_x64_10.x.x.cab*
     - *SNFS_x64_6.0.x.xxx.cab*
   - *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:
     - *GrassValley_STRATUS_Application_x.x.x.cab*
     - *GrassValley_STRATUS_ControlPanel_x.x.x.cab*

The package appears in the Managed Packages list for the selected deployment group. SiteConfig creates new software deployment tasks for the package and displays them in the Tasks list view.

Related Topics

Complete listing of device types, roles, and software packages for GV STRATUS devices on page 194

Upgrade Render Engine and EDIUS software

- If installing to an EDIUS Workgroup client PC on which you have previously installed EDIUS manually (not with SiteConfig), EDIUS Workgroup and supporting software must first be uninstalled manually, before attempting to install with SiteConfig.
- QuickTime must be installed on the machine to which you are installing the GV STRATUS Render Engine software.
- Windows High Priority updates are required and must be installed. For more details, refer to *Install Important Windows updates for EDIUS* on page 148.

NOTE: Expect long deployment times when installing Render Engine and EDIUS software. EDIUS software and Render Engine software can take several minutes to install. Allow the installation to complete. Do not attempt to stop the installation.

This task applies to GV STRATUS/EDIUS client PCs and Render Engine Server. Use SiteConfig for software deployment.

Install software as follows:

a) In one SiteConfig deployment session, install EDIUS and Render Engine software.

b) Restart the device to which you installed the software.

Installing EDIUS application software without SiteConfig

- If installing to a PC on which you have previously installed EDIUS Pro (not EDIUS for STRATUS), EDIUS and supporting software must first be uninstalled before attempting to install EDIUS for STRATUS.
- The PC must meet GV STRATUS Client PC system requirements.
- Windows High Priority updates are required and must be installed. For more details, refer to *Install Important Windows updates for EDIUS* on page 148.

The recommended process for software installation and upgrades is to use SiteConfig from a network connected control point PC and remotely deploy software. However, if SiteConfig installation is not possible, you may install manually on the local PC. Use these steps to manually install the EDIUS application.

1. Procure the following:
   - EDIUS STRATUS Standalone Installation Kit (SIK). This is a directory of files and sub-directories containing components to support the installation.
2. Copy the `EDIUS_STRATUS_SIK` directory to any location on the GV STRATUS/EDIUS client PC.

3. Open the *EDIUS_STRATUS_SIK\deliverables\Modules* directory and identify the EDIUS software cab file, if any, that is in the directory, then proceed as follows:
   - If the EDIUS software cab file is the correct version to install, skip ahead to the next step.
   - If the EDIUS software cab file is not the correct version to install, delete the file, then copy the correct cab file to the directory.
4. Open *EDIUS_STRATUS_SIK\deliverables\Setup*.

   A **cmd** window opens and an **EDIUS Installer** dialog box opens and reports installation progress.
5. When prompted, restart the GV STRATUS/EDIUS client PC.

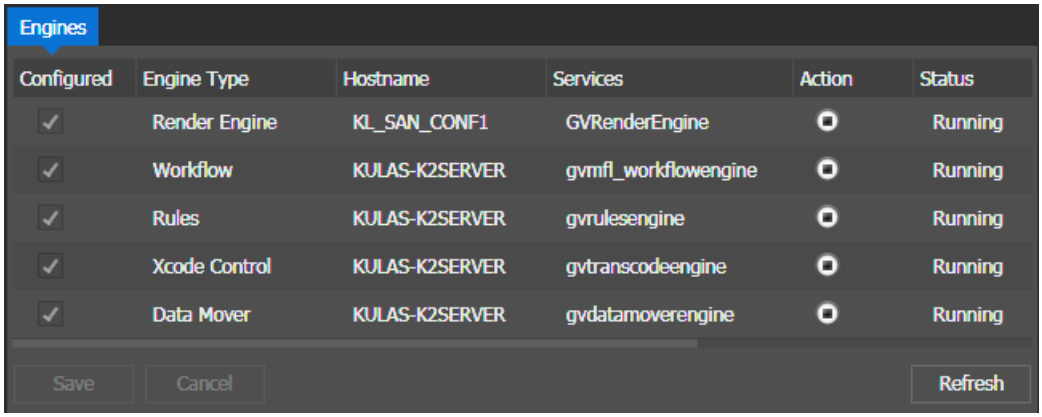
Configuring Control Panel settings: Render Engine

Configure these settings in GV STRATUS Control Panel.

To locate these settings, click **Core | Engines**

Depending on the workflow and bandwidth requirements of your system, Grass Valley may provide a system design in which multiple engines of the same type run on one or more servers. Configure engines as specified by your system design.

1. In the Control Panel application, open Engines settings.



Settings are described as follows:

Setting or button	Description
Configured	Selects an Engine for which settings are saved.
Hostname	The name of a GV STRATUS server that hosts the Engine.
Engine Type	The Engine components installed on the GV STRATUS server.
Status	Indicates if the Engine service is running or stopped.
Action	Starts and stops the Engine service.
Save	Saves current settings to selected GV STRATUS servers.
Cancel	Returns settings to their last saved state.
Refresh	Updates the list.

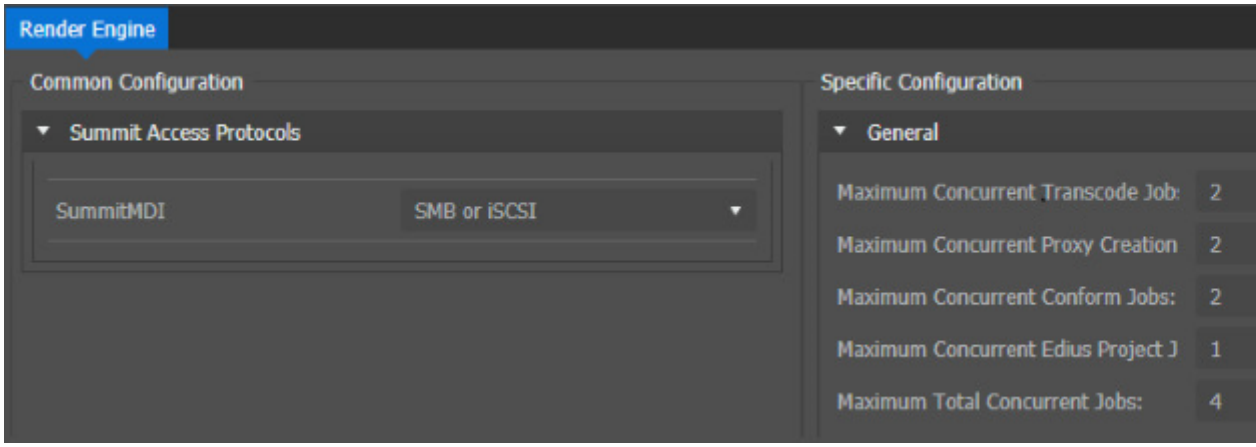
2. Click **Refresh** to make sure the list has the latest information from SiteConfig.
3. Verify that GV STRATUS servers with role of Render Engine are listed, and that those servers are set to Engine Type **Render Engine**.
4. In the **Configured** column, select each server with role of Render Engine, with Engine Type **Render Engine**.

   You must save settings at initial install/config and any time a GV STRATUS server with an Engine Type role is added, removed, or modified in SiteConfig.
5. Click **Save**.

   Settings are saved to the selected GV STRATUS servers.

6. Select the Render Engine and click **Modify**.

   The Render Engine configuration page displays.



7. Configure settings as follows:

Setting or button	Description
Summit Access Protocols	The Summit Access protocol is a common configuration that must be the same for all GV Render Engine servers. Different K2 Summit servers might be accessed via different protocols. Select the Summit Access Protocol for your Render Engine server from the following: • **FTP**: Setting for FTP protocol to be used by Render Engine to access K2 Summits. • **SMB or iSCSI**: Setting for SMB or iSCSI protocol to be used by Render Engine to access K2 Summits. ***NOTE: When a Render Engine accesses high-res media on a standalone K2 Summit or a K2 Central server, FTP is ALWAYS the preferred method. It is recommended to use iSCSI with K2 SAN configurations, and SMB with Isilon shared storage configurations.***
Maximum Concurrent Transcode Jobs	Setting to specify the maximum number of concurrent transcode jobs allowed on the Render Engine server.
Maximum Concurrent Proxy Creation Jobs	Setting to specify the maximum number of concurrent proxy encoder jobs allowed on the Render Engine server.
Maximum Concurrent Conform Jobs	Setting to specify the maximum number of concurrent conform jobs allowed on the Render Engine server.
Maximum Concurrent EDIUS Project Jobs	Setting to specify the maximum number of concurrent EDIUS project jobs allowed on the Render Engine server.
Maximum Total Concurrent Jobs	Setting to specify the maximum number of total concurrent jobs allowed on the Render Engine server. ***NOTE: The maximum number for the setting is up to 4 concurrent jobs in total.***

Use these settings to balance resource load on the GV STRATUS server hosting the engine.

NOTE: The total number of maximum concurrent jobs is limited by the number of available simultaneous connections with K2 Summits. If set to zero, the Render Engine does not process jobs of that type.

8. Click **Save**.

   Render Engine settings are saved to the selected server.

Configure Proxy Config settings

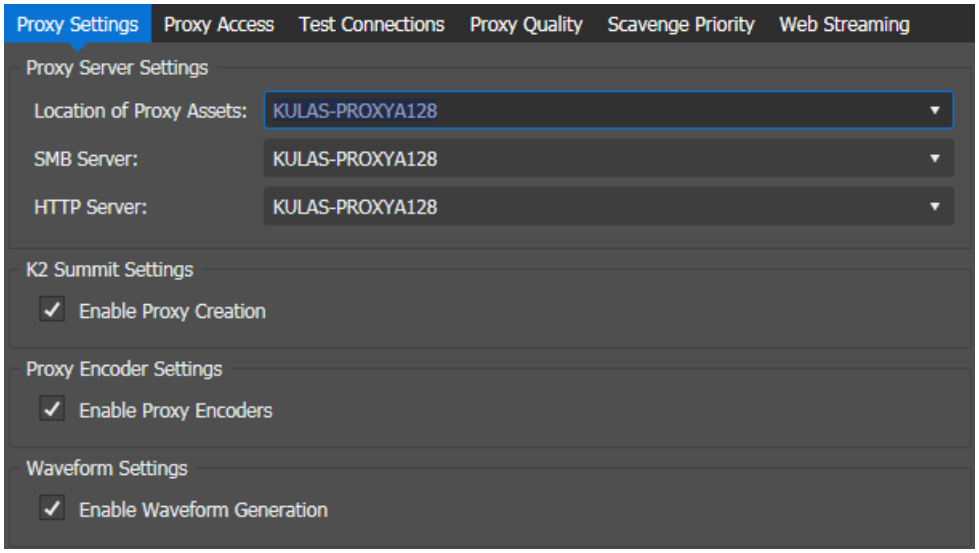
If you received your system pre-configured from Grass Valley, your Proxy Config settings are already configured so you can skip these tasks. Otherwise, work through this section sequentially to configure your Proxy Config settings.

NOTE: A GV STRATUS system must have only one proxy location and server, so these settings apply to all K2 Summit systems, both standalone and SAN.

NOTE: On an operational system, consult with Grass Valley Support before attempting to change Location of Proxy Assets, SMB Server, or HTTP Server settings. Changing these settings requires a purge of the GV STRATUS database and a new K2 storage file system, which results in a loss of high-resolution and low-resolution media. Grass Valley Support can provide methods to avoid this loss of media.

To locate these settings, click **Core | Proxy Config**

1. In the Control Panel application, open Proxy Config settings.



NOTE:* GV STRATUS *versions lower than 3.0 had only one Proxy Server setting. With version 3.0 and higher, the SMB Server and HTTP Server settings must be configured to replace the Proxy Server setting.

2. If your GV STRATUS system stores its proxy on a GV STRATUS Express server, configure as follows:

Setting or button	Description
Location of Proxy Assets	The name of the system that stores proxy files generated by K2 Summit and GV STRATUS systems, as follows: • For proxy stored on the GV STRATUS Express server, this is the network name of the server with role GV STRATUS Core Server Express, as configured in SiteConfig.
SMB Server	The network machine name of the device hosting the server to which proxy files are written, as follows: • For proxy stored on the GV STRATUS Express server, this is the network name of the server with role GV STRATUS Core Server Express, as configured in SiteConfig.
HTTP Server	The network machine name of the device hosting the server from which GV STRATUS clients read proxy files. Typically the SMB Server and the HTTP Server are hosted by the same device. • For proxy stored on the GV STRATUS Express server, this is the network name of the server with role GV STRATUS Core Server Express, as configured in SiteConfig.

3. If your GV STRATUS system stores its proxy on an online or production K2 SAN (A1), configure as follows:

Setting or button	Description
Location of Proxy Assets	The name of the system that stores proxy files generated by K2 Summit and GV STRATUS systems, as follows: • For proxy stored on the K2 SAN (A1), this is the name of the K2 SAN, as named in K2Config.
SMB Server	The network machine name of the device hosting the server to which proxy files are written, as follows: • For proxy stored on the K2 SAN (A1), this is the network name of the GV STRATUS Proxy server attached to the K2 SAN, as configured in K2Config.
HTTP Server	The network machine name of the device hosting the server from which GV STRATUS clients read proxy files. Typically the SMB Server and the HTTP Server are hosted by the same device. • For proxy stored on the K2 SAN (A1), this is the network name of the GV STRATUS Proxy server attached to the K2 SAN, as configured in K2Config.

4. If your GV STRATUS system stores its proxy on a dedicated Proxy Storage system (B1, C1), configure as follows:

Setting or button	Description
Location of Proxy Assets	The name of the system that stores proxy files generated by K2 Summit and GV STRATUS systems, as follows: • For proxy stored on the dedicated Proxy Storage system (B1, C1), this is the name of the Proxy Storage system, as named in K2Config.
SMB Server	The network machine name of the device hosting the server to which proxy files are written, as follows: • For proxy stored on the dedicated Proxy Storage system (B1, C1), this is the network name of the GV STRATUS Proxy Storage file system server, as configured in K2Config.
HTTP Server	The network machine name of the device hosting the server from which GV STRATUS clients read proxy files. Typically the SMB Server and the HTTP Server are hosted by the same device. • For proxy stored on the dedicated Proxy Storage system (B1, C1), this is the network name of the GV STRATUS Proxy Storage file system server, as configured in K2Config.

5. On the **Test Connections** tab, click **Test Connections**.

   The GV STRATUS system populates a list of K2 Storage devices. Verify that this list is correct.

6. Select **Enable Proxy Creation**.

   This allows K2 Summit systems to create proxy assets when high resolution assets are recorded.

7. Select **Enable Proxy Encoders**.

   This allows the system to create proxy assets for any high resolution assets that do not currently have a corresponding low-resolution proxy asset. This setting applies to proxy created by Render Engine servers. If your system instead has Proxy Encoder servers, which are no longer supported, the setting then applies to proxy created by your Proxy Encoder servers.

8. Click **Save**.
9. If you changed Location of Proxy Assets, SMB Server, or HTTP Server settings, under supervision of Grass Valley Support, you must purge the GV STRATUS database and make a new K2 storage file system.

Configuring settings: Render Engine work directory

Only systems with a Render Engine require this process.

To specify the path of work directory for the Render Engine, do the following:

1. On the Render Engine server at *..\Program Files\Grass Valley\XREServer 9\Settings*, copy the *EdiusRenderer.conf* file.
2. Paste the file into *..\Program Files\Grass Valley\XREServer 9*, and open *EdiusRenderer.conf* in a text editor.

```
# **** Configuration file for EdiusRendrerer.exe ****
  work = c:\temp
```

3. Enter a different **work** directory for your GV STRATUS operation, if applicable.

   The work directory consists of temporary files for the proxy operation.
4. Save and close the *EdiusRenderer.conf* file.
5. Restart the Render Engine server.

Configure EDIUS settings in Control Panel

Do not do the tasks in this section if:

- You are upgrading EDIUS software, Render Engine software, or converting EDIUS XRE Servers to Render Engine servers. EDIUS settings are retained in GV STRATUS Control Panel and do not require configuration.

Do the tasks in this section if:

- You are adding EDIUS to your GV STRATUS system for the first time. Configure EDIUS settings in GV STRATUS Control Panel as instructed by the following tasks.

Create EDIUS project folder

If you use the Render Engine to render EDIUS projects, you must create a location for the EDIUS projects.

1. On the K2 media file system (the *V:* drive), create a folder.
2. Name the folder with a meaningful name.

   For example create the following folder:

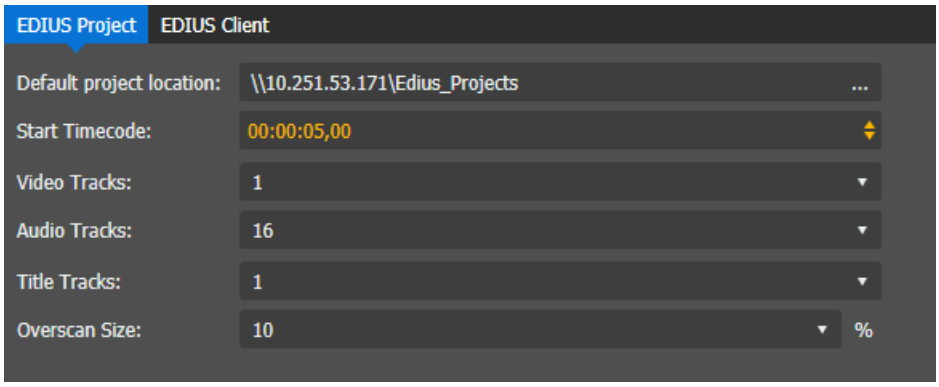
   V:\EDIUS_Projects
3. Make sure the folder is shared with permission granted so that your GV STRATUS/EDIUS XS client PCs, Render Engine Servers, and EDIUS Workgroup client PCs can access the folder.

   On the Render Engine Server, the internal system account, which by default is GVAdmin, accesses the folder.

EDIUS Settings

These settings are only required on GV STRATUS systems with EDIUS.

To locate these settings, in GV STRATUS Control Panel click **Applications | EDIUS | EDIUS Project**



Setting or button	Description
Default project location	The default location for your EDIUS projects. The location is a folder on K2 storage. Make sure this path uses the standard convention of UNC path with hostname (not drive letter) for EDIUS access to K2 storage.
Start timecode	The start timecode of your project or conformed asset. The default is set to 00:00:00,00.
Video Tracks	The number of video tracks for your project.
Audio Tracks	The number of audio tracks for your project.
Title Tracks	The number of title tracks for your project.
Overscan Size	The percentage ratio of overscan size for your project. Set to 0 if you are not using the overscan feature.

Format settings define the format of projects.

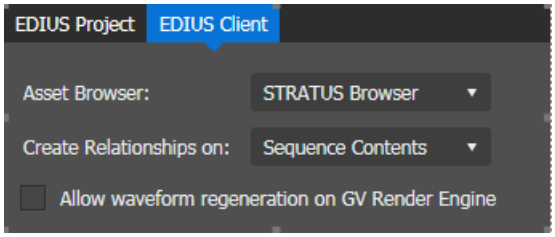
Related Topics

Format settings on page 161
If you have trouble launching EDIUS XS on page 169
Access K2 storage for EDIUS using standard convention on page 282
Access K2 storage for EDIUS using standard convention on page 282

EDIUS Client Settings

These settings are only required on GV STRATUS systems with EDIUS clients.

To locate these settings, in GV STRATUS Control Panel click **Applications | EDIUS | EDIUS Client**



Setting or button	Description
Asset Browser	The asset browser to be used in the EDIUS application. Select one from the following: • **STRATUS App** - utilizes GV STRATUS ActiveX panel in the EDIUS application. • **STRATUS Browser** - utilizes STRATUS browser in the EDIUS application to browse and search GV STRATUS assets.
Create Relationships on	Associates GV STRATUS assets in the EDIUS application. Select one from the following: • **Project Contents** - associates all assets used in the EDIUS project; including those loaded in the project bin only. • **Sequence Contents** - only associates assets used in sequences on the timeline of the EDIUS project.
Allow waveform regeneration on GV Render Engine	Enables or disables the re-creation of waveform cache (*.ewc2) files in proxy server for the use in EDIUS client. Waveform cache files are usually generated in EDIUS when users expand audio tracks on the timeline.

Format settings

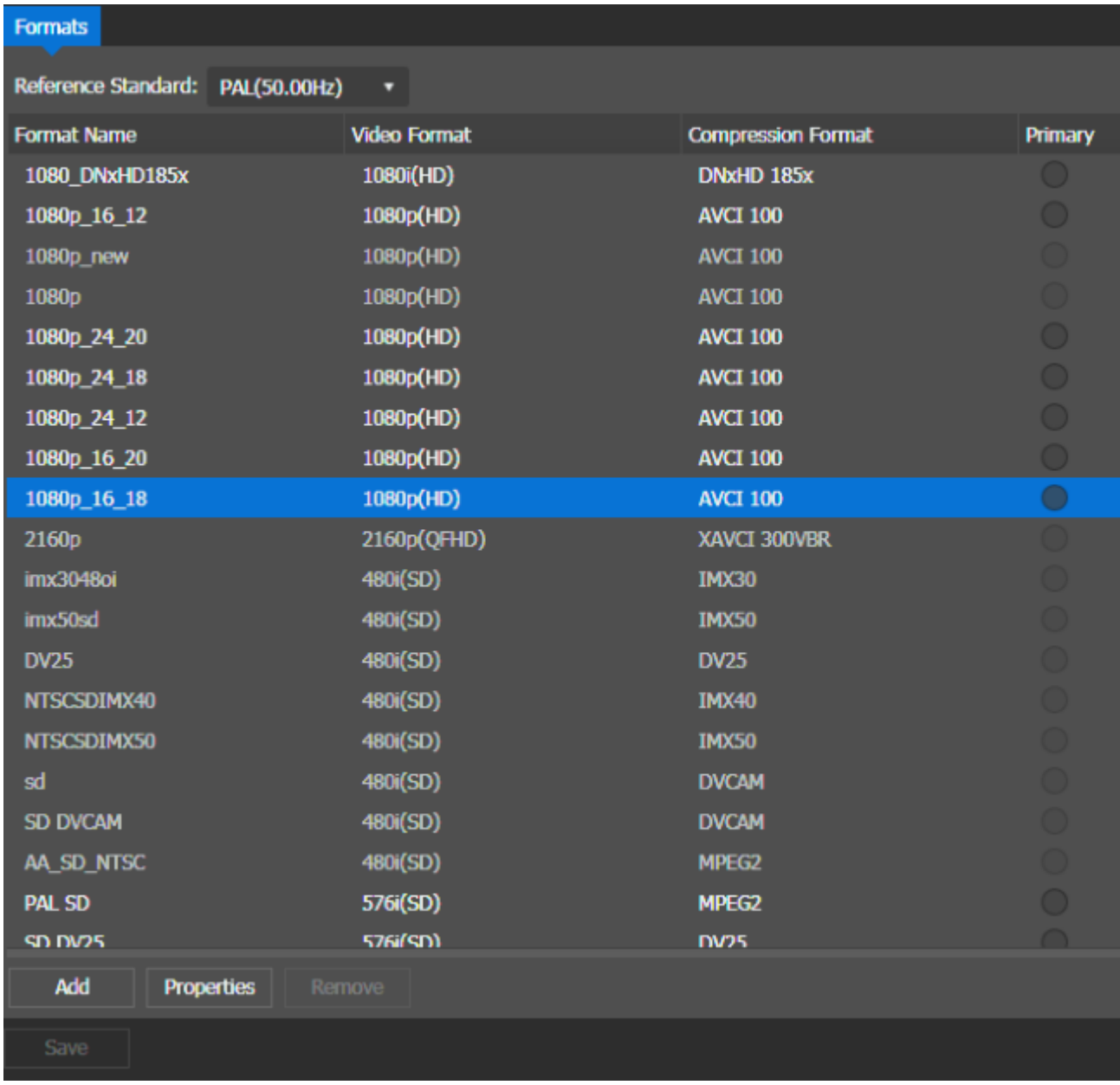
These settings are required on all GV STRATUS systems.

Format settings let you configure video and audio settings. The GV STRATUS application uses these settings as follows:

Conform	When the Render Engine conforms a complex asset, such as a GV STRATUS sequence, into a simple clip, the Format settings define the format of the simple clip.
EDIUS XS	Format settings are inherited by EDIUS XS when the application is launched and a new project is created.
GV STRATUS Rundown	Format settings define the video standard settings, such as PAL or NTSC.
GV I/O Appliance	Format settings define the valid format for configured channels and ingested assets.
Storyboard and Source Viewer	Format settings define the video standard, audio reference, etc.

Access these settings in the GV STRATUS Control Panel application.

To locate these settings, click **General | Format | Formats**



Setting or button	Description
Reference Standard	Sets the GV STRATUS formats available according to their Reference Standard, to match the current Reference Standard on the K2 system. Formats that do not match this setting are disabled in the list. When changing and saving this setting, a corresponding primary format must be selected.
Format Name, Video Format, Compression Format, etc	Format settings, as configured in the **Format Settings** dialog box.

Setting or button	Description
Primary	The default format for configuration. For example, when configuring a Send Destination, the primary format is set by default, but a different format can be selected if desired. ***NOTE: A primary format must be selected. Multiple primary formats are not allowed.***
Locked	Indicates if a format name can be modified. A format that is currently configured in a Send Destination displays a closed lock icon. A dialog box prompts for confirmation before a locked format name can be modified.
Add	Opens the **Format Settings** dialog box for you to add formats.
Properties	Opens the **Format Settings** dialog box for you to view properties of the selected format.
Remove	Removes the selected format. The format currently selected as the primary format can not be removed.
Save	Saves the current configuration of added formats and their order.

Clicking column heads and/or arrow buttons on the right reorders the list of formats.

Related Topics

K2 - Send Destination settings on page 370

Send Destination Add/Modify settings on page 372

Configuring Format settings: Required

EDIUS/GV Render Engine Setup

1. Install/upgrade EDIUS and GV Render Engine software as directed by standard instructions in GV STRATUS customer documentation.

   Make sure you follow the proper sequence for installation and running applications.

2. Verify that the `V:` drives of your K2 Summit system(s) have been shared, in order to allow the GV Render Engine(s) to access them.

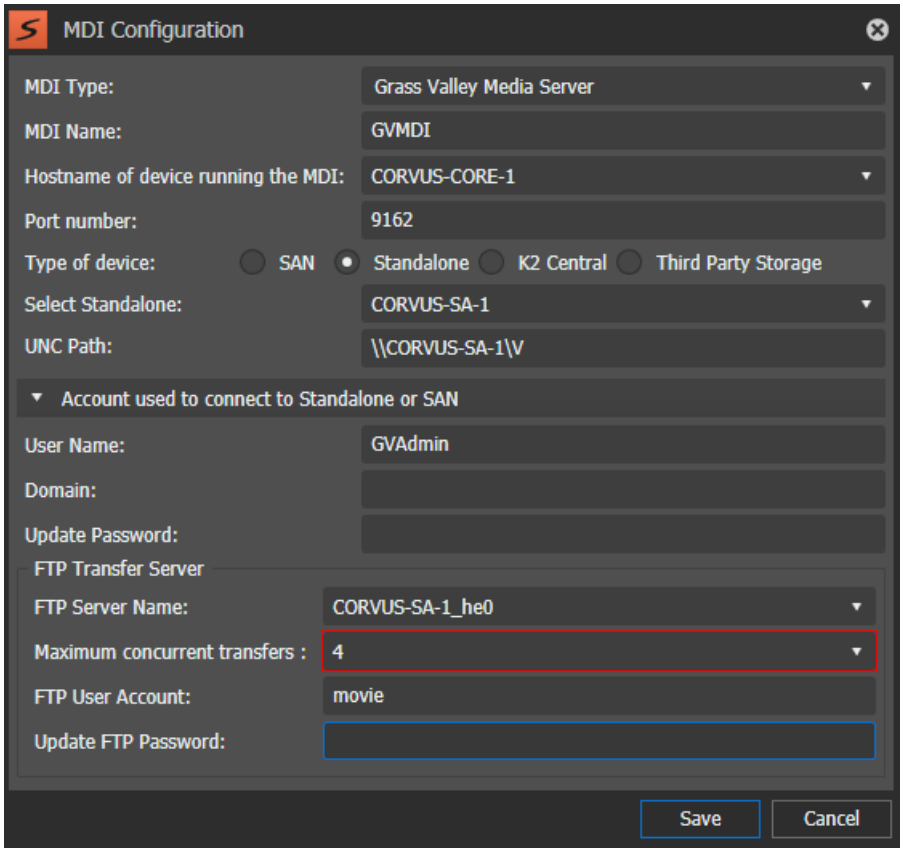
   NOTE: If the GV Render Engines are clients of a K2 SAN, the K2 SAN's V: drive does not need to be shared.

3. Add an EDIUS project folder at the root of the `V:` drive, as directed by standard instructions in GV STRATUS customer documentation.

4. In GV STRATUS Control Panel, set the UNC path as follows:
   - For EDIUS XS and Workgroup, click **Applications | EDIUS | EDIUS Project** and set **Default project location** to the UNC path of the above EDIUS folder. For a GV STRATUS Express system with K2 Summit standalone systems, use a path such as the following:

     `\\K2SummitStandaloneName\V\[EDIUSFolderName]`
   - For the GV Render Engine server, click **Core | MDI Configuration | Add | Grass Valley Media Server** and do the following:
     - Select **Standalone** for the type of K2 device. Then set the UNC path for the K2 Summit standalone system, use a path such as the following:

       `\\standalone_summit\V`



5. If you have EDIUS Workgroup or EDIUS XS workstations; on EDIUS Server Settings, configure as follows:

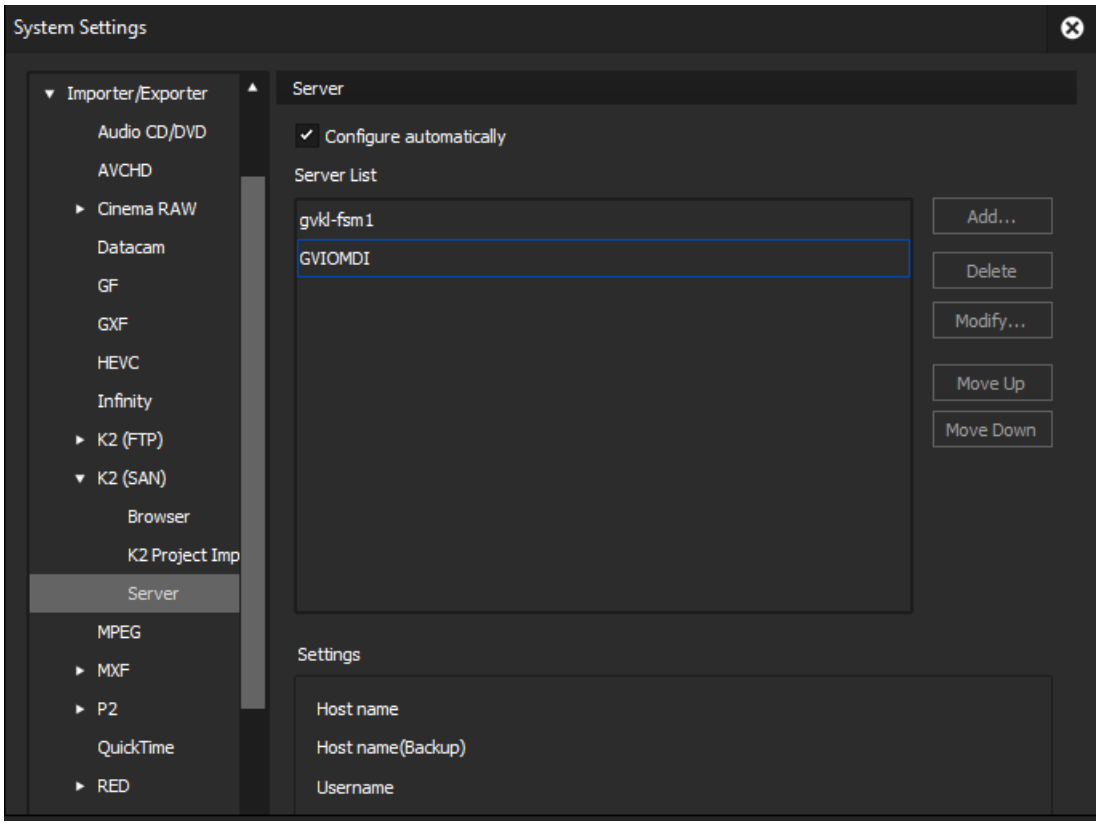
   These settings must be the same as your UNC path already configured on the GV STRATUS Control Panel. The settings identify the storage locations EDIUS accesses. A K2 storage location can be a K2 Summit standalone system or for a K2 SAN, the K2 Media Server with role of file system server (FSM).

   a) From the EDIUS application, click **Settings | System Settings**.

      EDIUS System Settings window opens.

   b) In the Importer/Exporter tree-view, click **K2 (SAN)**.

      Server settings open.



   c) Users are recommended to select the **Configure automatically** check-box.

      For the **Configure automatically** setting, take note of the following:

      - If the **Configure automatically** check-box is selected, the K2(SAN) drives will be automatically populated after each installation or software upgrade.

        NOTE: If the Grass Valley Media Server MDI has UNC path settings configured for third party storage, K2 central, or K2 Summit standalone; each server will be mapped according to its UNC path and not to a drive letter.

      - If the **Configure automatically** check-box is not selected, configure the K2 storage location following these steps below.

   d) In **Server** section, click **Add**.

The **Server Settings** dialog box opens.

e) Verify or make settings as follows.

Table 2: Server Settings

Setting	Value
Name	Enter a name that identifies the K2 storage location to display in the folder view.
Address	Enter the IP address or DNS name of the server that is the K2 storage location.
Address(Backup)	If the K2 storage location is a redundant K2 SAN, the IP address or DNS name of the redundant K2 Media Server with role of file system server (FSM).
Username	Enter the user name required when making the connection to the server configured above. For example, GVAdmin.
Password	Enter the password required for the user name configured above.
Domain	Enter the domain for the user credentials configured above. If not a domain account, leave this setting blank.
Storage Drive	Select the K2 storage location. It must be a drive available on the local system. For a K2 SAN this is typically the `v:` drive. For a K2 Summit standalone system this is typically a mapped network drive.
Show only SNFS drives	For a K2 SAN, select this setting. For a K2 Summit standalone system, clear this setting.
Connection Test	Click this button to test the connection to the server with the settings entered in the **Server settings** dialog box.

f) Click **OK** to save settings and close.

6. Follow the instructions in the this Topic Library to complete EDIUS and GV Render Engine setup.

Related Topics

Configuring CIFS Render Engine settings

Using the EDIUS Project Migration tool

To work on existing EDIUS projects after upgrading to GV STRATUS version 4.5 and above, you need to migrate your projects using the EDIUS Project Migration tool.

The project migration tool does not reconstruct contents locks. It only creates associations between EDIUS Project Group and EDIUS Project file in the GV STRATUS database.

The EDIUS Project Migration tool will be installed automatically when EDIUS XS is deployed with SiteConfig or the Standalone Installation Kit.

You must launch the MS-DOS Command Prompt on the GV STRATUS Core server and use the command line below to utilize the EDIUS Project Migration tool.

```
EdiusProjectMigration.exe [Action] [Options] <host>
```

NOTE: Only [Options] are optional in the command line.

Refer to the table below for the list of supported commands for the EDIUS Project Migration tool:

Command Line	Description
-m, --migrate	[Action] : Migrate EDIUS projects or templates into GV STRATUS server.
--deleteGroup={URI}	[Action] : Delete content of the group specified in {URI} of the GV STRATUS server.
-t, --test	[Action] : Test the migration with GV STRATUS server only. There is no change in the GV STRATUS database.
--deleteLocks	[Action] : Delete the EDIUS Lock bin after the project tree is constructed.
-h, --help	[Action] : Show options for the project migration tool.
-p, --port={PORT}	[Option] : Port number in order to use the Asset API.
-s, --scanFilesystem	[Option] : Scan not only the EDIUS lock bin, but also the whole file system.
-d, --destination={URI}	[Option] : Destination of EDIUS projects to be migrated specified in {URI} of the GV STRATUS server.
--templates	[Option] : Migrate EDIUS templates only instead of EDIUS projects.
-x, --xml={DIRECTORY}	[Option] : Directory to store the XML file. When this option is specified, the tool will not construct project tree in GV STRATUS core server.
-i, --interactive	[Option] : Wait for key input before updating the GV STRATUS database.
<host>	Host name of the GV STRATUS Core server. It is mandatory to include the host name in the command line.

Migrating EDIUS projects

- You have existing EDIUS projects created with GV STRATUS version 4.0 and below in your system.
- You just upgraded your GV STRATUS system to version 4.5 and above.
- You have installed the EDIUS Project Management tool.
- The EDIUS Lock bin must not be deleted until all projects are saved again in EDIUS.

You must use the EDIUS Project Migration tool to migrate your projects after upgrading the GV STRATUS application.

1. Launch the MS-DOS Command Prompt and change directory to the location of the EDIUS Project Migration tool.

2. To test the migration and view the EDIUS project structure in an XML file, you need to use the "–x" option and do one of the following:

   - If you have EDIUS Lock in your system, enter the following command:

     ```
     EDIUSProjectMigration.exe -x=c:\temp -t core-server-name
     ```

   - If you don't have EDIUS Lock in your system, enter the following command:

     ```
     EDIUSProjectMigration.exe -x=c:\temp -t -s core-server-name
     ```

     NOTE: The "-s" option is needed to scan the entire file system. If not, the tool will only scan the EDIUS Lock bin.

   You can view the XML file in the directory that you specified on the command line.

3. To migrate your EDIUS projects, do one of the following:

   - If you have EDIUS Lock in your system, use the following command:

     ```
     EDIUSProjectMigration.exe -m core-server-name
     ```

   - If you don't have EDIUS Lock in your system, use the following command:

     ```
     EDIUSProjectMigration.exe -m -s core-server-name
     ```

     NOTE: The "-s" option is needed to scan the entire file system for EDIUS projects.

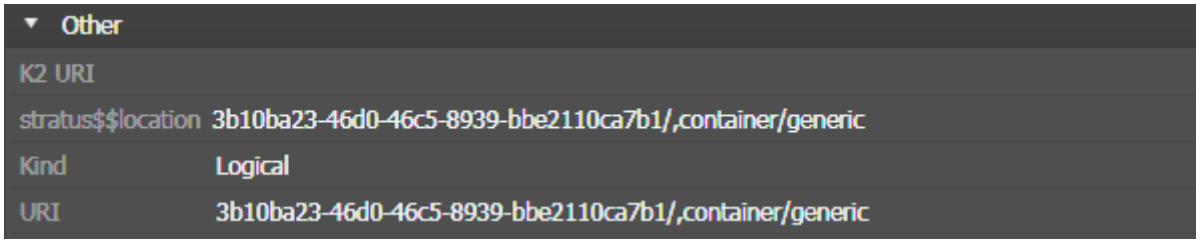
EDIUS Projects directory displays under the EDIUS Projects node in GV STRATUS and EDIUS applications.

Removing EDIUS projects from Assets | EDIUS Projects node

- Existing EDIUS projects have been migrated using the EDIUS Project Migration tool.
- You already saved a backup of the folder to be removed.

1. In the EDIUS Projects node of the GV STRATUS Navigator, select the group folder of EDIUS projects that you want to remove.
2. Drag the selected bin and drop it into the Inspector.

   The group folder properties load into the Inspector.
3. On the **Properties** tab, click the arrow ▶ to display **Other** properties.
4. Right-click on the URI and select **Copy "URI" value** to copy the Group ID of the folder.



5. Launch the MS-DOS Command Prompt and change directory to the location of the EDIUS Project Migration tool.

6. To delete projects in the group folder, enter the following command:

```
EDIUSProjectMigration.exe --deleteGroup=URI-value core-server-name
```

Below is the example of the command line:

```
EDIUSProjectMigration.exe
--deleteGroup=3b10ba23-46d0-46c5-8939-bbe2110ca7b1/,container/generic
```

The EDIUS project and its sub-folders are removed from the group folder. However, the group folder is not deleted via the EDIUS Project Migration tool.

Deleting EDIUS Lock bin

- You already have a backup of the EDIUS Lock bin in your system.
- Existing EDIUS projects have been migrated using the EDIUS Project Migration tool.
- The EDIUS Lock bin must not be deleted until all projects are saved again in EDIUS.

1. Launch the MS-DOS Command Prompt and change directory to the location of the extracted EDIUS Project Migration tool.
2. To delete the EDIUS Lock bin, enter the following command:

```
EDIUSProjectMigration.exe --deleteLocks core-server-name
```

EDIUS Lock bin and its contents are removed from GV STRATUS and K2 AppCenter applications.

NOTE: If an asset or part of the asset is in use or referenced, the asset will not be deleted. If you are a user with the Media Manager role, you can first unlink the reference to EDIUS Project or sequence in the Delete Type window, and then delete the asset.

If you have trouble launching EDIUS XS

Confusion about EDIUS for GV STRATUS licensing can cause problems.

The following is required in order to launch the EDIUS for GV STRATUS as a low-resolution editor (EDIUS XS) correctly:

- Your GV STRATUS system must have a Flex, Pro, or Elite license.
- You must be logged on with the EDIUS XS role assigned.
- The client PC on which you are launching EDIUS must not be licensed for EDIUS Workgroup. This is an EDIUS license, intstalled on the client PC and managed by EDIUS license management. It is not a Sabretooth license.

The EDIUS for GV STRATUS application can launch and operate as follows:

- A high resolution editor, identified as EDIUS Workgroup, which can operate in STRATUS mode or in standalone mode. In STRATUS mode, the EDIUS for GV STRATUS application can access GV STRATUS high resolution assets. In standalone mode, the EDIUS for GV STRATUS application cannot access GV STRATUS high resolution assets.
- A low resolution proxy editor, identified as EDIUS XS, which operates in a single mode that must access GV STRATUS proxy assets.

Both of these applications can launch from the **EDIUS** icon .

The same EDIUS software installation package is used to install both types of EDIUS for GV STRATUS applications, so there can be confusion about which application is being launched. This is especially true if licenses for both applications apply to the same client PC, which is not supported. When you launch an EDIUS for GV STRATUS application, it detects the licensing on the client PC. If licensed for EDIUS Workgroup, you are prompted to logon and the EDIUS Workgroup application always launches. You cannot launch EDIUS XS. If not licensed for EDIUS Workgroup you are prompted to logon. Based on your logon, the application checks licensing and roles on the GV STRATUS Core server. If the license includes EDIUS XS and your logon account is assigned the EDIUS XS role, EDIUS XS launches. Therefore, if you have ever licensed the client PC for EDIUS Workgroup, do not use that PC for EDIUS XS.

Upgrade Workflow Server, license, configure Rules

Follow the topics in this section to upgrade Workflow Server components in your system.

Only systems with a Workflow Server require this process. Use SiteConfig for network setup and software install.

GV STRATUS supports a separate workflow server. The separate workflow server is recommended for B1 (FT) and C1 (FT) configurations.

The separate Workflow Server allows the separation of GV STRATUS Engines (Workflow-, Rules-, XCodeControl- and optional DataMover-Engine) away from the Core Server for large system setups where rules and workflows are used intensively paired with lots of file exports. Since the release of version 5.5, all GV STRATUS Databases are running on one Database Server, which is usually the Core Server. Be aware that the Workflow- and Rules Engine must run as singletons in the system. So when you remove the role from the Core Server and assign it to the new Workflow Server make sure the Engine software is uninstalled from the Core Server. In case there is a problem with the communication between the Engines and the SQL Database running on the Core Server, verify that the SQL Server has the TCP/IP Protocol enabled.

For very large scaled systems, it is possible to deploy the GV STRATUS Databases on a separate server away from the Core Server. When you want to move engines away from the Core server to a new Workflow Server, there is no need anymore to move the Workflow and Rules Databases. They both remain on the Core server, even when the engines are running on a separate server machine. There is no separate SQL-Server license required for the separate Workflow Server. Just remove the roles from the old server in SiteConfig, assign the roles of the engines (WFE, RUE, XCE, and DME) to the new server machine, deploy the software, and check later on whether those engines are enabled using GV STRATUS Control Panel.

NOTE: Make sure the new separate Workflow Server has the same image as the Core Server.

This section also contains topics for licensing and configuring GV STRATUS Rules. These topics apply to a Workflow Server. The topics can also apply to your Core Server, if you host the software that supports GV STRATUS Rules on your Core Server rather than on a Workflow Server.

SiteConfig Workflow Server software install

Only systems with a Workflow Server require this process.

If you received your system pre-configured from Grass Valley, software is already installed, so you can skip these tasks. Otherwise, work through the tasks in this section as follows:

- If your GV STRATUS system has one or more GV STRATUS servers that are Workflow Servers, install software on those servers.

If your GV STRATUS system has a single GV STRATUS Express server or a GV STRATUS Core server and no Workflow Servers, the GV STRATUS Express server or GV STRATUS Core server has Workflow Server software installed. Follow software installation instructions for the GV STRATUS Express server or GV STRATUS Core server, rather than the instructions in this section.

Upgrade software on a Workflow Server

Only systems with one or more GV STRATUS servers that are Workflow Servers require this process. Use SiteConfig to install software on the Workflow Servers.

1. Verify the SiteConfig roles currently assigned to the server. If the roles are not correct for your system design, add or remove roles accordingly. Roles are as follows:
   - GV STRATUS Workflow Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
   - GV STRATUS Rules Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
   - GV STRATUS SocialMedia Engine (Optional)
   - GV STRATUS ExternalMedia Engine (Optional)
   - GV STRATUS Xcode Control Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
   - GV STRATUS Control Panel
   - GV Log Manager
2. Add the server to a deployment group, such as the GV STRATUS deployment group.

3. Add the following files to the deployment group:

   - *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
     - *GrassValley_STRATUS_Mediaflow_x.x.x.cab*
     - *GrassValley_STRATUS_Rules_x.x.x.cab*
     - *GrassValley_STRATUS_SocialMedia_x.x.x.cab*
     - *GrassValley_STRATUS_ExternalMedia_x.x.x.cab*
     - *GrassValley_STRATUS_Transcode_x.x.x.cab*
     - *GrassValley_STRATUS_TrafficGateway_x.x.x.cab*
     - *GrassValley_Sabretooth_Application_x.x.x.cab*
     - *GrassValley_LogManager_x.x.x.cab*
   - *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:
     - *GrassValley_STRATUS_ControlPanel_x.x.x.cab*
   - *GrassValley_K2system_x.x.x.cab* for K2 9.8.x systems.
   - *GrassValley_K2Plus_x.x.x.cab* for K2 10.x systems.

   Refer to release notes for version numbers.

4. Do the SiteConfig **Check Software** operation on the server.

   NOTE: If an "Unable to copy ... to target" error appears for a device that has the Grass Valley Embedded Security solution, apply the* Embedded Security *solution one-time initial deployment process to the device. After the one-time process is complete the error does not appear and it is no longer necessary to put* Embedded Security *in Update mode.

5. Verify that deployment tasks are set to **Install** for the files listed above.

   If a WFRegMon install task appears, install it as well. It is required to support Grass Valley software installers. There is no uninstall task.

6. Deploy software to the server.
7. Restart as prompted.

When running the Data Mover Engine on the Workflow Server, make sure the Workflow Server can access all potential communication partners for the DME, including the FTP network of the K2 SAN and standalone systems.

Next, install an optional XCODECONTROL license, if appropriate for your system.

SabreTooth Rules, Xcode license process

Only the GV STRATUS server with role of Common Services requires this process.

The Workflow license is installed on the GV STRATUS server with role of Common Services. Typically the GV STRATUS Core server has the role of Common Services.

One STRATUS-RULES license is required for the Rules Engine software component in your GV STRATUS system. This is a SabreTooth floating license. Optional licenses for associated functionality include the following:

- STRATUS-TRANSCODE

- STRATUS-XCODECONTROLCARBONCODER
- STRATUS-XCODECONTROLVANTAGE
- STRATUS-XCODECONTROLELEMENTAL
- STRATUS-ASPERA
- STRATUS-XCODECONTROLMEWS
- STRATUS-XCODECONTROLMEWSEXT

If you received your system pre-configured from Grass Valley, licenses are already installed, so you can skip these tasks. Otherwise, do the following:

1. Refer to the license sheet that you received with your GV STRATUS license. The license sheet has the Sales Order number that you need.
2. On the GV STRATUS server with role of Common Services, run the SabreTooth License Manager, generate a unique ID, and send the email to Grass Valley requesting your license or licenses.

   Refer to this Topic Library for detailed licensing procedures.
3. When you receive your license file, use SabreTooth License Manager and install it on the server.

Upgrading GV STRATUS Rundown systems

This section contains the tasks necessary for the upgrade to this release of software.

Upgrading GV STRATUS Rundown devices with SiteConfig

This section contains the tasks for using SiteConfig to upgrade to this release of software. Work through the tasks sequentially to complete the upgrade.

About upgrading GV STRATUS Rundown devices with SiteConfig

With the installation instructions in this section, you use SiteConfig from a network connected control point PC and remotely install/upgrade software simultaneously on your system devices. This is the recommended process for software installation and upgrades. When installing the GV STRATUS application or the GV STRATUS Control Panel application, if SiteConfig installation is not possible, you may install manually on the local PC. You must uninstall before installing.

NOTE: Do not use the upgrade instructions in this document if upgrading with SiteConfig for the first time.

If SiteConfig was not used for your previous software install, do not use the upgrade instructions in these release notes. Instead, use the *SiteConfig Migration Instructions*. Before you upgrade software using SiteConfig, each of your product devices must be migrated to become a SiteConfig managed device. This includes installing SiteConfig support on the device, manually uninstalling any and all components, and qualifying the device for communication with SiteConfig. These instructions are in the *SiteConfig Migration Instructions*. Also refer to the *SiteConfig User Manual* or *SiteConfig Help Topics*.

The upgrade instructions in this document apply to the following device:

- GV STRATUS Rundown Server and Client

To upgrade software using SiteConfig, you must first have SiteConfig set up for system management and software deployment in your facility. These upgrade instructions assume that you have already done that for your K2 SAN. Then you add your product devices to the SiteConfig system description that you are using for your K2 SAN.

NOTE: Do not attempt to upgrade software incrementally across the devices of a K2 SAN while media access is underway. Online software upgrading is not supported.

The following installation tasks provide information specifically for the upgrade to this version of software. Read the information in these sections carefully before attempting any upgrade to software.

Prepare for upgrade

Before upgrading, do the following:

- Procure the software installation files for this release via the appropriate distribution method, such as download, CD-ROM, network drive, or external drive.
- Start up the devices you are upgrading, if they are not already started.
- Stop all media access on the devices you are upgrading.
- Shut down all applications including the SDB Server on the devices you are upgrading.

Apply these steps to devices in the SiteConfig system description.

- If your system includes Aurora Playout, do the following:
  a) On the Core/Express server, remove the **Aurora Playout Server Components** role.
  b) On the Core/Express server, add the **GV STRATUS Rundown Server Components** role.
  c) On GV STRATUS/Aurora Playout client PCs, remove the **Aurora Playout Application** role.
  d) On GV STRATUS/Aurora Playout client PCs, add the **GV STRATUS Rundown Application** role.

Prepare SiteConfig for software deployment

Do the following to prepare SiteConfig for the software upgrade.

1. Make the following files accessible to the SiteConfig control point PC:
   - GV STRATUS Rundown software installation (`*.cab`) file
   - GV STRATUS Control Panel software installation (`*.cab`) file
   - DiscoveryAgent_x.x.xxx(`*.cab`) file
2. If a newer version of SiteConfig is available for upgrade and you have not yet upgraded SiteConfig, do the following:
   a) From Windows **Programs and Features**, uninstall the current version of SiteConfig from the control point PC.
   b) Install the new version of SiteConfig on the control point PC.
3. If not already present in the SiteConfig system description, configure deployment groups as follows:
   - A deployment group that contains your GV STRATUS Rundown devices.

Install Grass Valley Prerequisite Files on the SiteConfig PC

GV STRATUS VTR Ingest, GV STRATUS VTR Controller, and GV STRATUS Rundown share Microsoft .NET as common prerequisite software. This common software is installed with `Prerequisite Files 2.0.exe`, which is part of a separate installation package. You install this prerequisite software package on the control point PC so that when SiteConfig deploys any software that needs the prerequisite software, it uses the software installation files from the common package. This reduces the size of `.cab` files overall and makes software download more manageable.

1. Check release notes for the required version of prerequisite files, if any.
2. On the SiteConfig PC, open Windows Add/Remove programs and look for **Grass Valley Prerequisite Files**, then proceed as follows:
   - If the required version of prerequisite files is installed, do not proceed with this task.
   - If prerequisite files are not installed or are not at the required version, proceed with this task.
3. Procure the required prerequisite software installation file as listed in the following:

Product	Prerequisite file	Location
GV STRATUS Rundown, GV STRATUS VTR Ingest, GV STRATUS VTR Controller	GrassValley_PrerequisiteFiles_2.0.0.zip (Microsoft .NET installer)	Grass Valley website *SiteConfig Application software download page*.

4. On the SiteConfig PC, run the installation file. The installation program copies prerequisite files to `C:\Program Files\Grass Valley\Prerequisite Files`.

After installing prerequisite files on the SiteConfig PC, use SiteConfig and deploy software to client PCs.

Configure Playout Servers

You need to configure playout servers in the GV STRATUS Control Panel to enable automatic transfer of assets into the playout servers. When assets are dragged from GV STRATUS into the GV STRATUS Rundown playlist, the system would trigger a transfer – from the media server to the playout server of GV STRATUS Rundown.

For each of your GV STRATUS Rundown Playout Servers, in GV STRATUS Control Panel do the following:

a) Configure a Grass Valley Media Server MDI.

b) Add the Playout Server.

Related Topics

Grass Valley Media Server MDI standalone settings on page 304

Grass Valley Media Server MDI SAN settings on page 306

Rundown Add/Modify Server settings on page 394

Upgrade K2 systems

- All K2 Summit systems must upgrade to the latest Microsoft .NET Framework version, if that version of .NET is not already installed.

- You have procured the necessary software and documentation for the upgrade. Go to *http://www.grassvalley.com/dl/k2_summit* and refer to the "Release Notes" section of the K2 Topic Library to determine the compatible software versions and documentation required.
- All standalone K2 Summit systems must be offline (all media access stopped) or shut down. The power must be off for a few seconds before switching it on again.
- If upgrading a K2 SAN, all SAN clients must be offline (all media access stopped) or shut down. The power must be off for a few seconds before switching it on again. Depending on your system design, this could include devices such as SAN-attached K2 Summit systems, GV STRATUS servers, and GV STRATUS Client PCs.

***NOTE: When upgrading from a K2 software version lower than 9.x to a K2 software version at 9.x or higher, you must reimage each* K2 Summit system. *Hardware upgrades might also be required on a* K2 Summit system.**

1. Upgrade your K2 systems to the compatible version of K2 system software. This includes K2 SAN systems and stand-alone K2 Summit systems.

   When upgrading for compatibility with GV STRATUS, use `GrassValley_K2system_x.x.x.cab` file, which contains the required `GrassValley_STRATUS_SummitServices_x.x.x.cab` file.

2. On systems running Embedded Security, do the one-time initial deployment process for the Embedded Security solution, if you have not already done so.
3. Configure the Grass Valley Media Server MDI settings in GV STRATUS Control Panel for each K2 Summit system that you use with the GV STRATUS Rundown application.

Distribute devices into deployment groups

If you have not already done so, configure your deployment groups. The recommended deployment group distribution is as follows. Depending on your system design, your system might not have all the device types listed.

Add your GV STRATUS Rundown Server(s) and GV STRATUS Rundown clients to the deployment group.

- In a deployment group named "GV STRATUS Rundown", place the following devices:
  - GV STRATUS Rundown client PC connected on the corporate LAN for low-resolution (proxy) workflow
  - GV STRATUS Rundown client PC connected on the media (iSCSI) network for high-resolution workflow
  - GV STRATUS core server with roles as follows:
    - GV STRATUS Rundown Server Components
    - GV STRATUS Rundown Hot Standby SDB

Install Important Windows updates (recommended)

- For systems running the full (not embedded) Windows operating system, Windows "Important" updates are recommended , but not required. While your computer is in an offline state to upgrade software, check for updates to install. Use standard Windows procedures.

  ⚠ ***CAUTION: Only "Important Updates" should be installed. Do not install other Windows or driver updates unless specifically directed by product documentation or by Grass Valley Support.***

  NOTE: If a computer does not have the Grass Valley* Embedded Security *solution one-time initial deployment process applied, do not install any Windows updates. Apply the one-time process before installing Windows updates.

Check all currently installed software on GV STRATUS Rundown devices

- The device must be assigned in the SiteConfig system description and network connectivity must be present.
- SiteConfig must be able to log in to the device using the username/password credentials assigned to the device.
- The SiteConfig PC must not have a network drive mapped to an administrative share (such as C$) on a device on which you are checking software.
- If Aurora product software at a version lower than 6.5.2 is currently installed, it must be manually uninstalled. For more information refer to *SiteConfig Migration Instructions*.

Do the following steps on the device that you are upgrading.

1. In the **Software Deployment | Deployment Groups** tree view, right-click the top-most node for the group or any individual device and select **Check Software**.

   NOTE: If you have access problems, verify that the administrator account on the device has credentials as currently configured in SiteConfig.

   NOTE: If an "Unable to copy ... to target" error appears for a device that has the Grass Valley Embedded Security solution, apply the* Embedded Security *solution one-time initial deployment process to the device. After the one-time process is complete the error does not appear and it is no longer necessary to put* Embedded Security *in Update mode.

   The Check Software dialog box appears. SiteConfig searches for software on the selected device or devices and gathers information. Progress is reported.

2. When the check is complete, close the Check Software dialog box.

An updated list of all currently installed software is displayed in the **Software Deployment | Devices | Installed Software** list view. If software is a SiteConfig managed software package, information is displayed in the Managed Package and Deployment Group columns.

Add software package to deployment group for GV STRATUS Rundown devices

Prerequisites for this task are as follows:

- You can access the software package file from the SiteConfig control point PC.

- The devices to which you are deploying software are in a deployment group.

Use the following procedure to add one or more software packages to the deployment group that contains your GV STRATUS Rundown devices. For this release of software, identify and add software installation file as follows:

Software	File name
GV STRATUS Rundown software	*GV_STRATUS_Rundown_x.x.x.x.cab*
GV STRATUS Control Panel application on SDB/XMOS server	*GrassValley_STRATUS_ControlPanel_x.x.x.xx.cab*

1. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.
2. Click the **Add** button.

   The Add Package(s) dialog box opens.
3. Do one of the following to select the software package:
   - Select from the list of packages then click **OK**.
   - Click **Browse**, browse to and select the package, then click **Open**.
4. If one or more EULAs are displayed, accept them to proceed. If you do not accept a EULA, the associated software is not assigned to the deployment group.

   SiteConfig adds the package to the deployment group.

The package appears in the Managed Packages list for the selected deployment group. SiteConfig creates new software deployment tasks for the package and displays them in the Tasks list view.

Upgrade software on GV STRATUS Rundown devices

- The devices that you are upgrading must be in a deployment group.
- For the software you are upgrading, a newer version of that managed software package must be added to the deployment group.
- Grass Valley Prerequisite Files must be installed on the control point PC.
- A SiteConfig "Check Software" operation must be performed on the devices you are upgrading.

If you are upgrading multiple software components for which there is a required sequence, you must check and uncheck tasks and run multiple deployment sessions to control the sequence. For some software components, SiteConfig aids you by enforcing dependencies. For each individual software component, SiteConfig enforces an uninstall of the current version of software before installing the upgrade version. SiteConfig provides uninstall deployment tasks and install deployment tasks to indicate the taskflow. SiteConfig can do the uninstall/install in a single deployment session.

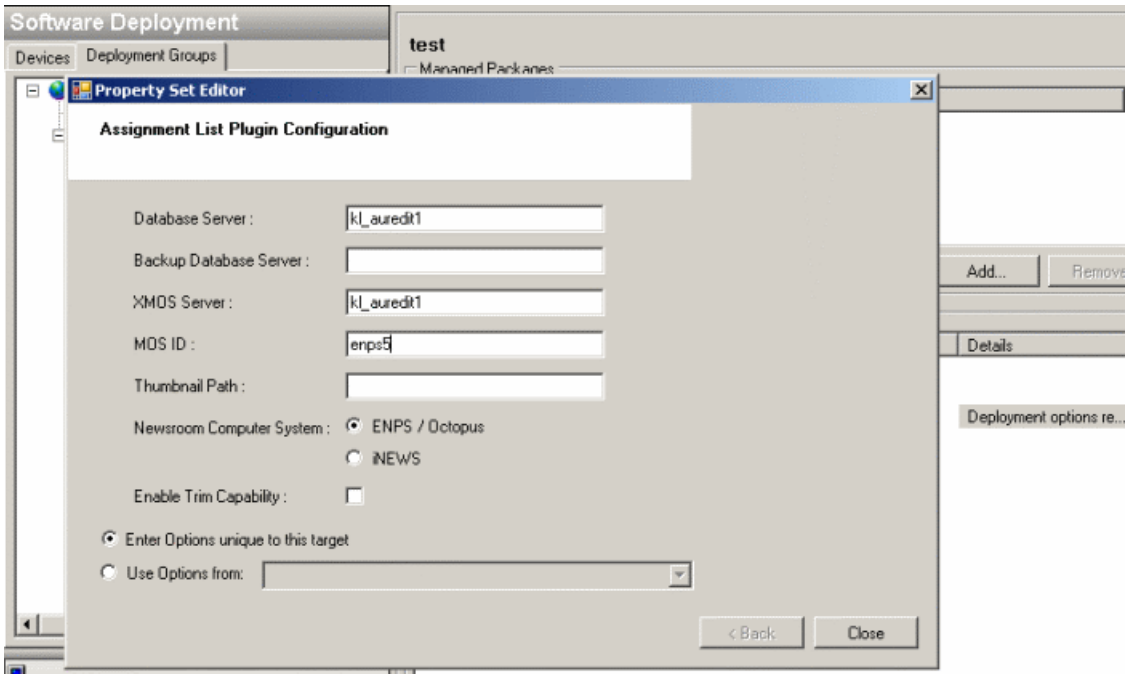
1. In the **Software Deployment | Deployment Groups** tree view, select the device or the group of devices to which you are deploying software.

   The corresponding software deployment tasks are displayed in the Tasks list view.
2. For the software you are deploying, select the **Deploy** check box in the row for the uninstall task.

3. For the software you are installing, select the **Deploy** check box in the row for the install task.

   If you have the Assignment List Plugin role assigned to a playout device, then you will have to set deployment options. The **Details** column will indicate **Deployment options required**.

   Click the **Deployment options required** link and a wizard page appears.



Key-in the Database Server, XMOS Server, MOS ID and select the appropriate Newsroom Computer System in your operation. Then, click **Close**.

For upgrading GV STRATUS Rundown to this release, deploy the following tasks:

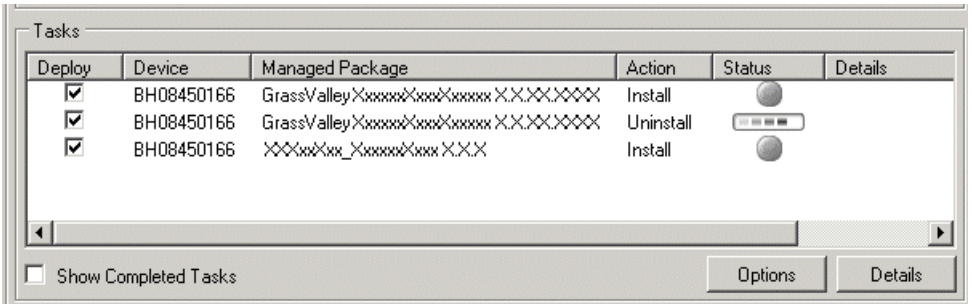
Deploy	Managed Package	Action
✓	GV_STRATUS_Rundownxxxx.xxxx	Uninstall
✓	GV_STRATUS_Rundown x.x.x.x	Install
✓	GrassValley_STRATUS_ControlPanel_xxxx.xxx	Install

NOTE: If there are dependencies, SiteConfig can enforce that some tasks be deployed together.

4. Check the area next to the Start Deployment button for a message.

   If a message instructs you to upgrade the Discovery Agent, on the control point PC go to the directory to which SiteConfig is installed, find the `DiscoveryAgent_x.x.x.x.cab` file, add it to the deployment group, and deploy the Discovery Agent software as well.

5. Click the **Start Deployment** button.



   Deployment tasks run and software is uninstalled. Progress is reported and next steps are indicated in both the Status and Details columns. If an error appears regarding prerequisite software, install the Grass Valley Prerequisite Files on the control point PC and then repeat this step.

6. When the Status or Details columns indicate next steps, identify the software in the row, then do one of the following:

   - For K2 software, when Details displays a **Restart required** link (but not "Visible dialog pending..."), click the link and when prompted "...are you sure...", click **Yes**.

   The device restarts. This restart is required by the GV STRATUS Rundown software uninstall.

   Deployment tasks run and software is installed. Progress is reported and next steps are indicated in both the Status and Details columns.

7. When the Status or Details columns indicate next steps, identify the software in the row, then do one of the following:

   - For K2 software, when Details displays a **Restart required** link (but not "Visible dialog pending..."), click the link and when prompted "...are you sure...", click **Yes**.

   The device restarts.

8. Monitor progress as indicated by both the Status and Details column. When finished, the Status column indicates complete.

Upgrade NAS systems

- K2 systems must be upgraded to the compatible version of K2 system software.

- GV STRATUS Rundown systems must be upgraded to the compatible versions of software.

  Upgrade the Proxy NAS (K2 Nearline SAN) to the compatible version of K2 software. Use SiteConfig and deploy software, using steps similar to those for other systems.

  a) Check software on the Nearline SAN's K2 Media Servers.
  b) Add software `*.cab` file to the deployment group that contains the K2 Media Servers.
  c) Upgrade software on K2 Media Servers via a SiteConfig deployment session.

Installing and Upgrading GV STRATUS VTR Ingest/GV STRATUS VTR Controller

This section contains the tasks necessary to install this release of software.

About installing GV STRATUS VTR Ingest/GV STRATUS VTR Controller devices with SiteConfig

With the installation instructions in this section, you use SiteConfig from a network connected control point PC and remotely install/upgrade software simultaneously on your system devices. This is the recommended process for software installation and upgrades. When installing the GV STRATUS application or the GV STRATUS Control Panel application, if SiteConfig installation is not possible, you may install manually on the local PC. You must uninstall before installing.

If SiteConfig was not used for your previous software install, do not use the upgrade instructions in these release notes. Instead, use the *SiteConfig Migration Instructions*. Before you upgrade software using SiteConfig, each of your product devices must be migrated to become a SiteConfig managed device. This includes installing SiteConfig support on the device, manually uninstalling any and all components, and qualifying the device for communication with SiteConfig. These instructions are in the *SiteConfig Migration Instructions*. Also refer to the *SiteConfig User Manual* or *SiteConfig Help Topics*.

The upgrade instructions in this document apply to the following devices:

- GV STRATUS VTR Ingest
- GV STRATUS VTR Controller

To upgrade software using SiteConfig, you must first have SiteConfig set up for system management and software deployment in your facility. These upgrade instructions assume that you have already done that for your GV STRATUS VTR Ingest and GV STRATUS VTR Controller. Then add your product devices to the SiteConfig system description that you are using for your software.

NOTE: To upgrade GV STRATUS VTR Ingest/GV STRATUS VTR Controller to version 11.8.x.x (and above) in SiteConfig, you are required to select the previous version of the package and run the uninstallation process of this version first. Then select GV STRATUS VTR Ingest/GV STRATUS VTR Controller package 11.8.x.x (and above) to install.

The following installation tasks provide information specifically for the upgrade to this version of software. Read the information in these sections carefully before attempting any upgrade to software.

Prepare for install

Before installing, do the following:

- Procure the software installation files for this release via the appropriate distribution method, such as download, CD-ROM, network drive, or external drive.
- Start up the devices to which you are installing, if they are not already started.
- Stop all media access on the devices to which you are installing.
- Uninstall Aurora VTR Ingest/VTR Controller manually if you have them in your device, before installing GV STRATUS VTR Ingest.

Prepare SiteConfig for software deployment

Do the following to prepare SiteConfig for the software upgrade.

1. Make the following files accessible to the SiteConfig control point PC:
   - Files for GV STRATUS VTR Ingest and GV STRATUS VTR Controller devices:
     - GV STRATUS VTR Ingest software installation (`*.cab`) file
     - GV STRATUS VTR Controller software installation (`*.cab`) file
2. If a newer version of SiteConfig is available for upgrade and you have not yet upgraded SiteConfig, do the following:
   a) From Windows **Programs and Features**, uninstall the current version of SiteConfig from the control point PC.
   b) Install the new version of SiteConfig on the control point PC.
3. If adding a new 64-bit Windows 7 device in SiteConfig, make sure to select x64 as the platform type. This will enable the 64 bit versions of iSCSI and SNFS to be installed instead of the default 32-bit.
4. If not already present in the SiteConfig system description, configure deployment groups as follows:
   - A deployment group that contains your GV STRATUS VTR Ingest devices

Install Important Windows updates (recommended)

- For systems running the full (not embedded) Windows operating system, Windows “Important” updates are recommended , but not required. While your computer is in an offline state to upgrade software, check for updates to install. Use standard Windows procedures.

  ⚠ ***CAUTION: Only “Important Updates” should be installed. Do not install other Windows or driver updates unless specifically directed by product documentation or by Grass Valley Support.***

  NOTE: If a computer does not have the Grass Valley* Embedded Security *solution one-time initial deployment process applied, do not install any Windows updates. Apply the one-time process before installing Windows updates.

Upgrade K2 systems

- All K2 Summit systems must upgrade to the latest supported version of .NET if not already installed.
- You have procured the necessary software and documentation for the upgrade. Go to *http://www.grassvalley.com/dl/k2_summit* and refer to the "Release Notes" section of the K2 Topic Library to determine the compatible software versions and documentation required.
- All standalone K2 Summit systems must be offline (all media access stopped) and shut down. The power must be off for a few seconds before switching it on again.
- If upgrading a K2 SAN, all SAN clients must be offline (all media access stopped) and shut down. The power must be off for a few seconds before switching it on again. Depending on your system design, this could include devices such as SAN-attached K2 Summit systems, GV STRATUS servers, and GV STRATUS Client PCs.

***NOTE: When upgrading from a K2 software version lower than 9.x to a K2 software version at 9.x or higher, you must reimage each* K2 Summit system. *Hardware upgrades might also be required on a* K2 Summit system.**

1. Upgrade your K2 systems to the compatible version of K2 system software. This includes K2 SAN systems and stand-alone K2 Summit systems.

   When upgrading for compatibility with GV STRATUS, use `GrassValley_K2system_x.x.x.cab` file, which contains the required `GrassValley_STRATUS_SummitServices_x.x.x.cab` file.

2. For K2 storage systems, do the following:

   - If any K2 Summit clients have a GVRE/Encoder set as an FTP Server, do the following:
     - Go to each K2 Summit client with a GVRE/Encoder FTP server and click the **Change Server** button.
     - Verify that the FTP Server settings change to a desired FTP Server.
     - Reboot the K2 Summit clients.
   - Remove all GVREs/Encoders from K2Config and add them back without the FTP Server role.
   - Sync K2Config to the GV STRATUS core server.

3. For Grass Valley SMB Storage systems, do the following:

   - Remove all GVREs/Encoders from K2Config.
   - Map the V: drive manually on each GVRE.
   - Sync K2Config to the GV STRATUS core server.

4. On systems running Embedded Security, do the one-time initial deployment process for the Embedded Security solution, if you have not already done so.

Install Grass Valley Prerequisite Files on the SiteConfig PC

GV STRATUS VTR Ingest, GV STRATUS VTR Controller, and GV STRATUS Rundown share Microsoft .NET as common prerequisite software. This common software is installed with `Prerequisite Files 2.0.exe`, which is part of a separate installation package. You install this prerequisite software package on the control point PC so that when SiteConfig deploys any software

that needs the prerequisite software, it uses the software installation files from the common package. This reduces the size of `.cab` files overall and makes software download more manageable.

1. Check release notes for the required version of prerequisite files, if any.
2. On the SiteConfig PC, open Windows Add/Remove programs and look for **Grass Valley Prerequisite Files**, then proceed as follows:
   - If the required version of prerequisite files is installed, do not proceed with this task.
   - If prerequisite files are not installed or are not at the required version, proceed with this task.
3. Procure the required prerequisite software installation file as listed in the following:

Product	Prerequisite file	Location
GV STRATUS Rundown, GV STRATUS VTR Ingest, GV STRATUS VTR Controller	GrassValley_PrerequisiteFiles_2.0.0.zip (Microsoft .NET installer)	Grass Valley website *SiteConfig Application software download page*.

4. On the SiteConfig PC, run the installation file. The installation program copies prerequisite files to `C:\Program Files\Grass Valley\Prerequisite Files`.

After installing prerequisite files on the SiteConfig PC, use SiteConfig and deploy software to client PCs.

Installing GV STRATUS VTR Ingest/GV STRATUS VTR Controller with SiteConfig

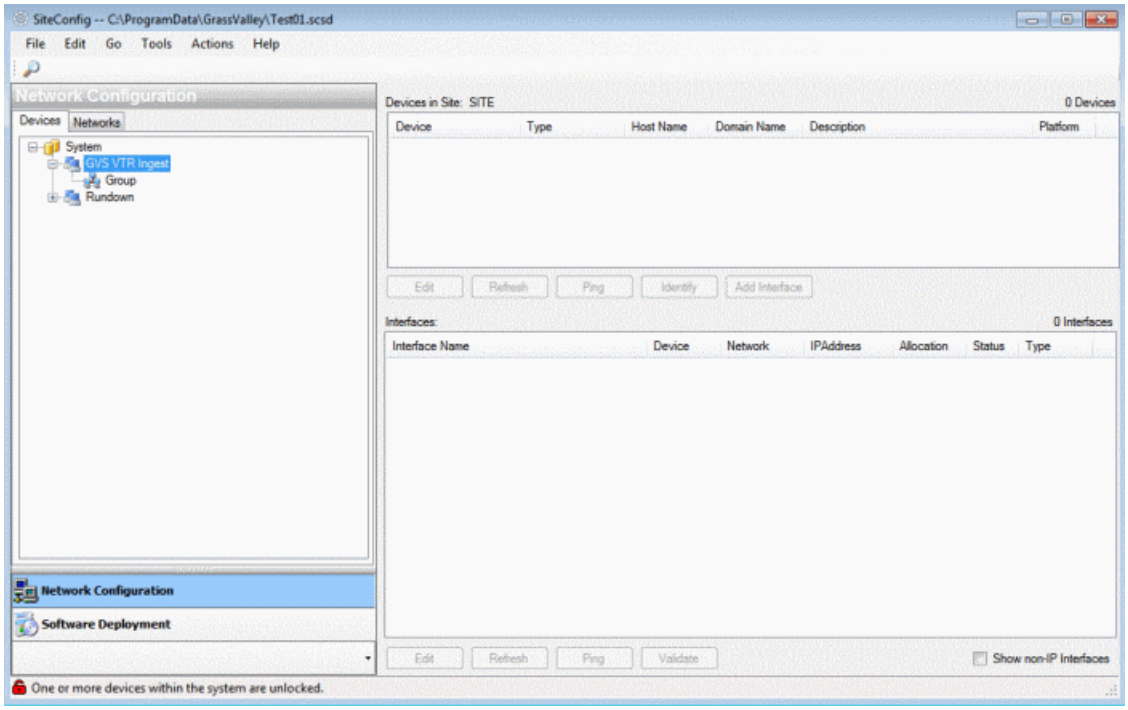
Follow the steps below for initial installation or upgrade of GV STRATUS VTR Ingest/GV STRATUS VTR Controller software with SiteConfig.

NOTE: To upgrade GV STRATUS VTR Ingest/GV STRATUS VTR Controller to version 11.8.x.x (and above) in SiteConfig, you are required to select the previous version of the package and run the uninstallation process first. Then select GV STRATUS VTR Ingest/GV STRATUS VTR Controller package 11.8.x.x (and above) to install.

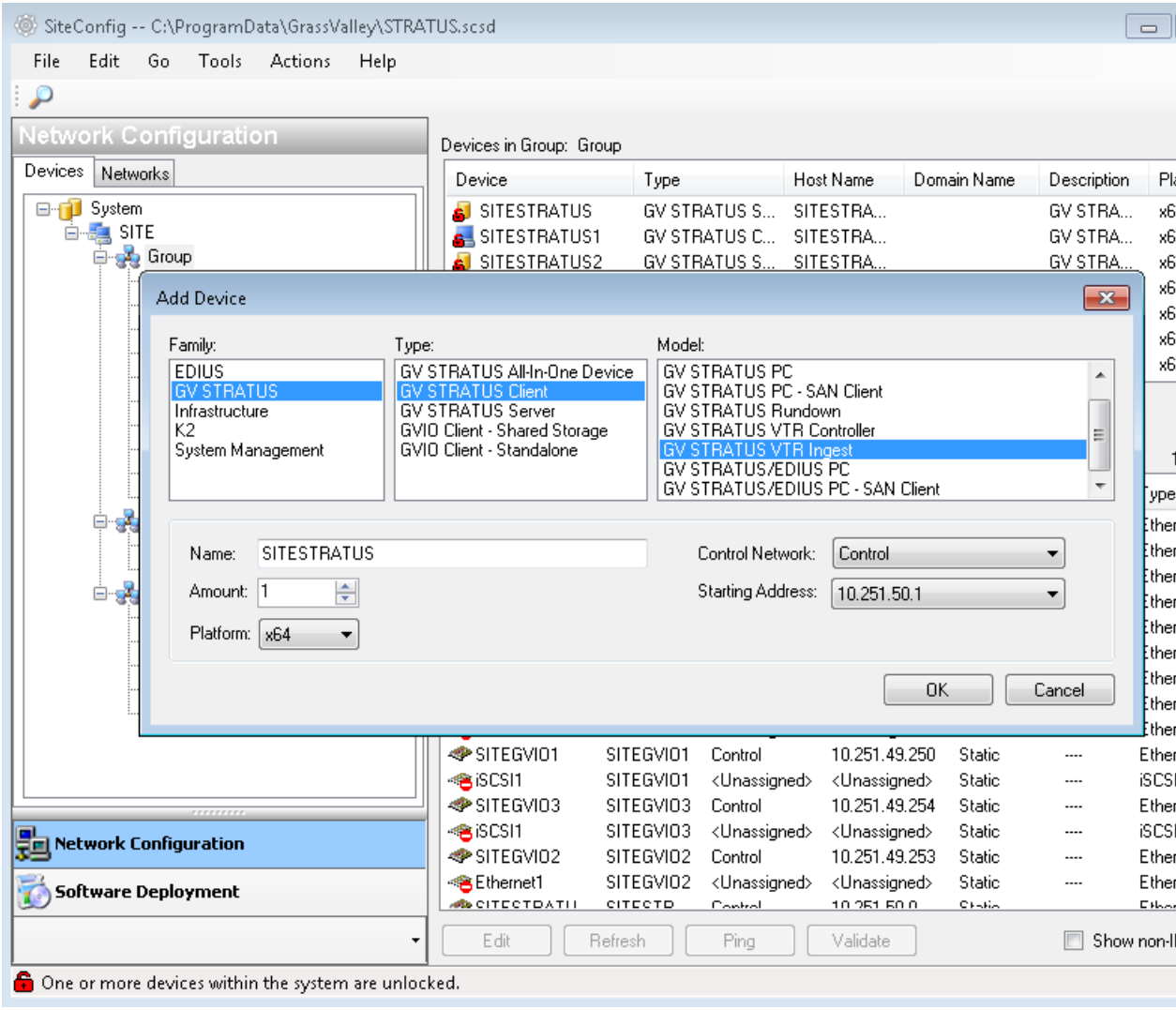
For an upgrade, you can modify steps accordingly.

1. Use the SiteConfig shortcut on the Windows desktop or in the Start menu to open SiteConfig.

2. The SiteConfig main window opens.



3. In the **Network Configuration | Devices** tab, right-click on a group and select **Add Device**.



The Add Device dialog box opens.

4. Configure settings for the GV STRATUS VTR Ingest as follows:

   - Family – Choose GV STRATUS.
   - Type - Choose GV STRATUS Client.
   - Model - Choose GV STRATUS VTR Ingest or GV STRATUS VTR Controller.
   - Name – Enter the GV STRATUS VTR Ingest or GV STRATUS VTR Controller device name.

     NOTE: This is the device name, as displayed in the SiteConfig device tree view and device list view. This name can be different than the host name (network name). You can accept the default name or enter a name of your choice. Devices in the tree view are sorted alphabetically.

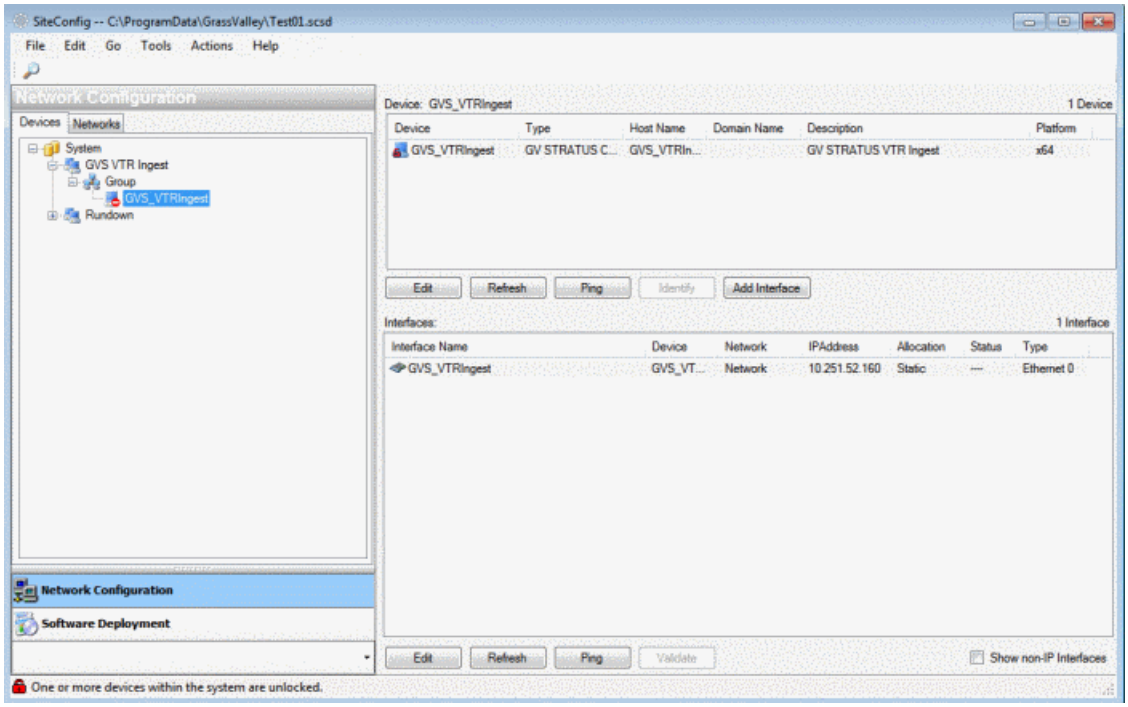
   - Amount – Select 1 since you are only adding one device.
   - Platform type - Select x64 if the device has a 64 bit OS.

     NOTE: Select x86 if the device has a 32 bit OS, x64 if it has a 64 bit OS.

   - Control Network – Defaulted to Control.
   - Starting Address – Select from the list of available addresses on the selected control network. If adding multiple devices, this is the starting address, with addresses assigned sequentially to each device added.

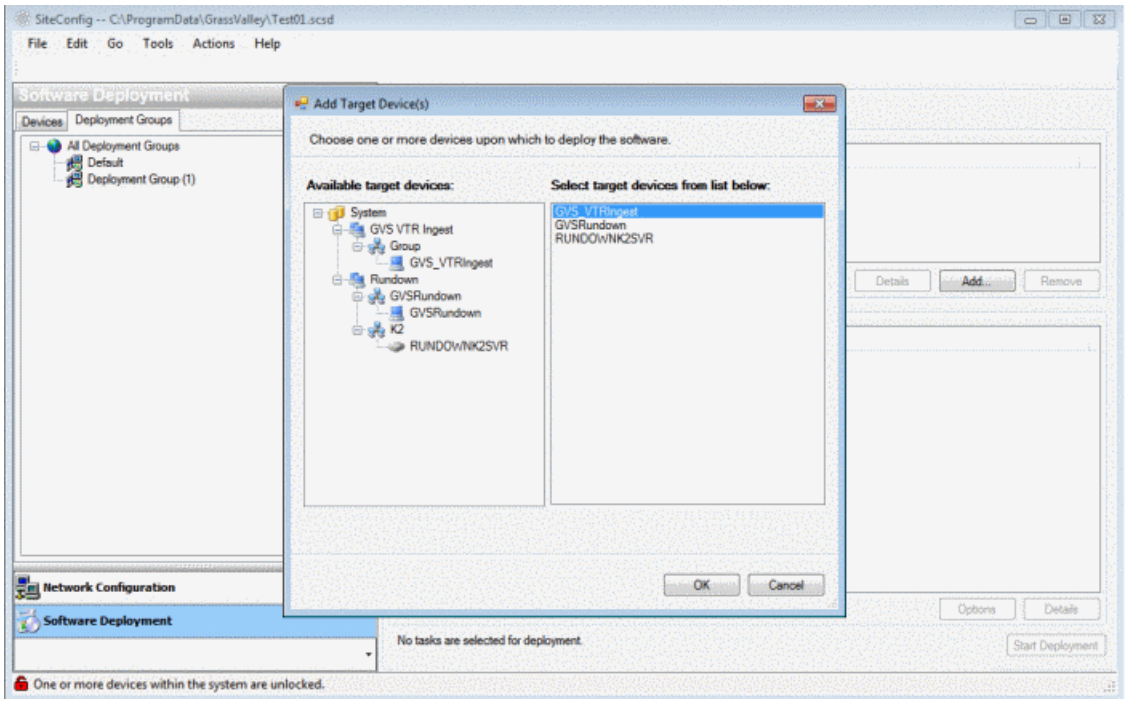
5. Click **OK** to save settings and close.

   A new device GV STRATUS VTR Ingest is successfully added.



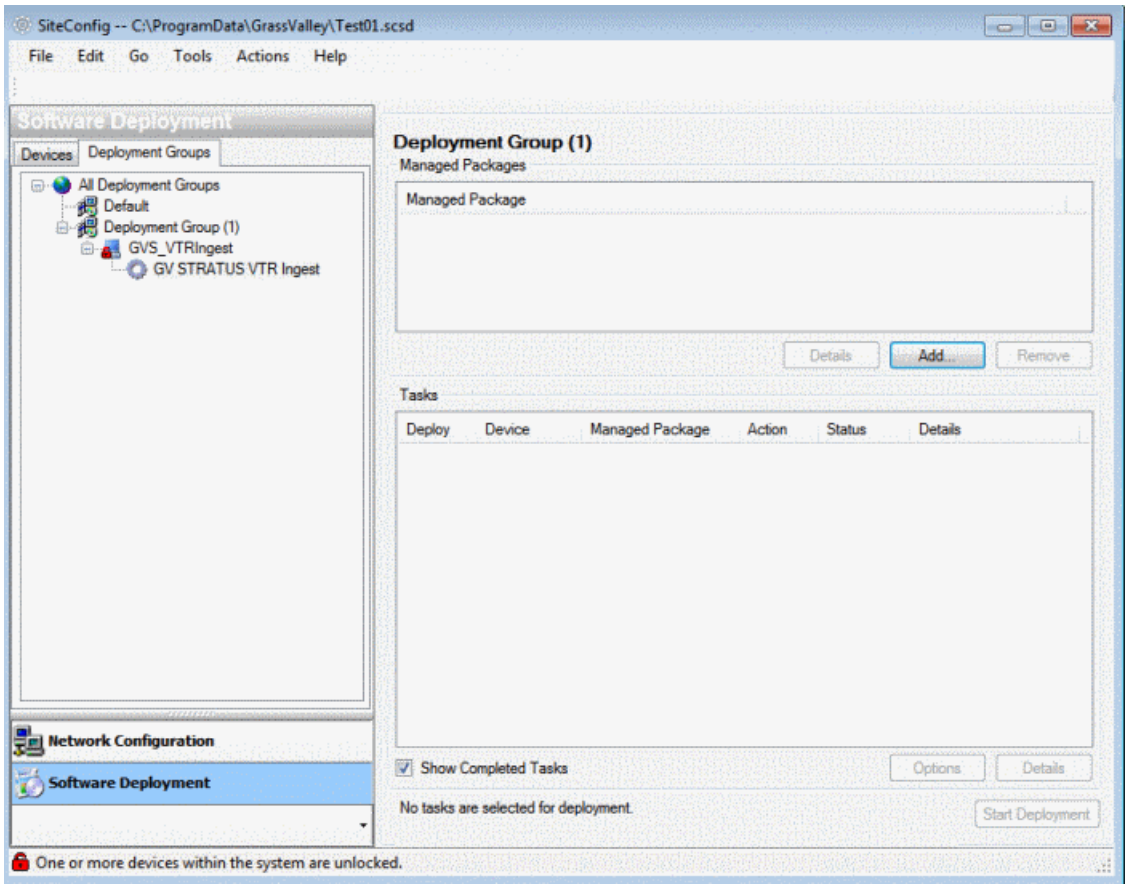
6. In the **Software Deployment | Deployment Groups** tab, right-click to add a new deployment group. Then right-click on the new deployment group and select **Add Target Device**.

   The Add Target Device(s) wizard opens.



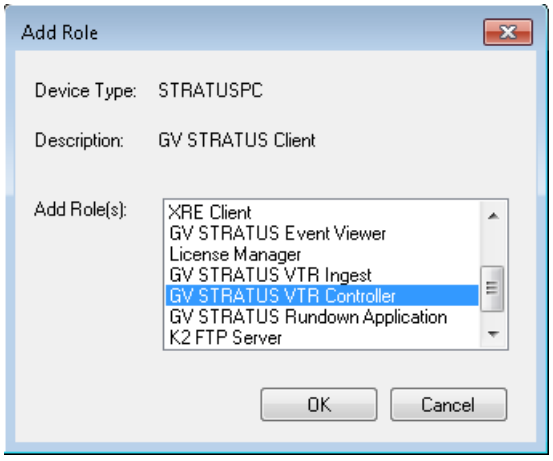
7. Select the device that you added earlier and click **OK**.

   GV STRATUS VTR Ingest appears in the Deployment Groups tree view under the deployment group.



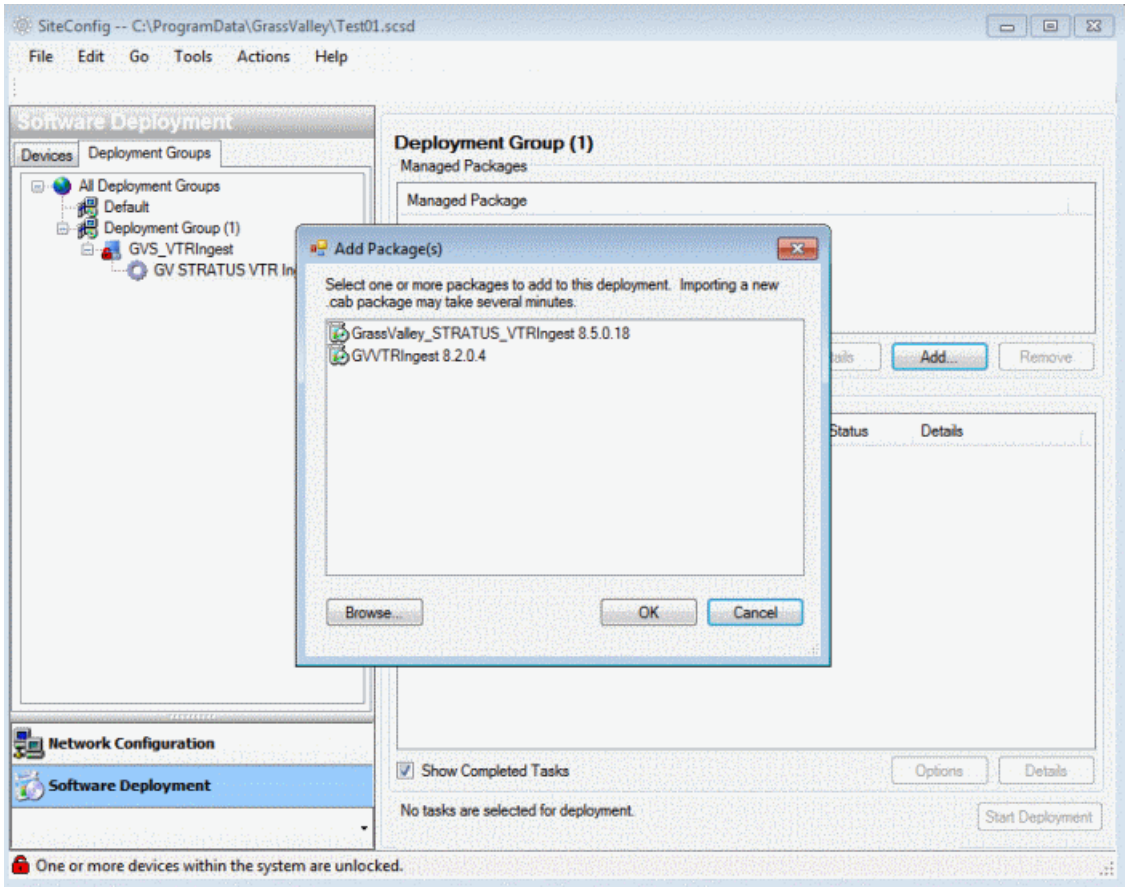
   You can also add GV STRATUS VTR Controller device if both are going to be installed on separate devices.

8. To add GV STRATUS VTR Controller to the same device, right-click on the device and select **Add Role | GV STRATUS VTR Controller**.



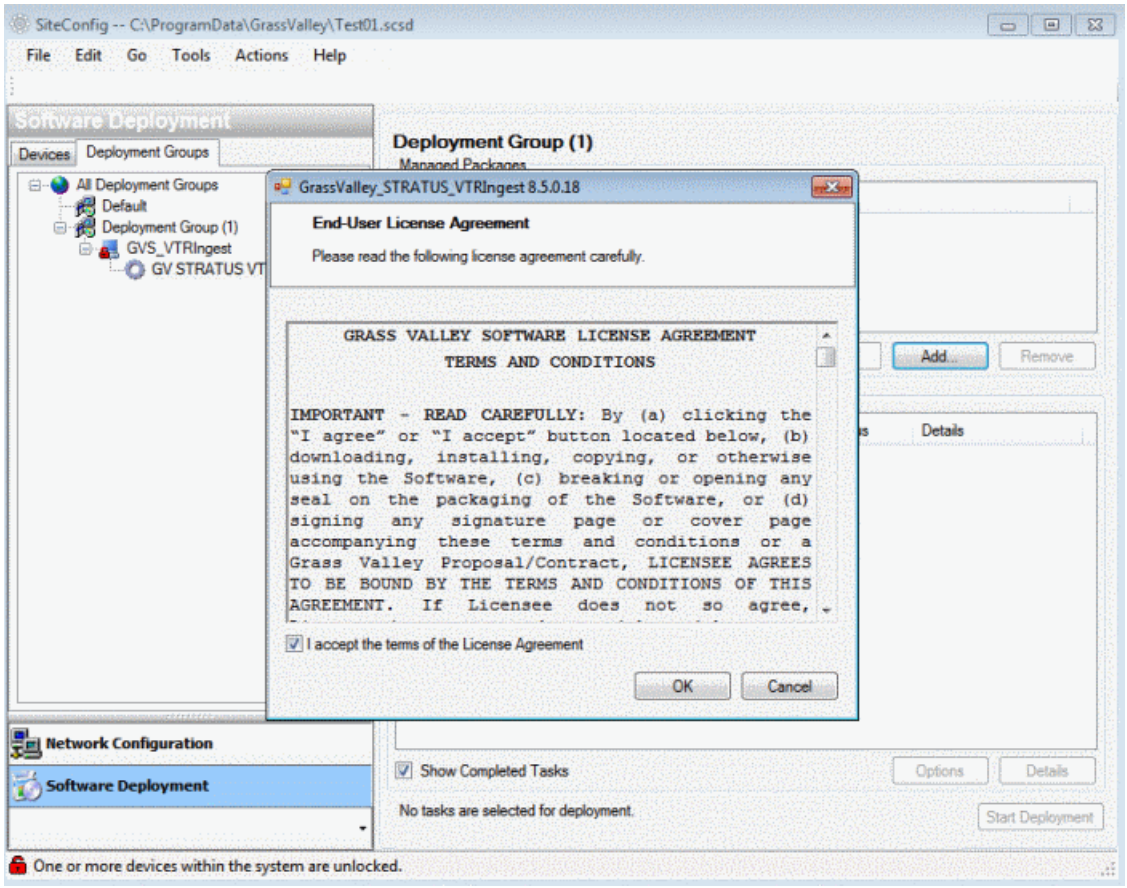
9. Click **OK**.
10. To add a software package to the deployment group, click the **Add** button on the right of the SiteConfig application.

    The Add Package(s) dialog box opens.



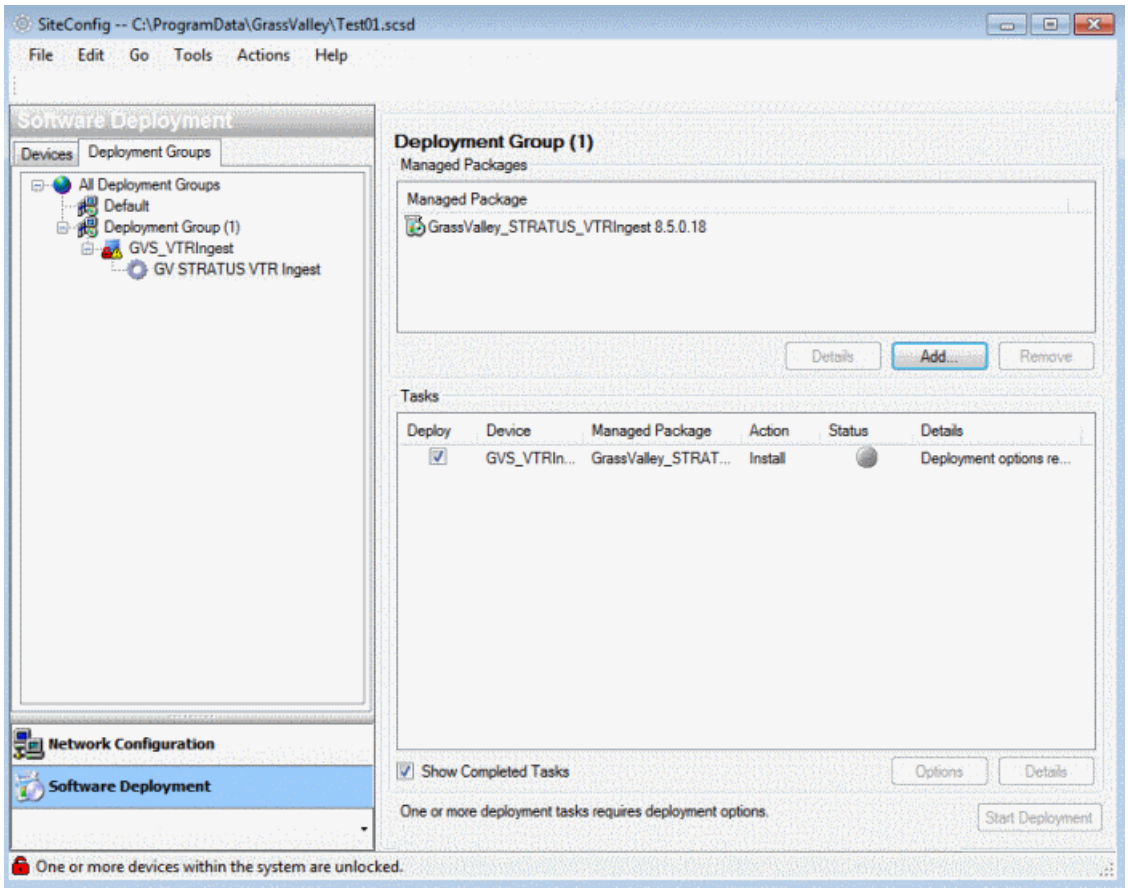
11. Select the GV STRATUS VTR Ingest/GV STRATUS VTR Controller package or both packages, and click **OK**.

12. EULA is displayed as follows and accept them to proceed.



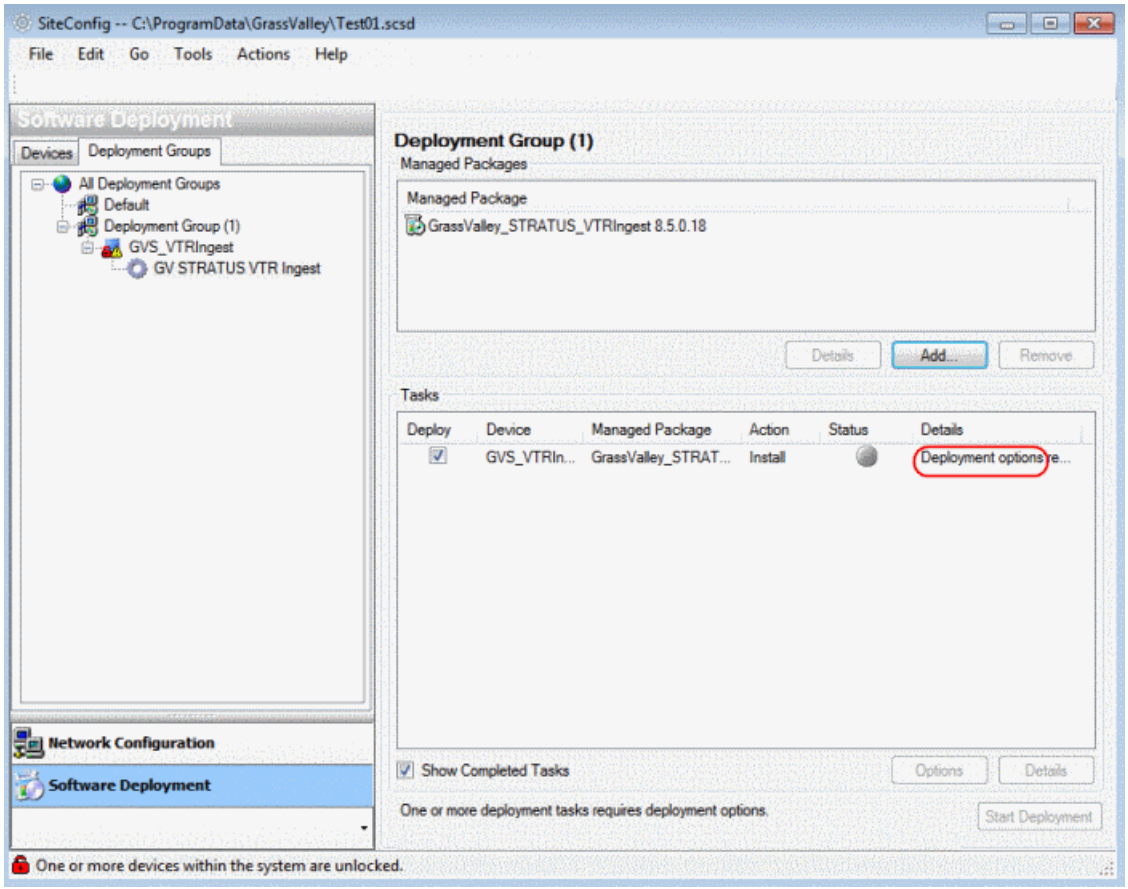
SiteConfig adds the package to the deployment group.

The package appears in the Managed Packages list for the selected deployment group. SiteConfig creates new software deployment tasks for the package and displays them in the Tasks list view.

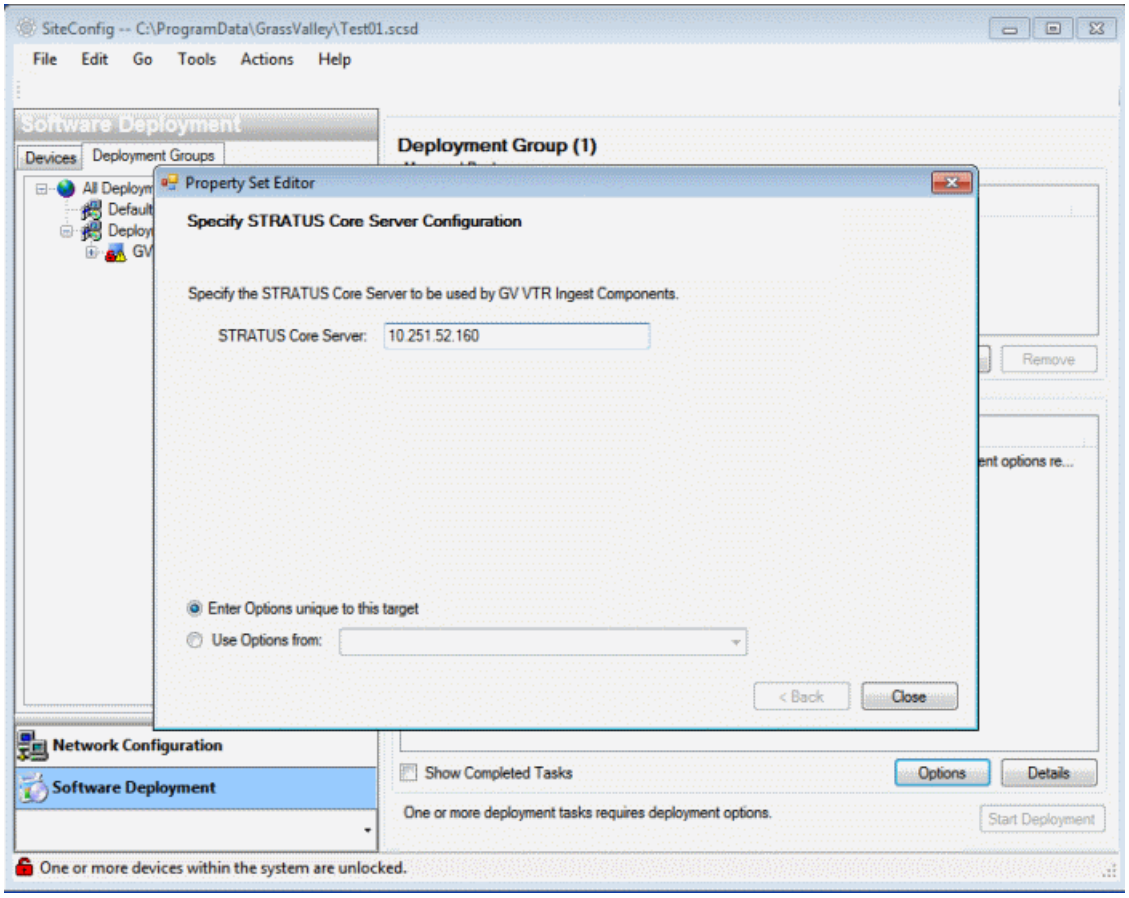

SiteConfig -- C:\ProgramData\GrassValley\Test01.scsd
File
Edit
Go
Tools
Actions
Help
Software Deployment
Devices
Deployment Groups
All Deployment Groups
Default
Deployment Group (1)
GVS_VTRIngest
GV STRATUS VTR Ingest
Network Configuration
Software Deployment
Deployment Group (1)
Managed Packages
Managed Package
GrassValley_STRATUS_VTRIngest 8.5.0.18
Details
Add...
Remove
Tasks
Deploy
Device
Managed Package
Action
Status
Details
GVS_VTRIn...
GrassValley_STRAT...
Install
Deployment options re...
Show Completed Tasks
Options
Details
One or more deployment tasks requires deployment options.
Start Deployment
One or more devices within the system are unlocked.

13. Do one of the following to set deployment options:

- Double-click the task.
- Select the task and click the **Options** button.



14. Work through the wizard to set options. In this example, the system is configured to connect to the GV STRATUS Core Server.



15. Click **Close** to save the deployment option.
16. Click the **Start Deployment** button to install GV STRATUS VTR Ingest/GV STRATUS VTR Controller.

Additional Topics

Refer to topics in this section as necessary as you work through upgrade processes.

Complete listing of device types, roles, and software packages for GV STRATUS devices

Software packages are SiteConfig `*.cab` files. You add packages to a SiteConfig deployment group in order to make the software available for deployment to the devices in the group. When a correctly added device has its SiteConfig roles assigned correctly, SiteConfig installs the appropriate package.

GV STRATUS Client PC low-resolution (proxy):

- SiteConfig "Add Device":
  - Family: GV STRATUS

    NOTE: Do not select the EDIUS family.
  - Device Type: GV STRATUS Client
  - Model: GV STRATUS PC or GV STRATUS/EDIUS PC (if using EDIUS XS)
- SiteConfig roles:
  - GV STRATUS Application
  - EDIUS (Required for EDIUS XS)
- Software packages:
  - *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValley_STRATUS_Application_x.x.x.cab*
    - *EDIUS_x.x.x.cab* (Required for EDIUS XS)

GV STRATUS Client PC high-resolution (iSCSI):

- SiteConfig "Add Device":
  - Family: GV STRATUS

    NOTE: Do not select the EDIUS family.
  - Device Type: GV STRATUS Client
  - Model: GV STRATUS PC - SAN Client or GV STRATUS/EDIUS PC - SAN Client (if using EDIUS Workgroup)
- SiteConfig Roles:
  - GV STRATUS Application
  - StorNext File System Client (non K2 only)
  - Generic iSCSI Client (non K2 only)

    NOTE: First install StorNext File System Client, then install Generic iSCSI Client via SiteConfig for the following:
    - ***First installation of GV STRATUS application into a system.***
    - ***When there is an upgrade of the StorNext File System Client.***
  - EDIUS (Required for EDIUS Workgroup)

- Software packages:
  - *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValley_STRATUS_Application_x.x.x.cab*
    - *GenericISCSI_x64_ x.x.x.cab*
    - *SNFS_nonK2_x64_x.x.x.cab*
    - *EDIUS_x.x.x.cab* (Required for EDIUS Workgroup).

GV STRATUS Express server:

- SiteConfig "Add Device":
  - Family: GV STRATUS
  - Device Type: GV STRATUS Server
  - Model: GV STRATUS Core Server Express

- SiteConfig Roles:
  - GV STRATUS Ingest Services (Required)
  - GV STRATUS Control Panel Service (Required)
  - GV STRATUS Common Services (Required)
  - License Manager (Required)
  - GV STRATUS Data Mover Engine (Required)
  - GV STRATUS Proxy Express Server (Required on Express server)
  - GV STRATUS Control Panel (Required)
  - GV STRATUS Core Services (Required)
  - GV STRATUS Database (Required)
  - GV STRATUS Summit MDI (Required)
  - GV STRATUS Common RESTful Archive MDI (Optional)
  - GV STRATUS Diva MDI (Optional)
  - GV STRATUS FlashNet MDI (Optional)
  - GV STRATUS Masstech MDI (Optional)
  - GV STRATUS Generic FTP MDI (Optional)
  - GV STRATUS Proxy Streaming Service (Optional)
  - GV STRATUS Rules Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV STRATUS Scheduled Transfer Engine (Optional)
  - GV STRATUS Scheduled Ingest Engine (Not used in this GV STRATUS release)
  - GV STRATUS Scheduled Ingest Manager (Not used in this GV STRATUS release)
  - GV STRATUS SocialMedia Engine (Optional)
  - GV STRATUS ExternalMedia Engine (Optional)
  - GV STRATUS Traffic Gateway (Optional)
  - GV STRATUS Topic Service Bus (Not used in this GV STRATUS release)
  - GV STRATUS Web Apps (Required. Must be assigned to Express/Core server to display Statistics panel via Dashboard)
  - GV STRATUS Web Client (Optional)
  - GV STRATUS Workflow Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV STRATUS Xcode Control Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV Log Manager (Required)
  - GV Log Viewer (Required)
  - GV STRATUS Rundown Server Components (Optional)
  - GV STRATUS Application (Use for test purposes only)
  - If optionally used as a Render Engine, these additional roles:
    - GV STRATUS Render Engine

- Software packages:
  - *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValley_STRATUS_IngestServices_x.x.x.cab*
    - *GrassValley_STRATUS_ControlPanelService_x.x.x.cab*
    - *GrassValley_STRATUS_CommonServices_x.x.x.cab*
    - *GrassValley_STRATUS_CoreServices_x.x.x.cab*
    - *GrassValley_STRATUS_ControlPanel_x.x.x.cab*
    - *GrassValley_STRATUS_Databases_x.x.x.cab*
    - *GrassValley_STRATUS_DataMover_x.x.x.cab*
    - *GrassValley_STRATUS_ExternalMedia_x.x.x.cab*
    - *GrassValley_STRATUS_HttpProxyServer_x.x.x.cab*
    - *GrassValley_STRATUS_Mediaflow_x.x.x.cab*
    - *GrassValley_STRATUS_CRArchive_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_DIVA_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_FlashNet_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_Masstech_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_GFTP_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_Summit_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_Proxy_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_ProxyStreamingService_x.x.x.cab*
    - *GrassValley_STRATUS_RenderEngine_x.x.x.cab*
    - *GrassValley_STRATUS_Rules_x.x.x.cab*
    - *GrassValley_STRATUS_ScheduledTransferEngine_x.x.x.cab*
    - *GrassValley_STRATUS_SocialMedia_x.x.x.cab*
    - *GrassValley_STRATUS_Transcode_x.x.x.cab*
    - *GrassValley_STRATUS_TrafficGateway_x.x.x.cab*
    - *GrassValley_STRATUS_WebApps_x.x.x.cab*
    - *GrassValley_STRATUS_WebClient_x.x.x.cab*
    - *GrassValley_Sabretooth_Application_x.x.x.cab*
    - *GrassValley_DeviceKeyService_x.x.x.cab*
    - *GrassValley_LogManager_x.x.x.cab*
    - *GrassValley_LogViewer_x.x.x.cab*
    - *GV_STRATUS_Rundown_x.x.x.cab*
  - *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValley_STRATUS_ControlPanel_x.x.x.cab*
    - *GrassValley_STRATUS_Application_x.x.x.cab* (Use for test purposes only)
  - *GrassValley_K2system_x.x.x.cab* for K2 9.8.x systems.
  - *GrassValley_K2Plus_x.x.x.cab* for K2 10.x systems.

GV STRATUS Core server:

- SiteConfig "Add Device":
  - Family: GV STRATUS
  - Device Type: GV STRATUS Server
  - Model: GV STRATUS Core Server
- SiteConfig Roles:
  - GV STRATUS Ingest Services (Required)
  - GV STRATUS Control Panel Service (Required)
  - GV STRATUS Common Services (Required)
  - License Manager (Required)
  - GV STRATUS Control Panel (Required)
  - GV STRATUS Core Services (Required)
  - GV STRATUS Database (Required)
  - GV STRATUS Data Mover Engine (Required)
  - GV STRATUS Summit MDI (Required)
  - GV STRATUS Common RESTful Archive MDI (Optional)
  - GV STRATUS Diva MDI (Optional)
  - GV STRATUS FlashNet MDI (Optional)
  - GV STRATUS Masstech MDI (Optional)
  - GV STRATUS Generic FTP MDI (Optional)
  - GV STRATUS Proxy Streaming Service (Optional)
  - GV STRATUS Rules Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV STRATUS Scheduled Transfer Engine (Optional)
  - GV STRATUS Scheduled Ingest Engine (Not used in this GV STRATUS release)
  - GV STRATUS Scheduled Ingest Manager (Not used in this GV STRATUS release)
  - GV STRATUS SocialMedia Engine (Optional)
  - GV STRATUS ExternalMedia Engine (Optional)
  - GV STRATUS Traffic Gateway (Optional)
  - GV STRATUS Topic Service Bus (Not used in this GV STRATUS release)
  - GV STRATUS Workflow Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV STRATUS Xcode Control Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV Log Manager (Required)
  - GV Log Viewer (Required)
  - GV STRATUS Web Apps (Required. Must be assigned to Express/Core server to display Statistics panel via Dashboard)
  - GV STRATUS Web Client (Optional)
  - GV STRATUS Rundown Server Components (Optional)
  - GV STRATUS Application (Use for test purposes only)

- Software packages:
  - *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValley_STRATUS_IngestServices_x.x.x.cab*
    - *GrassValley_STRATUS_ControlPanelService_x.x.x.cab*
    - *GrassValley_STRATUS_CommonServices_x.x.x.cab*
    - *GrassValley_STRATUS_CoreServices_x.x.x.cab*
    - *GrassValley_STRATUS_ControlPanel_x.x.x.cab*
    - *GrassValley_STRATUS_Databases_x.x.x.cab*
    - *GrassValley_STRATUS_DataMover_x.x.x.cab*
    - *GrassValley_STRATUS_ExternalMedia_x.x.x.cab*
    - *GrassValley_STRATUS_CRArchive_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_DIVA_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_FlashNet_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_Masstech_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_GFTP_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_Summit_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_Proxy_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_ProxyStreamingService_x.x.x.cab*
    - *GrassValley_STRATUS_Mediaflow_x.x.x.cab*
    - *GrassValley_STRATUS_Rules_x.x.x.cab*
    - *GrassValley_STRATUS_ScheduledTransferEngine_x.x.x.cab*
    - *GrassValley_STRATUS_SocialMedia_x.x.x.cab*
    - *GrassValley_STRATUS_Transcode_x.x.x.cab*
    - *GrassValley_STRATUS_TrafficGateway_x.x.x.cab*
    - *GrassValley_STRATUS_WebApps_x.x.x.cab*
    - *GrassValley_STRATUS_WebClient_x.x.x.cab*
    - *GrassValley_Sabretooth_Application_x.x.x.cab*
    - *GrassValley_DeviceKeyService_x.x.x.cab*
    - *GrassValley_LogManager_x.x.x.cab*
    - *GrassValley_LogViewer_x.x.x.cab*
    - *GV_STRATUS_Rundown_x.x.x.cab*
  - *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValley_STRATUS_ControlPanel_x.x.x.cab*
    - *GrassValley_STRATUS_Application_x.x.x.cab* (Use for test purposes only)
  - *GrassValley_K2system_x.x.x.cab* for K2 9.8.x systems.
  - *GrassValley_K2Plus_x.x.x.cab* for K2 10.x systems.

GV STRATUS Proxy server:

- SiteConfig "Add Device":
  - Family: GV STRATUS
  - Device Type: GV STRATUS Server
  - Model: GV STRATUS Proxy Server
- SiteConfig Roles:
  - GV STRATUS Proxy K2 SAN Server
  - GV Log Manager
  - StorNext File System Client
- Software packages:
  - *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValley_STRATUS_HttpProxyServer_x.x.x.cab*
    - *GrassValley_LogManager_x.x.x.cab*
  - *GrassValley_STRATUSClient_x.x.x.cab*.
  - For K2 9.8.x systems; use *GrassValley_K2system_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValleyK2Server_x64_9.8.x.x.cab*
    - *SNFS_x64_4.7.x.xxx.cab*
  - For K2 10.x systems; use *GrassValley_K2Plus_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValleyK2Server_x64_10.x.x.cab*
    - *SNFS_x64_6.0.x.xxx.cab*

GV STRATUS Proxy Storage file system server:

- SiteConfig "Add Device":
  - Family: GV STRATUS
  - Device Type: GV STRATUS Server
  - Model: GV STRATUS Proxy Storage File System Server
- SiteConfig Roles:
  - GV STRATUS Proxy Storage Server
  - GV Log Manager
  - StorNext File System Server
  - StorNext File System Client

- Software packages:
  - *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValley_STRATUS_HttpProxyServer_x.x.x.cab*
    - *GrassValley_LogManager_x.x.x.cab*
  - *GrassValley_STRATUSClient_x.x.x.cab*.
  - For K2 9.8.x systems; use *GrassValley_K2system_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValleyK2Server_x64_9.8.x.x.cab*
    - *SNFS_x64_4.7.x.xxx.cab*
  - For K2 10.x systems; use *GrassValley_K2Plus_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValleyK2Server_x64_10.x.x.cab*
    - *SNFS_x64_6.0.x.xxx.cab*

GV STRATUS Render Engine Server:

- SiteConfig "Add Device":
  - Family: GV STRATUS
  - Device Type: GV STRATUS Server
  - Model: GV STRATUS Render Engine
- SiteConfig Roles:
  - GV STRATUS Control Panel
  - GV Log Manager
  - StorNext File System Client
  - GV Embedded Security Manager
  - GV STRATUS Render Engine

- Software packages:
  - *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValley_STRATUS_RenderEngine_x.x.x.cab*
    - *GVEmbeddedSecurityManager_x.x.x.cab*
    - *GrassValley_Sabretooth_Application_x.x.x.cab*
    - *GrassValley_LogManager_x.x.x.cab*
  - For K2 9.8.x systems; use *GrassValley_K2system_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValleyK2Server_x64_9.8.x.x.cab*
    - *SNFS_x64_4.7.x.xxx.cab*
  - For K2 10.x systems; use *GrassValley_K2Plus_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValleyK2Server_x64_10.x.x.cab*
    - *SNFS_x64_6.0.x.xxx.cab*
  - *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValley_STRATUS_Application_x.x.x.cab*
    - *GrassValley_STRATUS_ControlPanel_x.x.x.cab*

GV STRATUS Workflow Server:

- SiteConfig "Add Device":
  - Family: GV STRATUS
  - Device Type: GV STRATUS Server
  - Model: GV STRATUS Workflow Server
- SiteConfig Roles:
  - GV STRATUS Workflow Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV STRATUS Rules Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV STRATUS SocialMedia Engine (Optional)
  - GV STRATUS ExternalMedia Engine (Optional)
  - GV STRATUS Xcode Control Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV STRATUS Control Panel
  - GV Log Manager

- Software packages:
  - *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValley_STRATUS_Mediaflow_x.x.x.cab*
    - *GrassValley_STRATUS_Rules_x.x.x.cab*
    - *GrassValley_STRATUS_SocialMedia_x.x.x.cab*
    - *GrassValley_STRATUS_ExternalMedia_x.x.x.cab*
    - *GrassValley_STRATUS_Transcode_x.x.x.cab*
    - *GrassValley_STRATUS_TrafficGateway_x.x.x.cab*
    - *GrassValley_Sabretooth_Application_x.x.x.cab*
    - *GrassValley_LogManager_x.x.x.cab*
  - *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValley_STRATUS_ControlPanel_x.x.x.cab*
  - *GrassValley_K2system_x.x.x.cab* for K2 9.8.x systems.
  - *GrassValley_K2Plus_x.x.x.cab* for K2 10.x systems.

GV STRATUS roles matrix

Key:

- AA = Automatically Added for a User or Group with that license (except during version upgrades).
- P = Possible to add for a User or Group with that license.
- X = Not available to be added for a User or Group with that license.

	News room Basic	Express	Flex	Pro	Elite	Enables a Group or User:
Advanced Editor	X	X	AA	AA	AA	Enables a Group or User: Access to Go! Web Client Editor.
Advanced Logging	X	X	X	AA	AA	Access to Advanced Logging tool.
Archive Rights	X	AA	AA	AA	AA	Ability to archive Assets.
Assignment List	AA	AA	AA	AA	AA	Access to Assignment List tool.
Auto Logout	AA	AA	AA	AA	AA	To be automatically logged off as part of Auto Logout scope.
Bin Creation Rights	AA	AA	AA	AA	AA	Ability to create Bins.

Change Thumbnail Rights	AA	AA	AA	AA	AA	Ability to upload, set, and delete Thumbnails.
Channel Panel	X	X	X	AA	AA	Access to Channel Panel tool.
Copy Metadata	AA	AA	AA	AA	AA	Ability to copy and paste Metadata.
Dashboard	X	P	P	P	P	Access to Dashboard node.
Dashboard - Channel Status	X	X	P	P	P	Access to Channel Status Dashboard (Dashboard Role Also Required).
Dashboard - Quotas	X	P	P	P	P	Access to Quota Dashboard (Dashboard Role Also Required).
Dashboard - Social Media	X	P	P	P	P	Access to Social Media Dashboard (Dashboard Role Also Required).
Dashboard - Statistics	X	P	P	P	P	Access to Statistics Dashboard (Dashboard Role Also Required).
Dashboard - Storage	X	P	P	P	P	Access to Storage Dashboard (Dashboard Role Also Required)
Delete Rights	AA	AA	AA	AA	AA	Ability to delete Bins, Assets, and Associations.
Edius Project Management	X	P	P	P	P	Access to EDIUS Projects node.
Edius XS	X	X	AA	AA	AA	Ability to launch Assets into EDIUS XS.
Export Rights	AA	AA	AA	AA	AA	Ability to export Assets.
Media Manager	X	P	P	P	P	See note below.
Missing Material List	P	P	P	P	P	GV Developer Use Only.
Move Rights	AA	AA	AA	AA	AA	Ability to move Assets (Locations and Groups) (Delete Rights Role Also Required).
Multisite Access	X	AA	AA	AA	AA	Access and search for remote Assets.
Playlist Editor	X	X	X	AA	AA	Access to Playlist Editor tool.

Queue Management	X	AA	AA	AA	AA	Ability to set job priority within Job Monitor.
Rename Asset Rights	AA	AA	AA	AA	AA	Ability to rename Assets.
Rename Bin Rights	AA	AA	AA	AA	AA	Ability to rename Bins in Locations node.
Restore Rights	X	AA	AA	AA	AA	Ability to restore Assets as copy.
RMI	X	X	X	AA	AA	Access to RMI tool.
Schedule Monitor	X	AA	AA	AA	AA	Access to Schedule Monitor under Monitors node.
Scheduled Transfer	X	X	X	X	P	Access to Scheduled Transfer tool.
Scheduler	X	X	X	X	AA	Access to Scheduler tool.
Scheduler (Read Only)	X	AA	AA	AA	P	Access to Read-Only Scheduler tool.
Security Manager	X	P	P	P	P	Bypass security/permissions, modify any Bin, Group, or Asset permissions, owner, and owner hint, plus all Media Manager functionality.
Segmentation	X	AA	AA	AA	AA	Access to Segmentation tool and House Number tool. Ability to make Segments in Web Client.
Send Message	X	AA	AA	AA	AA	Access to Send Message tool.
Simple Editor	X	AA	AA	AA	AA	Access to Simple Editor tool and Lost and Found group.
Source Viewer	X	AA	AA	AA	AA	Access to Source Viewer tool.
Storyboard Editor	X	AA	AA	AA	AA	Access to Storyboard Editor tool.
Trim Rights	AA	AA	AA	AA	AA	Ability to Trim and Untrim Assets.
Web Monitor	X	AA	AA	AA	AA	Access to Web Monitor tool for web pages.
Web Access	AA	AA	AA	AA	AA	Access to GV STRATUS Web Client shortcut nodes.

Notes:

Media Manager Role:

- Enables Archive Rights
- Enables Restore Rights as copy and also as move
- Enables Extended Delete Type Options (Delete Rights Role Also Required)
- Enables the ability to save Public Searches
- Enables access to the Lost and Found group
- Enables access to the Archives in Devices node
- Enables the ability to copy and paste Metadata even if Denied
- Enables an API account to create Custom Metadata for Markers and Keywords

The Deny Role option disables a role's functionality or tool(s) for a specific User or Group.

Example: Enable Delete Rights for Group X members, then Deny Delete Rights for User Y of Group X.

Related Topics

If you have trouble launching EDIUS XS on page 169

About Auto Logout

The purpose of the Auto Logout role is to release the GV STRATUS license that is assigned to a system that has been idle for a long period of time. This returns the license to the pool of available licenses and makes it available for use by another GV STRATUS application.

In GV STRATUS Control Panel, the Auto Logout role can be assigned to groups and users. When a user account with this role is logged on to the GV STRATUS application, the GV STRATUS system monitors the host PC for activity and triggers the auto logout process if appropriate. This process is configured in Auto Logout settings.

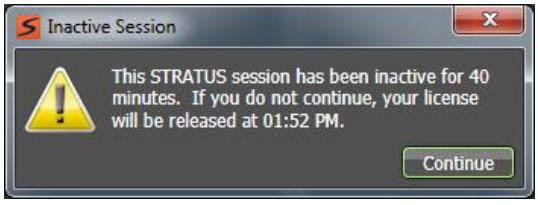
To locate these settings, click **General | License Management | Auto Logout**

The following setting specifies the timing of the auto logout process:

Setting or button	Description
STRATUS Application Timeout	The length of time the PC that hosts the GV STRATUS application must sit idle, with no activity, before that PC's GV STRATUS license is released.

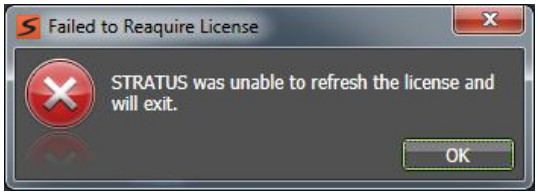
The auto logout process occurs as follows:

1. Five minutes before the timeout, a dialog box opens with a message specifying the time the license is to be released.



2. If a user clicks **Continue** within five minutes, the auto logout process is discontinued and the timeout is reset.
3. If there is no interaction with the message dialog box within five minutes, the dialog box closes and another dialog box opens. This second dialog box displays a message that the license is released and provides options to log off the GV STRATUS application or to refresh the license.

4. The license used currently by the GV STRATUS application is returned to the pool of available licenses. Until an option is selected, the GV STRATUS application and the dialog box remain open. The GV STRATUS application is unusable, but current work is retained.
5. When the option to refresh the license is selected, if a license is available, the GV STRATUS application is licensed and becomes usable. If a license is not available, a dialog box opens with a message about the license. Clicking **OK** logs out and closes the GV STRATUS application.



Related Topics

Auto Logout settings on page 368

Summary of previous GV STRATUS upgrades

Previous upgrades are summarized in the following topics. To upgrade to a previous version, refer to the upgrade instructions for the specific version. Do not attempt a previous upgrade based on the information in these topics alone.

Summary of upgrade from version 1 to version 2

Several STRATUS servers are affected by the version 1 to version 2 upgrade, as follows:

- Core/Common server — In version 1, the STRATUS server provided licensing and user preference functionality, and was referred to as a "Common" server. In version 2 the server additionally provides extended media management functionality, including the STRATUS database and associated software components. The version 2 server is referred to as a "Core" server. The added functionality in version 2 requires that the server be removed and then reconfigured in the STRATUS system.

- Proxy Encoder — A STRATUS server that creates low resolution proxy assets. If a high resolution asset does not yet have associated proxy, the Proxy Encoder creates it. The Proxy Encoder software that provides this functionality can run on a dedicated Proxy Encoder server or on a STRATUS server that has other roles as well, such as a STRATUS Express server. The Proxy Encoder is a new type of STRATUS server for version 2.
- Express server — Similar to Core/Common server, the version 2 Express server provides extended media management functionality. If the STRATUS system does not have a Proxy Encoder, the Express server can also provide functionality similar to the Proxy Encoder. The added functionality in version 2 requires that the server be removed and then reconfigured in the STRATUS system.

Several upgrade tasks are specific to the version 1 to version 2 upgrade. Apply upgrade tasks as appropriate for your system design, as follows:

- Express system — Remove the Express server from SiteConfig and then add it back to SiteConfig, in order to reconfigure roles appropriate for version 2 functionality. If your system does not include a Proxy Encoder, make sure Express server roles support proxy encoding. If your system includes a Proxy Encoder, add it to your system.
- A1, B1 systems — Remove the Common/Core server from SiteConfig and then add it back to SiteConfig, in order to reconfigure roles appropriate for version 2 functionality. Also add one or more Proxy Encoders to your system.

Summary of upgrade from version 1 to version 2.5

GV STRATUS servers are affected by the version 1 to version 2.5 upgrade, as follows:

- Core/Common server — In version 1, the GV STRATUS server provided licensing and user preference functionality, and was referred to as a "Common" server. In version 2.0 and higher the server additionally provides extended media management functionality, including the GV STRATUS database and associated software components. The version 2.0 and higher server is referred to as a "Core" server. The added functionality requires that the server be removed and then reconfigured in the GV STRATUS system.
- Proxy Encoder — A GV STRATUS server that creates low resolution proxy assets. If a high resolution asset does not yet have associated proxy, the Proxy Encoder creates it. The Proxy Encoder software that provides this functionality can run on a dedicated Proxy Encoder server or on a GV STRATUS server that has other roles as well, such as a GV STRATUS Express server. The Proxy Encoder is a new type of GV STRATUS server for version 2.0 and higher.
- Conform Server — A GV STRATUS server dedicated to hosting the Conform Engine Service. This service renders a complex asset, such as a sequence, into a clip that can be played on a K2/Summit system. The Conform Server is a new type of GV STRATUS server for version 2.5.
- Express server — Similar to Core/Common server, the version 2.0 and higher Express server provides extended media management functionality. If the GV STRATUS system does not have a Proxy Encoder, the Express server can also provide functionality similar to that server. The added functionality requires that the server be removed and then reconfigured in the GV STRATUS system.

Several upgrade tasks are specific to the version 1 to version 2.5 upgrade. Apply upgrade tasks as appropriate for your system design, as follows:

- Express system:
  - Remove the Express server from SiteConfig and then add it back to SiteConfig, in order to reconfigure roles appropriate for new functionality.
  - If your Express system does not include a dedicated Proxy Encoder, make sure Express server roles support that functionality. If your system includes dedicated Proxy Encoders, add the Proxy Encoder servers to your system.
  - If your system includes dedicated Conform Servers, add the Conform Servers to your system.
  - If your Express system includes an archive system, configure SiteConfig roles, install software and licenses and configure as appropriate for your archive system.
- A1, B1 systems:
  - Remove the Common/Core server from SiteConfig and then add it back to SiteConfig, in order to reconfigure roles appropriate for new functionality.
  - Add one or more Proxy Encoders to your system.
  - Add one or more Conform Servers to your system.
  - If your A1/B1 system includes an archive system, configure SiteConfig roles, install software and licenses and configure as appropriate for your archive system.

Summary of upgrade from version 2.0 to version 2.5

GV STRATUS servers are affected by the version 2 to version 2.5 upgrade, as follows:

- Conform Server — A GV STRATUS server dedicated to hosting the Conform Engine Service. This service renders a complex asset, such as a GV STRATUS sequence, into a simple clip. The Conform Server is a new type of GV STRATUS server for version 2.5.

Several upgrade tasks are specific to the version 2 to version 2.5 upgrade. Apply upgrade tasks as appropriate for your system design, as follows:

- Express system:
  - If your system includes dedicated Conform Servers, add the Conform Servers to your system.
  - If your Express system includes an archive system, configure SiteConfig roles, install software and licenses and configure as appropriate for your archive system.
- A1, B1 systems:
  - Add one or more Conform Servers to your system.
  - If your A1/B1 system includes an archive system, configure SiteConfig roles, install software and licenses and configure as appropriate for your archive system.

Summary of upgrade from version 2.5 to version 2.7

GV STRATUS servers are affected by the version 2.5 to version 2.7 upgrade, as follows:

- EDIUS XRE Server — A server dedicated to hosting EDIUS XRE Management Server/XRE Node and XRE Monitor (management node) software. This software performs a rendering process when exporting a project created in EDIUS. The EDIUS XRE Server is a new type of GV STRATUS server for version 2.7.

Several upgrade tasks are specific to the version 2.5 to version 2.7 upgrade. Apply upgrade tasks as appropriate for your system design, as follows:

- All systems:
  - The following items are lost when upgrading, so before you upgrade make a record of your settings with version 2.5 so that you can reconfigure after upgrading to version 2.7:
    - Authorization Manager settings, including all assignments of license and roles to groups and users.
    - Favorites
    - Saved searches
  - Rules: After the upgrade you can configure export and delete rules.
  - Delete Rights: After the upgrade you can deny delete rights to groups and users.
  - EDIUS XS: After the upgrade you can install the EDIUS application on your STRATUS Client PCs. Requires EDIUS license.
- A1, B1 systems:
  - Add one or more EDIUS XRE Servers to your system.

Summary of upgrade from version 2.5 to version 2.7.5

GV STRATUS servers are affected by the version 2.5 to version 2.7 upgrade, as follows:

- EDIUS XRE Server — A server dedicated to hosting EDIUS XRE Management Server/XRE Node and XRE Monitor (management node) software. This software performs a rendering process when exporting a project created in EDIUS. The EDIUS XRE Server is a new type of GV STRATUS server for version 2.7.

Several upgrade tasks are specific to the version 2.5 to version 2.7 upgrade. Apply upgrade tasks as appropriate for your system design, as follows:

- All systems:
  - The following items are lost when upgrading, so before you upgrade make a record of your settings with version 2.5 so that you can reconfigure after upgrading to version 2.7:
    - Authorization Manager settings, including all assignments of license and roles to groups and users.
    - Favorites
    - Saved searches
  - Rules: After the upgrade you can configure export and delete rules.
  - Delete Rights: After the upgrade you can deny delete rights to groups and users.
  - EDIUS XS: After the upgrade you can install the EDIUS application on your STRATUS Client PCs. Requires EDIUS license.
- A1, B1 systems:
  - Add one or more EDIUS XRE Servers to your system.

Summary of upgrade from version 2.5 to version 2.8

GV STRATUS servers are affected by the version 2.5 to version 2.8 upgrade, as follows:

- EDIUS XRE Server — A server dedicated to hosting EDIUS XRE Management Server/XRE Node and XRE Monitor (management node) software. This software performs a rendering process when exporting a project created in EDIUS. The EDIUS XRE Server is a new type of GV STRATUS server for version 2.7.
- Workflow Server — A GV STRATUS server dedicated to hosting the Workflow Engine Service, the Rules Engine Service, and the Xcode Control Engine Service. These services support rules-based operations. The Workflow Server is a new type of GV STRATUS server for version 2.8.

Several upgrade tasks are specific to the version 2.5 to version 2.8 upgrade. Apply upgrade tasks as appropriate for your system design, as follows:

- All systems:
  - The following items are lost when upgrading. For settings you want to save, make a record of your settings with version 2.5 so that you can reconfigure after upgrading to version 2.8:
    - Authorization Manager settings, including all assignments of license and roles to groups and users.
    - Favorites
    - Saved searches
  - Rules: After the upgrade you can configure export, transfer, and delete rules.
  - Delete Rights: After the upgrade you can deny delete rights to groups and users.
  - EDIUS XS: After the upgrade you can install the EDIUS application on your GV STRATUS Client PCs. Requires EDIUS license.
  - EDIUS Elite: If you have existing high-resolution (iSCSI SAN-attached) client PCs with EDIUS Elite installed, you must manually uninstall EDIUS and supporting software before upgrading.
  - Segmentation: After the upgrade, you can configure and use Segmentation features if desired.
- A1, B1, C1 systems:
  - Add one or more EDIUS XRE Servers to your system.
  - Add one or more Workflow Servers to your system.

Summary of upgrade from version 2.7 to version 2.8

GV STRATUS servers are affected by the version 2.7 to version 2.8 upgrade, as follows:

- Workflow Server — A GV STRATUS server dedicated to hosting the Workflow Engine Service, the Rules Engine Service, and the Xcode Control Engine Service. These services support rules-based operations. The Workflow Server is a new type of GV STRATUS server for version 2.8.

Several upgrade tasks are specific to the version 2.7 to version 2.8 upgrade. Apply upgrade tasks as appropriate for your system design, as follows:

- All systems:
  - Rules: If you configured export and delete rules before the upgrade, after the upgrade you can additionally configure transfer rules. If you license your GV STRATUS system and install the Harmonic ProMedia™ Carbon (formerly Carbon Coder™) application, you can also configure an export rule with transcode functionality.

- A1, B1, C1 systems:
  - Add one or more Workflow Servers to your system.

    If you currently have the GV STRATUS Rules Engine and the GV STRATUS Workflow Engine installed on your Core Server and you are adding a Workflow server, you must do the following:

    - Uninstall the GV STRATUS Rules Engine and the GV STRATUS Workflow Engine from the Core Server.
    - Reconfigure your rules on the Workflow Server

Summary of upgrade from version 2.8 to version 3.1

Several upgrade tasks are new or require special consideration with the upgrade from version 2.8 to version 3.1. Apply upgrade tasks as appropriate for your system design, as follows:

- All systems:
  - Windows update: KB2859537 and KB2872339 not supported on Grass Valley devices.
  - .NET upgrade: All GV STRATUS servers (including EDIUS XRE) and all client PCs hosting a GV STRATUS application and/or an EDIUS application must upgrade to .NET 4.5, if that version of .NET is not already installed.
  - Services: In SiteConfig, for your GV STRATUS Express server or GV STRATUS Core server add roles to install GV STRATUS Data Mover Engine.
  - GV Event Viewer: In SiteConfig, for all STRATUS servers, add a role to install GV Event Viewer.
  - HTTP server: After the upgrade, in GV STRATUS Control Panel, configure settings for HTTP server and SMB server.
  - Trim Rights: After the upgrade, in GV STRATUS Control Panel, assign the "Trim Rights" role to users and groups.
  - Rules: After the upgrade you can additionally configure archive rules and transfer rules. If you license your GV STRATUS system to work with your transcoding application, you can also configure an export rule with transcode functionality.
  - Licenses: The following optional licenses are available with this release.
    - STRATUS-XCODECONTROLVANTAGE (Optional): If you license your GV STRATUS system and install the Telestream Vantage™ application, you can configure an export rule with Vantage transcode functionality.
    - STRATUS-MULTISITE (Optional): If you have multiple sites with GV STRATUS systems, you can license one or more systems and configure them to access assets on remote sites.
  - Search index: After the upgrade, the GV STRATUS database is automatically indexed to support enhanced search features. This can take several hours, depending on the size of your GV STRATUS database. During this time Search features and Rules features are not fully functional. In GV STRATUS Control Panel, click **Core | Search Index Config** to view indexing progress.

- Systems using Segmentation features:
  - Services: In SiteConfig, for your GV STRATUS Express server or GV STRATUS Core server add roles to install GV STRATUS Traffic Gateway.
- Systems with high-resolution client PCs, such as those using the RMI tool or a high-resolution editor:
  - After the upgrade, in GV STRATUS Control Panel Proxy Access settings, add GV STRATUS client PCs and set them to high resolution.
- Systems with EDIUS:
  - Upgrade sequence: On GV STRATUS/EDIUS client PCs and EDIUS XRE Server you must uninstall/install in the following order:
    1. Uninstall EDIUS/XRE and GVG_Mlib.
    2. Restart.
    3. Uninstall the GV STRATUS Application.
    4. Install the GV STRATUS Application.
    5. Restart.
    6. Install EDIUS/XRE.
    7. Restart.

    The GVG_Mlib uninstall is required because it is no longer installed separately for EDIUS XS version 7 and EDIUS XRE Server version 7.
  - XRE Server settings: After upgrade, verify and, if necessary, reconfigure XRE Server settings.
  - License: You must re-license to support EDIUS 7.
- Systems using Adobe Premiere:
  - After the upgrade, you can install the GV STRATUS plug-in for Adobe Premiere if desired. To do so, follow installation instructions in this Topic Library.

Summary of upgrade from version 3.0 to version 3.1

Several upgrade tasks are new or require special consideration with the upgrade from version 3.0 to version 3.1. Apply upgrade tasks as appropriate for your system design, as follows:

- All systems:
  - Windows update: KB2859537 and KB2872339 not supported on Grass Valley devices.
  - .NET upgrade: All GV STRATUS servers (including EDIUS XRE) and all client PCs hosting a GV STRATUS application and/or an EDIUS application must upgrade to .NET 4.5, if that version of .NET is not already installed.
- Systems with high-resolution client PCs, such as those using the RMI tool or a high-resolution editor:
  - After the upgrade, in GV STRATUS Control Panel Proxy Access settings, add GV STRATUS client PCs and set them to high resolution.

- Systems using Adobe Premiere:
  - After the upgrade, you can install the GV STRATUS plug-in for Adobe Premiere if desired. To do so, follow installation instructions in this Topic Library.

Summary of upgrade from version 3.0 or 3.1 to version 3.5

Several upgrade tasks are new or require special consideration with the upgrade from version 3.0 or 3.1 to version 3.5. Apply upgrade tasks as appropriate for your system design, as follows:

- All systems:
  - Move Rights, Rename Bins Rights, Queue Management, Auto Logout: After the upgrade, existing users and groups do not have these roles assigned, so you must assign the roles if appropriate. If you create new users and groups, these roles are assigned by default, so you must remove the roles if appropriate.
  - Auto Logout settings: If assigning the Auto Logout role to users/groups, configure the desired application timeout.
  - Rules: After the upgrade you can additionally configure rule-based import of content and metadata.
  - .NET upgrade: All K2 Summit systems, GV STRATUS servers, and all client PCs hosting a GV STRATUS application and/or an EDIUS application must upgrade to .NET 4.5, if that version of .NET is not already installed.
  - Embedded Security: You must do a one-time initial deployment process on all GV STRATUS and K2 systems that run Embedded Security. Refer to the task *Deploy Embedded Security solution - One-time process*. This task isolates the steps required for the one-time process. If you have sufficient knowledge of systems and upgrades, you can modify your software upgrade steps as necessary to do the one-time process at the same time as your other software upgrades, rather than as isolated steps. After the one-time process is complete, it is not necessary to put Embedded Security in Update Mode when installing software.

    NOTE: A re-image of the computer might be necessary if the Embedded Security one-time process is done incorrectly. Follow instructions carefully.

    NOTE: After this process is complete, Embedded Security must remain in Enabled Mode for normal operation and during software upgrade/install. Do not put Embedded Security in Update Mode.

    Also, Windows updates KB2859537 and KB2872339 can be installed.
  - Internal system account: If the internal system account for your GV STRATUS system is on a fully qualified domain or is not the default GVAdmin account, configure settings at GV STRATUS Control Panel **Core | STRATUS Core Services | Primary Site** as appropriate for your system.

- Systems with Conform Server and/or XRE Server:
  - Both Conform Server and XRE Server functionality is combined into the GV STRATUS Render Engine. Conform Server and XRE Server are no longer supported on the GV STRATUS system. You must convert all Conform Servers and XRE Servers to Render Engine servers. The required steps for this conversion are integrated in the main upgrade process and in the section *Upgrade GV Render Engine server software and EDIUS client software* on page 148.

- Systems with Aurora Playout:
  - Aurora Playout is now GV STRATUS Rundown. Aurora Playout is no longer supported on the GV STRATUS system. You must convert all Aurora Playout devices and components to GV STRATUS Rundown.

Summary of upgrade from version 3.1 to version 4.0

Several upgrade tasks are new or require special consideration with the upgrade from version 3.1 or 3.5 to version 4.0. Apply upgrade tasks as appropriate for your system design, as follows:

- All systems:
  - GV STRATUS software installation automatically creates and installs a security certificate on the GV STRATUS Core server. No manual steps are required.
  - Schedule Monitor, Security Manager, Move Rights, Rename Bins Rights, Queue Management, Auto Logout: After the upgrade, existing users and groups do not have these roles assigned, so you must assign the roles if appropriate. If you create new users and groups, some roles are assigned by default, so you must remove those roles if appropriate.
  - Auto Logout settings: If assigning the Auto Logout role to users/groups, configure the desired application timeout.
  - Rules: After the upgrade you can additionally configure rule-based import of content and metadata.
  - .NET upgrade: All K2 Summit systems, GV STRATUS servers, and all client PCs hosting a GV STRATUS application and/or an EDIUS application must upgrade to .NET 4.5, if that version of .NET is not already installed.
  - Embedded Security: You must do a one-time initial deployment process on all GV STRATUS and K2 systems that run Embedded Security. Refer to the task *Deploy Embedded Security solution - One-time process*. This task isolates the steps required for the one-time process. If you have sufficient knowledge of systems and upgrades, you can modify your software upgrade steps as necessary to do the one-time process at the same time as your other software upgrades, rather than as isolated steps. After the one-time process is complete, it is not necessary to put Embedded Security in Update Mode when installing software.

    NOTE: A re-image of the computer might be necessary if the Embedded Security one-time process is done incorrectly. Follow instructions carefully.

    NOTE: After this process is complete, Embedded Security must remain in Enabled Mode for normal operation and during software upgrade/install. Do not put Embedded Security in Update Mode.

    Also, Windows updates KB2859537 and KB2872339 can be installed.
  - Internal system account: If the internal system account for your GV STRATUS system is on a fully qualified domain or is not the default GVAdmin account, configure settings at GV STRATUS Control Panel **Core | STRATUS Core Services | Primary Site** as appropriate for your system.

- Systems with Remote Site configured:
  - Verify and configure Remote Site settings. GV STRATUS security requires re-entering existing information and configuring new settings.

- Systems with EDIUS and GV Render Engine server:
  - Requires the installation of Windows High Priority updates. For more details, refer to *Install Important Windows updates for EDIUS* on page 148.
  - When using SiteConfig to install the GV Render Engine cab, the server might reboot and gives a false indication that the cab installs.
- Systems with Conform Server and/or XRE Server:
  - Both Conform Server and XRE Server functionality is combined into the GV STRATUS Render Engine. Conform Server and XRE Server are no longer supported on the GV STRATUS system. You must convert all Conform Servers and XRE Servers to Render Engine servers. The required steps for this conversion are integrated in the main upgrade process and in the section *Upgrade GV Render Engine server software and EDIUS client software* on page 148.
- Systems with MEWS Server:
  - Set up the MEWS Server in SiteConfig and deploy the MEWS Service software.
- Systems with Aurora Playout:
  - Aurora Playout is now GV STRATUS Rundown. Aurora Playout is no longer supported on the GV STRATUS system. You must convert all Aurora Playout devices and components to GV STRATUS Rundown.
  - To enable automatic transfer of assets into a playout server, configure the Summit MDI in GV STRATUS Control Panel for the K2 system that is a playout server.
- Systems with DIVA archive:
  - If upgrading to DIVA version 7.2, update DIVA MDI configuration.

Summary of upgrade from version 3.5 to version 4.0

Several upgrade tasks are new or require special consideration with this upgrade. Apply upgrade tasks as appropriate for your system design, as follows:

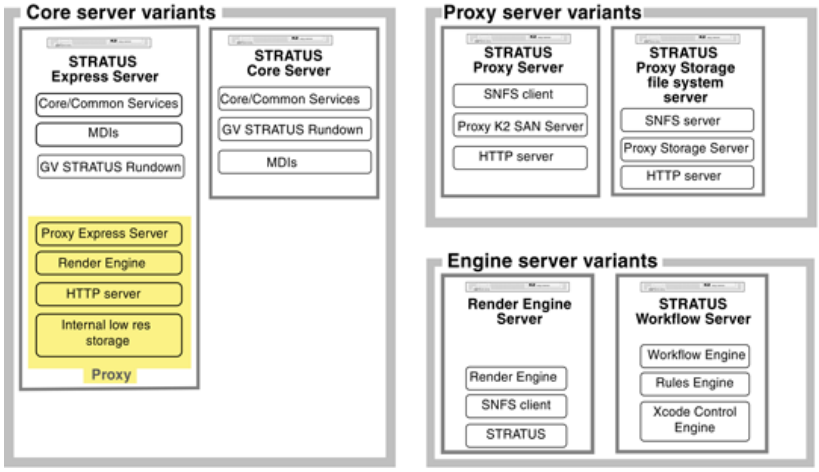
- All systems:
  - GV STRATUS software installation automatically creates and installs a security certificate on the GV STRATUS Core server. No manual steps are required.
  - Schedule Monitor, Security Manager: After the upgrade, existing users and groups do not have these roles assigned, so you must assign the roles if appropriate. If you create new users and groups, some roles are assigned by default, so you must remove those roles if appropriate.
  - Require the upgrade of SNFS (StoreNext File System) version 4.7.2 if you are upgrading to K2 9.5 system. For more details, refer to the "Upgrading K2 systems" section of the K2 Topic Library.
- Systems with EDIUS and GV Render Engine server:
  - Require the installation of Windows High Priority updates. For more details, refer to *Install Important Windows updates for EDIUS* on page 148.

- Systems with Remote Site configured:
  - Verify and configure Remote Site settings. GV STRATUS security requires re-entering existing information and configuring new settings.
- Systems with MEWS Server:
  - Set up the MEWS Server in SiteConfig and deploy the MEWS Service software.
- Systems with GV STRATUS Rundown:
  - To enable automatic transfer of assets into a playout server, configure the Summit MDI in GV STRATUS Control Panel for the K2 system that is a playout server.
- Systems with DIVA archive:
  - If upgrading to DIVA version 7.2, update DIVA MDI configuration.
- Systems with routers using SMS7000 protocol:
  - Verify that router source and destination IDs do not include invalid characters. For more details, refer to *Characters not allowed in router source and destination IDs* on page 557.
- Systems with Ingest database:
  - Disable the **Auto Close** feature on Ingest database to prevent inaccessibility problems. For more details, refer to *Disabling the Auto Close feature in Ingest Database* on page 689.

Overview of the GV STRATUS System

GV STRATUS system and server variants

The GV STRATUS server is the primary device that supports GV STRATUS system functionality. These servers can be configured in a variety of ways to support the workflow requirements of specific GV STRATUS systems. This topic describes some of the server variants for typical GV STRATUS systems, as an aid to understanding the scope of GV STRATUS systems in general. Other system configurations can require server variants not described here. Those other variants are available if needed to meet unique workflow requirements. Consult with your Grass Valley representative to determine your needs.



Variants of the GV STRATUS server include the following:

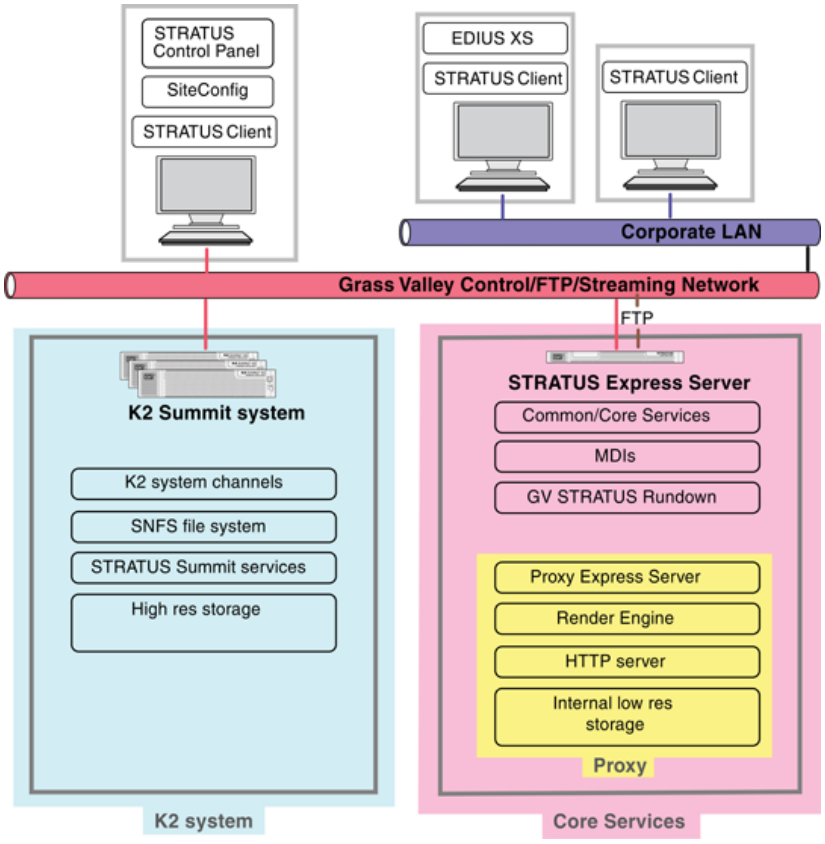
- GV STRATUS Express server — A GV STRATUS server with all the roles necessary for a basic GV STRATUS system, including the role of Proxy Express Server. The server has larger drives than other GV STRATUS servers to accommodate the low-resolution proxy media that is stored on the local server. This server is designed for use on smaller GV STRATUS systems where no other GV STRATUS servers or proxy systems are present.
- GV STRATUS Core server — A GV STRATUS server that has the role of Core Services on a system with multiple GV STRATUS servers. The server provides media management functionality, including the GV STRATUS database and associated software components.
- Proxy server — The GV STRATUS server on an online or production K2 SAN that provides access to the low-resolution proxy media stored on the SAN. The server has the role of Proxy K2 SAN Server and SNFS file system client.
- Proxy Storage file system server — The GV STRATUS server on a dedicated Proxy Storage system that provides access to the low-resolution proxy media stored on the system. The server has the roles of Proxy Storage Server and SNFS file system server for the Proxy Storage system.

- Render Engine — A GV STRATUS server that functions as a proxy encoder and as a conform server. As a proxy encoder, the server creates low-resolution proxy assets. If a high-resolution asset does not yet have associated proxy, the server creates it. The software that provides the proxy encoder functionality can run on a dedicated Render Engine server or on a GV STRATUS server that has other roles as well, such as a GV STRATUS Express server. As a conform server, the server hosts the Render Engine Service. The service renders a complex asset, such as a GV STRATUS sequence or a project created in EDIUS, into a simple clip.
- Workflow Server — A GV STRATUS server dedicated to hosting the Workflow Engine Service, the Rules Engine Service, and the Xcode Control Engine Service. These services support rules-based operations.

Related Topics

GV STRATUS system and server variants on page 220
GV STRATUS server on page 227
GV STRATUS server partitions on page 524

Small (Express) system description: Proxy on Core Services server



A small (Express) GV STRATUS system is characterized by proxy stored on a GV STRATUS Express server, which is a GV STRATUS server with all roles, including the roles of Proxy Server and Render Engine. Consult with Grass Valley for alternate configurations, such as the Render

Engine on a dedicated server, as appropriate for your workflow. The GV STRATUS Express server has internal storage with expanded capacity to store proxy media. The server provides an HTTP server that GV STRATUS client PCs access for proxy. A SMB share is also required to which servers such as K2 systems and Render Engines write proxy.

This small GV STRATUS system is designed for a basic workflow and consists of K2 Summit systems, a GV STRATUS Express server, and one or more GV STRATUS client PCs. The K2 Summit systems can be one or several standalone systems, a K2 SAN, or a combination of a SAN and standalone systems. Client PCs use a proxy media workflow and are connected to the Corporate LAN or to the control network. At least one PC must host the GV STRATUS Control Panel application. A designated PC on the control network hosts the SiteConfig application.

In addition to its role of Proxy Server, the GV STRATUS Express server hosts components that provide the underlying functionality to the overall GV STRATUS system. These components provide media management, license manager, and user preference functionality.

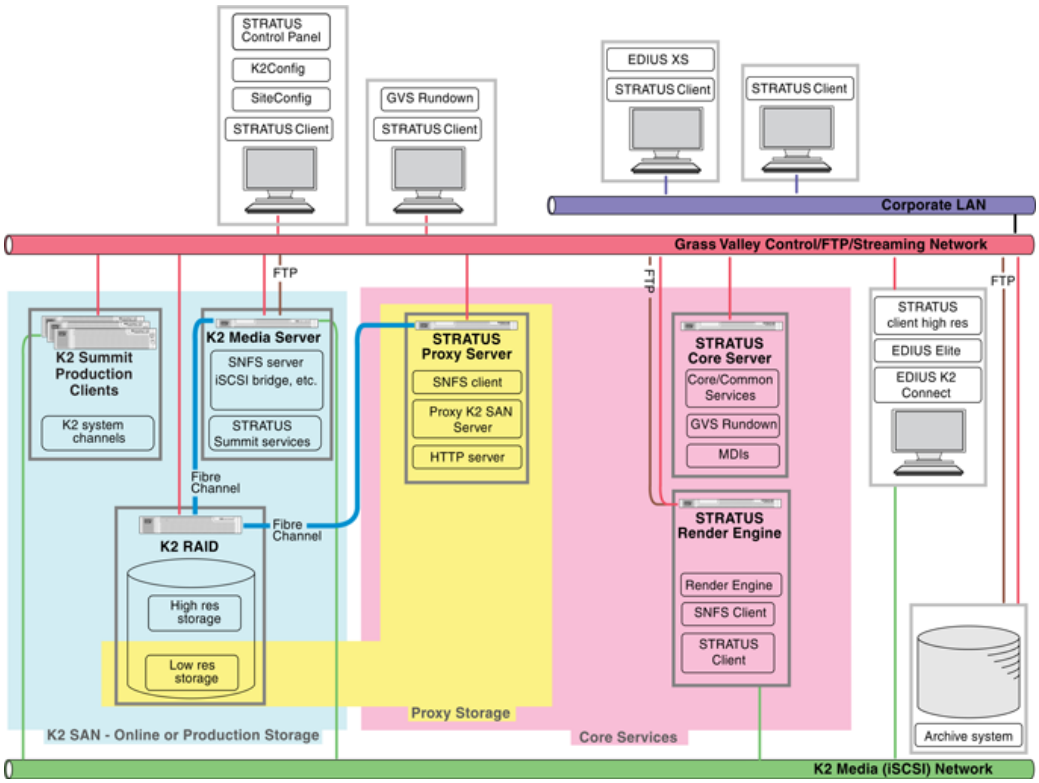
Related Topics

About roles on page 443

Devices components: Roles, cab files, services, and licenses on page 444

CIFS storage configuration

Medium (A1) system description: Proxy on K2 Summit SAN



A medium (A1) GV STRATUS system is characterized by proxy stored on the online or production K2 Summit SAN. Attached to the K2 SAN is a Proxy server, which is a GV STRATUS server with role of Proxy K2 SAN Server. This Proxy server provides access to the low resolution proxy media stored on the K2 SAN. The server provides an HTTP server that GV STRATUS client PCs access for proxy. A SMB share is also required to which servers such as K2 systems and Render Engines write proxy.

This medium GV STRATUS system is designed for a typical workflow and consists of a K2 Summit online or production SAN, multiple GV STRATUS servers, and multiple GV STRATUS client PCs. Client PCs that use a proxy media workflow are connected to the Corporate LAN or to the control network. Client PCs that use a high resolution media workflow are connected to the media (iSCSI) network. At least one PC must host the GV STRATUS Control Panel application. A designated PC on the control network hosts the SiteConfig application and the K2Config application. GV STRATUS Control Panel, SiteConfig, and K2Config applications can all be on the same PC, and that PC can be the K2 SAN control point PC.

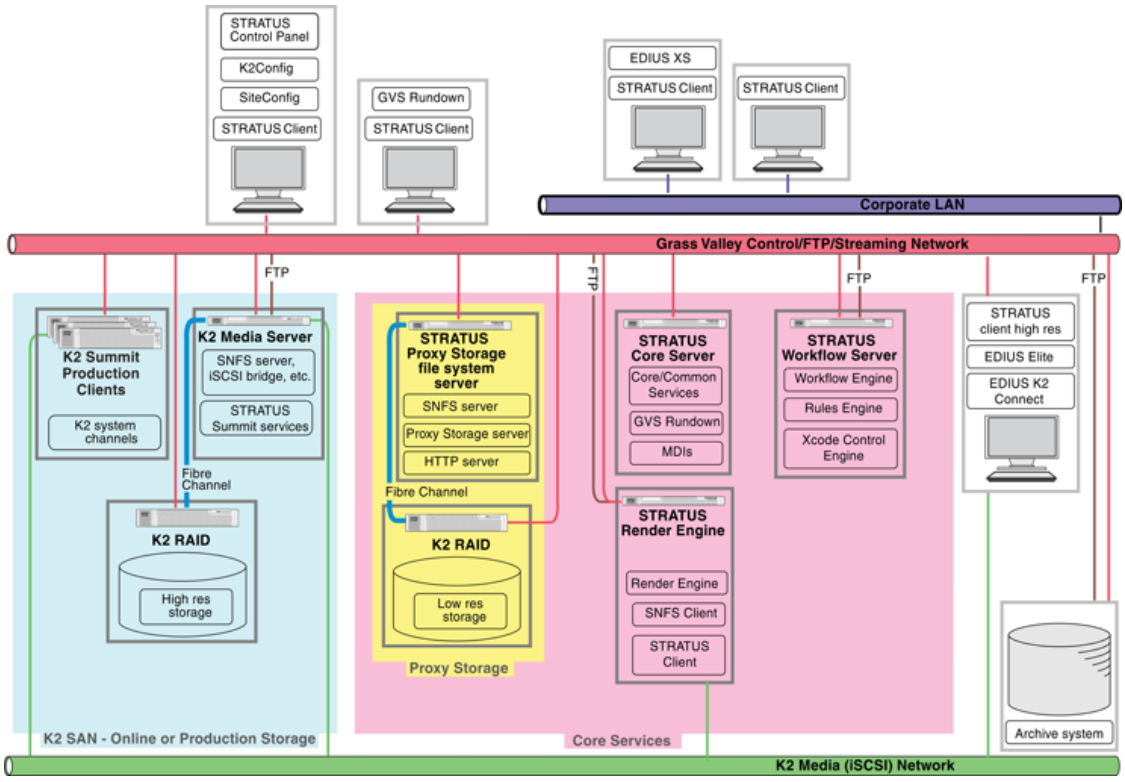
In addition to the Proxy Server, one or more GV STRATUS servers host components that provide the underlying functionality to the overall GV STRATUS system. Components can be distributed across multiple GV STRATUS servers to provide processing power as needed to support the workflow.

Related Topics

About roles on page 443

Devices components: Roles, cab files, services, and licenses on page 444

Large (B1, C1) system description: Proxy on dedicated Proxy Storage system



A large (B1, C1) GV STRATUS system is characterized by proxy stored on a dedicated Proxy Storage system. The Proxy Storage system is similar to a K2 Nearline SAN, or NAS. The Proxy Storage system stores the low resolution proxy media. The Proxy Storage file system server is a GV STRATUS server that has the role of Proxy Storage Server. This server is the SNFS file system server for the Proxy Storage system. The server provides an HTTP server that GV STRATUS client PCs access for proxy. A SMB share is also required to which servers such as K2 systems and Render Engines write proxy.

This large GV STRATUS system is designed for a large-scale workflow and consists of a K2 Summit online or production SAN, a Proxy Storage system, multiple GV STRATUS servers, and multiple GV STRATUS client PCs. Client PCs that use a proxy media workflow are connected to the Corporate LAN or to the control network. Client PCs that use a high resolution media workflow are connected to the media (iSCSI) network. At least one PC must host the GV STRATUS Control Panel application. A designated PC on the control network hosts the SiteConfig application and the K2Config application. GV STRATUS Control Panel, SiteConfig, and K2Config applications can all be on the same PC, and that PC can be the K2 SAN control point PC.

In addition to the Proxy Storage file system server, one or more GV STRATUS servers host components that provide the underlying functionality to the overall GV STRATUS system. Components can be distributed across multiple GV STRATUS servers to provide processing power where it is needed to support your workflow. A system with one GV STRATUS Core server is

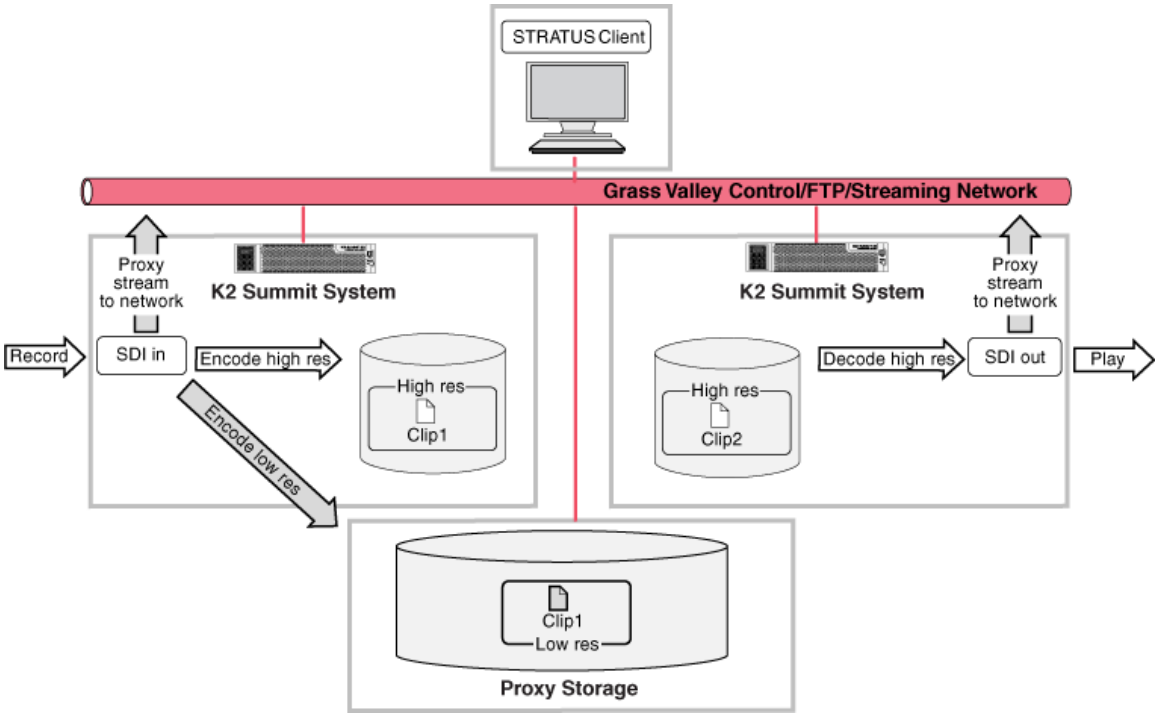
classified as a B1 system. A system with core server functionality distributed across multiple GV STRATUS Core servers is classified as a C1 system.

Related Topics

About roles on page 443

Devices components: Roles, cab files, services, and licenses on page 444

Proxy and live streaming workflow overview



When licensed and configured, a K2 Summit system creates low-resolution representations of high-resolution media. Similar to PB/EE functionality, the K2 Summit System creates a live stream of low-resolution media at the SDI input and a live stream of low-resolution media at the SDI output, whether or not record/play operations are underway. These streams are multicast to the network and are available to applications on the network. When media is recorded, the K2 Summit system encodes a high resolution clip and a low resolution proxy clip. The system keeps these clips associated so any changes take effect simultaneously for both clips.

The GV STRATUS application accesses the low-resolution media over the network. When you monitor the K2 Summit system SDI inputs and outputs, the application displays the live stream. When you view an asset, the application displays the proxy representation of the asset. When you edit an asset, the K2 Summit system makes your changes on both the proxy and the high resolution asset.

The K2 Summit system can also generate low-latency streaming media for use by DynoZoom and live monitoring. Refer to related topics in the "Configuring the K2 System" section of the K2 Topic Library.

Related Topics

Corporate LAN network description on page 414
Control network description on page 412

HTTP server overview

The GV STRATUS system HTTP server provides access to low resolution proxy media.

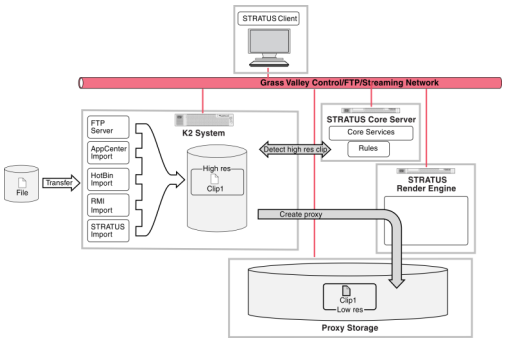
The GV STRATUS application accesses the proxy using a HTTP URL. This supports efficient, high-speed, and simultaneous access to proxy from multiple GV STRATUS clients. In addition, the HTTP server supports remote access for GV STRATUS clients.

The HTTP server is on the GV STRATUS device designated the proxy server. This can be one of the following devices, depending on the GV STRATUS system configuration:

- GV STRATUS Express server
- Proxy server
- Proxy Storage file system server

GV STRATUS components that create the low resolution proxy media must write the proxy files to a location served by the HTTP server. This location is SMB proxy share. The GV STRATUS Control Panel creates the proxy share automatically when you configure Proxy Config settings. The proxy share is shared with full permission granted to the internal system account, which by default is GVAdmin. The K2 system and the Render Engine create proxy media and therefore require this SMB access to the proxy share.

Proxy encoding overview



When you transfer a file into the K2 system, it is stored as a high resolution clip. GV STRATUS Rules Wizard detects the presence of the clip in the K2 storage. The Rules Wizard checks to see if the clip has associated proxy. If no proxy exists, the Rules Wizard checks rules. GV STRATUS rules specify that all high resolution clips must have proxy, so the Rules Wizard sends a transcode job to a Render Engine. If there are multiple high resolution clips to be transcoded, the transcode

jobs are queued up sequentially and the next available Render Engine transcodes the next job in the sequence. The Render Engine transcodes the high resolution clip to create the proxy. The Render Engine generates proxy media for high-resolution clips with one video track. Clips with more than one video track are not supported.

Functional descriptions

The topics in this section describe the components of the GV STRATUS system.

K2 system

A K2 system can include one or more standalone K2 Summit systems, an online or production K2 Summit SAN, or a combination of standalone and SAN systems.

The K2 system records, plays, and stores high-resolution media. It also generates low-resolution proxy media so that network connected GV STRATUS clients can be included in the media workflow without direct access to the high-resolution media. The K2 system generates the low-resolution media as a live video stream at SDI inputs and outputs. When the K2 system records a high-resolution clip, it creates low-resolution media files that are the proxy for the high-resolution clip.

Related Topics

Devices components: Roles, cab files, services, and licenses on page 444

GV STRATUS server

The GV STRATUS server hosts the software services and databases of the GV STRATUS system. There can be one or more GV STRATUS servers in a GV STRATUS system, with services and databases distributed across servers as appropriate for the size of the system. For smaller GV STRATUS systems, the GV STRATUS Express server can also store low-resolution proxy media.

Components that can reside on a GV STRATUS server include the following:

- License management — Services that manage the assignment of licenses and roles to groups and users.
- User preferences — The settings you make in the STRATUS application. When you log in to the GV STRATUS application with the same credentials, the settings you make on one PC are available on other PCs.
- Proxy Server — Services that manage the location of proxy media and the GV STRATUS application's access to the proxy media.
- Databases — Includes information for the following:
  - Media asset management
  - Metadata
  - Rules
  - Transfers
  - GV STRATUS Rundown SDB (Simple Database)
  - Scheduler
  - Rules Engine
  - Workflow Engine

- MDI — MDI is the acronym for Managed Device Interface. An MDI is a software component that provides an interface for the GV STRATUS database to access a device. Typically these are devices on which media resides, such as K2 systems, NAS devices, and archive devices. Each type of device has its own MDI. For most MDIs, the MDI software component is hosted on the GV STRATUS Core server, rather than being hosted on the same machine that it accesses. MDIs include the following:
  - Grass Valley Media Server
  - Summit Standalone
  - Summit SAN
  - DIVA
  - FlashNet
  - Generic FTP
  - Masstech
- Render Engine — A GV STRATUS server that functions as a proxy encoder and as a conform server. As a proxy encoder, the server creates low-resolution proxy assets. If a high-resolution asset does not yet have associated proxy, the server creates it. The software that provides the proxy encoder functionality can run on a dedicated Render Engine server or on a GV STRATUS server that has other roles as well, such as a GV STRATUS Express server. As a conform server, the server hosts the Render Engine Service. The service renders a complex asset, such as a GV STRATUS sequence or a project created in EDIUS, into a simple clip.
- Workflow Server — A GV STRATUS server dedicated to hosting the Workflow Engine Service, the Rules Engine Service, and the Xcode Control Engine Service. These services support rules-based operations.

A Fault Tolerant (FT) GV STRATUS server is also available. This is an enhanced platform designed to reduce the risk of system failure.

Related Topics

Devices components: Roles, cab files, services, and licenses on page 444
Connect Core server to corporate LAN on page 250
About GV STRATUS system databases on page 418
GV STRATUS system and server variants on page 220
GV STRATUS server on page 227
GV STRATUS server partitions on page 524

Proxy Storage system

The Proxy Storage system is a type of K2 Nearline SAN. It stores the low-resolutions assets on the network.

The Proxy Storage system includes the following:

- A Proxy Storage file system server, which is a GV STRATUS server that manages the Proxy Storage media file system. It also provides the GV STRATUS application access to low-resolution assets. K2 server software is required on the Proxy Storage file system server.
- K2 RAID

- Ethernet switch

Related Topics

Devices components: Roles, cab files, services, and licenses on page 444

GV STRATUS client

The GV STRATUS application functions as a client to the GV STRATUS Core Services. The GV STRATUS application runs on a GV STRATUS client PC. With the appropriate licensing, the EDIUS application can also run on a GV STRATUS client PC. GV STRATUS client PCs are supplied by the customer. By default, the GV STRATUS application and the EDIUS XS application access low-resolution live streaming and proxy media. If the PC is set to high-resolution in GV STRATUS Control Panel Proxy Access settings, the GV STRATUS application accesses high-resolution media. This also requires a high-resolution license.

Related Topics

Devices components: Roles, cab files, services, and licenses on page 444
About GV STRATUS client PCs on page 416
Client PC set up process on page 253

Preparing for installation

About installing the GV STRATUS system

This manual provides two paths for installing your GV STRATUS system, as follows:

- Commissioning process — Follow this process as your primary path. It assumes you received your system completely set up and configured from Grass Valley.
- Complete system installation process — Use this process only if you must change the system configuration or if there are system setup or configuration processes that are incomplete. Browse this process and do the appropriate items.

Read the following to familiarize yourself with your GV STRATUS system before you begin the commissioning process:

- GV STRATUS system software and documentation is available for download from the Grass Valley website.
- The GV STRATUS application runs on off-the-shelf Windows operating system computers. These GV STRATUS client PCs are supplied by the customer that owns the GV STRATUS system. Grass Valley does not supply these computers.
- GV STRATUS services run on one or more GV STRATUS servers that are supplied by Grass Valley with all the necessary hardware and software installed. GV STRATUS software licenses are required to support the customer workflow. Licenses are installed on the GV STRATUS server with role of Common Services.
- The GV STRATUS Control Panel application runs on a PC that has network access to the GV STRATUS Core server.

- With the installation instructions in this section, you use SiteConfig from a network connected control point PC and remotely install/upgrade software simultaneously on your system devices. This is the recommended process for software installation and upgrades. When installing the GV STRATUS application or the GV STRATUS Control Panel application, if SiteConfig installation is not possible, you may install manually on the local PC. You must uninstall before installing.
- There should be just one instance of SiteConfig installed on a single PC.
- A designated Control Point PC is optional for the GV STRATUS system. If your GV STRATUS system access a K2 SAN, then the SAN's Control Point PC typically functions as the Control Point PC for the GV STRATUS system as well. GV STRATUS Control Panel, SiteConfig, K2Config, and SNMP manager applications are installed on the Control Point PC.
- Refer to release information and upgrade information for instructions on obtaining software licenses and upgrading the GV STRATUS system.

Related Topics

System requirements for GV STRATUS client PC on page 52

Commissioning process

Use the following list to guide the overall task flow of commissioning your system. This commissioning process assumes you received your system completely set up and configured from Grass Valley.

1. *Rack, cable, and power on process* on page 232. All systems require this process.
2. *Test system setup and configuration process* on page 246. All systems require this process. Verify that your cabling is correct, the system is operational as when pre-staged by Grass Valley, and to complete procedures by logging in to all devices and applications as user `Administrator`.
3. *Customer network, licenses, and roles process* on page 250. All systems require this process. Set up the GV STRATUS Core server on the customer's network and assign GV STRATUS licenses and roles to the customer's groups and users.
4. *Client PC set up process* on page 253. All systems require this process. Add the customer's GV STRATUS client PCs to the system.

Complete system installation process

Use the following list if you must change the system configuration or if there are system setup or configuration processes that are incomplete. Browse this process and do the appropriate items.

1. *Rack, cable, and power on process* on page 232. All systems require this process.
2. *SiteConfig software deployment process* on page 857. All systems require this process when updating to new versions of Grass Valley product software.
3. *K2 system set up process* on page 722. All systems require this process.
4. *Express/Core server set up process* on page 724. All systems require this process. Use SiteConfig for network setup and software install. On the GV STRATUS server with role of Common Services, use SabreTooth and install GV STRATUS licenses.

5. *Proxy Server/Storage set up process* on page 738. Only systems with proxy on the K2 SAN (A1) or with proxy on dedicated Proxy Storage (B1, C1) require this process. Use SiteConfig for network setup and software install, then use K2Config for SAN setup.
6. *Render Engine Server set up process* on page 768. Only systems with a Render Engine Server require this process. On the GV STRATUS Core server, use SabreTooth and install the STRATUS-CONFORM license. Use SiteConfig for network setup and software install. Then use K2Config for SAN setup.
7. *Standalone Database Server set up process* on page 829. Only systems with a Standalone Database Server require this process. Use SiteConfig for network setup and software install.
8. *Workflow Server set up process* on page 898. Only systems with a Workflow Server require this process. Use SiteConfig for network setup and software install. On the GV STRATUS Core server, use SabreTooth and install the STRATUS-RULES license optional transfer/transcode licenses.
9. *GV STRATUS Control Panel system configuration process* on page 839. All systems require this process. Use GV STRATUS Control Panel to configure the GV STRATUS system for your site's workflow.
10. *Customer network, licenses, and roles process* on page 250. All systems require this process. Set up the GV STRATUS Core server on the customer's network and assign GV STRATUS licenses and roles to the customer's groups and users.
11. *Client PC set up process* on page 253. All systems require this process. Add the customer's GV STRATUS client PCs to the system.
12. *Archive system set up process* on page 874. Only systems with an archive system require this process. Configure the archive system with the K2 Summit/SAN system, use SabreTooth to install the STRATUS-ARCHIVE license, and in GV STRATUS Control Panel configure an archive MDI.

Commissioning a system

Commissioning process

Use the following list to guide the overall task flow of commissioning your system. This commissioning process assumes you received your system completely set up and configured from Grass Valley.

1. *Rack, cable, and power on process* on page 232. All systems require this process.
2. *Test system setup and configuration process* on page 246. All systems require this process. Verify that your cabling is correct, the system is operational as when pre-staged by Grass Valley, and to complete procedures by logging in to all devices and applications as user `Administrator`.
3. *Customer network, licenses, and roles process* on page 250. All systems require this process. Set up the GV STRATUS Core server on the customer's network and assign GV STRATUS licenses and roles to the customer's groups and users.
4. *Client PC set up process* on page 253. All systems require this process. Add the customer's GV STRATUS client PCs to the system.

Rack, cable, and power on process

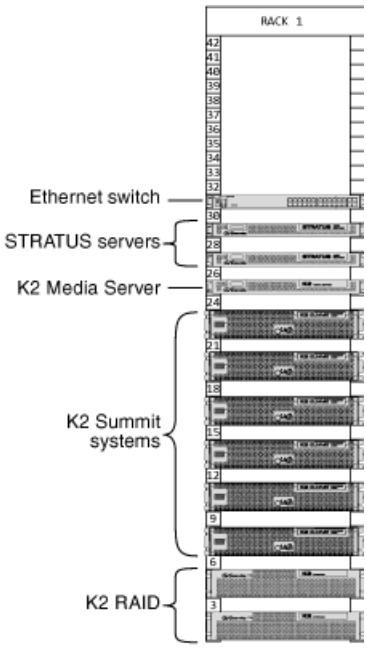
All systems require this process.

1. *Rack-mount devices* on page 232. All systems require this process.
2. *Cable K2 systems* on page 236. All systems require this process.
3. *Cable GV STRATUS server* on page 236. All system require this process. Cable the GV STRATUS servers that are in your system design.
4. *Cable Proxy Storage system* on page 242. Only systems with proxy on a dedicated Proxy Storage system require this process.
5. *Power on K2 and GV STRATUS system devices* on page 245. All systems require this process.

Rack-mount devices

All systems require this process.

Follow the instructions you received with the rack-mount hardware to install each component of the system. One rack-unit spacing is recommended between components for ventilation. The recommended arrangement of devices is as follows:



HP ProCurve Switch Rack specifications

Use the following specifications to determine load, spacing, power, and other factors when planning system racks.

Table 3: Mechanical specifications

Characteristic	Specification
Cabinet Type	Rack-mount
Rack units	1
External Dimensions	443 (w) x 44 (h) x 392 (d) mm
Weight	Maximum 7 kg

Table 4: Power specifications

Characteristic	Specification
Type	100-127 VAC/200-240 VAC; 50/60 Hz
Power Consumption	4.0/2.0 A, 200W

Dell R620 Rack specifications

Use the following specifications to determine load, spacing, power, and other factors when planning system racks.

Table 5: Mechanical specifications

Characteristic	Specification
Cabinet Type	Rack-mount
Rack units	1
External Dimensions	482.4 (w) x 42.8 (h) x 683.7 (d) mm
Weight	Maximum 18.6kg , 40.96 lbs

Table 6: Power specifications

Specification	1100W DC	1100W AC	750W AC	495W AC
Current consumption	32A	12A-6.5A	10A-5A	6.5A-3A
Supply voltage	-48V to -60V DC	100-240VAC	100-240VAC	100-240VAC
Frequency	N/A	50/60Hz	50/60Hz	50/60Hz
Heat dissipation (BTU/hr max)	4416	4100	2843	1908

Specification	1100W DC	1100W AC	750W AC	495W AC
Maximum inrush current	55A	55A	55A	55A

K2 Summit 3G Rack specifications

Use the following specifications to determine load, spacing, power, and other factors when planning system racks. These specifications apply to K2 Summit 3G chassis.

Table 7: Mechanical specifications

Characteristic	Specification
Cabinet Type	Rack-mount
Rack units	2
External Dimensions	447 x 617 x 89 mm
Weight	25.0 kg maximum

Table 8: Power specifications

Characteristic	Specification
Power conditions	Dual, redundant
Mains Input Voltage	90 to 260V auto-range, 47-63Hz
Maximum power consumption (when operating in a 25° C environment)	450W typical (standalone) 390W typical (SAN client) Maximum AC current 8A @ 115VAC, 4A @ 230VAC

K2 RAID Rack specifications

Use the following specifications to determine load, spacing, power, and other factors when planning system racks. These specifications apply to K2 10Gv3 RAID (M110) chassis.

Table 9: Mechanical specifications

Characteristic	Primary chassis	Expansion chassis
Cabinet Type	Rack-mount	Rack-mount
Rack units	2	2
External Dimensions	482 x 556.0 x 87.4 mm (no front bezel)	482 x 556.0 x 87.4 mm (no front bezel)
Weight	33 kg maximum	33 kg maximum

Table 10: Power specifications

Characteristic	Primary chassis	Primary chassis
Power conditions	100 to 240 VAC, single-phase 50/60 Hz	100 to 240 VAC, single-phase 50/60 Hz

FT Server Rack specifications

Use the following specifications to determine load, spacing, power, and other factors when planning system racks.

Table 11: Mechanical specifications

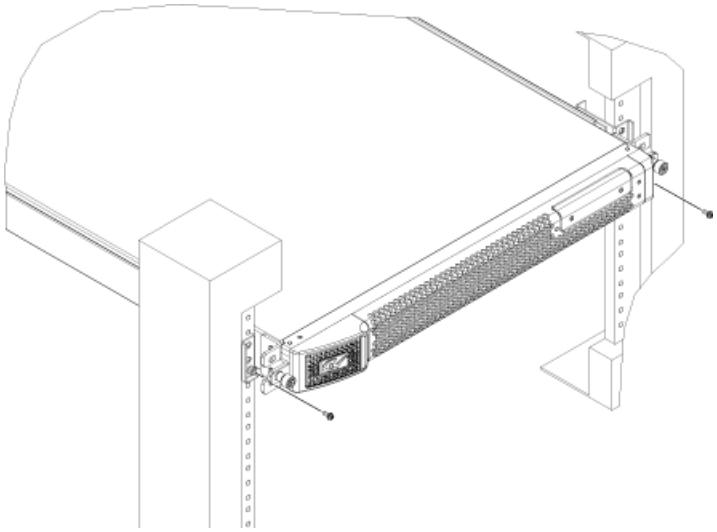
Characteristic	Type I and Type II Specification
Cabinet Type	Rack-mount
Rack units	4
External Dimensions	483 (w) x 178 (h) x 736 (d) mm, 19.0 in. (w) x 7.0 in. (h) x 28.9 in. (d)
Rack clearance	40 cm or more on top, 1 m or more on the front and rear, 60 cm or more on the right and left.
Weight	Maximum 51.5kg , 113.3 lbs

Table 12: Power specifications

Power Supply	Type I Specifications	Type II Specifications
Type	AC 100V-240V +/- 10%, 50/60Hz +/- 3Hz	AC 100V-240V +/- 10%, 50/60Hz +/- 3Hz
Power Consumption	1400VA, 1390W	1300VA, 1290W

Securing a server to a rack

Follow the instructions provided in the shipping box to install the rack rails and position the server in the rack. For the Dell 1RU PowerEdge Server, follow the illustration below to secure the system to the rack.



Install a screw in the bottom hole of the bracket on each side. Do not attempt to install a screw in the top hole of the bracket.

Cable K2 systems

All systems require this process.

Cable the K2 systems that store and serve your high-resolution assets. This includes any K2 SAN systems and K2 standalone systems in your system design.

For K2 SAN systems, refer to the "Cabling K2 Storage" section of the K2 Topic Library and "K2 10G SAN Installation and Service Manual" for instructions.

For K2 standalone systems, refer to the "Configuring the K2 System" section of the K2 Topic Library for instructions.

Cable GV STRATUS server

All system require this process. Cable the GV STRATUS servers that are in your system design.

The topics in this section apply to GV STRATUS servers as follows:

- GV STRATUS Express server
- GV STRATUS Core server
- Proxy server
- Render Engine
- Workflow Server

Other topics apply to a GV STRATUS server that is a Proxy Storage file system server.

Related Topics

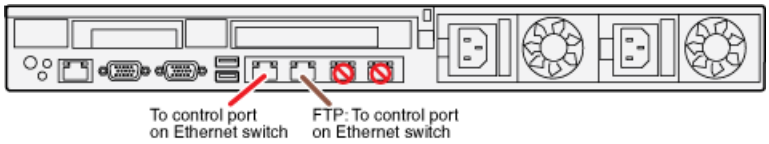
STRATUS-CS server: Proxy Storage file system server Dell R620 on page 243

STRATUS-CS server: Express, Core (A1, B1, C1) Dell R620

These cabling instructions apply to GV STRATUS Express server and GV STRATUS Core server, specified as follows:

- Dell R620 PowerEdge server with one or more roles from the following list only:
  - GV STRATUS Ingest Services (Required)
  - GV STRATUS Control Panel Service (Required)
  - GV STRATUS Common Services (Required)
  - License Manager (Required)
  - GV STRATUS Data Mover Engine (Required)
  - GV STRATUS Proxy Express Server (Required on Express server)
  - GV STRATUS Control Panel (Required)
  - GV STRATUS Core Services (Required)
  - GV STRATUS Database (Required)
  - GV STRATUS Summit MDI (Required)
  - GV STRATUS Common RESTful Archive MDI (Optional)
  - GV STRATUS Diva MDI (Optional)
  - GV STRATUS FlashNet MDI (Optional)
  - GV STRATUS Masstech MDI (Optional)
  - GV STRATUS Generic FTP MDI (Optional)
  - GV STRATUS Proxy Streaming Service (Optional)
  - GV STRATUS Rules Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV STRATUS Scheduled Transfer Engine (Optional)
  - GV STRATUS Scheduled Ingest Engine (Not used in this GV STRATUS release)
  - GV STRATUS Scheduled Ingest Manager (Not used in this GV STRATUS release)
  - GV STRATUS SocialMedia Engine (Optional)
  - GV STRATUS ExternalMedia Engine (Optional)
  - GV STRATUS Traffic Gateway (Optional)
  - GV STRATUS Topic Service Bus (Not used in this GV STRATUS release)
  - GV STRATUS Web Apps (Required. Must be assigned to Express/Core server to display Statistics panel via Dashboard)
  - GV STRATUS Web Client (Optional)
  - GV STRATUS Workflow Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV STRATUS Xcode Control Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV Log Manager (Required)
  - GV Log Viewer (Required)
  - GV STRATUS Rundown Server Components (Optional)
  - GV STRATUS Application (Use for test purposes only)
  - If optionally used as a Render Engine, these additional roles:
    - GV STRATUS Render Engine

These roles require a connection to the control network and the FTP/streaming network.

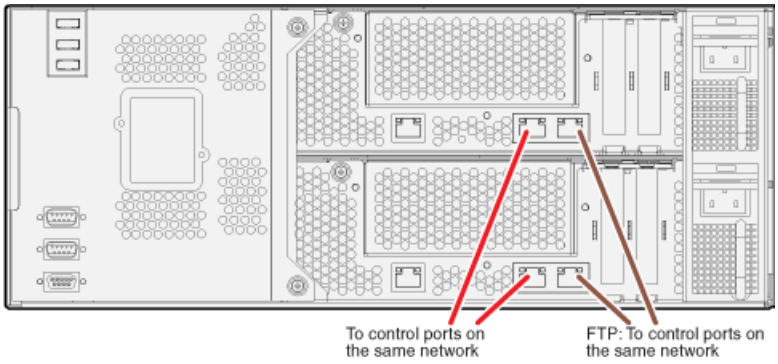

To control port
on Ethernet switch
FTP: To control port
on Ethernet switch

STRATUS-CS-FT server: Core (B1, C1)

These cabling instructions apply to GV STRATUS Express server and GV STRATUS Core server, specified as follows:

- Grass Valley FT server with one or more roles from the following list only:
  - GV STRATUS Ingest Services (Required)
  - GV STRATUS Control Panel Service (Required)
  - GV STRATUS Common Services (Required)
  - License Manager (Required)
  - GV STRATUS Data Mover Engine (Required)
  - GV STRATUS Proxy Express Server (Required on Express server)
  - GV STRATUS Control Panel (Required)
  - GV STRATUS Core Services (Required)
  - GV STRATUS Database (Required)
  - GV STRATUS Summit MDI (Required)
  - GV STRATUS Common RESTful Archive MDI (Optional)
  - GV STRATUS Diva MDI (Optional)
  - GV STRATUS FlashNet MDI (Optional)
  - GV STRATUS Masstech MDI (Optional)
  - GV STRATUS Generic FTP MDI (Optional)
  - GV STRATUS Proxy Streaming Service (Optional)
  - GV STRATUS Rules Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV STRATUS Scheduled Transfer Engine (Optional)
  - GV STRATUS Scheduled Ingest Engine (Not used in this GV STRATUS release)
  - GV STRATUS Scheduled Ingest Manager (Not used in this GV STRATUS release)
  - GV STRATUS SocialMedia Engine (Optional)
  - GV STRATUS ExternalMedia Engine (Optional)
  - GV STRATUS Traffic Gateway (Optional)
  - GV STRATUS Topic Service Bus (Not used in this GV STRATUS release)
  - GV STRATUS Web Apps (Required. Must be assigned to Express/Core server to display Statistics panel via Dashboard)
  - GV STRATUS Web Client (Optional)
  - GV STRATUS Workflow Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV STRATUS Xcode Control Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV Log Manager (Required)
  - GV Log Viewer (Required)
  - GV STRATUS Rundown Server Components (Optional)
  - GV STRATUS Application (Use for test purposes only)
  - If optionally used as a Render Engine, these additional roles:
    - GV STRATUS Render Engine

These roles require a connection to the control network and the FTP/streaming network.



NOTE: Network ports on CPU/IO module 1 and on CPU/IO 2 both connect to the same network. For example, both control ports connect to the same control network. Do not attempt to connect to different networks.

Related Topics

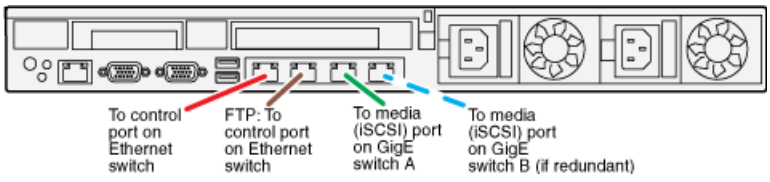
Devices components: Roles, cab files, services, and licenses on page 444

STRATUS-CS-RE server: Render Engine Dell R620

These cabling instructions apply to a GV STRATUS server, specified as follows:

- Dell R620 PowerEdge server with roles from the following list:
  - GV STRATUS Control Panel
  - GV Log Manager
  - StorNext File System Client
  - GV Embedded Security Manager
  - GV STRATUS Render Engine

For the Render Engine server, these roles require connections to the media (iSCSI) network and the control network. Grass Valley policy requires an additional connection to the FTP/streaming network.



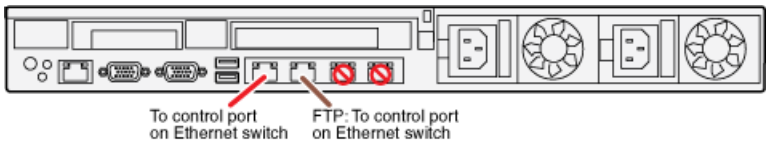
If a basic, non-redundant K2 SAN, connect port 2 to the one media (iSCSI) network. If a redundant K2 SAN, connect port 2 to media network A and port 3 to media network B.

STRATUS-CS-WFE server: Workflow Dell R620

These cabling instructions apply to a GV STRATUS server, specified as follows:

- Dell R620 PowerEdge server with roles from the following list:
  - GV STRATUS Workflow Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV STRATUS Rules Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV STRATUS SocialMedia Engine (Optional)
  - GV STRATUS ExternalMedia Engine (Optional)
  - GV STRATUS Xcode Control Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV STRATUS Control Panel
  - GV Log Manager

For the Workflow server, these roles require connections to the control network and the FTP/streaming network.

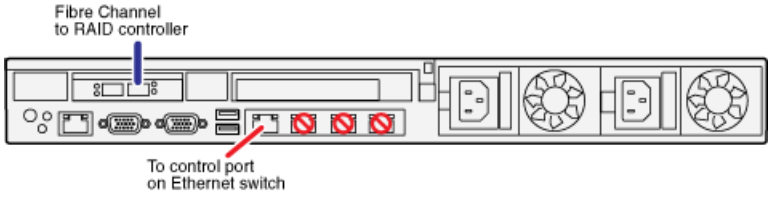


STRATUS-CS server: Proxy Dell R620

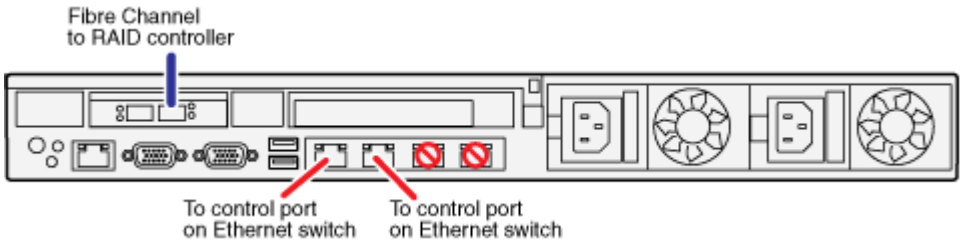
These cabling instructions apply to a GV STRATUS Proxy server, specified as follows:

- Dell R620 PowerEdge server connected to on an online or production K2 SAN, with the following roles:
  - GV STRATUS Proxy K2 SAN Server
  - GV Log Manager
  - StorNext File System Client

These roles require connections to the control network and a Fibre Channel connection to the K2 RAID. The server can have other roles as well.



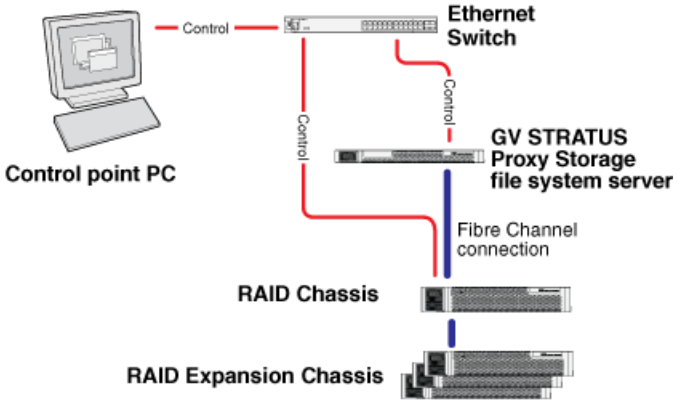
If network redundancy is required, control network teaming can be configured on the server, with 2 physical Control connections as shown in the diagram below:



Cable Proxy Storage system

Only systems with proxy on a dedicated Proxy Storage system require this process.

Proxy Storage system



To cable this device…	Of this model or platform…	Turn to these instructions:
Gigabit Ethernet Switch	HP 2910	*K2-SWE basic Proxy Storage* on page 243
GV STRATUS Proxy Storage file system server	Dell R620	*STRATUS-CS server: Proxy Storage file system server Dell R620* on page 243
K2 RAID	K2 10Gv2 RAID	*K2 RAID basic Proxy Storage* on page 244

Cable Ethernet switch

As directed by the system diagram for your storage system, cable the switch or switches for your system using the instructions in this section.

These instructions are for the HP ProCurve switch 29xx series and Dell Networking switch N1500 series.

If a different brand of switch, such as a Cisco Catalyst switch, is required by your site, apply the information in the following procedures accordingly. Refer to the documentation you received with the switch as necessary.

Install the switch in its permanent location. When installing in a video equipment rack, use 10-32 screws. Do not use HP's 12-24 screws, as they can cause thread damage.

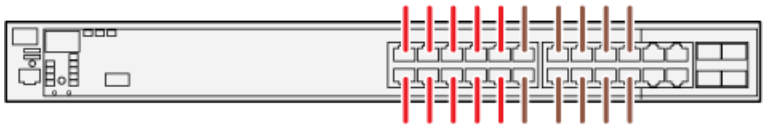
Provide power to the switch.

K2-SWE basic Proxy Storage

These cabling instructions apply to the following:

- HP 29xx series Gigabit Ethernet switch on a Proxy Storage system.

Front view



Ports are for control connections as well as FTP connections from Grass Valley and 3rd party systems.

GV STRATUS server: Proxy Storage

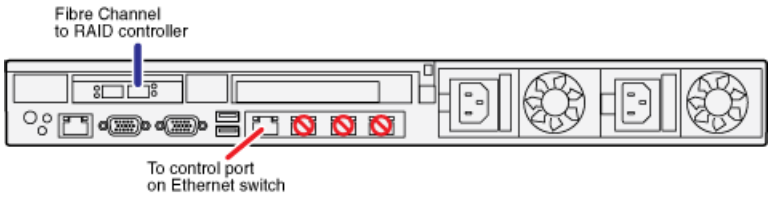
As directed by the system diagram for your Proxy Storage system, cable the GV STRATUS server that is the Proxy Storage file system server using the instructions in this section

STRATUS-CS server: Proxy Storage file system server Dell R620

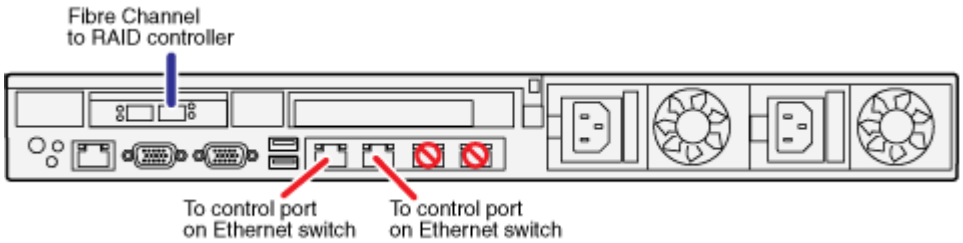
These cabling instructions apply to GV STRATUS Proxy Storage file system server, specified as follows:

- Dell R620 PowerEdge server with the following roles on a Proxy Storage system:
  - GV STRATUS Proxy Storage Server
  - GV Log Manager
  - StorNext File System Server
  - StorNext File System Client

These roles require connections to the control network and a Fibre Channel connection to the Proxy Storage system's K2 RAID. The server can have other roles as well.



If network redundancy is required, control network teaming can be configured on the server, with 2 physical Control connections as shown in the diagram below:



Related Topics

Devices components: Roles, cab files, services, and licenses on page 444

Cable K2 RAID

Before cabling, install the K2 RAID chassis in its permanent location. After mounting the chassis in the rack, you must secure brackets to the front rail to support the Grass Valley bezel. Refer to related topics in the "Installing and Servicing the K2 SAN" section of the K2 Topic Library for rack mount instructions.

You do not need to manually set a Fibre Channel address ID on controllers or a chassis address on Expansion chassis.

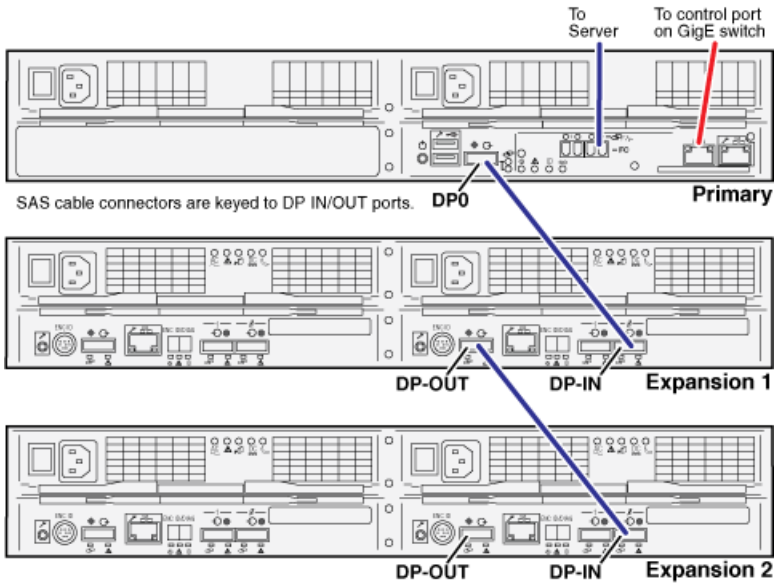
As directed by the system diagram for your storage system, cable the K2 RAID devices using the instructions in this section.

Once the RAID storage is connected and configured, do not swap Expansion chassis or otherwise reconfigure storage. If you connect an Expansion chassis in a different order or to the wrong controller, the controller will see a configuration mismatch and fault.

K2 RAID basic Proxy Storage

These cabling instructions apply to the following:

- K2 10Gv2 RAID (M100) on basic Proxy Storage.



Continue this cable pattern for additional Expansion Chassis.

Power on K2 and GV STRATUS system devices

All systems require this process.

1. Power on K2 systems.
   - For a K2 SAN, follow instructions in the "Installing and Servicing the K2 SAN" section of the K2 Topic Library.
   - For standalone K2 Summit systems, follow instructions in "K2 Summit Production Client Quick Start Guide".
2. If you have a Proxy Storage system, do the following:
   a) Power on K2 RAID and Ethernet switches.
   b) Power on the Proxy Storage file system server.
3. Power on all GV STRATUS servers.

GV STRATUS servers logon account

In an operational GV STRATUS system, GV STRATUS servers must be running and logged on to the Windows operating system. The logon account must be the GV STRATUS system internal system account. The internal system account is the account that the GV STRATUS system uses to access assets and some internal system functions. By default this is the GVAdmin account. Under supervision of Grass Valley, the internal system account can be changed.

NOTE: Do not enter a domain or otherwise modify account settings except under the supervision of qualified Grass Valley Support personnel. Extensive system configuration is required to achieve a working GV STRATUS system.

Related Topics

STRATUS Core Services settings on page 296

Test system setup and configuration process

All systems require this process. Verify that your cabling is correct, the system is operational as when pre-staged by Grass Valley, and to complete procedures by logging in to all devices and applications as user `Administrator`.

1. *Identify test applications and setup* on page 246. All systems require this process. Locate the applications pre-installed for test purposes and verify test environment.
2. *Test K2 systems* on page 248. All systems require this process.
3. *Pinging devices from the PC that hosts SiteConfig* on page 268.
4. *Install Important Windows updates (required)* on page 106.
5. *Test required GV STRATUS configuration settings* on page 249. All systems require this process.

Identify test applications and setup

All systems require this process. Locate the applications pre-installed for test purposes and verify test environment.

Grass Valley pre-installs all the applications you need to test basic system functionality. Before beginning with your tests, find the applications and make sure you understand the system setup you are testing.

When Grass Valley pre-installs applications for test purposes, in some cases the applications are installed on systems that do not meet the application's system requirements. This can cause minor functional anomalies that should not be interpreted as system problems. For example, a server platform does not have the graphics support required for the GV STRATUS application, so some

complex graphic displays, such as overlay transport controls, do not appear. In these cases use the application for basic system test purposes only.

1. Find test applications according to your system design, as follows:
   - GV STRATUS system (Express) with no K2 SAN:
     - K2 Summit systems — K2 AppCenter
     - GV STRATUS Express server — SiteConfig, GV STRATUS Control Panel, and GV STRATUS applications. All applications for test purposes only.
   - GV STRATUS system (A1, B1, C1) with a K2 SAN:
     - K2 Summit systems — K2 AppCenter
     - The K2 SAN's control point PC — SiteConfig and GV STRATUS Control Panel applications. Also the GV STRATUS application, for test purposes only.
2. Verify the state of your system at first power up, as follows:
   - GV STRATUS systems ship from Grass Valley with network configuration set to a workgroup named GRASS VALLEY.
   - All Windows operating system devices are a part of the GRASS VALLEY workgroup, with the same user groups, accounts, and passwords.
   - If your system has a GV STRATUS Express server, your site's GV STRATUS licenses (SabreTooth) are installed on that server. Otherwise they are installed on the GV STRATUS server with role of Common Services.
   - In the GV STRATUS Control Panel application, all licenses are assigned to the user group Administrators, which includes the user GVAdmin.
   - In the GV STRATUS Control Panel application, for your highest level license, all roles are assigned to the user GVAdmin.
3. Leave network configuration set to workgroup to perform initial tests at first power up.

   With your system in this state you can validate basic operations without introducing potential networking/permissions problems.
4. When testing, log in to all devices and applications as user `Administrator`.
5. After the system is commissioned and all operations are fully verified, ensure that applications installed on system devices for test purposes only are not used as part of the site's operational workflow. Applications are not supported for operation with full production workloads in these locations.

Test K2 systems

All systems require this process.

Whether you received your K2 system already set up from Grass Valley or you set up your K2 system on site, you should test the K2 system before proceeding.

This topic applies to the K2 systems that store and serve your high-resolution assets.

Test basic record and play operations using K2 AppCenter.

Refer to the "Using K2 AppCenter" section of the K2 Topic Library.

Related Topics

Identify test applications and setup on page 246

Pinging devices from the PC that hosts SiteConfig

All systems require this process. With SiteConfig, send the ping command to one or more devices.

- The devices you are pinging must be in the SiteConfig system description.

You can send the ping command to one or more devices in the system description over the network to which the SiteConfig host PC is connected. Typically this is the control network.

1. In the **Network Configuration** | **Networks** tree view, select a network, site, or system node.
2. In the Devices list view, select one or more devices. Use Ctrl + Click or Shift + Click to select multiple devices.
3. Right-click the selected device or devices and select **Ping**.

   The Ping Devices dialog box opens and lists the selected device or devices.

The Ping Devices dialog box reports the progress and results of the ping command per device.

Related Topics

Identify test applications and setup on page 246

Install Important Windows updates (required)

Grass Valley requires the installation of all Microsoft Windows Important updates on all GV STRATUS client and server devices, except as specifically instructed otherwise by Grass Valley.

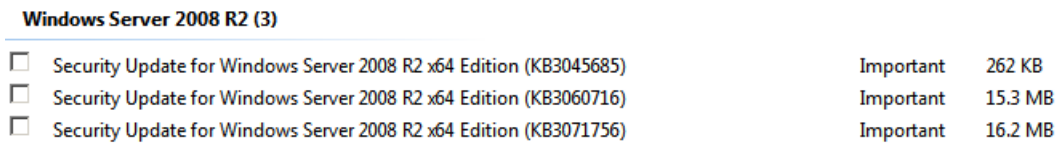
If a computer does not have the Grass Valley Embedded Security solution one-time initial deployment process applied, do not install any Windows updates. Apply the one-time process before installing Windows updates.

⚠ ***CAUTION: Only "Important Updates" should be installed. Do not install other Windows or driver updates unless specifically directed by product documentation or by Grass Valley Support.***

Prerequisite: Always install the required Microsoft Visual C++ redistributable update before installing the latest Windows Important Updates.

1. Go to **Start | Control Panel | Windows Updates | Check for updates**.

2. If these updates appear, right-click on them and select **Hide update**.



3. Install other “Important Updates”.
4. Reboot all GV STRATUS client and server devices after installing those Windows updates.

Related Topics

Deploy Embedded Security solution - One-time process

Test required GV STRATUS configuration settings

All systems require this process.

Whether you received your system pre-configured from Grass Valley or you configured your system on site, you should test the system operation before proceeding.

GV STRATUS client test

Do this for all systems. Whether you received your system pre-configured from Grass Valley or you configured your system on site, you should test the GV STRATUS application from one GV STRATUS client PC before proceeding.

In the GV STRATUS application, do the following:

a) In the Navigator, verify access to K2 Summit system bins.
b) Create a Channel Panel and test record/play operations.
c) In the Navigator, select assets on the K2 Summit system.
   The assets appear in the Asset List.
d) Double-click an asset in the Asset List.
   The asset opens in the Inspector.
e) In the Inspector, verify that the asset has a proxy association.

Related Topics

Identify test applications and setup on page 246

GV STRATUS proxy encoding test

Do this for all systems with Render Engines. Whether you received your system pre-configured from Grass Valley or you configured your system on site, you should test the proxy encoding from one GV STRATUS client PC before proceeding.

1. In the GV STRATUS application, identify a high-resolution asset and do the following:
   a) In the Navigator, select the high-resolution asset on the K2 Summit system.
      The asset appears in the Asset List.
   b) Display the **Has Proxy** column in the Asset List.
   c) Verify that the asset has a proxy association.
   d) Make sure the asset has not recently been used by any GV STRATUS tool or panel.

      An asset can retain an association with the tool or panel that recently used it and prevent proxy from being regenerated.
2. In the Asset List, right-click the high-resolution asset and select **Regenerate Proxy**.
3. Verify the following behavior:
   a) In the **Associations** tab of the Inspector, the proxy association is momentarily not visible.
      This occurs as the GV STRATUS system deletes the proxy asset.
   b) In the **Associations** tab of the Inspector, the proxy association shows as recording.
      This occurs due to the GV Render Engine is in the process of regenerating the proxy asset.
   c) In the **Associations** tab of the Inspector, the proxy association is visible again.
      This occurs as a result of the GV Render Engine has finished regenerating the proxy asset.

Customer network, licenses, and roles process

All systems require this process. Set up the GV STRATUS Core server on the customer's network and assign GV STRATUS licenses and roles to the customer's groups and users.

1. *Connect Core server to corporate LAN* on page 250. All systems require this process. Provide GV STRATUS servers access to the corporate LAN.
2. *Configuring licenses and roles settings: Required* on page 251. All systems require this process. Assign GV STRATUS licenses and roles to groups and users.

Connect Core server to corporate LAN

All systems require this process. Provide GV STRATUS servers access to the corporate LAN.

Corporate LAN access is required for GV STRATUS server variants of Express, Core, Proxy server, and Proxy Storage file system server.

Both local and remote GV STRATUS client PCs must be able to resolve the hostname of the core server.

If your GV STRATUS system is on a domain, all servers and client PCs on that system that have any interaction with Grass Valley components must be logged on to Windows with a domain user account. Do not use a local user account.

1. Work with the IT personnel at the customer site to configure Domain, DNS, DHCP, or any other settings required by the site's LAN.
2. If you have GV STRATUS applications on a different Windows domain from the server, define a trust relationship (one way or two way).

   For example, you could have your GV STRATUS on Windows domain A with a trust in the B domain. GV STRATUS applications running on Windows domain B can then connect to the server on Windows domain A.

Related Topics

About groups and users on a GV STRATUS system on page 37

License Management settings on page 365

Devices components: Roles, cab files, services, and licenses on page 444

Configuring licenses and roles settings: Required

All systems require this process. Assign GV STRATUS licenses and roles to groups and users.

- The groups and users to which you are assigning licenses and roles must be set up, either on a workgroup or on a domain, on the following:
  - The GV STRATUS server with role of Common Services.
- The GV STRATUS server with role of Common Services must have the site's GV STRATUS licenses installed.

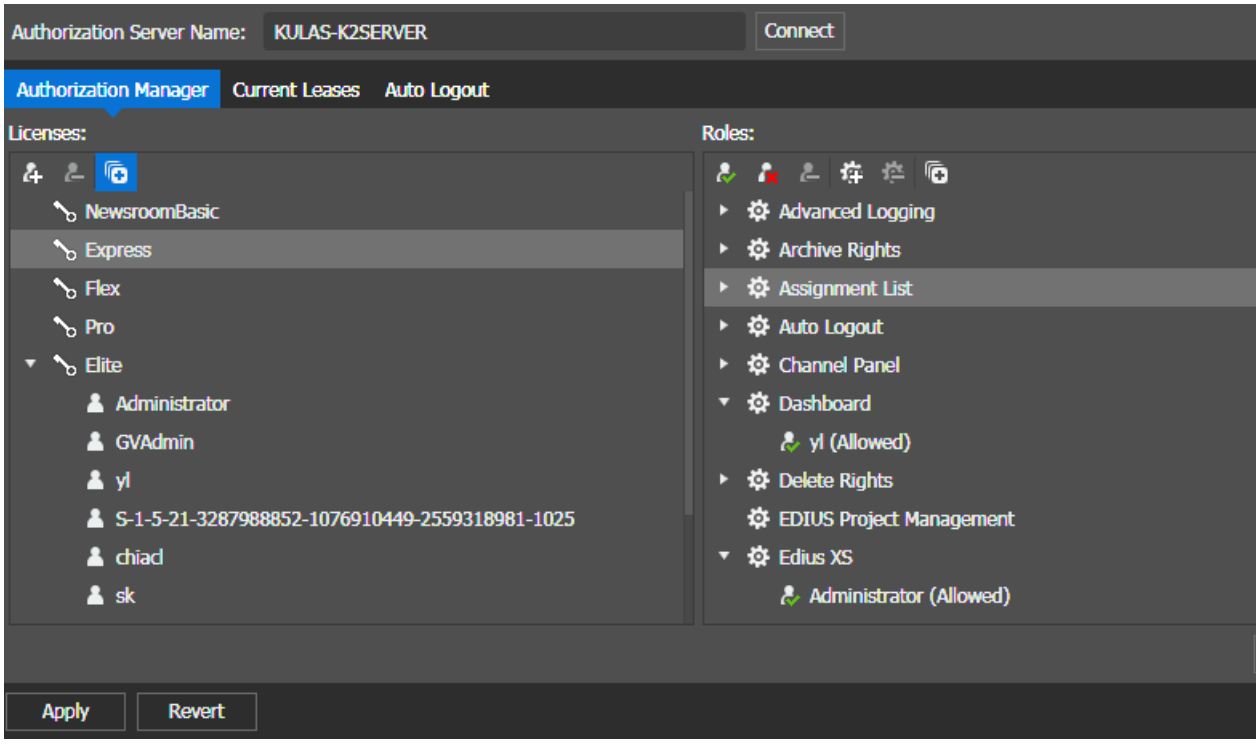
If on a network Workgroup, to configure Authorization Manager settings, you must be running GV STRATUS Control Panel on the GV STRATUS Core server.

When you receive your GV STRATUS system from Grass Valley, it is configured to workgroup, with all licenses and roles assigned to GVAdmin by default. Change the default configuration as appropriate for your site.

If you have temporary GV STRATUS licenses, GV STRATUS Control Panel allows you to configure Authorization Manager settings while you are waiting to install your permanent licenses. Authorization Manager displays indicators informing you of your license status.

To locate these settings, click **General | License Management | Authorization Manager**

1. In the GV STRATUS Control Panel application, open **License Management** settings.



2. On the Authorization Manager tab, enter the following:
   - **Authorization Server Name**: The name of GV STRATUS server with role of Common Services.
3. Click the following:
   - **Connect**: Connects to the GV STRATUS server and populates settings. If the Connect button is disabled, it means you are already connected.
4. Assign licenses according to the following description:
   - **Licenses**: Settings to assign licenses to user groups. When you select a license and click **Assign**, you can use standard Windows operating system processes to assign a group to the license. This can be either Workgroup or Domain, as appropriate for your site's user accounts. When you first assign a license to a group, all users in the group are assigned all of that license's roles. These are floating license so you may over-assign. If you over-assign you must ensure that the number of licenses checked out at any one time does not exceed the number of licenses available.

5. Assign roles according to the following description:

   - **Roles**: Settings to assign tools and other functionality to users or groups. When you expand a node and select one of its groups or users, you can allow or deny the group or user the use of that operation. You can also remove the group or user from the node. If a tool is not assigned to a user, when that user logs into the GV STRATUS application, the tool does not appear in the GV STRATUS application. If a new version of GV STRATUS software adds a role to a license, make sure it is assigned correctly to existing users.

   You can click the **Expand All** button to expand all licenses and roles on the **Authorization Manager** tab.

6. Click **Apply** to save your current settings, or click **Revert** to return to the last saved settings.

Related Topics

Identify test applications and setup on page 246
GV STRATUS roles matrix on page 37
Adding a custom role on page 466

Client PC set up process

All systems require this process. Add the customer's GV STRATUS client PCs to the system.

Your GV STRATUS system can have client PCs on different networks, depending on your system design and licensing. Work through the tasks in this section as appropriate for your GV STRATUS client PCs.

1. *System requirements for GV STRATUS client PC* on page 52. All systems require one or more GV STRATUS client PCs. Verify that all GV STRATUS client PCs meet system requirements.
2. *Cabling for high-resolution client PC* on page 256. Only systems with GV STRATUS client PCs on the K2 media (iSCSI) network require this process. Connect the PC to the control network and to the media network.
3. *Set firewall for application ports* on page 257. All systems require this process. Each GV STRATUS client PC must have the necessary port settings opened to ensure the GV STRATUS client application can connect to all servers.
4. *Install/configure for SiteConfig support on client PC* on page 261. All systems require this process. Prepare each GV STRATUS client PC so that it can be managed by SiteConfig.
5. *SiteConfig network setup for corporate LAN* on page 265. Only systems with GV STRATUS client PCs on the corporate LAN require this process. Add the corporate LAN to the SiteConfig system description.
6. *SiteConfig placeholder setup for client PC* on page 266. All systems require this process. Add client PCs as placeholder devices to the SiteConfig system description.
7. *SiteConfig corporate LAN setup for client PC* on page 268. Only systems with GV STRATUS client PCs on the corporate LAN require this process. Establish communication between SiteConfig and corporate LAN PCs without using device discovery.

8. *SiteConfig control network setup for client PC* on page 269. Only systems with GV STRATUS client PCs on the control network require this process. Add client PCs to SiteConfig using device discovery.
9. *SiteConfig software installation for client PC* on page 277. All systems require this process. Install GV STRATUS software for the first time on your GV STRATUS client PCs.
10. *K2Config setup for high-resolution client PC* on page 287. Only systems with GV STRATUS client PCs on the K2 media (iSCSI) network require this process. Add the PCs as clients to the K2 SAN.
11. *Set GV STRATUS client PC to high-resolution* on page 293. Only systems with GV STRATUS client PCs that use a high-resolution media workflow require this process. Configure the PC in GV STRATUS Control Panel.

Related Topics

About GV STRATUS client PCs on page 416

GV STRATUS client on page 229

System requirements for GV STRATUS client PC

All systems require one or more GV STRATUS client PCs. Verify that all GV STRATUS client PCs meet system requirements.

Virtual Machines, Remote Desktop, and other modes of remote access are not supported. Lack of robust video/graphic support can cause video display problems.

It is also recommended not to run multiple GV STRATUS desktop clients at a time logged in as the same user.

GV STRATUS Web client

These minimum requirements apply to a device running the following:

- The GV STRATUS Web Client

Characteristic	Specification
Web Browser	Recommended: Google Chrome
Frame accurate Streaming	Browser must support webRTC GV STRATUS system must be licensed with GV STRATUS Streaming Server.

GV STRATUS Laptop, and low-resolution Client workstation

These minimum requirements apply to a PC running one or more of the following:

- The GV STRATUS application with a proxy media workflow.
- The GV STRATUS Control Panel application.
- The SiteConfig application.

Characteristic	Specification
Processor	Minimum: Intel Core i3 mid-range processors and above Recommended: Intel Core i5 processor and above
Memory	Minimum: 4GB RAM Recommended: 8GB RAM (Especially when shared with 3rd party applications)
Graphics	Direct 3D 9+ support
System drive	Minimum: 80GB 7200RPM hard drive
Network	Single Ethernet 1000 Base-T network interface
Operating system	Microsoft Windows 7 SP1 32-bit (supported) or 64-bit (preferred) Microsoft Windows 10 64 bit
Microsoft .NET Framework	Version 4.7.1
Web Browser	Recommended: Google Chrome
Other support	DirectX 9 compatible

GV STRATUS/EDIUS XS Laptop, and low-resolution Client workstation

These minimum requirements apply to a PC running the following:

- The GV STRATUS application and the EDIUS XS application, with a proxy media workflow.

Characteristic	Specification
Processor	Intel Core i5 4 core processor and above
Memory	8GB RAM
Graphics	Integrated or discrete graphics with Direct 3D 9 or better
System drive	Minimum: 80GB 7200RPM hard drive Recommended: 128GB SSD drive or larger
Network	Single Ethernet 1000 Base-T network interface
Operating system	Microsoft Windows 7 SP1 32-bit (supported) or 64-bit (preferred) Microsoft Windows 10 64-bit ***NOTE: 64-bit required for EDIUS XS***
Microsoft .NET Framework	Version 4.7.1
Web Browser	Recommended: Google Chrome
Other support	DirectX 9 compatible

GV STRATUS high-resolution workstation

These requirements apply to a PC running the following:

- The GV STRATUS application with a high-resolution media workflow. This requires access to high-resolution assets.
- The EDIUS Workgroup application with a high-resolution media workflow. This requires access to high-resolution assets.

Characteristic	Specification
Processor	Recommended: Intel Core i7 4 Core 4GHz (For desktop grade machines) OR Recommended: Intel Xeon E5-2630 Quad Core 2.4 GHz (For workstation grade machines)
Memory	Minimum: 8GB RAM Recommended: 16GB RAM
Graphics	Integrated or discrete graphics with Direct 3D 9 or better
System drive	256GB SSD drive recommended OR 1TB 7200RPM hard drive (if SSD not available)
Network	Dual Ethernet 1000 Base-T network interface
Operating system	Microsoft Windows 7 SP1 64-bit Microsoft Windows 10 64-bit (on systems with SNFS 6.0.6 installed) ***NOTE: 64-bit required for EDIUS Workgroup.***
Microsoft .NET Framework	Version 4.7.1
Other support	DirectX 9 compatible

Cabling for high-resolution client PC

Only systems with GV STRATUS client PCs on the K2 media (iSCSI) network require this process. Connect the PC to the control network and to the media network.

A GV STRATUS client PC on the K2 media (iSCSI) network must have at least two Ethernet 1000 Base-T network interfaces.

- Connect one network interface to the control network.
- Connect one network interface to the media network.

Set firewall for application ports

If there is a firewall between systems running client applications and those application's servers, you must configure the firewall to ensure communication between client and server.

Related Topics

Ports and services mapping on page 715

GV STRATUS application ports

Port settings must be open so that the GV STRATUS client application can connect to servers as follows:

80	Protocol: TCP. Traffic: HTTP. Used by any GV STRATUS server, MediaFrame server, and Flexera server for EDIUS Workgroup license activation. Used by GV STRATUS Core Services.
443	Protocol: TCP. Used by SNFS for GUI (Java). Used by GV STRATUS applications for HTTPS secure communication with GV STRATUS Core Server. Used by EDIUS Workgroup applications for HTTPS secure communication with Flexera server for license activation.
445	Protocol: TCP. Used by SDB and XMOS Server and NAS. Used by SiteConfig. File and printer sharing. Used by SMB. Used by GV STRATUS Proxy Storage System. GV STRATUS clients and K2 Summit systems need access to shared folder for import and export.
2000	Protocol: TCP. Used by SDB Server incoming, and by GV STRATUS and GV STRATUS Rundown clients outgoing.
2001	Protocol: TCP. Used by SDB Server incoming, and by GV STRATUS and GV STRATUS Rundown clients outgoing.
2002	Protocol: TCP. Used by backup SDB Server incoming, and by GV STRATUS and GV STRATUS Rundown clients outgoing.
2003	Protocol: TCP. Used by backup SDB Server incoming, and by GV STRATUS and GV STRATUS Rundown clients outgoing.
3000	Protocol: TCP. Used by XMOS Server incoming, and by GV STRATUS and GV STRATUS Rundown clients outgoing.
3001	Protocol: TCP. Used by XMOS Server incoming, and by GV STRATUS and GV STRATUS Rundown clients outgoing.
3838	Protocol: TCP. Used by GV STRATUS Ingest services. Used by GV STRATUS Ingest DB Management Service. Used by GV STRATUS Core Server.
3839	Protocol: TCP. Used by GV STRATUS Ingest services. Used by GV STRATUS Core Server.
7144	Protocol: TCP. Traffic: HTTP. Used by GV STRATUS Router Config service for configuration. Used by GV STRATUS Ingest Services. Used by GV STRATUS Core Server.
7145	Protocol: TCP. Traffic: HTTP. Used by router config data service. Used by GV STRATUS Ingest Services. Used by GV STRATUS Core Server.

7213	Protocol: TCP. Used by GV STRATUS Router Controller service. Used by GV STRATUS Ingest Services. Used by GV STRATUS Core Server.
8000 - 8032	Protocol: TCP. Traffic: HTTP. Port 8000 used as follows: GV STRATUS Common Services, including preferences, licensing, authorization; Proxy config, Web Monitor data service; Ignite for Radamec SCP and Shotoku, IP to 422 Serial Communication (Camera Preset Recall). Ports 8000 to 8032 used by Ignite as follows: Digicart, IP to 422 Serial Communication; MDS-B5 and MDS-E11, IP to 422 Serial Communication (Audio Deck Control); Chyron Aprisa SSX, Chyron Duet, Inscriber MOS, and Multi Deko, IP to 232 Serial Communication (CG Graphic Load and Playout); GV Cameraman, IP to 232 Serial Communication (Camera Preset Recall); Under Monitor Display, IP to 422 Serial Communication (Sends Clip +/- time to external device); CalrecMixer, IP to 422 or 232 Serial Communication (Audio Mixer Control); VCR (BVW), IP to 422 Serial Communication (Deck Control); VDCP, IP to 422 Serial Communication (Deck/Video Server Control). Ports 8000 - 8032 used by Comtrol Devicemaster RTS. Used by GV STRATUS Core Server.
8080	Protocol: TCP. Traffic: HTTP. Used by GV STRATUS Summit Services. Used by WCF service provided by the GV STRATUS Workflow Engine. Used by WCF service provided by the GV STRATUS Rules Engine. Used by standalone K2 Summit system and by K2 Media Server with role of media file system manager.
8190	Protocol: TCP. Traffic: HTTP. Used by WCF service provided by DeviceKey Service.
8511	Protocol: TCP. Traffic: HTTP. Used by playout config data service. Used by GV STRATUS Control Panel Services. Used by GV STRATUS Core Server.
8732	Protocol: TCP. Traffic: HTTP. Used by Site Config data service . Used by GV STRATUS Control Panel Services. Used by GV STRATUS Core Server.
8733	Protocol: TCP. Traffic: HTTP. Used by K2 Config data service . Used by GV STRATUS Control Panel Services. Used by GV STRATUS Core Server.
8734	Protocol: TCP. Traffic: HTTP. Used by Site Config data service . Used by GV STRATUS Control Panel Services. Used by GV STRATUS Core Server.
8735	Protocol: TCP. Traffic: HTTP. Used by K2 Config data service. Used by GV STRATUS Control Panel Services. Used by GV STRATUS Core Server.
8736	Protocol: TCP. Used by GV STRATUS Control Panel Services for third-party storage configuration.
8737	Protocol: TCP. Traffic: HTTP. Used by GV STRATUS Ingest Config service for configuration. Used by GV STRATUS Control Panel Services for K2 Remote storage configuration. Used by GV STRATUS Core Server.
8740	Protocol: TCP. Traffic: HTTP. Used by general config data service. Used by GV STRATUS Control Panel Services. Used by GV STRATUS Core Server.
8742	Protocol: TCP. Traffic: HTTP. Used by Send destination config data service. Used by GV STRATUS Control Panel Services. Used by GV STRATUS Core Server.
8744	Protocol: TCP. Traffic: HTTP. Used by RMI config data service. Used by GV STRATUS Control Panel Services. Used by GV STRATUS Core Server.
16210 - 16215	Protocol: TCP. Ports 16210 to 16215 used by GV STRATUS Send Message tool.
31820	Protocol: UDP. Used for live streaming from K2 Summit/Solo systems. This is the default base for UDP ports, with the range being 31820 to 31827. Other ranges are

possible, depending on the UDP port base configured on the K2 Summit/Solo system. Used by standalone K2 Summit system and by K2 Media Server.

49171 TCP: Used by Grass Valley AppService for AppCenter connection between control point PC and K2 client/Solo, and used by GV STRATUS application and services to connect to Grass Valley K2 AppService.

GV STRATUS Control Panel application ports

Port settings must be open so that the GV STRATUS Control Panel application can connect to servers as follows:

80 Protocol: TCP. Traffic: HTTP. Used by any GV STRATUS server, MediaFrame server, and Flexera server for EDIUS Workgroup license activation. Used by config service for an GV STRATUS Core Server: Express; Core; Conform; Proxy Encoder; Transcode Engine; Workflow. Used by GV STRATUS Core Services. Used by standalone K2 Summit system and by K2 Media Server with role of media file system manager. Used by K2Config.

443 Protocol: TCP. Used by SNFS for GUI (Java). Used by GV STRATUS applications for HTTPS secure communication with GV STRATUS Core Server. Used by EDIUS Workgroup applications for HTTPS secure communication with Flexera server for license activation.

1433 TCP: Used by DSM. Used by GV STRATUS Core Services. Connection to SQL database. Used by GV STRATUS Core Server.

3838 Protocol: TCP. Used by GV STRATUS Ingest services. Used by GV STRATUS Ingest DB Management Service. Used by GV STRATUS Core Server.

3839 Protocol: TCP. Used by GV STRATUS Ingest services. Used by GV STRATUS Core Server.

7144 Protocol: TCP. Traffic: HTTP. Used by GV STRATUS Router Config service for configuration. Used by GV STRATUS Ingest Services. Used by GV STRATUS Core Server.

7145 Protocol: TCP. Traffic: HTTP. Used by router config data service. Used by GV STRATUS Ingest Services. Used by GV STRATUS Core Server.

7213 Protocol: TCP. Used by GV STRATUS Router Controller service. Used by GV STRATUS Ingest Services. Used by GV STRATUS Core Server.

8190 Protocol: TCP. Traffic: HTTP. Used by WCF service provided by DeviceKey Service.

8511 Protocol: TCP. Traffic: HTTP. Used by playout config data service. Used by GV STRATUS Control Panel Services. Used by GV STRATUS Core Server.

8732 Protocol: TCP. Traffic: HTTP. Used by Site Config data service . Used by GV STRATUS Control Panel Services. Used by GV STRATUS Core Server.

8733 Protocol: TCP. Traffic: HTTP. Used by K2 Config data service . Used by GV STRATUS Control Panel Services. Used by GV STRATUS Core Server.

8734 Protocol: TCP. Traffic: HTTP. Used by Site Config data service . Used by GV STRATUS Control Panel Services. Used by GV STRATUS Core Server.

8735 Protocol: TCP. Traffic: HTTP. Used by K2 Config data service. Used by GV STRATUS Control Panel Services. Used by GV STRATUS Core Server.

8736 Protocol: TCP. Used by GV STRATUS Control Panel Services for third-party storage configuration.

8737 Protocol: TCP. Traffic: HTTP. Used by GV STRATUS Ingest Config service for configuration. Used by GV STRATUS Control Panel Services for K2 Remote storage configuration. Used by GV STRATUS Core Server.

8740 Protocol: TCP. Traffic: HTTP. Used by general config data service. Used by GV STRATUS Control Panel Services. Used by GV STRATUS Core Server.

8742 Protocol: TCP. Traffic: HTTP. Used by Send destination config data service. Used by GV STRATUS Control Panel Services. Used by GV STRATUS Core Server.

8744 Protocol: TCP. Traffic: HTTP. Used by RMI config data service. Used by GV STRATUS Control Panel Services. Used by GV STRATUS Core Server.

16210 - 16215 Protocol: TCP. Ports 16210 to 16215 used by GV STRATUS Send Message tool.

GV STRATUS Web Client application ports

Port settings must be open so that the GV STRATUS Web Client application can connect to servers as follows:

80 Protocol: TCP. Traffic: HTTP. Used by any GV STRATUS server, MediaFrame server, and Flexera server for EDIUS Workgroup license activation. Used by GV STRATUS Core Services. Used for the Proxy Server.

443 Protocol: TCP. Used by SNFS for GUI (Java). Used by GV STRATUS applications for HTTPS secure communication with GV STRATUS Core Server. Used by EDIUS Workgroup applications for HTTPS secure communication with Flexera server for license activation.

GV STRATUS Rundown application ports

Port settings must be open so that the GV STRATUS Rundown client application can connect to servers as follows:

443 Protocol: TCP. Used by SNFS for GUI (Java). Used by GV STRATUS applications for HTTPS secure communication with GV STRATUS Core Server. Used by EDIUS Workgroup applications for HTTPS secure communication with Flexera server for license activation.

2000 Protocol: TCP. Used by SDB Server incoming, and by GV STRATUS and GV STRATUS Rundown clients outgoing.

2001 Protocol: TCP. Used by SDB Server incoming, and by GV STRATUS and GV STRATUS Rundown clients outgoing.

2002 Protocol: TCP. Used by backup SDB Server incoming, and by GV STRATUS and GV STRATUS Rundown clients outgoing.

2003 Protocol: TCP. Used by backup SDB Server incoming, and by GV STRATUS and GV STRATUS Rundown clients outgoing.

3000	Protocol: TCP. Used by XMOS Server incoming, and by GV STRATUS and GV STRATUS Rundown clients outgoing.
3001	Protocol: TCP. Used by XMOS Server incoming, and by GV STRATUS and GV STRATUS Rundown clients outgoing.
3811	Protocol: TCP. Used by Grass Valley AppService for 3rd party applications to communicate using AMP protocol. Used by SDB Server and GV STRATUS Rundown outgoing AMP communication to control playout channels. Used by Ignite for AMP, Video Server Control. Used by K2 Summit systems for playout.

Install/configure for SiteConfig support on client PC

All systems require this process. Prepare each GV STRATUS client PC so that it can be managed by SiteConfig.

With the installation instructions in this section, you use SiteConfig from a network connected control point PC and remotely install/upgrade software simultaneously on your system devices. This is the recommended process for software installation and upgrades. When installing the GV STRATUS application or the GV STRATUS Control Panel application, if SiteConfig installation is not possible, you may install manually on the local PC. You must uninstall before installing.

Related Topics

About GV STRATUS client PCs on page 416

Installing and configuring SiteConfig support for client PCs on corporate LAN

Before installing software, make sure the client PC meets system requirements, especially regarding Windows operating system and .NET version.

Use this topic to install software (if necessary) and configure PCs that are on the corporate LAN to prepare them for SiteConfig software deployment. This topic does not prepare the PC for SiteConfig network configuration, which requires that the SiteConfig Discovery Agent be installed. Since IT policies at many customer site's prohibit installation of software such as the SiteConfig Discovery Agent on corporate LAN PCs, this topic prepares the PC for software deployment only, without installing the Discovery Agent.

1. On the PC that hosts the SiteConfig application, navigate to the directory at which SiteConfig is installed.

   By default the location is `C:\Program Files (x86)\Grass Valley\SiteConfig`.

2. Copy the contents of the `ConnectivityKit` directory to a USB thumb drive, network drive, or some other shared location to make it easier to distribute to each corporate LAN PC.

3. To install and configure SiteConfig support locally at a corporate LAN PC, do the following:
   a) Copy the contents of the `ConnectivityKit` directory to the corporate LAN PC.
   b) On the corporate LAN PC, run `\Connectivity Kit\setup.exe`.
      If necessary, .NET software is installed.
   c) Open firewall port settings on the PC as follows.

445	Protocol: TCP. Used by SDB and XMOS Server and NAS. Used by SiteConfig. File and printer sharing. Used by SMB.
3389	TCP: Used by Remote Desktop for use by SiteConfig.
18262	TCP: Used by GV ProductFrame Configuration Service, ProductFrame Discovery Agent Service for use by SiteConfig. Used by GV NetConfig Service. gv-pf. UDP: Used by GV NetConfig Service. gv-pf.
18263	UDP: Used by ProductFrame Discovery Agent Service for GV NetConfig Device Broadcast/Unicast Protocol. Used by SiteConfig. Sent by ControlPoint, received by Devices
18264	UDP: Used by ProductFrame Discovery Agent Service for GV NetConfig Controller Protocol. Used by SiteConfig. Sent by Devices, received by ControlPoint
49168	HTTP/TCP: Used by Grass Valley K2 Config for K2Config application connection between a control point PC and the K2 system device configured. Used for most functions.
49169	TCP: Used by Grass Valley K2 Config for K2Config application connection between a control point PC and the K2 system device configured. Used for a few functions that require longer time periods.

   d) Restart the corporate LAN PC.

The corporate LAN PC is now prepared for SiteConfig software deployment.

Next, test access to proxy location.

Related Topics

System requirements for GV STRATUS client PC on page 52

Test access to proxy location

Do this test from a GV STRATUS client PC. This test does not require the GV STRATUS application to be installed on the client PC.

1. In a browser, enter the proxy URL and then press **Enter**.

   For example, if the computer that hosts the HTTP server is named `STRATUS-CS-Proxy`, the URL is as follows:

   `http://STRATUS-CS-Proxy/proxy`

2. A browser window should open to the proxy directory.

   This indicates that the proxy location is available from the HTTP server and that the GV STRATUS credentials are correct.

Installing and configuring SiteConfig support for client PCs on control network

Before installing software, make sure the client PC meets system requirements, especially regarding Windows operating system and .NET version.

Use this topic to install software and configure PCs that are on the control network to prepare them for SiteConfig discovery, network configuration, and software deployment. This requires that the SiteConfig Discovery Agent be installed. You do this locally at each PC on the control network.

1. On the PC that hosts the SiteConfig application, navigate to the directory at which SiteConfig is installed.

   By default the location is `C:\Program Files (x86)\Grass Valley\SiteConfig`.

2. Copy the contents of the `ConnectivityKit` directory and the `DiscoveryAgent Setup` directory to a USB thumb drive, network drive, or some other shared location to make it easier to distribute to each PC.

3. To install and configure SiteConfig support locally at a control network PC, do the following:
   a) Copy the contents of the `ConnectivityKit` directory and the `DiscoveryAgent Setup` directory to the control network PC.
   b) On the control network PC, check the Microsoft .NET Framework version and compare to system requirements for the software you intend to deploy with SiteConfig.
   c) If necessary, install .NET software and the required Windows update.

      You can find the installation file for a .NET version in the `ConnectivityKit` directory.
   d) On the control network PC, run `\DiscoveryAgent Setup\setup.exe`.

      The install wizard opens.
   e) Work through the install wizard and when prompted to select the device type, select **GenericDevice**.
   f) Finish the install wizard.
   g) Open firewall port settings on the PC as follows.

445	Protocol: TCP. Used by SDB and XMOS Server and NAS. Used by SiteConfig. File and printer sharing. Used by SMB.
3389	TCP: Used by Remote Desktop for use by SiteConfig.
18262	TCP: Used by GV ProductFrame Configuration Service, ProductFrame Discovery Agent Service for use by SiteConfig. Used by GV NetConfig Service. gv-pf. UDP: Used by GV NetConfig Service. gv-pf.
18263	UDP: Used by ProductFrame Discovery Agent Service for GV NetConfig Device Broadcast/Unicast Protocol. Used by SiteConfig. Sent by ControlPoint, received by Devices
18264	UDP: Used by ProductFrame Discovery Agent Service for GV NetConfig Controller Protocol. Used by SiteConfig. Sent by Devices, received by ControlPoint
49168	HTTP/TCP: Used by Grass Valley K2 Config for K2Config application connection between a control point PC and the K2 system device configured. Used for most functions.
49169	TCP: Used by Grass Valley K2 Config for K2Config application connection between a control point PC and the K2 system device configured. Used for a few functions that require longer time periods.

   h) Restart the control network PC.

The control network PC is now prepared for SiteConfig discovery, network configuration, and software deployment.

Next, add client PCs as placeholder devices to the SiteConfig system description.

Related Topics

System requirements for GV STRATUS client PC on page 52

SiteConfig network setup for corporate LAN

Only systems with GV STRATUS client PCs on the corporate LAN require this process. Add the corporate LAN to the SiteConfig system description.

1. Open the SiteConfig application.
2. In the **Network Configuration | Networks** tree view, select a System node or a Site node.

   The networks under that node are displayed in the list view.
3. If the corporate LAN is not already in the system description, proceed as follows:
   - To add a network under the currently selected node, in the tree view right-click the node and select **Add Network**.

   The Network Settings dialog box opens.
4. Configure the settings for the network as follows:
   - Type – Ethernet
   - Usage – Control
   - Redundancy – None
   - Name – Enter a name to identify the network in the system description
   - Exclude from Host Files – Select the checkbox
   - Unmanaged – Select this option, then select DNS and select the checkbox for IP Address Allocation via DHCP.
   - Base IP Address – Do not configure
   - Number of IP Addresses – Do not configure
   - Subnet Mask – Do not configure
   - DNS Servers – Servers providing DNS for name resolution. These DNS server can be for both managed and unmanaged networks.
   - Default Interface Name Suffix – The suffix added to the end of host names to identify interfaces on this network.
5. Click **OK** to save settings and close.
6. If you added a network, it appears in the **Network Configuration | Networks** tree view at the bottom of the list.

Related Topics

About the corporate LAN and SiteConfig on page 439
About software deployment on the corporate LAN on page 440
Corporate LAN network description on page 414

SiteConfig placeholder setup for client PC

All systems require this process. Add client PCs as placeholder devices to the SiteConfig system description.

Adding a GV STRATUS client PC to the system description

- The system description must contain a group.

1. In the **Network Configuration | Devices** tree view, right-click a group and select **Add Device**.

   The Add Device dialog box opens.

2. Configure settings for the device you are adding as follows:

   - Family – Select **GV STRATUS**.
   - Type – Select **GV STRATUS Client**.
   - Model – Select one of the following:

     - If the PC is connected to the corporate LAN or to the control network only, select **GV STRATUS PC**.
     - If the PC is connected to the control network and to the K2 media (iSCSI) network for access to high-resolution assets, select **GV STRATUS PC - SAN Client**.

   - Name – This is the device name, as displayed in the SiteConfig device tree view and device list view. This name can be different than the host name (network name). You can accept the default name or enter a name of your choice. Devices in the tree view are sorted alphabetically.
   - Amount – You can add multiple devices, as currently defined by your settings in the Add Device dialog box. An enumerator is added to the name to create a unique name for each device added.
   - Platform – Select **x86** for 32-bit operating system or **x64** for 64-bit operating system.
   - Control network – Select **Corporate LAN** or **Control**, as appropriate for the PC's network connection.
   - Starting Address – Select from the list of available addresses on the selected control network. If adding multiple devices, this is the starting address, with addresses assigned sequentially to each device added.

3. Click **OK** to save settings and close.
4. Repeat these steps for each of your devices.
5. If the PC is on the control network, verify that unmanaged control network interfaces are configured correctly and modify if necessary.

Related Topics

Modifying unassigned (unmanaged) control network interface on page 488

Set credentials

- The default credentials SiteConfig uses to access devices must be known.

- The credentials required to access your site's devices must be known.

1. At each local device, view the Windows administrator user account and verify that the credentials are the same as those that SiteConfig uses to access the device.
2. If necessary, change credentials so they match on the device and in SiteConfig, using one of the following methods:
   - Change the device's credentials to match the credentials that SiteConfig uses to access the device. This is recommended for K2, and GV STRATUS devices.
   - If your security policies prohibit changing the device's credentials, such as on PCs on the corporate LAN, in SiteConfig change the credentials that SiteConfig uses to access the device.

Related Topics

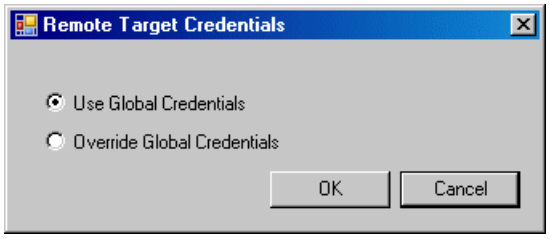
Changing passwords on page 710

Setting credentials for a specific device

For GV STRATUS client PCs on the corporate LAN, override global credentials so that SiteConfig has access to the PC for software deployment.

1. In the tree view, right-click a device and select **Credentials**.

   The Remote Target Credentials dialog box opens.



2. Proceed as follows:
   - If you previously applied credentials to the device that were different than the global credentials and now you want to apply the global device type credentials, select **Use Global Credentials**.
   - If you want to apply credentials to the device that are different than the device-type credentials, select **Override Global Credentials**.

   The Set Device Logon Credentials dialog box opens.
3. Enter the user name and password for the device and click **OK**. To test the credentials, right-click on the device and choose **Remote Desktop** to start a session to the device.

SiteConfig corporate LAN setup for client PC

Only systems with GV STRATUS client PCs on the corporate LAN require this process. Establish communication between SiteConfig and corporate LAN PCs without using device discovery.

Adding GV STRATUS client PCs on corporate LAN for software deployment

Only systems with GV STRATUS client PCs on the corporate LAN require this process. Establish communication between SiteConfig and corporate LAN PCs without using device discovery.

If you have PCs on the corporate LAN, use this topic to get the PCs communicating with SiteConfig in order to support software deployment. Do not attempt to use device discovery.

1. Select the placeholder device for the corporate LAN PC.
2. In the interfaces list view, right-click an interface and select **Edit**.

   The Unmanaged Network Interface Details dialog box opens.
3. Configure the settings for the interface as follows:
   - Network – Select the corporate LAN. This is an unmanaged network, which can use DHCP or an external hosts file.
   - IP Address – Make no selection.
   - DNS Suffix – For communication on some networks, a suffix, such as *mycorp.com*, must be added to host names.
   - Remaining settings are irrelevant, as SiteConfig does not manage this device's network.
4. Configure for the device name as follows:
   a) In the tree-view select the placeholder device.
   b) In the Device list view right-click the device and select **Edit**.

      The Edit Device dialog box opens.
   c) Edit the hostname.
   d) If using DHCP, specify a domain name.
   e) Click OK to save settings and close.
5. Click **OK** to save settings and close.
6. From the PC the hosts SiteConfig, ping the corporate LAN PC to verify communication.

Pinging devices from the PC that hosts SiteConfig

- The devices you are pinging must be in the SiteConfig system description.

You can send the ping command to one or more devices in the system description over the network to which the SiteConfig host PC is connected. Typically this is the control network.

1. In the **Network Configuration** | **Networks** tree view, select a network, site, or system node.
2. In the Devices list view, select one or more devices. Use Ctrl + Click or Shift + Click to select multiple devices.
3. Right-click the selected device or devices and select **Ping**.

   The Ping Devices dialog box opens and lists the selected device or devices.

The Ping Devices dialog box reports the progress and results of the ping command per device.

SiteConfig control network setup for client PC

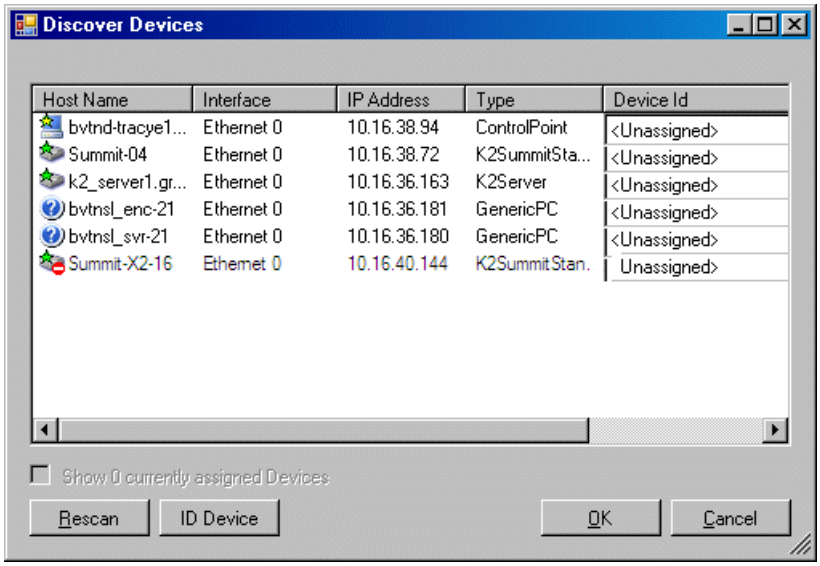
Only systems with GV STRATUS client PCs on the control network require this process. Add client PCs to SiteConfig using device discovery.

Discovering devices with SiteConfig

- The Ethernet switch or switches that support the control network must be configured and operational. If multiple switches, ISLs are connected and trunks configured.
- The PC that hosts SiteConfig must be communicating on the control network.
- There must be no routers between the PC that hosts SiteConfig and the devices to be discovered.
- Devices to be discovered must be Windows operating system devices, with SiteConfig support installed.
- Devices must be cabled for control network connections.

1. Open SiteConfig.
2. In the toolbar, click the discover devices button.

   The Discover Devices dialog box opens.



   A list of discovered devices is displayed.

3. Click **Rescan** to re-run the discovery mechanism. You can do this if a device that you want to discover has its network connection restored or otherwise becomes available. Additional devices discovered are added to the list.

Assigning discovered devices

- Devices must be discovered by SiteConfig
- Discovered devices must not yet be assigned to a device in the system description

- The system description must have placeholder devices to which to assign the discovered devices.

1. If the Discovered Devices Dialog box is not already open, click the discover devices button .

   The Discover Devices dialog box opens.

2. Identify discovered devices.

   - If a single device is discovered in multiple rows, it means the device has multiple network interfaces. Choose the interface that represents the device's currently connected control connection. This is typically Ethernet ... 0.
   - If necessary, select a device in the list and click **ID Device**. This triggers an action on the device, such as flashing an LED or ejecting a CD drive, to identify the device.

3. To also view previously discovered devices that have already been assigned to a device in the system description, select **Show … currently assigned devices**.

   The currently assigned devices are added to the list. Viewing both assigned and unassigned devices in this way can be helpful to verify the match between discovered devices and placeholder devices.

4. In the row for each discovered device, view items on the Device Id drop-down list to determine the match with placeholder devices, as follows:

   - If SiteConfig finds a match between the device-type discovered and the device-type of one or more placeholder devices, it displays those placeholder devices in the list.
   - If SiteConfig does not find a match between the device-type discovered and the device-type of a placeholder device, no placeholder device is displayed in the list.

5. In the row for a discovered device, click the Device Id drop-down list and select the placeholder device that corresponds to the discovered device.

   If there is no corresponding placeholder device currently in the system description, you can select **Add** to create a new placeholder device and then assign the discovered device to it.

6. When discovered devices have been assigned, click **OK** to save settings and close.
7. In the **Network Configuration | Devices** tree view, select each of the devices to which you assigned a discovered device.

Modifying managed control network interface

- The physical device you are configuring must be discovered and must be assigned to a device in the SiteConfig system description.
- SiteConfig must have communication with the device.

- The device must be defined in the system description with an appropriate network interface.

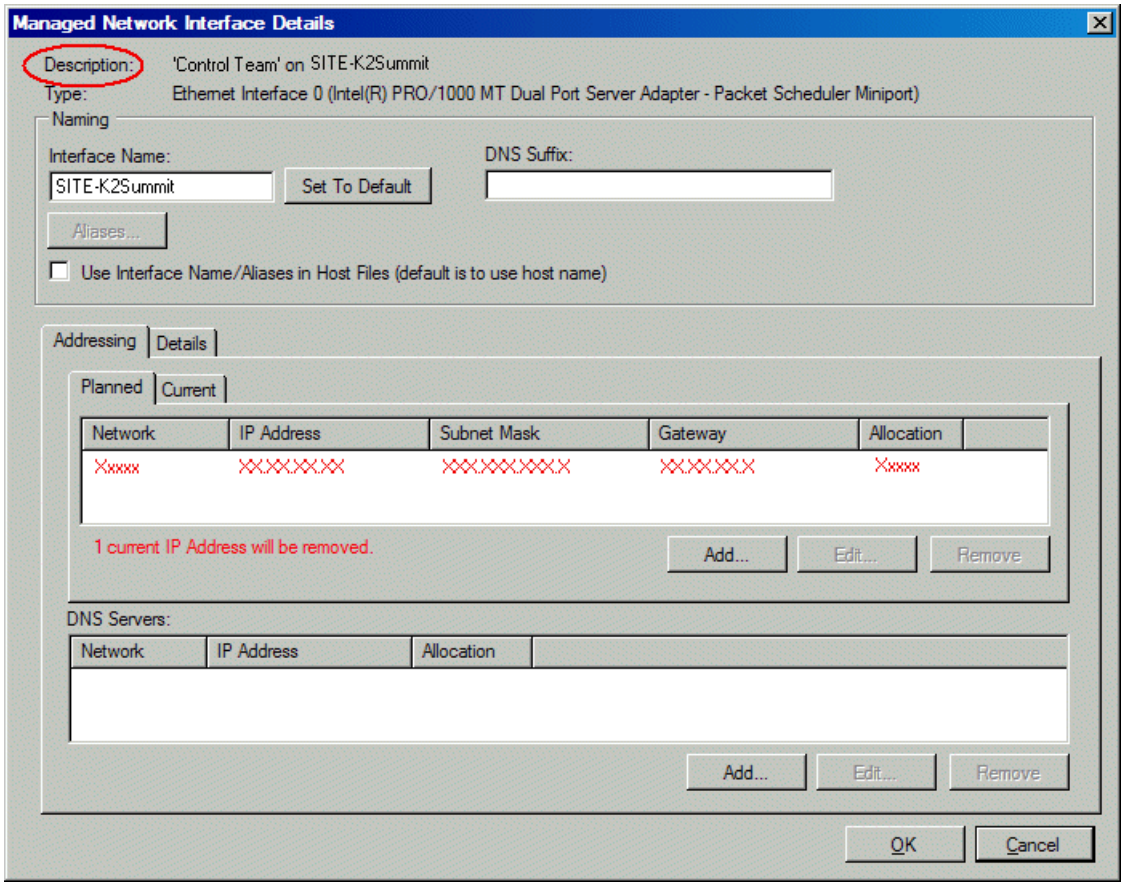
Use this task to modify managed the control network interface on a GV STRATUS Client PC:

1. In the Interfaces list view determine the interface to configure, as follows:
   - Identify the interface with which SiteConfig is currently communicating, indicated by the green star overlay icon. This should be the control network interface.
   - Verify that the interface over which SiteConfig is currently communicating is in fact the interface defined for the control network in the system description. If this is not the case, you might have the control network cable connected to the wrong interface port. The control connection should always be the first port on the motherboard, except when you have a loopback connection.
   - Configure the control network interface first before configuring any of the other interfaces.
   - A device can have multiple network interfaces that are not connected and are not required for system functionality. Give these interfaces a name such as "Unused" to aid identification.
2. In the Interfaces list view, check the icon for the interface you are configuring.

   If the icon has a red stop sign overlay, it indicates that current settings and planned settings do not match or that there is some other problem. Hover over the icon to read a tooltip with information about the problem.

3. In the Interfaces list view, right-click the control network interface and select **Edit**.

   The Managed Network Interface Details dialog box opens.



4. Identify the interface on the discovered device that you are configuring.

   - Identify Ethernet LAN adapters by their "Description" name. This is the Windows connection name. SiteConfig reads this name from the device and displays it at the top of this dialog box. This is the most accurate way to identify the network adapter on the discovered device that you are configuring.

   Make sure you are configuring the control network interface.

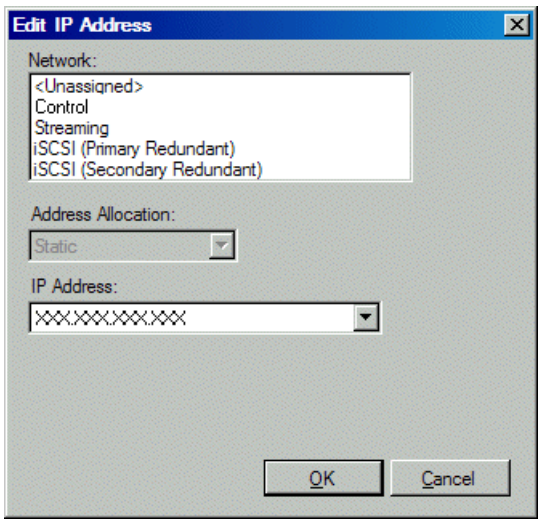
5. Configure naming settings as follows:

Setting...	For network interface Network Connection
Interface Name	The device host name. Required.
Set To Default	Not recommended
DNS Suffix	Allowed, if applicable to the network. The DNS suffix is added to the interface name.
Aliases	Not allowed
Use Interface Name/Aliases in Host Files	*Unselected* is required. Since not selected, the default behavior occurs, which is to use the device host name in the hosts file.

6. Evaluate settings on the Planned tab and change if necessary.
   - Compare settings on the Planned tab with settings on the Current tab.
   - If you want to keep the current settings as reported in the Current tab, click **Remove** to remove the planned settings.
   - Do not specify multiple IP addresses for the same interface. Do not use the Add button.

7. To modify planned settings, do the following:
   a) Select the network settings and click **Edit**.

      The Edit IP Address dialog box opens.



   b) Edit IP address settings as follows:

Setting...	For network interface Network Connection
Network	*Control* is required
Address Allocation	*Static* is recommended.
IP Address	The IP address for this interface on the network. Required.

      The networks listed in the Edit IP Address dialog box are those currently defined in the system description, with available settings restricted according to the network definition. If you require settings that are not available, you can close dialog boxes and go to the **Network Configuration | Networks** tab to modify network settings, then return to the Edit IP Address dialog box to continue.

8. When you have verified that the planned settings are correct, click **OK**, then **Yes** to apply settings to the device and close.

   A Contacting Device message box reports progress.

9. After configuring control network settings, do the following
   a) If a message informs you of a possible loss of communication, click **OK**.

      This message is normal, since this is the network over which you are currently communicating.

   b) In the Device list view, observe the device icon and wait until the icon displays the green star overlay before proceeding.

      The icon might not display the green star overlay for several seconds as settings are reconfigured and communication is re-established.

   c) In the Interface list view, right-click the interface and select **Ping**.

      The Ping Host dialog box opens.

      If ping status reports success, the interface is communicating on the control network.

Making the host name the same as the device name

1. Verify that the current device name, as displayed in the SiteConfig tree view, is the same as your desired host name.
2. In the **Network Configuration | Devices | Device** list view, right-click the device and select **Edit**.

   The Edit Device dialog box opens.
3. Identify the state of buttons as follows:
   - If the host name is different than the device name, the **Set to Device Name** button is enabled.
   - If the host name is the same as the device name, the **Set to Device Name** button is disabled.
4. If enabled, click **Set to Device Name**.

   This changes the host name to be the same as the device name.
5. Click **OK**.
6. When prompted, restart the device.

Pinging devices from the PC that hosts SiteConfig

- The devices you are pinging must be in the SiteConfig system description.

You can send the ping command to one or more devices in the system description over the network to which the SiteConfig host PC is connected. Typically this is the control network.

1. In the **Network Configuration** | **Networks** tree view, select a network, site, or system node.
2. In the Devices list view, select one or more devices. Use Ctrl + Click or Shift + Click to select multiple devices.
3. Right-click the selected device or devices and select **Ping**.

   The Ping Devices dialog box opens and lists the selected device or devices.

The Ping Devices dialog box reports the progress and results of the ping command per device.

Verify credentials

- The device you are verifying must be in the SiteConfig system description and must be communicating on the network.

  In the SiteConfig tree-view, right-click the device and select **Remote Desktop**, then proceed as follows:

  - If Remote Desktop opens without prompting you to log on, no further steps are necessary. SiteConfig credentials are set properly to allow access to the device.
  - If Remote Desktop prompts you to log on, check credentials in SiteConfig and on the device and reconcile as necessary.

Related Topics

About credentials in SiteConfig on page 42
Set credentials on page 266
Changing passwords on page 710

Generating host tables using SiteConfig

- Planned control network settings must be applied to control network interfaces and devices must be communicating on the control network as defined in the system description.
- Interfaces for networks that require name resolution via the hosts file, such as the FTP/streaming network, must have settings applied and must be communicating.
- Host names defined in the system description must be correct.
- The SiteConfig PC must be added to the system description so that it is included in the host tables generated by SiteConfig.

When you add or modify devices or their IP addresses in the SiteConfig system description, you should update host tables on all devices that use them.

1. In the **Network Configuration | Networks** tree view, select a network, site, or system node.
2. Click **View Hosts file**.

   A Hosts File Contents window opens that displays the contents of the hosts file as currently defined in the system description.

3. Verify the information in the hosts file.

4. Do one of the following:
   - If you are managing host table information yourself, click **Save As** and save a copy of the hosts file to a location on the control point PC. Then open the copy of the hosts file, copy the desired host table information from it, and paste it into your facility hosts file as desired. Then you can use your own process to distribute the facility hosts file to devices. Remember to distribute to the control point PC so that SiteConfig and other management applications such as K2Config can resolve network host names.
   - If SiteConfig is managing hosts files, do the following:

   NOTE: Writing hosts files to multiple devices consumes system resource and network bandwidth. Therefore it is recommended that you wait and do this after the system is complete and fully implemented, rather than updating hosts files incrementally as you discover/assign devices.

   a) In the **Network Configuration | Devices | Devices** list view, right-click a device to which you intend to write the hosts file and select **View Current Host File**.

      A Host File Contents window opens that displays the contents of the hosts file that is currently on that actual device.

   b) Verify that there is no information that you want to retain in the device's current hosts file that is not also in the hosts file as currently defined in the system description. If you need to save the device's current hosts file, click **Save As** and save to a different location.

   c) In the **Network Configuration | Devices | Devices** list view, right-click a device or use Ctrl + Click to select multiple devices, and select **Update Host File**.

      The current hosts file is overwritten with the hosts file as defined in the system description.

Related Topics

About hosts files and SiteConfig on page 440

SiteConfig software installation for client PC

All systems require this process. Install GV STRATUS software for the first time on your GV STRATUS client PCs.

With the installation instructions in this section, you use SiteConfig from a network connected control point PC and remotely install/upgrade software simultaneously on your system devices. This is the recommended process for software installation and upgrades. When installing the GV STRATUS application or the GV STRATUS Control Panel application, if SiteConfig installation is not possible, you may install manually on the local PC. You must uninstall before installing.

Related Topics

System requirements for GV STRATUS client PC on page 52

Verify software roles

All systems require this process.

Verify that the roles assigned to your GV STRATUS client PCs in SiteConfig are correct for your system design.

1. In the **Software Deployment | Devices** tree view, expand a device's node to expose the roles currently assigned to the device.
2. Identify roles as follows:
   - GV STRATUS client PCs on the corporate LAN for a proxy media workflow have the following role:
     - GV STRATUS Application
     - EDIUS (Required for EDIUS XS)
   - GV STRATUS client PCs on the control/media network for a high-resolution media workflow have the following roles:
     - GV STRATUS Application
     - StorNext File System Client (non K2 only)
     - Generic iSCSI Client (non K2 only)

       NOTE: First install StorNext File System Client, then install Generic iSCSI Client via SiteConfig for the following:

       - ***First installation of GV STRATUS application into a system.***
       - ***When there is an upgrade of the StorNext File System Client.***
     - EDIUS (Required for EDIUS Workgroup)
3. If the roles are not correct for your system design, add or remove roles accordingly.

Place GV STRATUS Client PCs into deployment group

1. Place your GV STRATUS client PCs into the GV STRATUS software deployment group.
2. Place GV STRATUS client PCs on which you intend to install EDIUS application software into an EDIUS deployment group.

Related Topics

Configuring deployment groups on page 80

Check all currently installed software on GV STRATUS devices

Check software on GV STRATUS devices.

- The device must be assigned in the SiteConfig system description and network connectivity must be present.
- SiteConfig must be able to log in to the device using the username/password credentials assigned to the device.

- The SiteConfig PC must not have a network drive mapped to an administrative share (such as C$) on a device on which you are checking software.
- Put devices that run Embedded Security into Update Mode. Refer to the related topic on the Embedded Security one-time initial deployment process.

  NOTE: A re-image of the computer might be necessary if the Embedded Security one-time process is done incorrectly. Follow instructions carefully.

Do the following steps on the devices on which you are installing or upgrading software.

1. In the **Software Deployment | Deployment Groups** tree view, right-click the top-most node for the group or any individual device and select **Check Software**.

   NOTE: If you have access problems, verify that the administrator account on the device has credentials as currently configured in SiteConfig.

   NOTE: If an "Unable to copy ... to target" error appears for a device that has the Grass Valley Embedded Security solution, apply the* Embedded Security *solution one-time initial deployment process to the device. After the one-time process is complete the error does not appear and it is no longer necessary to put* Embedded Security *in Update mode.

   The Check Software dialog box appears. SiteConfig searches for software on the selected device or devices and gathers information. Progress is reported.
2. When the check is complete, close the Check Software dialog box.

An updated list of all currently installed software is displayed in the **Software Deployment | Devices | Installed Software** list view. If software is a SiteConfig managed software package, information is displayed in the Managed Package and Deployment Group columns.

Related Topics

Complete listing of device types, roles, and software packages for GV STRATUS devices on page 194

Deploy Embedded Security solution - One-time process

Add software package to deployment group for GV STRATUS client PCs

- The GV STRATUS devices to which you are deploying software must have their SiteConfig roles correctly configured.
- The GV STRATUS devices to which you are deploying software must be in a deployment group.

GV STRATUS Client PC low-resolution (proxy):

- SiteConfig "Add Device":
  - Family: GV STRATUS

    NOTE: Do not select the EDIUS family.
  - Device Type: GV STRATUS Client
  - Model: GV STRATUS PC or GV STRATUS/EDIUS PC (if using EDIUS XS)
- SiteConfig roles:
  - GV STRATUS Application
  - EDIUS (Required for EDIUS XS)

- Software packages:
  - *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValley_STRATUS_Application_x.x.x.cab*
    - *EDIUS_x.x.x.cab* (Required for EDIUS XS)

1. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.
2. Click the **Add** button.

   The Add Package(s) dialog box opens.
3. Do one of the following to select the software package:
   - Select from the list of packages then click **OK**.
   - Click **Browse**, browse to and select the package, then click **Open**.
4. If one or more EULAs are displayed, accept them to proceed. If you do not accept a EULA, the associated software is not assigned to the deployment group.

   SiteConfig adds the package to the deployment group.

The package appears in the Managed Packages list for the selected deployment group. SiteConfig creates new software deployment tasks for the package and displays them in the Tasks list view.

About installing the GV STRATUS application

Use SiteConfig to deploy the GV STRATUS application software to all your GV STRATUS client PCs.

When you use SiteConfig to deploy the GV STRATUS application, SiteConfig configures the GV STRATUS Control Panel Host on each GV STRATUS client PC, providing the following prerequisites are in place:

- In the SiteConfig application, in **Tools | Options | Network Configuration**, the GV STRATUS Control Panel Services Host must be correctly configured.
- In the SiteConfig system description, the GV STRATUS client PC must have the role of GV STRATUS Application.

Installing GV STRATUS application with SiteConfig

- The devices to which you are installing software must be in a deployment group.
- For the software you are installing, the managed package must be added to the deployment group.
- The SiteConfig "Check Software" operation must have been recently done on the devices to which you are installing software.
- The PCs to which you are installing the GV STRATUS application meet GV STRATUS client system requirements, such as the Microsoft .NET Framework.
- The PCs to which you are installing the GV STRATUS application have the SiteConfig role of GV STRATUS Application and if high-resolution clients also the role of StorNext file system client.

- You have added `GrassValley_STRATUSClient_`x.x.x.cab to the deployment group. This system cab file contains all the cab files required for both proxy clients and high-resolution clients. Refer to release notes for version information.

1. In the **Software Deployment | Deployment Groups** tree view, select the device or the group of devices to which you are installing software. You can select a Device node, a Deployment Group node, or the All Deployment Groups node.

   The corresponding software deployment tasks are displayed in the Tasks list view.
2. Identify one or more deployment tasks listed as "Install" in the Action column.
3. Select the **Deploy** check box in the row for the install task for installing software that is not EDIUS software. If you want to install EDIUS software, select the appropriate check box.

   If a WFRegMon install task appears, install it as well. It is required to support Grass Valley software installers. There is no uninstall task.
4. Before starting the deployment session, verify the following for the installation deployment tasks:
   - The Deploy checkbox is selected.
   - The software package is the correct version.
   - The Action column reports Install.
   - The Status column indicates the planned icon.
   - The Details column does not indicate that deployment options are required.
5. Click the **Start Deployment** button.

   Deployment tasks run and software is installed. Progress is reported in both the Status and Details columns.

   NOTE: If an "Unable to copy ... to target" error appears for a device that has the Grass Valley Embedded Security solution, apply the* Embedded Security *solution one-time initial deployment process to the device. After the one-time process is complete the error does not appear and it is no longer necessary to put* Embedded Security *in Update mode.
6. Monitor progress as indicated by both the Status and Details column. When finished, the Status column indicates complete.

Installing EDIUS software with SiteConfig

- The devices to which you are installing software must be in a deployment group.
- For the software you are installing, the managed package must be added to the deployment group.
- The SiteConfig "Check Software" operation must have been recently done on the devices to which you are installing software.
- If installing to an EDIUS Workgroup client PC on which you have previously installed EDIUS manually (not with SiteConfig), EDIUS Workgroup and supporting software must first be uninstalled manually, before attempting to install with SiteConfig.
- The PCs to which you are installing the EDIUS application must have the SiteConfig role of EDIUS Application and if EDIUS Workgroup also the role of StorNext file system client.
- GV STRATUS client cab file and EDIUS cab file must be added to the EDIUS deployment group. This system cab file contains all the cab files required for both proxy clients and high-resolution clients. Refer to release notes for version information.
- Windows High Priority updates are required and must be installed. For more details, refer to *Install Important Windows updates for EDIUS* on page 148.

NOTE: Expect long deployment times when installing Render Engine and EDIUS software. EDIUS software and Render Engine software can take several minutes to install. Allow the installation to complete. Do not attempt to stop the installation.

1. In the **Software Deployment | Deployment Groups** tree view, select the device or the group of devices to which you are installing software. You can select a Device node, a Deployment Group node, or the All Deployment Groups node.

   The corresponding software deployment tasks are displayed in the Tasks list view.
2. Identify one or more deployment tasks listed as "Install" in the Action column.
3. For the software you are installing, select the **Deploy** check box in the row for the install task.

   If a WFRegMon install task appears, install it as well. It is required to support Grass Valley software installers. There is no uninstall task.
4. Before starting the deployment session, verify the following for the installation deployment tasks:

   - The Deploy checkbox is selected.
   - The software package is the correct version.
   - The Action column reports Install.
   - The Status column indicates the planned icon.
   - The Details column does not indicate that deployment options are required.
5. Click the **Start Deployment** button.

   Deployment tasks run and software is installed. Progress is reported in both the Status and Details columns.

   NOTE: If an "Unable to copy ... to target" error appears for a device that has the Grass Valley Embedded Security solution, apply the* Embedded Security *solution one-time initial deployment process to the device. After the one-time process is complete the error does not appear and it is no longer necessary to put* Embedded Security *in Update mode.
6. Monitor progress as indicated by both the Status and Details column. When finished, the Status column indicates complete.

Related Topics

If you have trouble launching EDIUS XS on page 169

Uninstall EDIUS Workgroup and supporting software on page 148

Access K2 storage for EDIUS using standard convention

EDIUS components require access to K2 storage. This access can be configured several ways, but problems can arise when different conventions are used. To reduce potential problems and make troubleshooting easier, use the same convention for all EDIUS devices and components. For example, with UNC paths, do not use a hostname for one setting and an IP address for another setting. This includes settings for EDIUS XRE Server, EDIUS XS, and EDIUS Workgroup.

The following types of access are used by EDIUS components to access K2 storage:

- Shared EDIUS projects folder: The device hosting EDIUS components uses a UNC path to access the EDIUS projects folder. The folder must be shared to allow access by the EDIUS device, but no drive mapping is required. This type of access is used by current EDIUS XS components and EDIUS Workgroup components.

- iSCSI: The device hosting EDIUS components is an iSCSI client to a K2 SAN. The entire K2 media file system, which is the V: drive, is accessible. This type of access is used by EDIUS Workgroup components and EDIUS XRE Server components.
- Mapped V: drive: The device hosting EDIUS components maps the entire K2 storage V: drive as a network drive. The V: drive must be shared to allow access by the EDIUS device. This type of access is used by previous versions of EDIUS XS components. If an EDIUS XRE Server is not an iSCSI client, this type of access can be used by EDIUS XRE Server components.

1. On the K2 storage system device, which is typically the K2 SAN's K2 Media Server (FSM), make sure the EDIUS projects folder is shared so that the following devices have Read/Write access:
   - EDIUS XS client PCs
   - EDIUS XRE Server
   - EDIUS Workgroup client PCs, if you have any in your system.
2. For the device that requires access to the EDIUS projects folder, such as an EDIUS XS client PC, verify UNC path access.

   For example, enter the following in Windows Explorer and verify that the directory opens:

   `\\k2-san-fsm\EDIUS_Projects`
3. For other settings to the EDIUS projects folder, use the same UNC path convention, such as `\\k2-san-fsm\EDIUS_Projects`. This includes the following settings:
   - In GV STRATUS Control Panel, the EDIUS XS default project location setting.
   - On the EDIUS XRE Server, XRE Management Server settings.
   - EDIUS Workgroup settings.

Whether typing in the path or browsing the network and selecting the folder, make sure the convention is the same for all EDIUS components.

Configure GVAdmin account

This task applies to a computer on which the following software is installed:

- GV STRATUS/EDIUS client PC
- EDIUS XRE Server
- Render Engine Server

Verify the following before doing this task:

- EDIUS or Render Engine software must be installed on the computer.

  Add the internal system account, which by default is GVAdmin, to the Administrators group on the computer.

Related Topics

GV STRATUS servers logon account on page 245

Install Grass Valley Prerequisite Files on the SiteConfig PC

GV STRATUS VTR Ingest, GV STRATUS VTR Controller, and GV STRATUS Rundown share Microsoft .NET as common prerequisite software. This common software is installed with `Prerequisite Files 2.0.exe`, which is part of a separate installation package. You install this

prerequisite software package on the control point PC so that when SiteConfig deploys any software that needs the prerequisite software, it uses the software installation files from the common package. This reduces the size of `.cab` files overall and makes software download more manageable.

1. Check release notes for the required version of prerequisite files, if any.
2. On the SiteConfig PC, open Windows Add/Remove programs and look for **Grass Valley Prerequisite Files**, then proceed as follows:
   - If the required version of prerequisite files is installed, do not proceed with this task.
   - If prerequisite files are not installed or are not at the required version, proceed with this task.
3. Procure the required prerequisite software installation file as listed in the following:

Product	Prerequisite file	Location
GV STRATUS Rundown, GV STRATUS VTR Ingest, GV STRATUS VTR Controller	GrassValley_PrerequisiteFiles_2.0.0.zip (Microsoft .NET installer)	Grass Valley website *SiteConfig Application software download page*.

4. On the SiteConfig PC, run the installation file. The installation program copies prerequisite files to `C:\Program Files\Grass Valley\Prerequisite Files`.

After installing prerequisite files on the SiteConfig PC, use SiteConfig and deploy software to client PCs.

Installing GV STRATUS and GV STRATUS Rundown applications with SiteConfig

- The devices that you are upgrading must be in a deployment group.
- For the software you are upgrading, a newer version of that managed software package must be added to the deployment group.
- Grass Valley Prerequisite Files must be installed on the control point PC.
- A SiteConfig "Check Software" operation must be performed on the devices you are upgrading.
- The PCs to which you are installing the GV STRATUS application must meet GV STRATUS client system requirements, such as the Microsoft .NET Framework.
- The PCs to which you are installing the GV STRATUS application must have the SiteConfig role of GV STRATUS Application and if high-resolution clients must also have the role of StorNext file system client.
- The PCs to which you are installing the GV STRATUS Rundown application must have the SiteConfig role of GV STRATUS Rundown Application. Refer to SiteConfig Core server software install related topics in this Topic Library to install GV STRATUS Rundown server components (SDB server and XMOS server).
- `GrassValley_STRATUSClient_`x.x.x.cab must be added to the deployment group. This system cab file contains all the cab files required for both proxy clients and high-resolution clients. Refer to release notes for version information.
- `GrassValley_CoreServer_`x.x.x.cab must be added to the deployment group. Refer to release notes for version information.
- `GrassValley_K2system_`x.x.x.cab must be added to the deployment group. Refer to release notes for version information.

If you are upgrading multiple software components for which there is a required sequence, you must check and uncheck tasks and run multiple deployment sessions to control the sequence. For some software components, SiteConfig aids you by enforcing dependencies. For each individual software

component, SiteConfig enforces an uninstall of the current version of software before installing the upgrade version. SiteConfig provides uninstall deployment tasks and install deployment tasks to indicate the taskflow. SiteConfig can do the uninstall/install in a single deployment session.

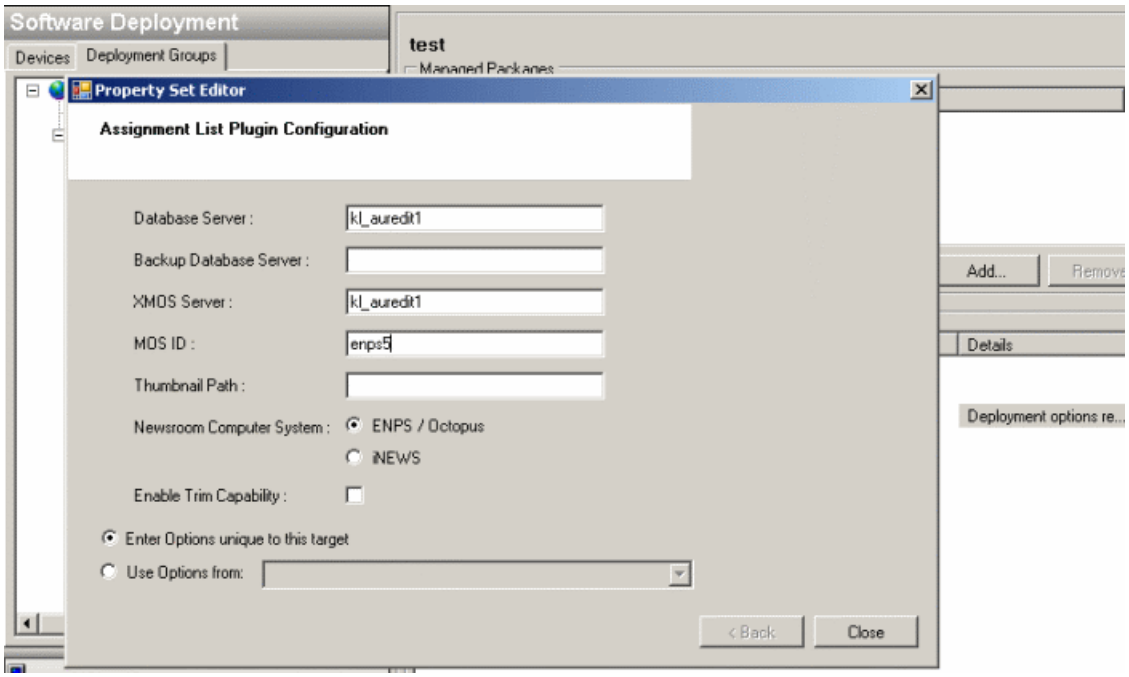
1. In the **Software Deployment | Deployment Groups** tree view, select the device or the group of devices to which you are deploying software.

   The corresponding software deployment tasks are displayed in the Tasks list view.

2. For the software you are deploying, select the **Deploy** check box in the row for the uninstall task.
3. For the software you are installing, select the **Deploy** check box in the row for the install task.

   If you have the Assignment List Plugin role assigned to a playout device, then you will have to set deployment options. The **Details** column will indicate **Deployment options required**.

   Click the **Deployment options required** link and a wizard page appears.



Key-in the Database Server, XMOS Server, MOS ID and select the appropriate Newsroom Computer System in your operation. Then, click **Close**.

For upgrading GV STRATUS Rundown to this release, deploy the following tasks:

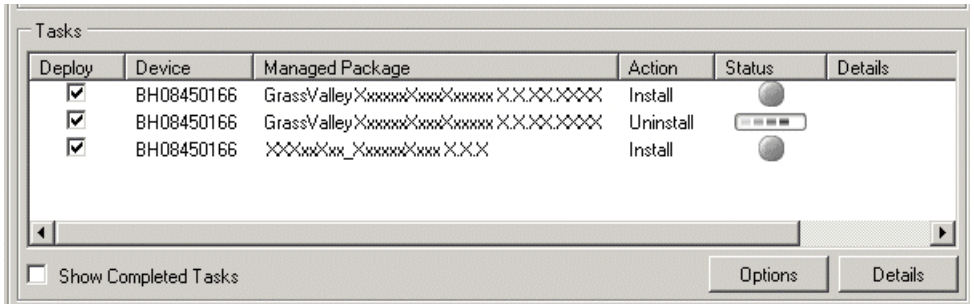
Deploy	Managed Package	Action
✓	GV_STRATUS_Rundown xxxx.xxxx	Uninstall
✓	GV_STRATUS_Rundown xxxx.xxxx	Install
✓	GrassValley_STRATUS_ControlPanel_ xxxx.xxxx	Install

NOTE: If there are dependencies, SiteConfig can enforce that some tasks be deployed together.

4. Check the area next to the Start Deployment button for a message.

   If a message instructs you to upgrade the Discovery Agent, on the control point PC go to the directory to which SiteConfig is installed, find the `DiscoveryAgent_x.x.x.x.cab` file, add it to the deployment group, and deploy the Discovery Agent software as well.

5. Click the **Start Deployment** button.



   Deployment tasks run and software is uninstalled. Progress is reported and next steps are indicated in both the Status and Details columns. If an error appears regarding prerequisite software, install the Grass Valley Prerequisite Files on the control point PC and then repeat this step.

6. When the Status or Details columns indicate next steps, identify the software in the row, then do one of the following:

   - For K2 software, when Details displays a **Restart required** link (but not "Visible dialog pending..."), click the link and when prompted "...are you sure...", click **Yes**.

   The device restarts. This restart is required by the GV STRATUS Rundown software uninstall.

   Deployment tasks run and software is installed. Progress is reported and next steps are indicated in both the Status and Details columns.

7. When the Status or Details columns indicate next steps, identify the software in the row, then do one of the following:

   - For K2 software, when Details displays a **Restart required** link (but not "Visible dialog pending..."), click the link and when prompted "...are you sure...", click **Yes**.

   The device restarts.

8. Monitor progress as indicated by both the Status and Details column. When finished, the Status column indicates complete.

Refer to ENPS, iNEWS or Octopus customer documentation in order to install your Newsroom Computer System.

K2Config setup for high-resolution client PC

Only systems with GV STRATUS client PCs on the K2 media (iSCSI) network require this process. Add the PCs as clients to the K2 SAN.

Work through the topics in this section sequentially to add a GV STRATUS client PC as a SAN client to your online or production K2 SAN. This gives the PC access to high-resolution assets on the K2 SAN.

K2 SAN prerequisites for adding devices

The following K2 SAN preparations are required to support adding a device to the SAN:

- All K2 Media Servers and/or K2 RAID storage devices must be installed and cabled.
- The control network must be operational with K2 devices communicating. At the command prompt, use the ping command to verify.
- The media network (non-redundant) or networks (redundant) must be operational. You can check this with the K2Config application.
- K2 RAID devices must have disks bound and be configured as required for operation on the K2 SAN.
- K2 Media Servers must be configured such that an operational media file system is present.
- K2 Ethernet switches must be configured and have V-LANs set up.
- The K2 Media Server with role of file system server must be licensed as appropriate for the design of your K2 SAN.

Verify license on K2 Media Server

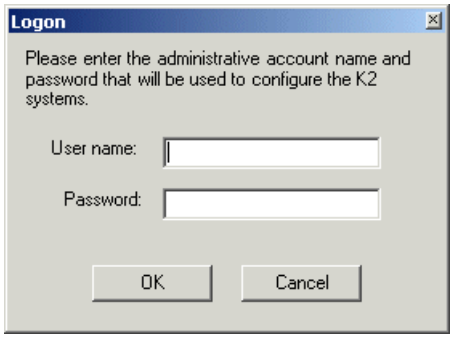
The K2 SAN license is installed on K2 Media Servers with role of iSCSI bridge. If a redundant system and/or a large system with multiple servers, the license must be installed on each K2 Media Server with role of iSCSI bridge. Use the following steps to verify the license on each K2 Media Server with role of iSCSI bridge.

1. On the K2 Media Server, open SabreTooth License Manager.
2. Verify that a license identified as K2-ISCSI-SVR is installed.

If the license for your K2 SAN license is not installed, you must install it before proceeding.

Adding a GV STRATUS client PC to a K2 SAN

1. On the PC that hosts K2Config, open the K2Config application.
   A log on dialog box opens.



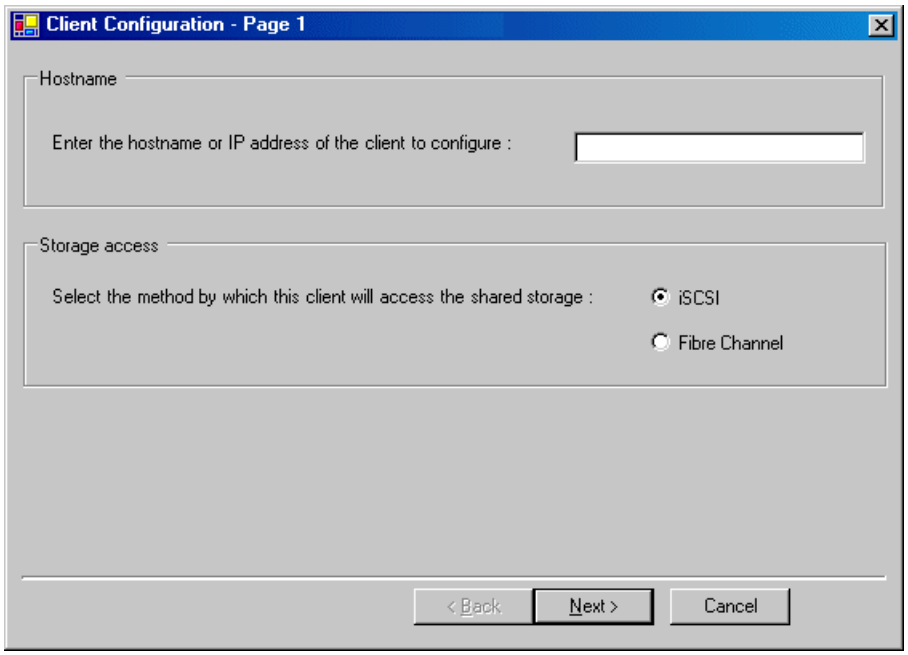
2. Log on to the K2Config application with the administrator account.
   The K2Config application opens.
3. In the K2Config application tree view, verify that the K2 SAN has the correct number of clients, according to your system design.
   If the correct number of clients is not currently added to the K2 SAN, you can add or remove clients now (before clients are configured), as follows:
   - To add a client, select the top node of the storage system and click the **Add Device** button. The Add Device dialog box opens. Select **Generic** and then click **OK**.
   - To remove a client, select an unconfigured client and click the **Remove** button.
4. Select a client and click the **Configure** button.

The configuration wizard opens to page 1.

NOTE: If your system has a large number of iSCSI clients, you are prompted to restart the server that has the role of SNFS file system server when you configure clients and cross the following thresholds: 64 clients; 80 clients; 96 clients.

Next, configure the GV STRATUS client PC on the K2 SAN.

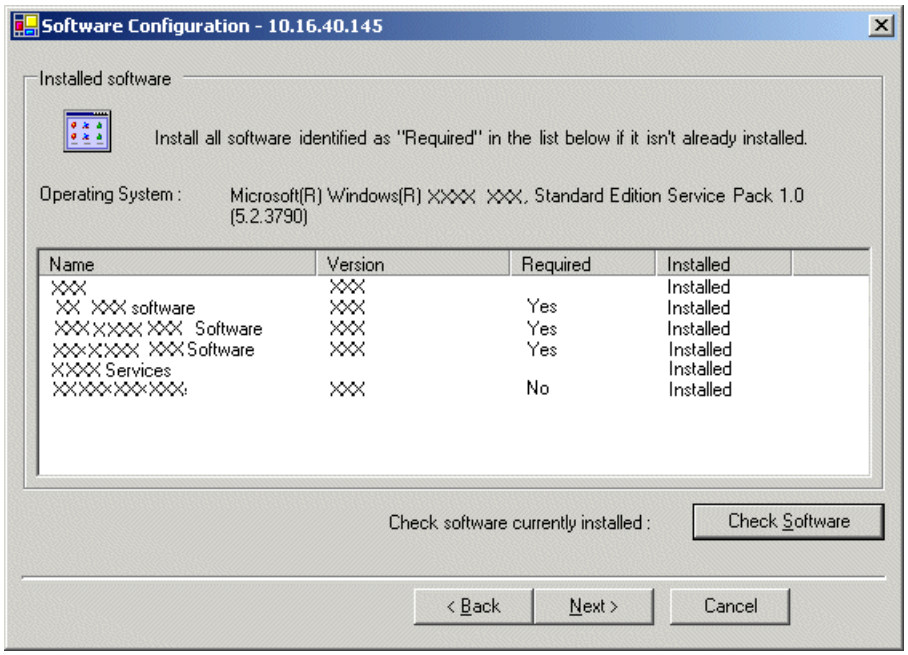
Configure page 1 - GV STRATUS client PC



1. Enter the IP address or network name for a SAN client, as currently configured on the client system.
2. For the Storage Access settings, leave iSCSI selected.
3. Click **Next**.

The Software Configuration page opens.

Configure Software Configuration page - GV STRATUS client PC

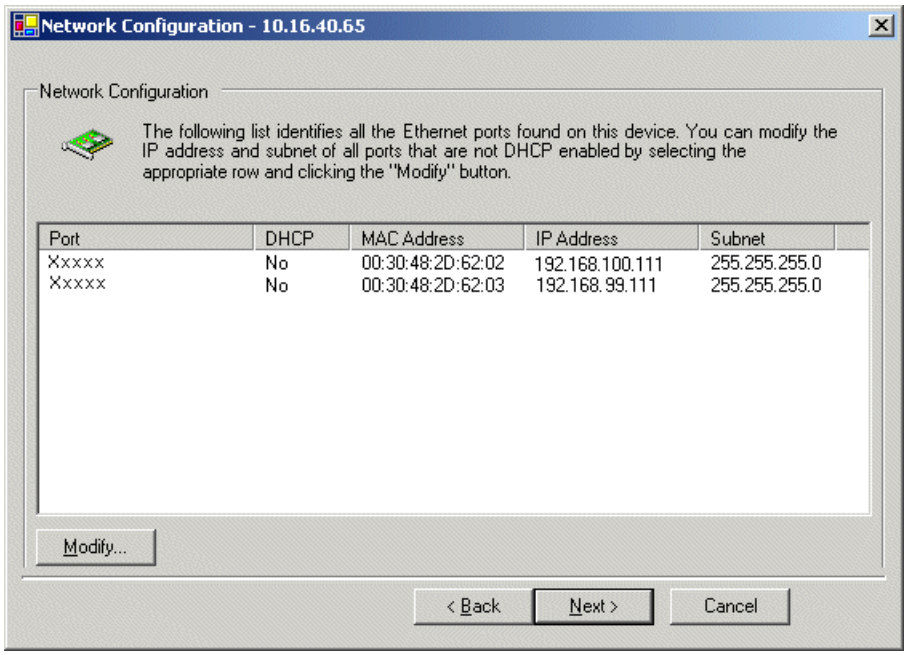


This page checks the client for required software.

1. If software with **Yes** in the Required column reports as **Not Installed**, install the software.
2. Click **Check Software**.
3. When all required software reports as **Installed**, click **Next**.

The Network Configuration page opens.

Configure Network Configuration page - GV STRATUS client PC



This page configures both control and media (iSCSI) network connections.

1. Verify that the top port is configured correctly.

   The top port is the port over which the K2Config application is communicating. If correctly configured, it is already assigned the control network IP address, as displayed on this page.

2. Select the other connection, which should be the media (iSCSI) connection, and then click **Modify**.

   A network configuration dialog box opens.

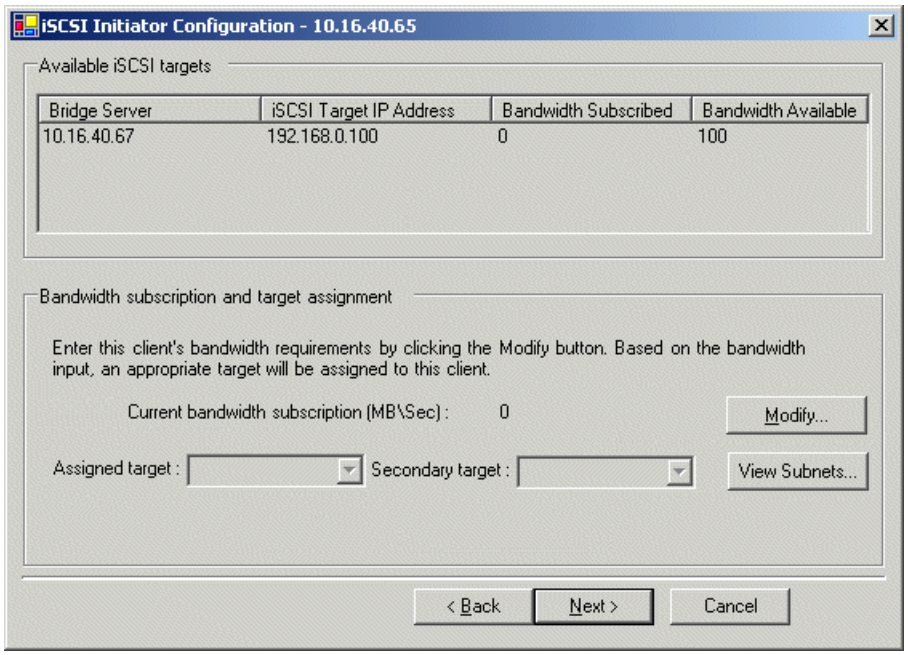
3. Verify or configure the media connection as follows:

   - Verify or enter the media network IP address. Also enter the subnet mask.

4. Click **Next**.

The File System Client Configuration page opens.

Configure iSCSI Initiator Configuration page - GV STRATUS SAN client



This page lists the iSCSI adapter on your K2 Media Server as an iSCSI target. The K2Config application subscribes the SAN client to the iSCSI target and allocates bandwidth, based on the bandwidth values that you enter. The K2Config application keeps track of each SAN client's bandwidth, and when the total amount allowed by the K2 SAN license is consumed, the K2Config application displays an informative message and then disables your ability to add more SAN clients. For large systems the K2Config application can load balance SAN clients across multiple iSCSI targets.

If a custom K2 SAN, qualified system designers can view subnets to help assign iSCSI targets.

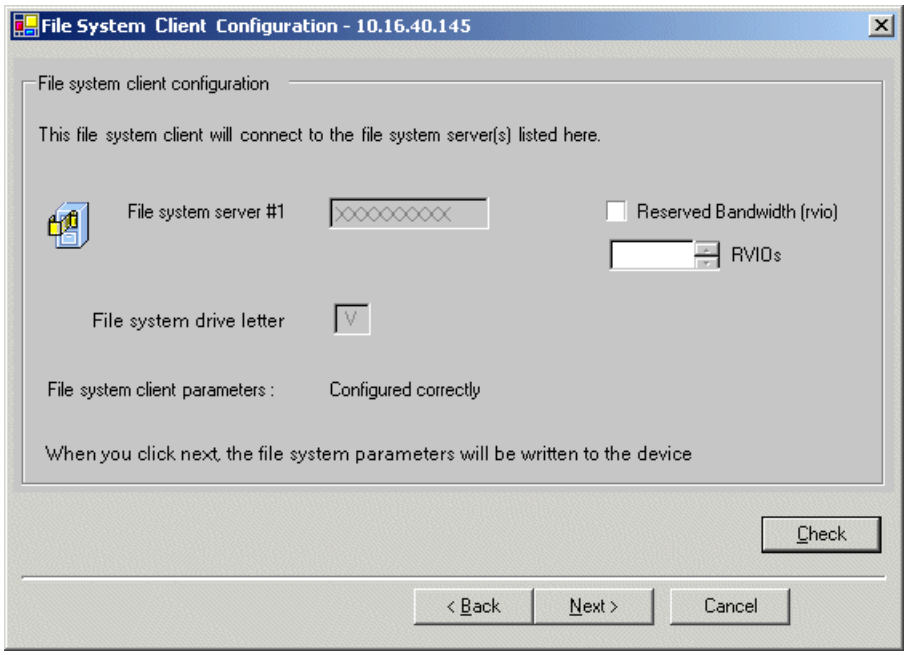
1. Click **Modify**.

   The Bandwidth Input dialog box opens.

2. In the Bandwidth Input dialog box, enter the bandwidth value specified in your system design and then click **OK**.
3. Click **Next**.

The File System Client Configuration page opens.

Configure File System Client Configuration page - GV STRATUS client PC



This system does not function as a file system server. It does function as a file system client, which is validated from this page.

1. Configure **Reserved Bandwidth** settings as specified by your system design.
2. Click **Check**.
3. When the wizard reports that the configuration is correct, click **Next**.

   If you get a "The V: will not be available until this device is rebooted…" message, you can safely continue now and reboot later when instructed to do so.

Set GV STRATUS client PC to high-resolution

Only systems with GV STRATUS client PCs that use a high-resolution media workflow require this process. Configure the PC in GV STRATUS Control Panel.

A GV STRATUS client PC that uses a high-resolution media workflow rather than proxy media workflow must have access to the high-resolution media. The following are examples of this high-resolution access:

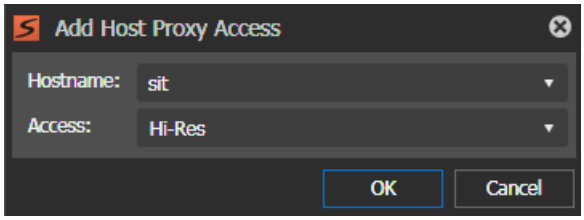
- High-resolution client PC on K2 media (iSCSI) network — This setup is for high-resolution workflows, such as those that integrate with a high-resolution editor such as EDIUS Workgroup. The GV STRATUS application accesses the high-resolution assets via the media network to support the workflow. Two connections are required: one to the control network and one to the media network. The PC must be set to high-resolution in GV STRATUS Control Panel Proxy Access settings to enable the GV STRATUS application to access high-resolution media. A GV STRATUS high-resolution license is also required for the client PC. The high-resolution license is not managed by the GV STRATUS server with role of Common Server. The EDIUS license is installed on the PC and is managed by EDIUS license management. Other authorization and licensing is identical to the client PC on the corporate LAN.

- Client PC with SMB mount connection to K2 storage — This setup is for high-resolution workflows, such as those that integrate with a high-resolution editor such as EDIUS Workgroup. The GV STRATUS application accesses the high-resolution assets via a SMB mount, typically to the `V:` drive, to support the workflow. Two connections are required: one to the control network and one to the Grass Valley storage. The PC must be set to high-resolution in GV STRATUS Control Panel Proxy Access settings to enable the GV STRATUS application to access high-resolution media. A GV STRATUS high-resolution license is also required for the client PC. The high-resolution license is not managed by the GV STRATUS server with role of Common Server. The EDIUS license is installed on the PC and is managed by EDIUS license management. Other authorization and licensing is identical to the client PC on the corporate LAN.

Use these steps to set the PC to high-resolution.

1. In GV STRATUS Control Panel, click **Core | Proxy Config | Proxy Access | Add**.

   The Add Host Proxy Access dialog box opens.



2. For Hostname, select the name of the GV STRATUS client PC that you are setting to high-resolution.
3. For Access, select **Hi-Res**.
4. Click **OK** to save settings and close.

Disabling CRL setting on GV STRATUS client PC with no internet access

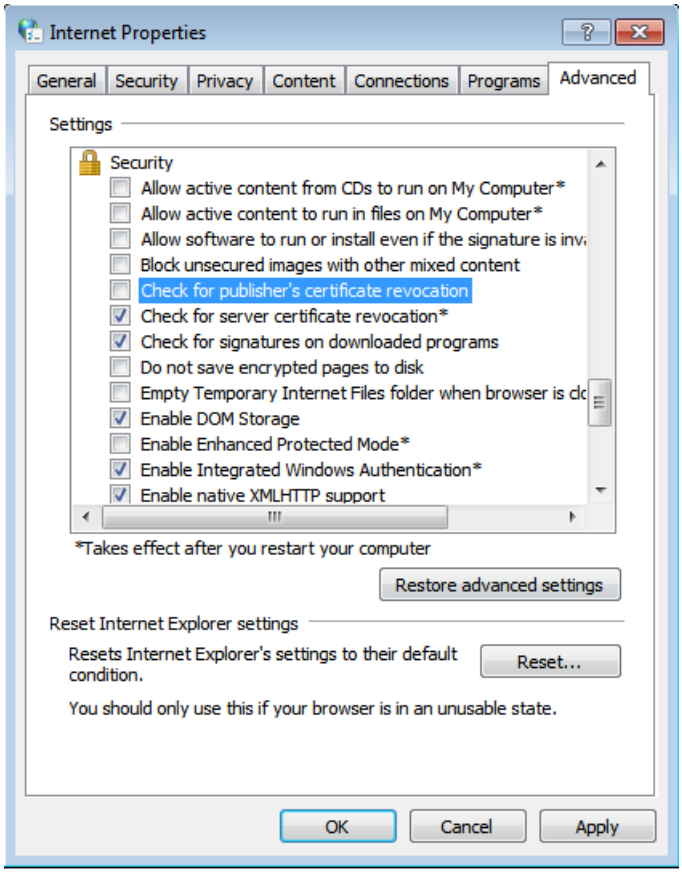
Only GV STRATUS client PCs with no internet access require this process. Configure the setting in the Windows Control Panel of GV STRATUS client PC.

The check of the Certificate Revocation List (CRL) requires an internet connection, so it must be disabled in GV STRATUS client PCs which are in a network with no internet access. This is to prevent multiple timeouts due to the CRL check, which could delay the launch of GV STRATUS application.

1. In the Windows operating system Control Panel, click **Internet Options**.

2. Select **Advanced** tab.

   The **Advanced** tab displays.



3. Scroll down to the **Security** section, and disable the **Check for publisher's certificate revocation** setting.
4. Click **Apply** and **OK**.

Installing EDIUS application software without SiteConfig

- If installing to a PC on which you have previously installed EDIUS Pro (not EDIUS for STRATUS), EDIUS and supporting software must first be uninstalled before attempting to install EDIUS for STRATUS.
- The PC must meet GV STRATUS Client PC system requirements.
- Windows High Priority updates are required and must be installed. For more details, refer to *Install Important Windows updates for EDIUS* on page 148.

The recommended process for software installation and upgrades is to use SiteConfig from a network connected control point PC and remotely deploy software. However, if SiteConfig installation is not possible, you may install manually on the local PC. Use these steps to manually install the EDIUS application.

1. Procure the following:

   - EDIUS STRATUS Standalone Installation Kit (SIK). This is a directory of files and sub-directories containing components to support the installation.

2. Copy the *EDIUS_STRATUS_SIK* directory to any location on the GV STRATUS/EDIUS client PC.
3. Open the *EDIUS_STRATUS_SIK\deliverables\Modules* directory and identify the EDIUS software cab file, if any, that is in the directory, then proceed as follows:
   - If the EDIUS software cab file is the correct version to install, skip ahead to the next step.
   - If the EDIUS software cab file is not the correct version to install, delete the file, then copy the correct cab file to the directory.
4. Open *EDIUS_STRATUS_SIK\deliverables\Setup*.

   A **cmd** window opens and an **EDIUS Installer** dialog box opens and reports installation progress.
5. When prompted, restart the GV STRATUS/EDIUS client PC.

Reference to GV STRATUS Control Panel settings

Reference to settings: Required and optional

All systems require GV STRATUS Control Panel settings, as appropriate for the site's unique workflow and GV STRATUS licenses.

If you received your system pre-configured from Grass Valley, your site's settings are already configured, so the system should not need any additional settings. Otherwise, refer to topics about Control Panel settings and configure as needed.

Control Panel settings are categorized as follows:

- Required settings — These are settings that must be configured for all GV STRATUS systems, regardless of the site's unique workflow and GV STRATUS license requirements.
- Optional settings — These are settings that might or might not be necessary, depending on the site's unique workflow and GV STRATUS license requirements.

Topics about configuring required settings provide the proper sequence and specific instructions for the required settings.

Topics that reference Control Panel settings describe all settings on all Control Panel configuration pages, including both required and optional settings. Choose the optional settings that are relevant to your site's unique workflow and GV STRATUS license requirements.

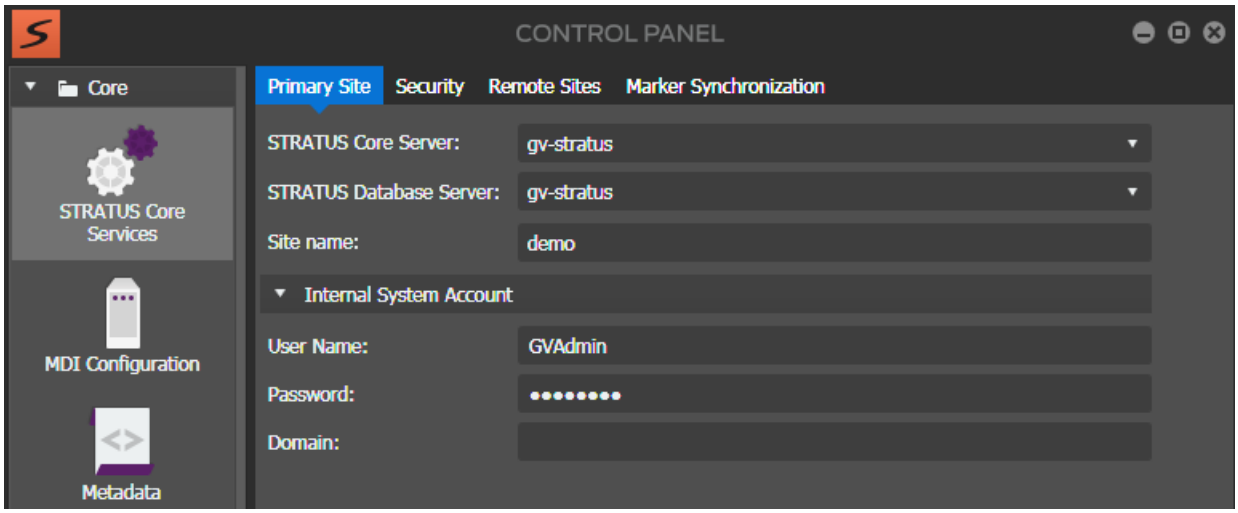
Related Topics

Configuring GV STRATUS Control Panel: Required settings on page 842

STRATUS Core Services settings

These settings are required on all GV STRATUS systems.

To locate these settings, click **Core | STRATUS Core Services | Primary Site**



Setting or button	Description
GV STRATUS Core Server	The GV STRATUS server with SiteConfig role of GV STRATUS Core Services. In a typical system, select the server from the drop-down list. The server or servers available on this drop-down list are provided by SiteConfig. For some system configurations, you can also enter the GV STRATUS server manually.
GV STRATUS Database Server	The GV STRATUS server with SiteConfig role of GV STRATUS Database. In a typical system, select the server from the drop-down list. The server or servers available on this drop-down list are provided by SiteConfig. The GV STRATUS Database Server is currently supported on the GV STRATUS Express, Core, and separate standalone servers.
Site name	Customizable name that can be set for the local GV STRATUS site.
Internal System Account User Name, Password, Domain	The internal system account is the account that the GV STRATUS system uses to access assets and some internal system functions. By default this is the GVAdmin account. If your site policies require a different account, such as a fully qualified domain account, that account must be configured here and throughout the GV STRATUS system. ***NOTE: Do not enter a domain or otherwise modify account settings except under the supervision of qualified Grass Valley Support personnel. Extensive system configuration is required to achieve a working GV STRATUS system.***
Save	Saves current settings.
Cancel	Returns settings to their last saved state.

Related Topics

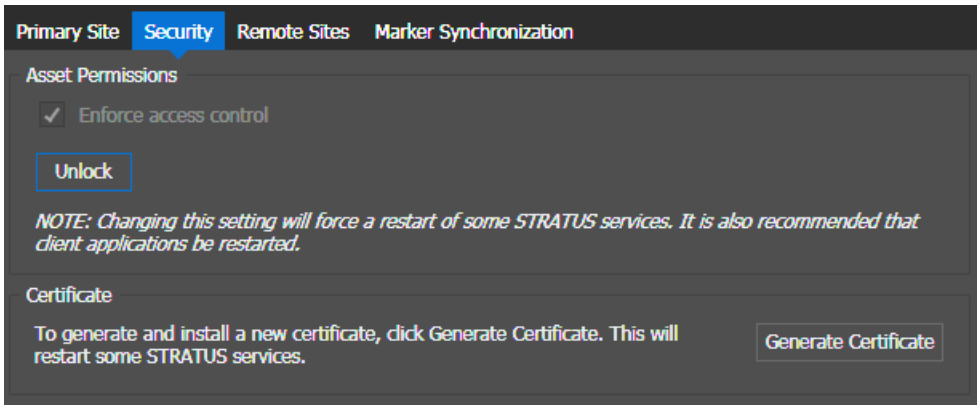
Configuring STRATUS Core Services settings: Required on page 843
Standalone Database Server set up process on page 829
About GV STRATUS markers, Dyno markers, and the K2 database on page 419
About Control Panel, SiteConfig, and K2Config settings on page 433
Rules engine settings on page 334

Enabling and disabling rules on page 636
Fully qualified domain configuration on page 913

GV STRATUS system security settings

These settings are required on all GV STRATUS systems.

In GV STRATUS Control Panel, to locate these settings, click **Core | STRATUS Core Services | Security**



Setting or button	Description
Enforce access control	When selected, the GV STRATUS system configures, retains, and enforces security settings on assets and bins. When not selected, the GV STRATUS system configures and retains, but does not enforce, security settings on assets and bins.
Lock/Unlock	Locks and unlocks the access control setting.
Generate Certificate	This creates a self-signed security certificate and installs it on the GV STRATUS Core server. Manually generating a certificate in this way is required only if the GV STRATUS Core server name changes, or if instructed to do so by Grass Valley Support. Otherwise, generating a certificate is handled automatically by GV STRATUS software installation.
Save	Saves current settings.
Cancel	Returns settings to their last saved state.

If settings are saved, GV STRATUS services are restarted automatically. All instances of the GV STRATUS currently open should be restarted manually.

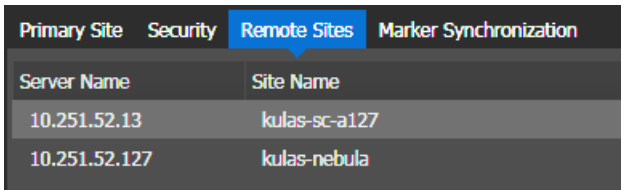
Remote Sites settings

These settings are optional on GV STRATUS systems.

These settings affect the following:

- Copying assets from a local site to a remote site
- Copying assets from a remote site to a local site

To locate these settings, click **Core | STRATUS Core Services | Remote Sites**



Setting or button	Description
Server name	The name or IP address of the remote GV STRATUS core server.
Site name	Customizable name that can be set for the remote GV STRATUS site.
Add	Opens the **Add New Remote Site** dialog box for you to add a remote GV STRATUS site. You can use the **Add** button repeatedly to add multiple remote sites.
Modify	Opens the **Edit Remote Site** dialog box to modify the setting of the selected remote site.
Remove	Removes the selected remote site.
Save	Saves current settings.
Cancel	Returns settings to their last saved state.

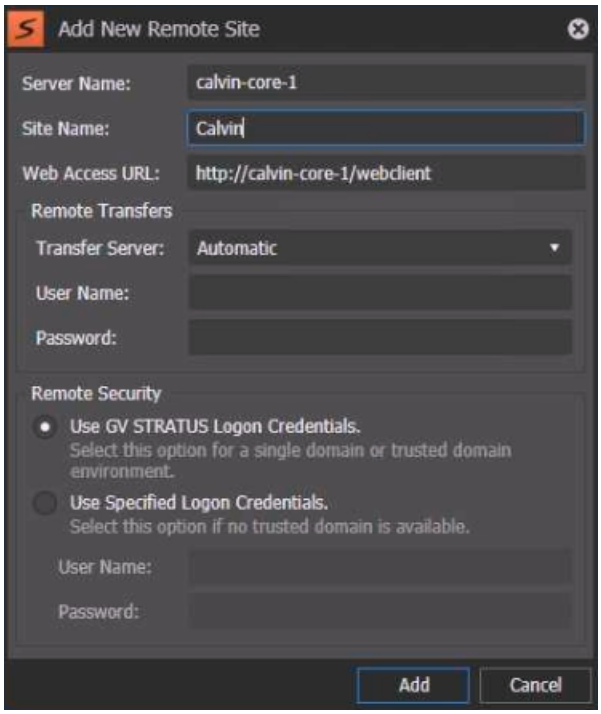
Related Topics

Remote and multiple site configuration on page 473

Remote Site Add/Modify settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Core | STRATUS Core Services | Remote Sites | Add** or **Modify**



Setting or button	Description
Server Name	The name or IP address of the remote GV STRATUS core server.
Site Name	Customizable name that can be set for the remote GV STRATUS site.
Web Access URL	The URL for users to access the remote GV STRATUS site via a web browser from **Web Access** node in the Navigator.
Remote Transfers: Transfer Server	Set to **Automatic**. ***NOTE: Local and remote FTP networks must be able to communicate with one another.***
Remote Transfers: User Name	Credentials for the administrator account at the remote site, for authorizing transfers.
Remote Transfers: Password	Credentials for the administrator account at the remote site, for authorizing transfers.
Remote Security: Use GV STRATUS Logon Credentials	If GV STRATUS security is enforced, when a GV STRATUS application accesses a remote site, the credentials of the user account logged on to the GV STRATUS application are used to determine access to assets. This requires a single domain for both local and remote sites or trusted domains between sites, so that user accounts can be authenticated.

Setting or button	Description
Remote Security: Use Specified Logon Credentials	If GV STRATUS security is enforced, when a GV STRATUS application accesses a remote site, the credentials entered here are used to determine access to assets, regardless of the user account logged on to the GV STRATUS application. This requires that only the credentials entered here be authenticated on the remote site, so a single domain for both local and remote sites or trusted domains between sites is not necessary.

NOTE: When using multiple* GV STRATUS *sites, make sure all sites either have security enabled or disabled. Do not attempt to run mixed environments.

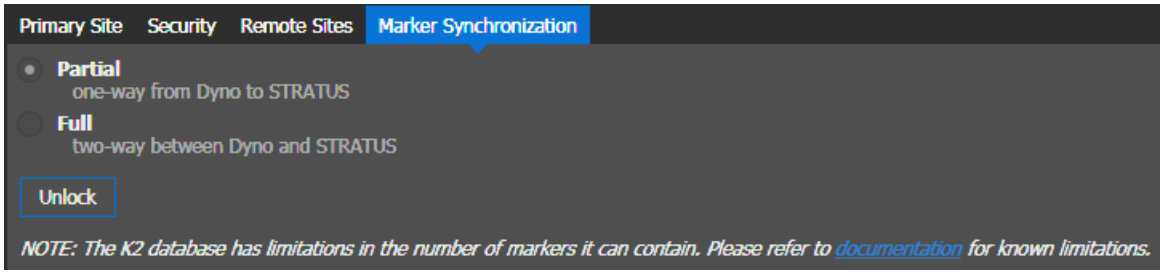
Related Topics

GV STRATUS security considerations on page 481

Marker Synchronization settings

These settings are required on all GV STRATUS systems.

To locate these settings, click **Core | STRATUS Core Services | Marker Synchronization**



Setting or button	Description
Partial	One-way marker creation from Dyno to GV STRATUS, then two-way marker modification and deletion. This is the recommended setting for all systems.
Full	Two-way creation, modification, and deletion between Dyno and GV STRATUS. Use this setting only if required by your K2 Dyno Controller workflow. Consider K2 database capacity limitations when using this setting.
Lock/Unlock	Locks and unlocks Marker Synchronization settings
Save	Saves current settings.
Cancel	Returns settings to their last saved state.

If the Marker Synchronization setting is changed, the GV STRATUS Core server and the K2 system must be restarted.

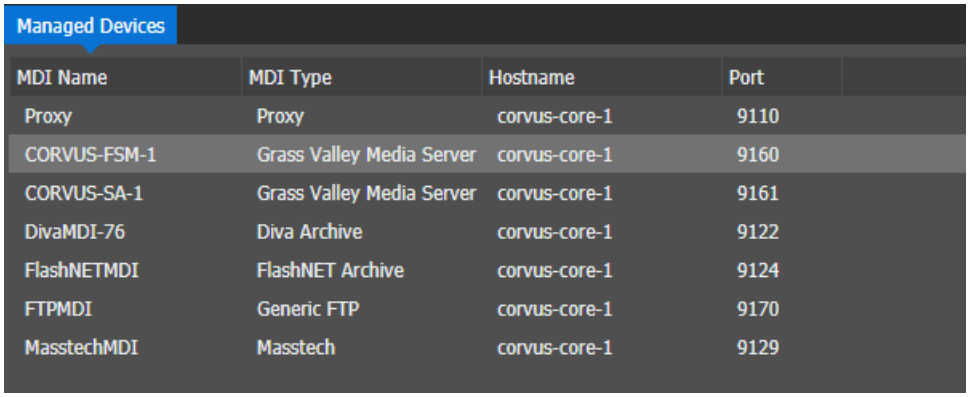
Related Topics

About GV STRATUS markers, Dyno markers, and the K2 database on page 419

MDI Configuration settings

These settings are required on all GV STRATUS systems.

To locate these settings, click **Core | MDI Configuration | Managed Devices**

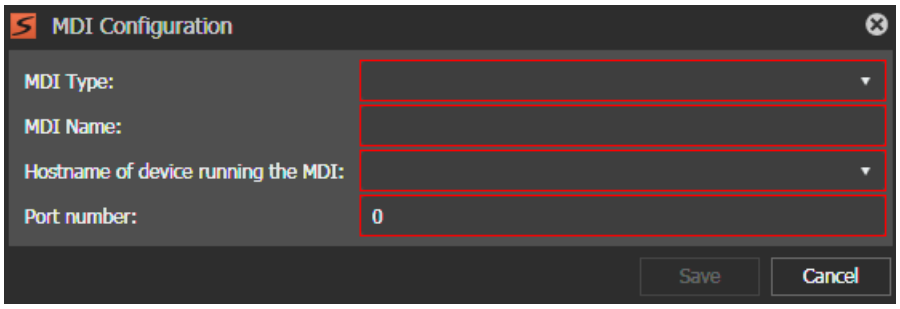


Setting or button	Description
MDI Type	The Managed Device Interface (MDI) type to which these settings apply.
MDI Name	A name for this instance of the MDI type. Do not use spaces in the MDI name.
Hostname of device running the MDI	The name of the GV STRATUS server that hosts this MDI.
Port	The port used by the currently configured MDI.
Add	Opens the MDI Configuration dialog box.
Modify	Opens the MDI Configuration dialog box for the selected MDI.

Setting or button	Description
Remove	Removes the selected MDI. Only for Grass Valley Media Server MDI, the **Delete Type** dialog box displays. Select a delete type from these options below and click the **Delete** button. • **MDI Only** - Deletes the Grass Valley Media Server MDI only, but leaves all logical assets and data in the GV STRATUS database. The Grass Valley Media Server MDI still appears under Locations node in the Navigator, but no changes can be made to the metadata. • **MDI with Special Group** - Deletes the Grass Valley Media Server MDI, moves all data of assets into a specially created group but no changes can be made to the metadata, and removes all high-resolution associations pointing to the deleted Grass Valley Media Server MDI. The name of specially created group for the deleted MDI has an appended suffix in this format: **MDI name_DELETED_Deletion date** ***NOTE: If the Grass Valley Media Server MDI is added back and appears under Locations, the specially created group remains under Groups until you manually remove it from the Groups node.*** • **MDI, Logical Assets, and Proxy Files** - Deletes the Grass Valley Media Server MDI, all assets and data in GV STRATUS database that map to the Grass Valley Media Server MDI, and all proxy files. However, it leaves media intact on disk. ***NOTE: When adding back a previously deleted Grass Valley Media Server MDI, make sure you use the same MDI name and port number to re-sync the MDI with all data in the GV STRATUS database.***

MDI Configuration Add/Modify settings

To locate these settings, click **Core | MDI Configuration | Managed Devices | Add**



Setting or button	Description
MDI Type	Provides a list of MDI types. Selecting a MDI type loads the appropriate settings for that MDI type.
MDI Name	Refer to the settings for the selected MDI Type

Setting or button	Description
Hostname of device running the MDI	Refer to the settings for the selected MDI Type
Port number	Refer to the settings for the selected MDI Type

Related Topics

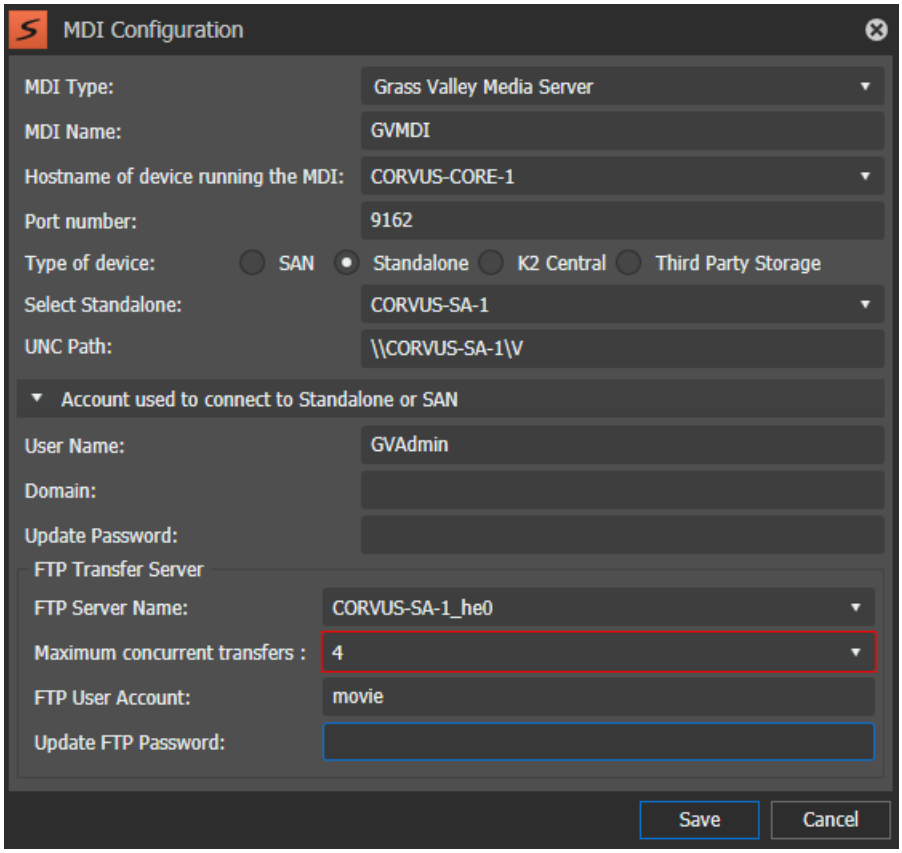
MDI and Encoder logical names convention on page 442

Grass Valley Media Server MDI standalone settings

These Grass Valley Media Server MDI settings for standalone and/or Grass Valley Media Server MDI settings for SAN are required on all GV STRATUS systems.

This type of MDI manages a K2 Summit system. This topic describes settings when the type of system is specified as Standalone.

To locate these settings, click **Core | MDI Configuration | Add | Grass Valley Media Server**



When you have multiple Grass Valley Media Server MDIs, they must each have their own process port number. For this purpose, numbers 9160 - 9169 increment in the **Port** field.

Setting or button	Description
MDI Type	The Managed Device Interface (MDI) type to which these settings apply.

Setting or button	Description
MDI Name	A name for this instance of the MDI type. Do not use spaces in the MDI name. The MDI name could be renamed later, if desired. ***NOTE: After renaming the MDI, you must restart the Render Engine server and its services. Then, reconfigure other settings on the Control Panel (such as Send Destinations, Rules, K2 Central storage, etc.) to use the new Grass Valley Media Server MDI name.***
Hostname of device running the MDI	The name of the GV STRATUS server that hosts this MDI.
Port number	The process port for this instance of the MDI type. Each instance must have its own process port. Port numbers must be in range 9160-9169.
Type of K2 device	Specifies either SAN-attached K2 Summit system , Standalone K2 Summit system, K2 Central system, or Third Party Storage system. When Standalone is selected, settings are as follows.
Select Standalone	The standalone K2 Summit system that this MDI accesses.
UNC Path	The UNC path to the standalone K2 Summit system.
User Name	The user name that this MDI uses to access the K2 Summit system. This is the internal system account, which by default is GVAdmin.
Domain	If on a domain, the domain that manages the account that this MDI uses to access the K2 Summit system. ***NOTE: Do not enter a domain or otherwise modify account settings except under the supervision of qualified Grass Valley Support personnel. Extensive system configuration is required to achieve a working GV STRATUS system.***
Update Password	The password that this MDI uses to access the K2 Summit system.
FTP Server Name	The FTP server name for the remote K2 Summit system. For the typical system where there is a separate FTP network, this is the name of the K2 SAN's FTP server with the `_he0` suffix added. The `_he0` suffix specifies the FTP network.
Maximum concurrent transfers	The maximum number of concurrent transfers allowed. The maximum is set in K2Config. You may select the maximum or a lesser number as designed for your system. The number of concurrent transfers as well as the device status can be checked once the system is configured in Resource Monitor of the GV STRATUS Control Panel.
FTP User Account	The FTP user name for the K2 Summit system this MDI accesses. Typically this is `movie`.
Update FTP Password	The FTP password for the K2 Summit system this MDI accesses. When this field is blank the system automatically uses the default password.

If you changed a standalone MDI setting, you must restart the GV STRATUS Core server system and the K2 Summit system. If SAN MDI settings, you must restart the entire K2 SAN system, including K2 Media Servers, attached K2 Summit systems, and other SAN clients. If you are changing multiple Grass Valley Media Server MDI settings, you can make all those settings first before

restarting these systems. Restarting the systems once is sufficient for multiple Grass Valley Media Server MDI settings changes.

When adding back a previously deleted MDI, you can re-sync the MDI with all data retained in the GV STRATUS database by doing the following:

- Reuse the same MDI name that was previously deleted
- Reuse the same port number that was used with the deleted MDI

Related Topics

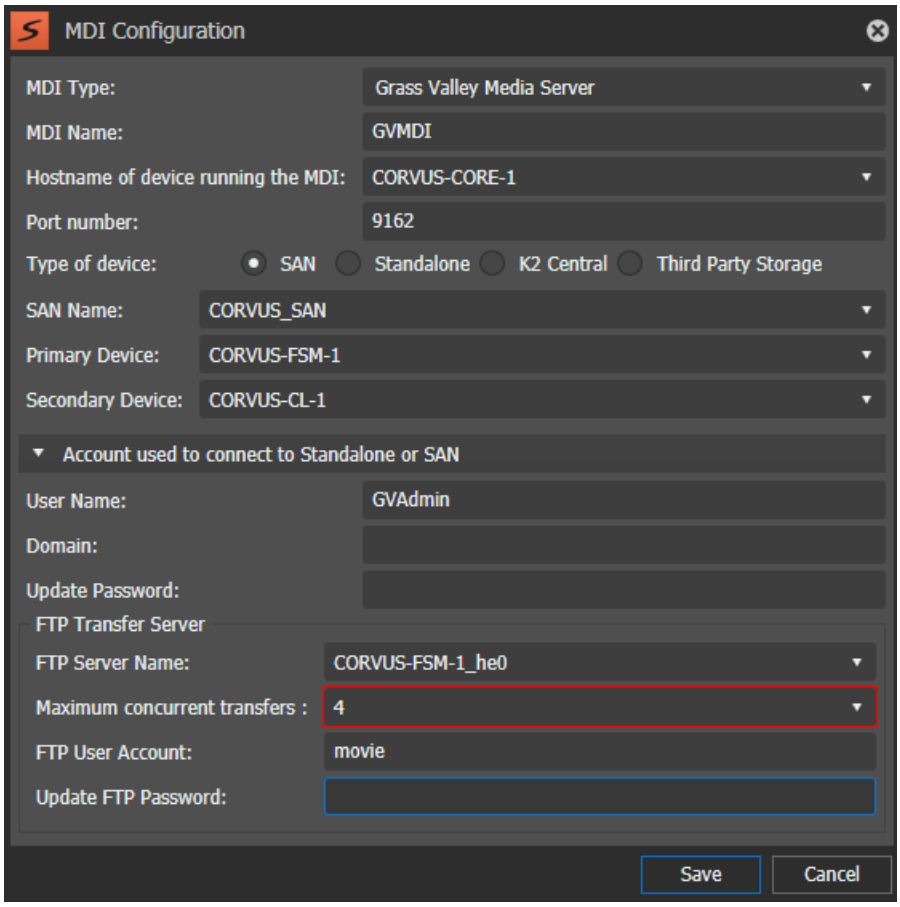
MDI and Encoder logical names convention on page 442
Proxy Encoder MDI settings
Configuring Grass Valley Media Server MDI settings: Required for standalone on page 845
Fully qualified domain configuration on page 913

Grass Valley Media Server MDI SAN settings

These Grass Valley Media Server MDI settings for SAN and/or Grass Valley Media Server MDI settings for standalone are required on all GV STRATUS systems.

This type of MDI manages K2 Summit Production Client systems. This topic describes settings for a K2 Summit SAN system.

To locate these settings, click **Core | MDI Configuration | Add | Grass Valley Media Server**



Designate SAN-attached K2 Summit systems to be the primary and secondary device for the entire K2 SAN storage system. Configure a Grass Valley Media Server MDI for those K2 Summit systems on the K2 SAN.

If you have multiple standalone K2 Summit systems, multiple K2 SAN systems, a combination of standalone and K2 SAN systems, a K2 Central system, or a SMB storage system, each system must have its own Grass Valley Media Server MDI.

When you have multiple Grass Valley Media Server MDIs, they must each have their own process port number. For this purpose, numbers 9160 - 9169 increment in the **Port** field.

Setting or button	Description
MDI Type	The Managed Device Interface (MDI) type to which these settings apply.
MDI Name	A name for this instance of the MDI type. Do not use spaces in the MDI name. The MDI name could be renamed later, if desired. ***NOTE: After renaming the MDI, you must restart the Render Engine server and its services. Then, reconfigure other settings on the* GV STRATUS Control Panel *(such as Send Destinations, Rules, K2 Central storage, etc.) to use the new Grass Valley Media Server MDI name.***
Hostname of device running the MDI	The name of the GV STRATUS server that hosts this MDI.
Port number	The process port for this instance of the MDI type. Each instance must have its own process port. Port numbers must be in range 9160-9169.
Type of K2 device	Specifies either SAN-attached K2 Summit system , Standalone K2 Summit system, K2 Central system, or Third Party Storage system.
SAN Name	The name of the K2 SAN, as named in K2Config. You can also enter the name of K2 Central system or third party storage device, if you have them in your operation.
Primary Device	The Summit client or server designated to be the primary managed device for the entire K2 SAN, K2 Central or Third Party Storage system. For optimum system performance it is recommended that if there are K2 Summit Clients, use them for the primary and secondary device. If there is only one client, use the client as the primary device and the FSM/Storage Manager as the secondary device. If it is a shared storage with no attached K2 Summit clients, configure the primary FSM or Storage Manager as the primary device and the secondary FSM (if exists) or FTP Server as the secondary device.
Secondary Device	The Summit client or server designated to the secondary managed device for the entire K2 SAN, K2 Central or Third Party Storage system.
UNC Path	The UNC path for a connection to the K2 Central and SMB Storage. The field for UNC path is only available for **K2 Central** and **Third Party Storage** settings.

Setting or button	Description
User Name	The user name that this MDI uses to access the K2 Summit system. This is the internal system account, which by default is GVAdmin.
Domain	If on a domain, it must be a fully qualified domain that this MDI uses to access the designated managed device. This field should only be set for fully qualified domain of third party storage system in your operation.
Update Password	The password that this MDI uses to access the K2 Summit system. ***NOTE: Do not enter a domain or otherwise modify account settings except under the supervision of qualified Grass Valley Support personnel. Extensive system configuration is required to achieve a working GV STRATUS system.***
FTP Server Name	The FTP server name for the remote K2 Summit system. The drop-down list consists of all FTP servers belonging to the Summit SAN. For the typical system where there is a separate FTP network, this is the name of the K2 SAN's FTP server with the `_he0` suffix added. The `_he0` suffix specifies the FTP network.
Maximum concurrent transfers	The maximum number of concurrent transfers allowed. The maximum is set in K2Config. You may select the maximum or a lesser number as designed for your system. The number of concurrent transfers as well as the device status can be checked once the system is configured in Resource Monitor of the GV STRATUS Control Panel.
FTP User Account	The FTP user name for the K2 Summit system this MDI accesses. Typically this is `movie`.
Update FTP Password	The FTP password for the K2 Summit system this MDI accesses. When this field is blank the system automatically uses the default password.

If you changed a standalone MDI setting, you must restart the GV STRATUS Core server system and the K2 Summit system. If SAN MDI settings, you must restart the entire K2 SAN system, including K2 Media Servers, attached K2 Summit systems, and other SAN clients. If you are changing multiple Grass Valley Media Server MDI settings, you can make all those settings first before restarting these systems. Restarting the systems once is sufficient for multiple Grass Valley Media Server MDI settings changes.

When adding back a previously deleted MDI, you can re-sync the MDI with all data retained in the GV STRATUS database by doing the following:

- Reuse the same MDI name that was previously deleted
- Reuse the same port number that was used with the deleted MDI

Related Topics

MDI and Encoder logical names convention on page 442
Proxy Encoder MDI settings
GV STRATUS Control Panel configuration for K2 Central on page 937
GV STRATUS Control Panel configuration for SMB storage on page 930
Configuring Grass Valley Media Server MDI settings: Required for SAN on page 847
Fully qualified domain configuration on page 913

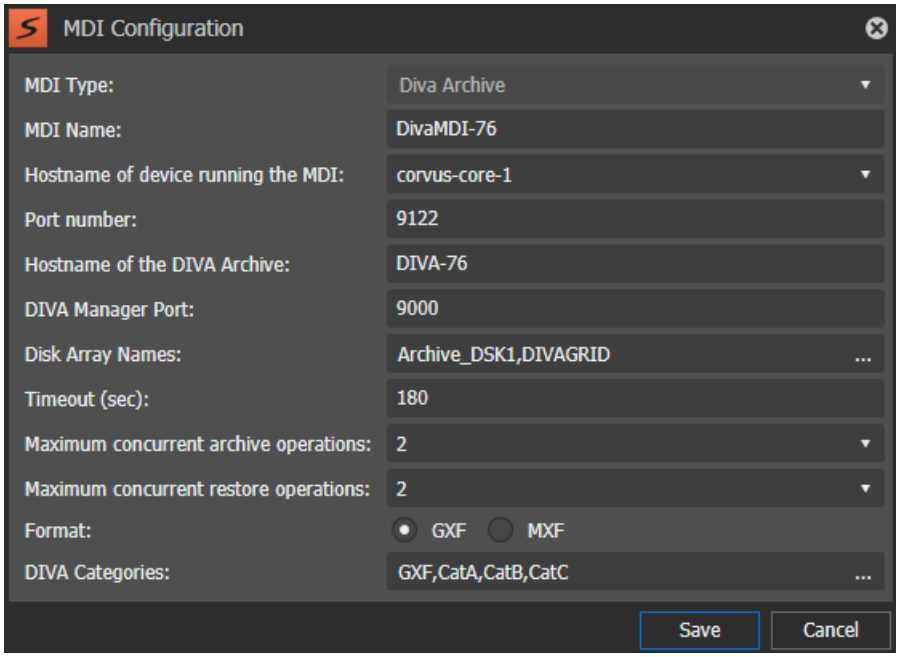
DIVA Archive MDI settings

These settings are optional on GV STRATUS systems.

Before archiving assets, your K2 system must be assigned with the role of FTP Server.

Since DIVA provides direction oriented FTP transfer and port configuration settings, it is recommended to configure the maximum concurrent number of supported archive and restore operations in this Diva Archive MDI setting. They should be identical to the configuration in the DIVA Manager.

To locate these settings, click **Core | MDI Configuration | Managed Devices | Add | Diva Archive**



Setting or button	Description
MDI Type	The Managed Device Interface (MDI) type to which these settings apply.
MDI Name	A name for this instance of the MDI type. Do not use spaces in the MDI name.
Hostname of device running the MDI	The name of the GV STRATUS server that hosts this MDI.
Port number	The port number of the port that this MDI listens to. The default port number is 9122. Other port numbers are also allowed.
Hostname of the DIVA Archive	The hostname or IP address of the DIVA Archive server. ***NOTE: The device status can be monitored in the Resource Monitor of* GV STRATUS Control Panel.**

Setting or button	Description
DIVA Manager Port	The default value for the DIVA Manager Port number is listed below: • DIVA version 7.1 and below: **9000** • DIVA version 7.2: **9072** Other DIVA Manager Port numbers are also allowed. Refer to your DIVA archive server for configuration details.
Disk Array Names	The disk arrays in DIVA that are exposed in GV STRATUS clients.
Timeout (sec)	The default timeout is 180 seconds.
Maximum concurrent archive operations	The maximum number of transfers that the MDI will process at the same time for archive operations. The number of maximum concurrent transfers can be monitored in the Resource Monitor of GV STRATUS Control Panel. The maximum number is set to 5 by default.
Maximum concurrent restore operations	The maximum number of transfers that the MDI will process at the same time for restore operations. The number of maximum concurrent transfers can be monitored in the Resource Monitor of GV STRATUS Control Panel. The maximum number is set to 5 by default.
Format	Specifies the format of the archived asset, either GXF or MXF. ***NOTE: In order for the format change to take effect, you need to click Save and restart your GV STRATUS clients.***
DIVA Categories	Specifies multiple DIVA categories for your archived material. All configured categories in DIVA Archive MDI settings will be accessible via the GV STRATUS Navigator. If this setting is empty, GXF category will be used and shown by default in DIVA Archive MDI.

NOTE: These special characters are not allowed to be included in DIVA Category and Disk Array Names: ? < >

Related Topics

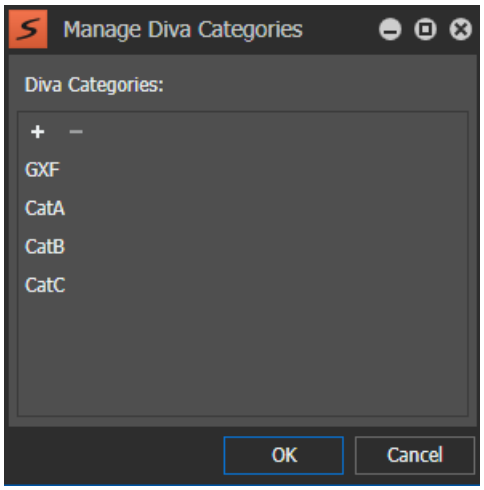
Configuring DIVA on page 875

Configuring the GV STRATUS system for DIVA, FlashNET, Masstech, and Common RESTful archives on page 890

DIVA Categories Add/Modify Field settings

To locate these settings, click **Core | MDI Configuration | Managed Devices | Add | MDI Type: Diva Archive | DIVA Categories | ...**

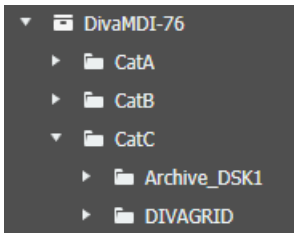
The **Manage Diva Categories** dialog displays.



Configure the Diva category field setting as below:

Setting or button	Description
Diva Categories	The list of DIVA Categories that will be visible via the Navigator in GV STRATUS clients. To add categories, click **+** and enter the new category name in the **Add Diva Category** dialog box. • Plus sign: Opens the **Add Diva Category** dialog box for users to enter the new category name. • Minus sign: Removes a selected Diva Category from the list. ***NOTE: These special characters are not allowed to be included in DIVA Category and Disk Array names: ? < >***
OK	Adds the new category to the DIVA Categories settings.
Cancel	Cancels changes to the DIVA Categories settings.

The newly created DIVA categories are now accessible via the Navigator in GV STRATUS clients.



Upgrade GV STRATUS system with the DIVA Category Update Utility

- The GV STRATUS software must have been upgraded on the GV STRATUS Core server.
- There are no currently processing or running archive/restore workflows between DIVA archive and the GV STRATUS system.

This task applies to the following:

- The GV STRATUS Core server

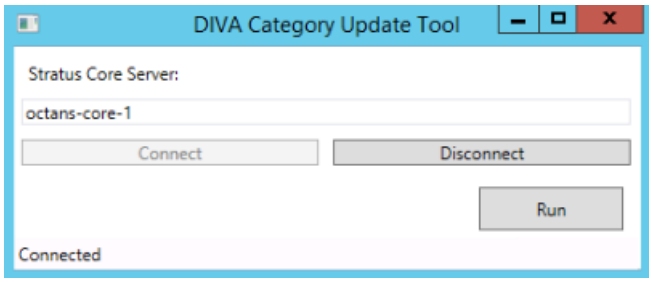
The `DivaCategoryUpdateUtility.exe` must be run on the GV STRATUS Core server after upgrading GV STRATUS software if you have DIVA archive in your system. Running the tool ensures existing GV STRATUS assets' associations paths are updated with the newly supported multiple DIVA categories.

1. Log on to the GV STRATUS Core server as an Administrator.
2. Locate the following file:

   `C:\Program Files\Grass Valley\STRATUS MDI DIVA\DivaCategoryUpdateUtility.exe`

   This file is copied to the GV STRATUS Core server during software deployment.
3. Run the `DivaCategoryUpdateUtility.exe` to update DIVA categories to assets' association paths in your GV STRATUS system.

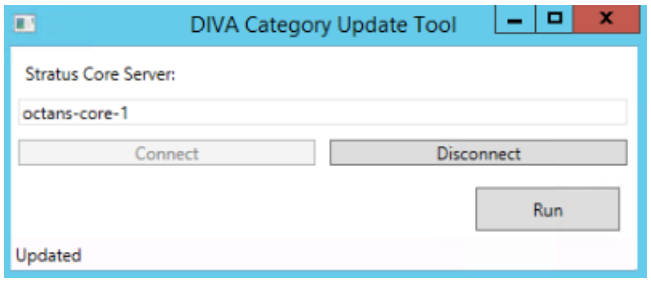
   The **DIVA Category Update Tool** opens.
4. Enter the name of the GV STRATUS Core server and click **Connect**.



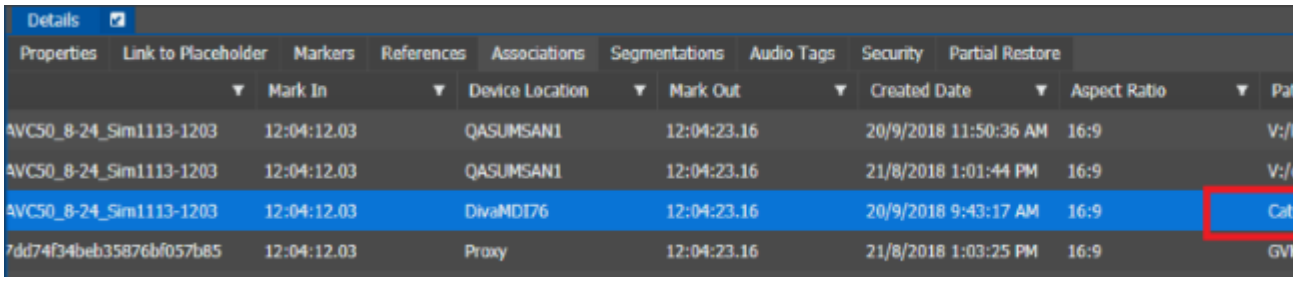
   If there are any conflicts, the **Resolve Conflict** section will be displayed.
5. Ensure the Name, Metadata ID (URN), and Category columns are shown (in that order), with a drop-down list in the Category column for users to select a DIVA category.
6. Do one of the following:

   - Resolve any conflicts by assigning the correct DIVA category to assets. Then click **Run**.
   - If there are no conflicts, just click **Run**.

   The process is completed when the status changes to **Updated** in the DIVA Category Update Tool.



With a successful run of the DIVA Category Update Utility, the DIVA Category and Disk Array name will be displayed in the **Path** column of the Associations tab when you load a DIVA archived asset into the Inspector.

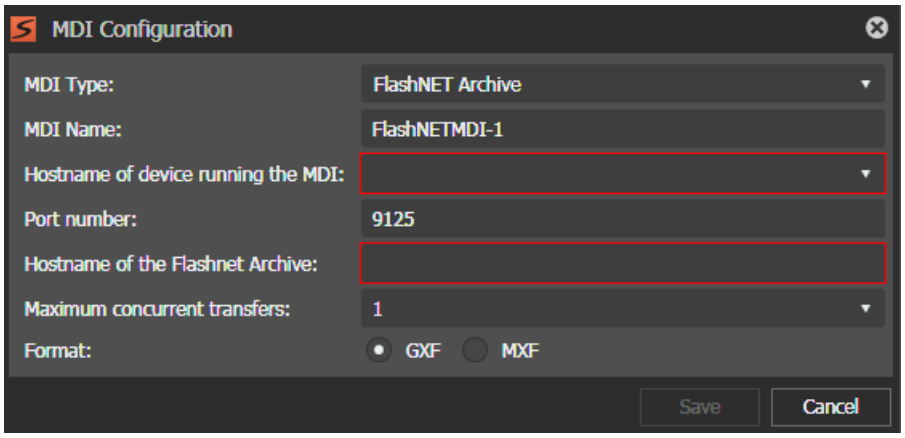


FlashNET Archive MDI settings

These settings are optional on GV STRATUS systems.

Before archiving assets, your K2 system must be assigned with the role of FTP Server.

To locate these settings, click **Core | MDI Configuration | Managed Devices | Add | FlashNET Archive**



Setting or button	Description
MDI Type	The Managed Device Interface (MDI) type to which these settings apply.
MDI Name	A name for this instance of the MDI type. Do not use spaces in the MDI name.
Hostname of device running the MDI	The name of the GV STRATUS server that hosts this MDI.
Port number	The port number of the port that this MDI listens to. The default port number is 9124. Other port numbers are also allowed.
Hostname of the FlashNET Archive	The name or IP address of the FlashNET Archive server. ***NOTE: The device status can be monitored in the Resource Monitor of* GV STRATUS Control Panel.**
Maximum concurrent transfers	The maximum number of transfers that the MDI will process at the same time. The number of maximum concurrent transfers can be monitored in the Resource Monitor of GV STRATUS Control Panel.

Setting or button	Description
Format	Specifies the format of the archived asset, either GXF or MXF. ***NOTE: In order for the format change to take effect, you need to click Save and restart your GV STRATUS clients.***

Related Topics

Configuring FlashNet on page 878

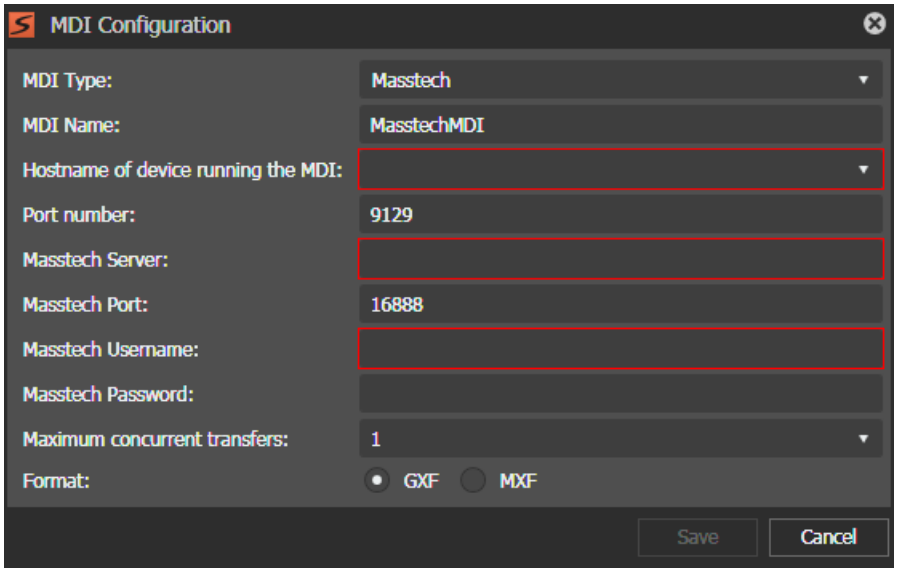
Configuring the GV STRATUS system for DIVA, FlashNET, Masstech, and Common RESTful archives on page 890

Masstech MDI settings

These settings are optional on GV STRATUS systems.

Before archiving assets, your K2 system must be assigned with the role of FTP Server.

To locate these settings, click **Core | MDI Configuration | Managed Devices | Add | Masstech**



Setting or button	Description
MDI Type	The Managed Device Interface (MDI) type to which these settings apply.
MDI Name	A name for this instance of the MDI type. Do not use spaces in the MDI name.
Hostname of device running the MDI	The name of the GV STRATUS server that hosts this MDI.
Port number	The port number of the port that this MDI listens to. The default port number is 9129. Other port numbers are also allowed.

Setting or button	Description
Masstech Server	The name or IP address of the Masstech server. ***NOTE: The device status can be monitored in the Resource Monitor of* GV STRATUS Control Panel.**
Masstech Port	The default value for the Masstech port is 16888.
Masstech Username	The Masstech username.
Masstech Password	The Masstech password.
Maximum concurrent transfers	The maximum number of transfers that the MDI will process at the same time. The number of maximum concurrent transfers can be monitored in the Resource Monitor of GV STRATUS Control Panel.
Format	Specifies the format of the archived asset, either GXF or MXF. ***NOTE: Click Save and restart your GV STRATUS clients to put a format change into effect.***

Related Topics

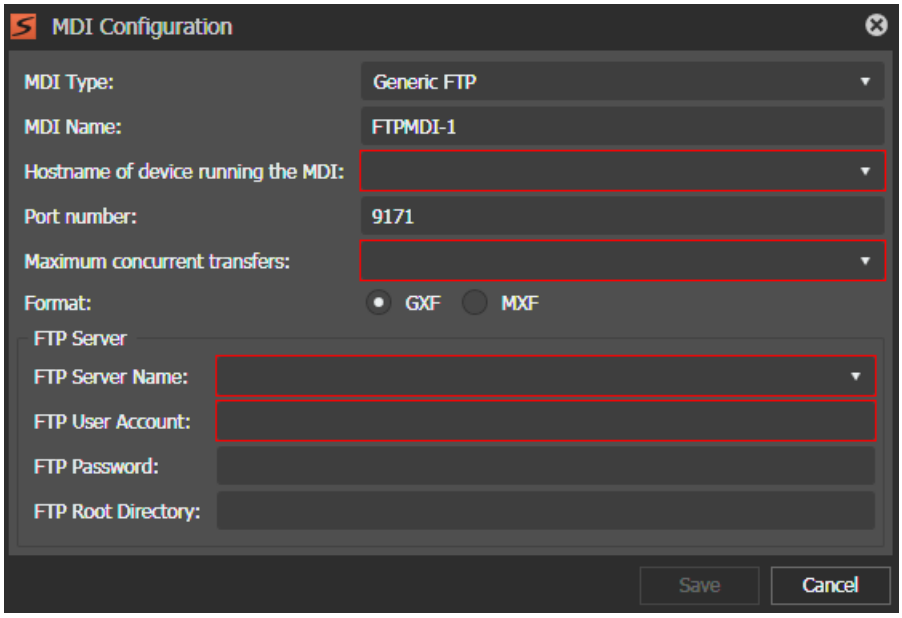
Configuring Masstech on page 880

Configuring the GV STRATUS system for DIVA, FlashNET, Masstech, and Common RESTful archives on page 890

Generic FTP MDI settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Core | MDI Configuration | Managed Devices | Add | Generic FTP**



Setting or button	Description
MDI Type	The Managed Device Interface (MDI) type to which these settings apply.
MDI Name	A name for this instance of the MDI type. Do not use spaces in the MDI name.
Hostname of device running the MDI	The name of the GV STRATUS server that hosts this MDI.
Port number	The port number of the port that this MDI listens to. The default port number is 9170. Other port numbers are also allowed.
Maximum concurrent transfers	The maximum number of transfers that the MDI will process at the same time. You can configure up to 10 concurrent transfers if you have large resources in your system. The number of maximum concurrent transfers can be monitored in the Resource Monitor of GV STRATUS Control Panel.
Format	Specifies the format of the archived asset, either GXF or MXF. ***NOTE: In order for the format change to take effect, you need to click Save and restart your GV STRATUS clients.***
FTP Server Name	The IP Address or the name resolving to the FTP server on the FTP server network where assets will be transferred to. If using a K2 nearline, configure the Generic FTP MDI to use the K2's nearline FTP. ***NOTE: The device status can be monitored in the Resource Monitor of* GV STRATUS Control Panel.**
FTP User Account	The FTP user name.
FTP Password	The FTP password.
FTP Root Directory	The root directory for the Generic FTP MDI. Once you set the root directory, only folders under the root directory are exposed in the Navigator of GV STRATUS application.

Related Topics

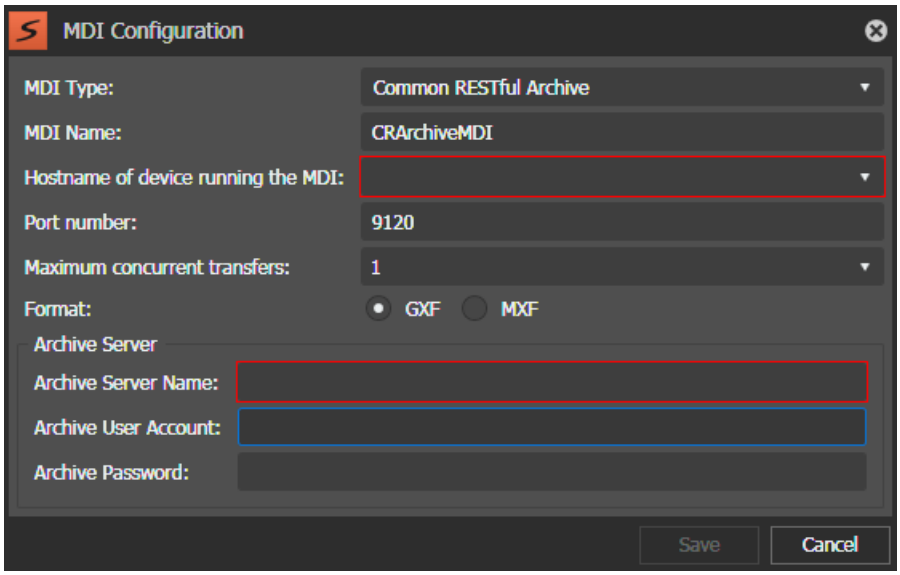
Installing and configuring FileZilla on page 884
Configuring the GV STRATUS system for FileZilla on page 889
Configuring the Generic FTP MDI role for Nearline K2 SAN on page 891

Common RESTful Archive MDI settings

These settings are optional on GV STRATUS systems.

You can configure up to 2 Common RESTful Archive MDIs in the GV STRATUS Control Panel, and both MDIs are able to archive assets in parallel at the same time.

To locate these settings, click **Core | MDI Configuration | Managed Devices | Add | Common RESTful Archive**



Setting or button	Description
MDI Type	The Managed Device Interface (MDI) type to which these settings apply.
MDI Name	A name for this instance of the MDI type. Do not use spaces in the MDI name.
Hostname of device running the MDI	The name of the GV STRATUS server that hosts this MDI.
Port number	The port number of the port that this MDI listens to. The default port number is 9120. Other port numbers are also allowed.
Maximum concurrent transfers	The maximum number of transfers that the MDI will process at the same time. The number of maximum concurrent transfers can be monitored in the Resource Monitor of GV STRATUS Control Panel.
Format	Specifies the format of the archived asset, either GXF or MXF. ***NOTE: In order for the format change to take effect, you need to click Save and restart your GV STRATUS clients.***
Archive Server Name	The name of the Archive Server.
Archive User Account	The user account to access the Archive Server.
Archive Password	The password for the user account.

NOTE: For Common RESTful Archives, transfers between archives are only supported between the Common RESTful Archive and Generic FTP servers.

Related Topics

Configuring the GV STRATUS system for DIVA, FlashNET, Masstech, and Common RESTful archives on page 890

Archiving an asset on page 1123

Metadata settings

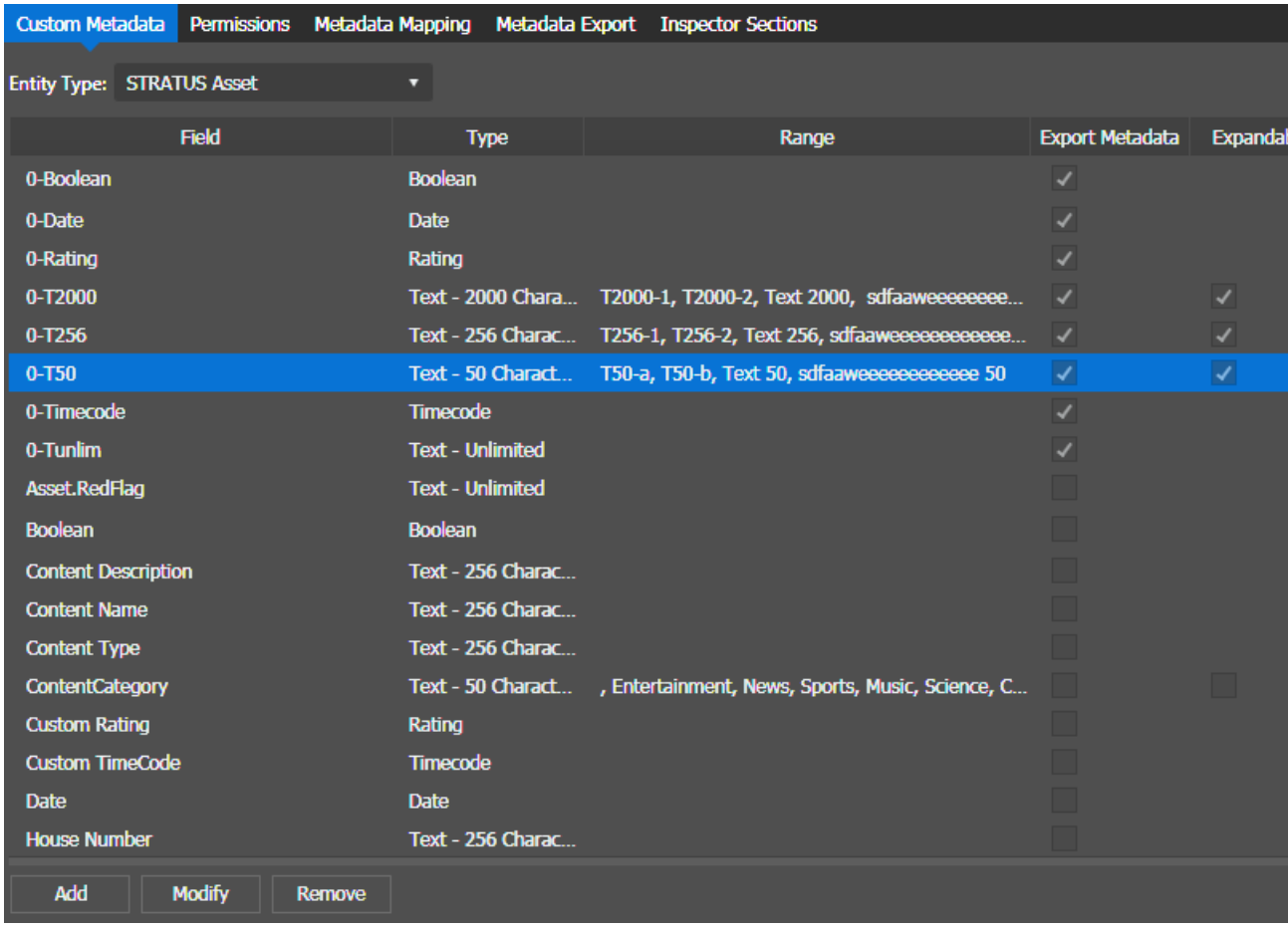
These settings are optional on GV STRATUS systems.

To locate these settings, click **Core | Metadata**

Custom Metadata settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Core | Metadata | Custom Metadata**



The GV STRATUS application prevents you from creating a custom metadata field with the same name as an existing metadata field. However, if you use K2 AppCenter to create metadata fields, it is possible to have multiple fields with the same name. If this occurs, the GV STRATUS application displays the first field only.

Custom metadata fields configured here are then available for use in the GV STRATUS application as follows:

- On the Inspector Panel properties tab
- As an Asset List column
- As a House Number List column
- As an Advanced Search criteria

- For inclusion in rules
- On a Segment Template
- On markers and keywords

Setting or button	Description
Entity Type	A list of available GV STRATUS entities for which you can configure custom metadata. ***NOTE: You can only configure custom metadata for markers and keywords if you are assigned with the Media Manager role.***
Add	Opens the Add Field dialog box to add metadata fields.
Modify	Opens the Modify Field dialog box for the selected field.
Remove	Removes the selected field.

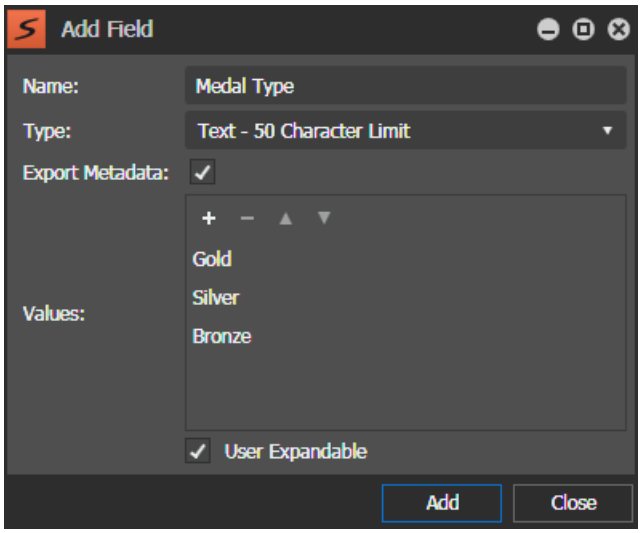
Tip: It is recommended to reset index after removing a custom metadata field. If not, a deleted custom metadata field will only be removed from the index after modifications of assets.

Related Topics

Search Index Config settings on page 353
About custom fields on page 422

Custom Metadata Add/Modify Field settings

To locate these settings, click **Core | Metadata | Custom Metadata | Add** or **Modify**



Setting or button	Description
Name	The name of the custom metadata field you are creating. This name is displayed in the GV STRATUS application.

Setting or button	Description
Type	The type of custom metadata field. When a type of field is used in the GV STRATUS application, it has characteristics as follows: • Boolean: A checkbox. • Date: A drop-down calendar from which dates can be selected. Text can also be entered in the field. • Number: A field in which numbers only can be entered, up to 9 digits. • Large Number: A field in which numbers only can be entered, up to 18 digits. • Text - 50 Character Limit: A drop-down list of values, if configured. Text up to 50 characters can also be entered. • Text - 256 Character Limit: A drop-down list of values, if configured. Text up to 256 characters can also be entered. • Text - 2000 Character Limit: A drop-down list of values, if configured. Text up to 2000 characters can also be entered. • Text - Unlimited: A drop-down list of values, if configured. Text of any length can also be entered. • Tags: A field in which tags can be entered as text, with commas separating individual tags. • Rating: A row of selectable stars. • Timecode: A field in which timecode values can be entered as numbers and adjusted with up/down arrows. ***NOTE: To optimize* GV STRATUS *application search performance, restrict the number of characters allowed in a field. Fields with a large number of characters slow search results.***
Export Metadata	If this checkbox is selected, the custom metadata field appears in the **Rule Editor** configuration window. Then, custom metadata can be added when configuring rules.
Values	If the field type is Text, the following controls configure a list of values for the field: • Plus sign: Opens the Add Field Value dialog box in which a value is entered. • Minus sign: Removes a value from the list. • Up arrow: Moves a value up the list. • Down arrow: Moves a value down the list.
User Expandable	If this checkbox is selected, the custom metadata values display in a drop-down list in the Inspector. You can also add other values for the custom metadata on the Properties tab of the Inspector.
Add	On Add Field dialog box. Adds the field to the list in Metadata settings while the Add Field dialog box remains open.
Close	On Add Field dialog box. Closes the Add Field dialog box without adding the field currently configured.
Update	On Modify Field dialog box. Updates the changes to the field.

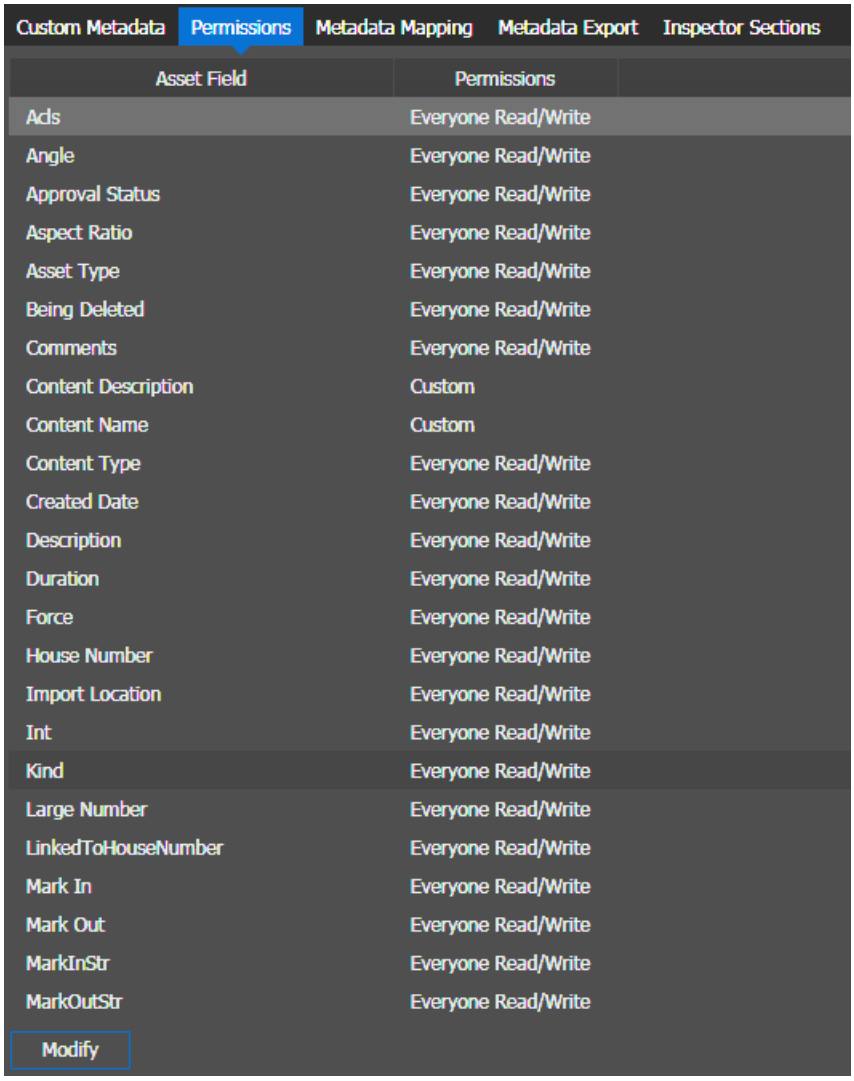
Setting or button	Description
Cancel	On Modify Field dialog box. Cancels changes to the field.

Related Topics

Using custom metadata in Inspector on page 1018

Permissions settings

To locate these settings, click **Core | Metadata | Permissions**.



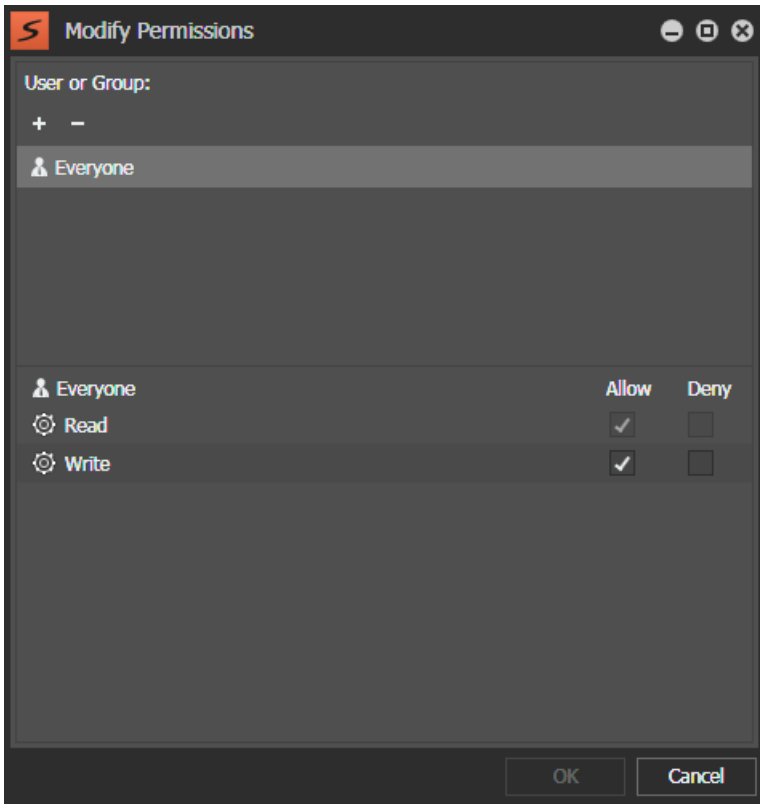
You can configure user permissions and access controls for metadata fields. By default, everyone has read and write access rights. Once modified, the permission displayed as **Custom**.

Setting or button	Description
Asset Field	The list of Asset Fields which you can configure permissions for.
Permissions	Configurable user permissions including read and write access controls.

Setting or button	Description
Modify	Opens the Modify Permissions dialog box for the selected field.

Permissions Modify Field settings

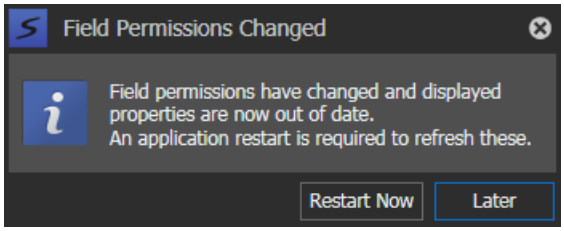
To locate these settings, click **Core | Metadata | Permissions | Modify**



Setting or button	Description
User or Group	The list of users or groups with permissions and access rights to the metadata. To assign permissions, click **+** and enter any user or group in the **Add Users or Groups** dialog box. If necessary, click **Advanced** to open Windows operating system dialog box to find and validate users or groups. • Plus sign: Opens the **Add Users or Groups** dialog box to assign users or groups with permissions. • Minus sign: Removes a user or group from the list.

Setting or button	Description
Allow / Deny	The type of access rights that can be configured for users and groups. By default, all assigned users and groups have Read and Write permissions as follows: • **Read**: Access right to read the metadata. • **Write**: Access right to modify the metadata. If **Deny** is selected, the metadata value is grayed out in the Inspector. Set permissions by selecting **Allow** or **Deny** as appropriate.
OK	Updates the changes to the Permissions settings.
Cancel	Cancels changes to the Permissions settings.

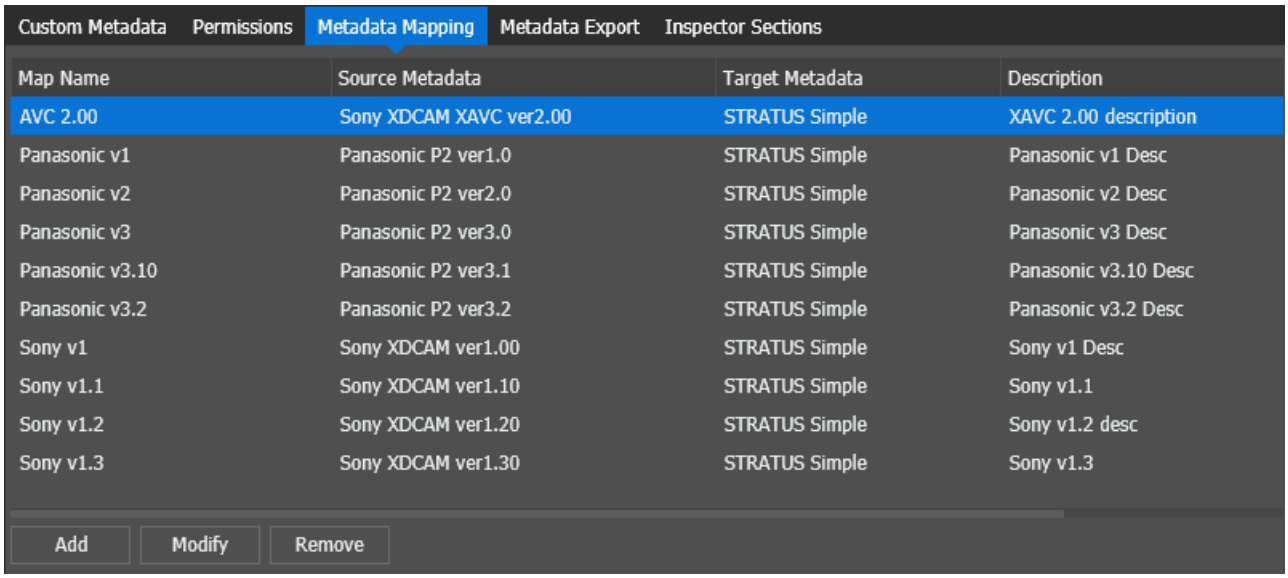
If **Read** permissions are changed from Deny to Allow, the **Field Permissions Changed** dialog appears. You must restart the GV STRATUS application in order to view those fields.



Metadata Mapping settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Core | Metadata | Metadata Mapping**



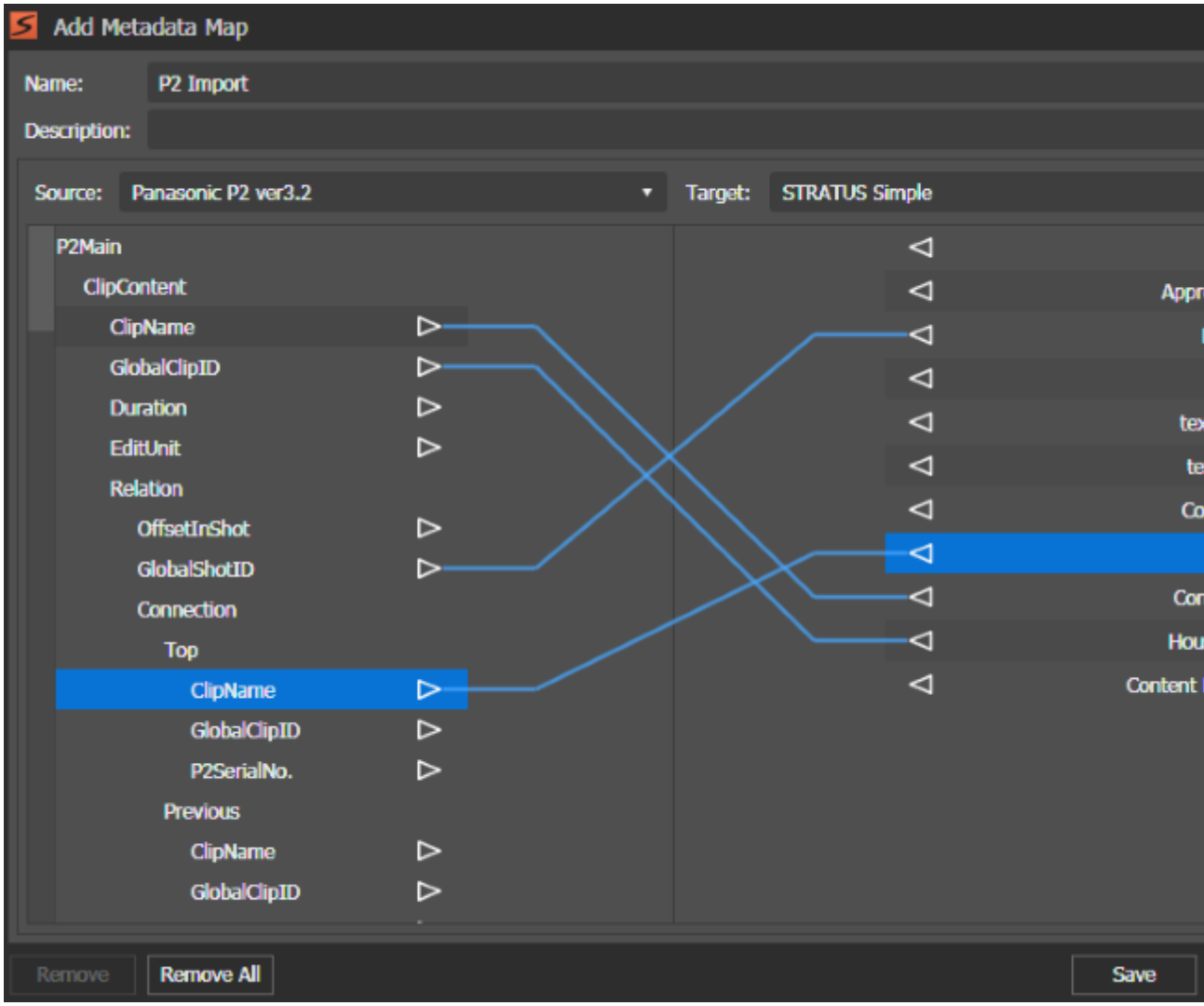
Setting or button	Description
Map Name	Name of the metadata map.

Setting or button	Description
Source Metadata	Source of metadata in the map.
Target Metadata	Target of metadata in the map.
Add	Opens the Add Metadata Map dialog box to create new metadata maps
Modify	Opens the Modify Metadata Map dialog to modify the selected map.
Remove	Removes the selected map.

After configuring metadata mapping, import an asset with mapped metadata, then view the imported asset in GV STRATUS Inspector to verify that metadata is inserted into mapped fields correctly.

Metadata Mapping Add/Modify Field settings

To locate these settings, click **Core | Metadata | Metadata Mapping | Add** or **Modify**

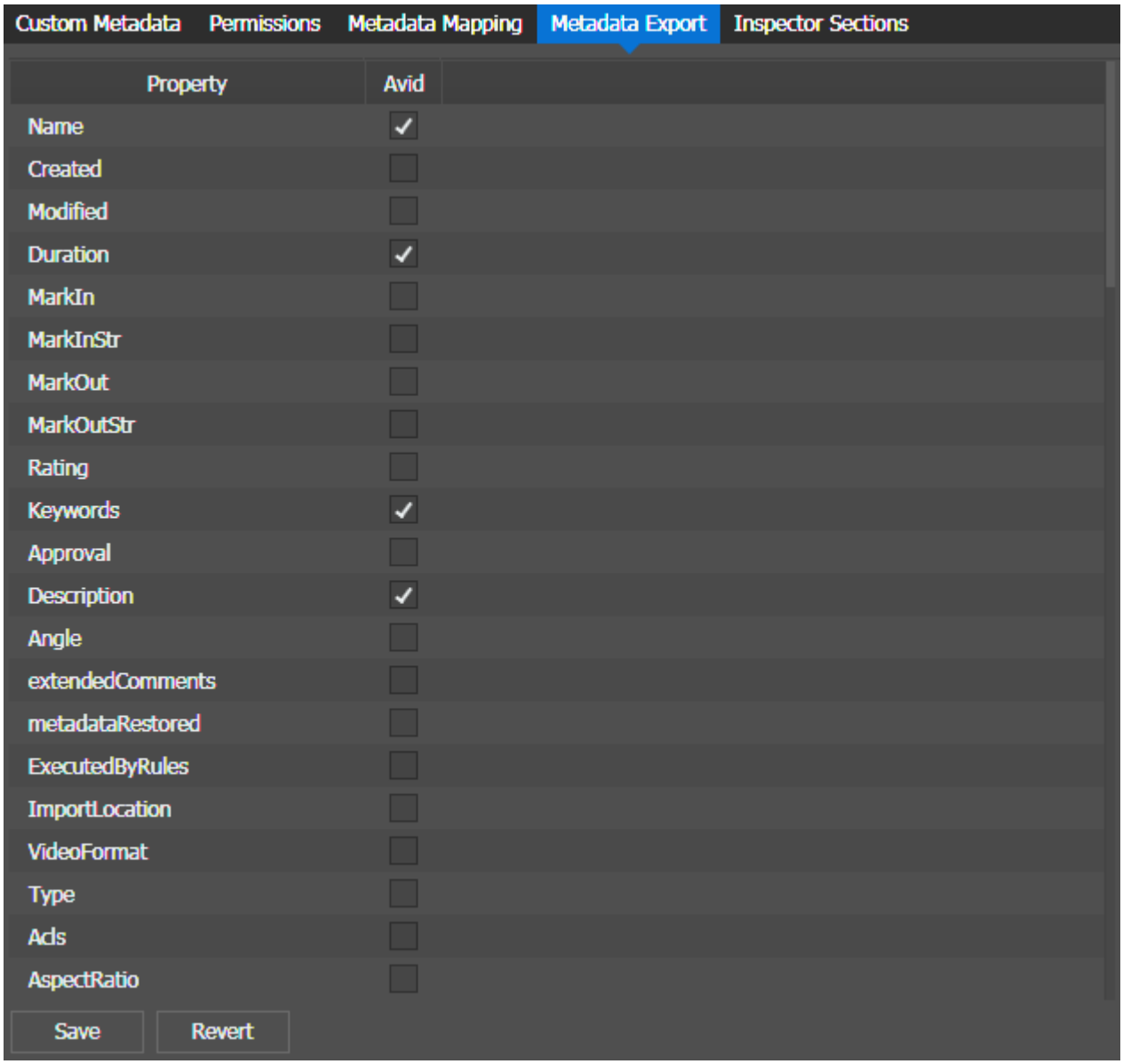


These settings apply to assets containing metadata that are imported with the RMI tool.

Setting or button	Description
Name	The name of the mapping. This can be any name, as appropriate for your workflow.
Description	The description of the mapping
Source	The metadata from which you are mapping. The list is populated with the metadata fields defined by the source XML or other schema. One source field can be mapped to one or more target fields using drag-and-drop, as indicated by a mapping line or lines. The metadata source must be a valid XML schema. Refer to *http://www.w3.org/TR/REC-xml/#charsets*. Incorrect standards are not supported.
Target	The metadata to which you are mapping the source metadata. The list is populated with the metadata fields defined by the target schema. One target field can be mapped to one source field using drag-and-drop, as indicated by a mapping line.
Remove	Removes the selected mapping line.
Remove All	Removes all mapping lines
Save	Saves the mapping. For the selected source, only one metadata mapping may be saved. Multiple mappings for the same source are not allowed.
Close	Closes the dialog box.

Metadata Export settings

To locate these settings, click **Core | Metadata | Metadata Export**.

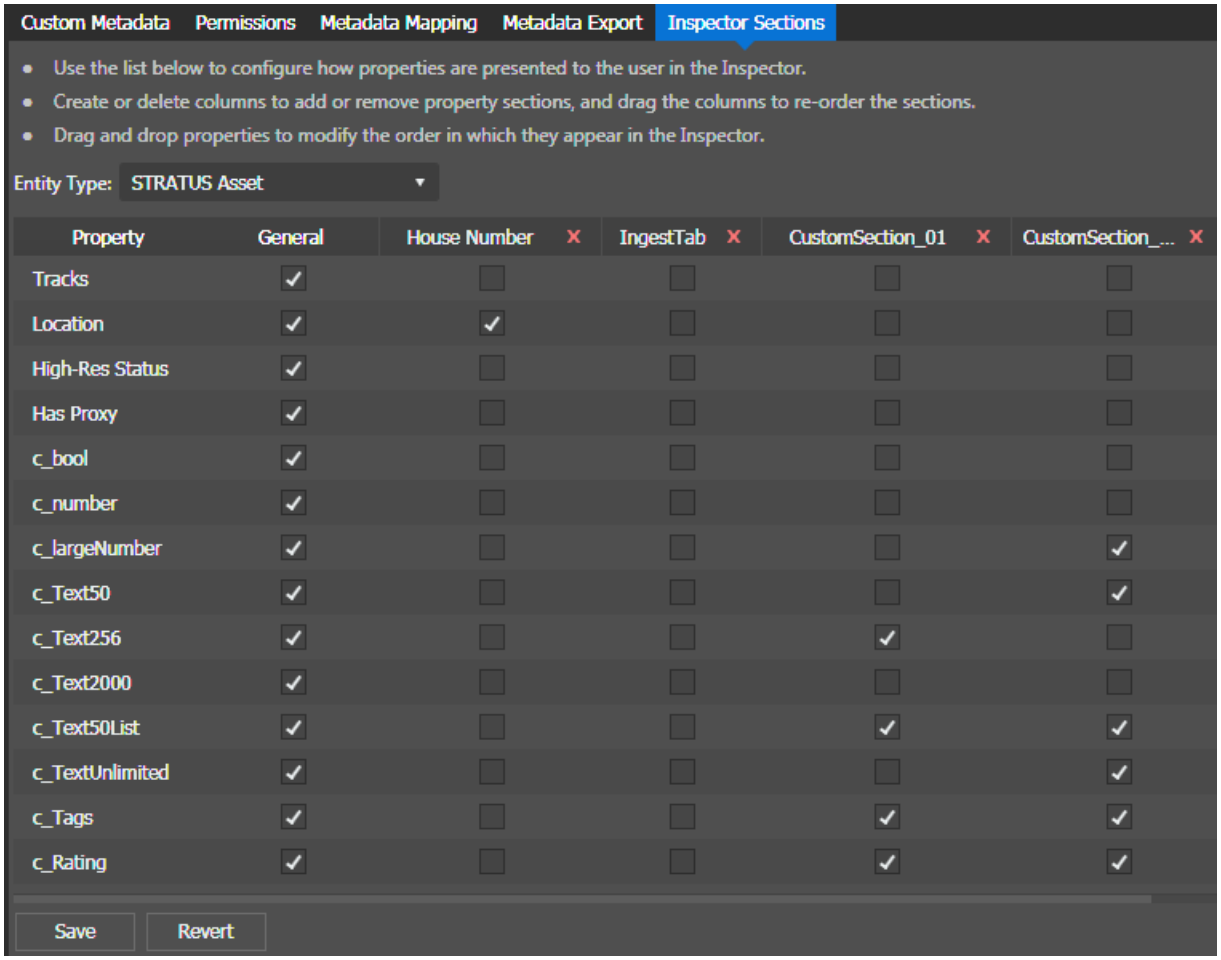


You can select to add metadata to be exported along with the asset after triggering transfer via context menu or the **Transfer to Avid** rule.

Setting or button	Description
Property	The name of the metadata field.
Avid	Rows selected in this column define metadata fields to be transferred with assets from GV STRATUS system into Avid.
Save	Saves the current settings.
Revert	Discards any new settings and reverts to the last saved settings.

Inspector Sections settings

To locate these settings, click **Core | Metadata | Inspector Sections**.



You can add and organize metadata and sections for display in Properties tab within the Inspector.

- Each row represents a metadata property. Properties can be reordered higher/lower using drag-and-drop.
- Each column represents a section that will be displayed in the Inspector. Added sections can be reordered left/right using drag-and-drop.

Setting or button	Description
Entity Type	Configures sections on tabs and property panels for STRATUS assets, markers, and segments.
Property	The name of the metadata field.
General	Rows selected in the column define the metadata fields display on the default **General** section in the **Properties** tab. This section cannot be removed or its position altered.

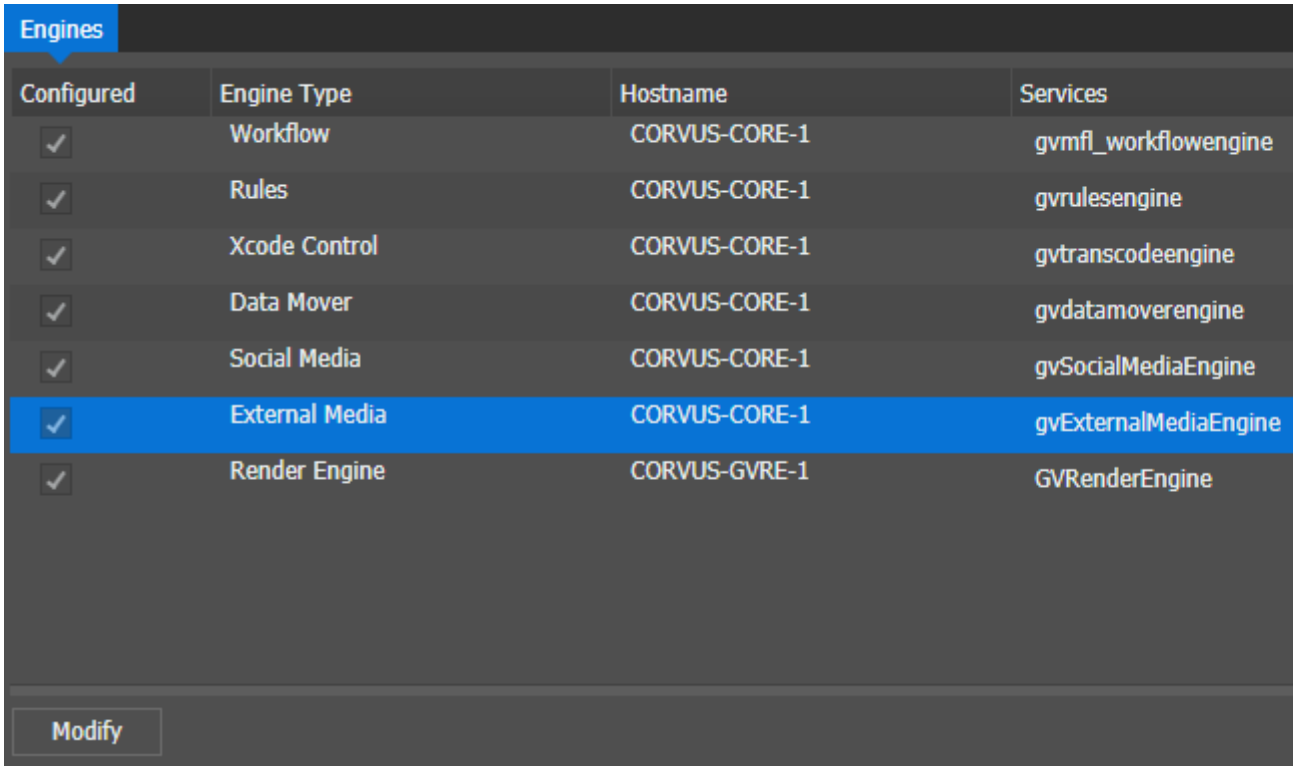
Setting or button	Description
+	Opens the **Add Tab** dialog box, which defines a new section name and adds the section. Rows selected in the column define the metadata fields displayed on the added section.
X	Removes an added column.
Save	Saves the current settings.
Revert	Discards any new settings and reverts to the last saved settings.

The GV STRATUS application must be restarted to put changes into effect.

Engines settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Core | Engines**



Setting or button	Description
Configured	Selects an Engine for which settings are saved.
Engine Type	The Engine components installed on the GV STRATUS server.
Hostname	The name of a GV STRATUS server that hosts the Engine.
Services	The services that support the Engine.
Action	Starts and stops the Engine service.

Setting or button	Description
Status	Indicates if the Engine service is running or stopped.
Save	Saves current settings to selected GV STRATUS servers.
Cancel	Returns settings to their last saved state.
Modify	When an Engine type that is modifiable is selected, opens settings to configure the engine.
Refresh	Updates the list.

Depending on the workflow and bandwidth requirements of your system, Grass Valley may provide a system design in which multiple engines of the same type run on one or more servers. Configure engines as specified by your system design.

For the Render Engine, GV STRATUS Control Panel Format settings define the format of conformed assets.

Related Topics

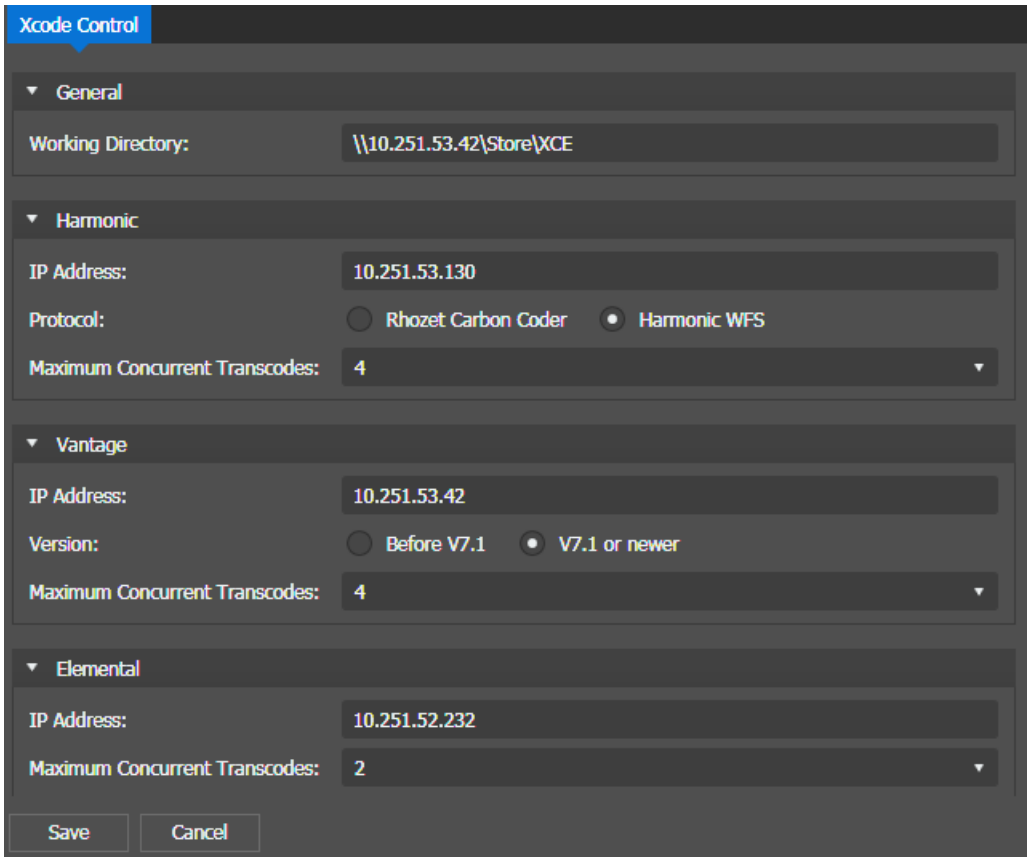
Format settings on page 161

Render Engine Settings on page 335

Xcode Control engine settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Core | Engines | Xcode Control | Modify**



Setting or button	Description
Working Directory	The directory in which the Xcode Engine temporarily places files while exporting an asset. The directory must have enough capacity for your largest concurrent exports. The directory must allow transcode rule access. Refer to related topics for more information about transcode rule access. ***NOTE: The location of working directories for the Workflow Engine and Xcode Control Engine must be on the same share, but configured on different sub-folders.***
Harmonic IP Address	The host name or IP address of the server that hosts or controls the application that transcodes the asset.
Harmonic Protocol	Selection for the protocol controlling the application, such as the Harmonic ProMedia™ Carbon (formerly Carbon Coder™) or Harmonic WFS.
Harmonic Maximum Concurrent Transcodes	Limits the number of simultaneous transcodes performed. Use to balance resource load on the transcode application host. The number of maximum concurrent transfers can be monitored in the Resource Monitor of GV STRATUS Control Panel.
Vantage IP Address	The host name or IP address of the server that hosts the Telestream Vantage™ application that transcodes the asset.

Setting or button	Description
Version	The Vantage software version number in your operation must be selected for the Xcode Control engine to work with your system. • **Before V7.1** OR • **V7.1 or newer**
Vantage Maximum Concurrent Transcodes	Limits the number of simultaneous transcodes performed. Use to balance resource load on the transcode application host. The number of maximum concurrent transfers can be monitored in the Resource Monitor of GV STRATUS Control Panel.
Elemental IP Address	The host name or IP address of the server that hosts the Elemental® application that transcodes the asset.
Elemental Maximum Concurrent Transcodes	Limits the number of simultaneous transcodes performed. Use to balance resource load on the transcode application host. The number of maximum concurrent transfers can be monitored in the Resource Monitor of GV STRATUS Control Panel.
Save	Restarts the Xcode Control engine and applies changes. ***NOTE: The device status can be monitored in the Resource Monitor of* GV STRATUS Control Panel.**
Cancel	Reverts to previously saved setting.

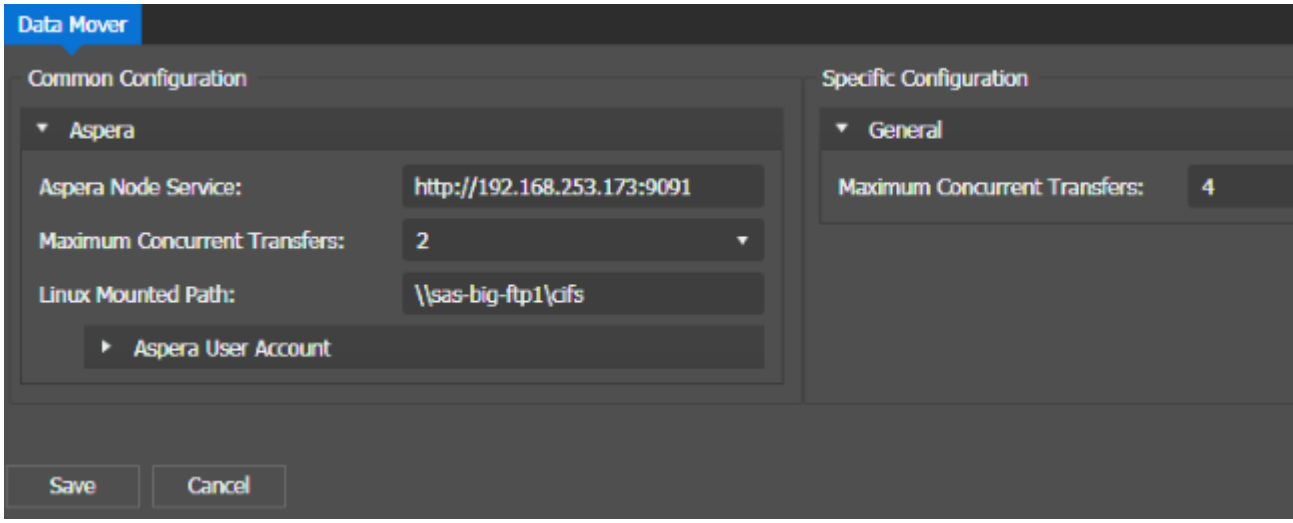
Related Topics

Transcode rule access on page 655

Data Mover engine settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Core | Engines | Data Mover | Modify**



Setting or button	Description
Aspera Node Service	Setting for the Aspera Node Service to support FASP transfer protocol in export workflow triggered by GV STRATUS Rules. This setting specifies the URL of the Aspera web service on either a Windows or Linux server. The convention must be *`http://<IP address of local Aspera Node Service>:<port number>`*. Port number is typically 9091.
Linux Mounted Path	Specifies the base part of the UNC path to be stripped for the relative path of an Aspera job order. The Data Mover Engine must strip the base part to make the UNC file path in the Aspera job relative to the Linux mount point. Leave this setting empty if your Aspera server is on a Windows system.
Aspera User Account	The user account and credential to access the Aspera Node Service. For an Aspera server running on the Linux system, enter the user name and password that have been configured under Linux with the **asnodeadmin** command.
Maximum Concurrent Transfers	Limits the number of simultaneous transfers performed by the Data Mover engine. Use to balance resource load on the system hosting the engine. The number of maximum concurrent transfers can be monitored in the Resource Monitor of GV STRATUS Control Panel.
Save	Restarts the Data Mover engine and applies changes. ***NOTE: The device status can be monitored in the Resource Monitor of* GV STRATUS Control Panel.**
Cancel	Reverts to previously saved setting.

Related Topics

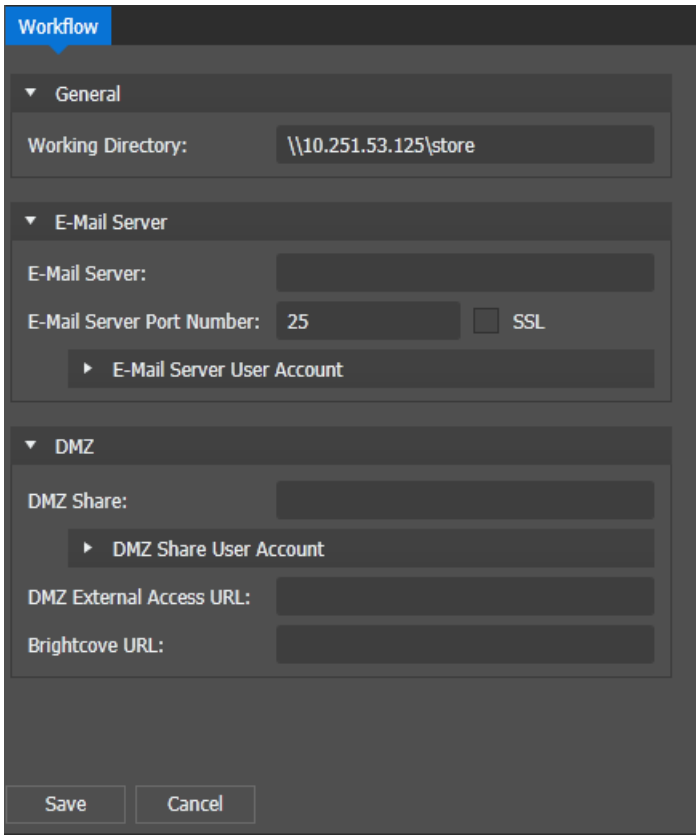
Example rule: Export to a YouTube channel

Configuring Aspera on page 653

Workflow engine settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Core | Engines | Workflow | Modify**

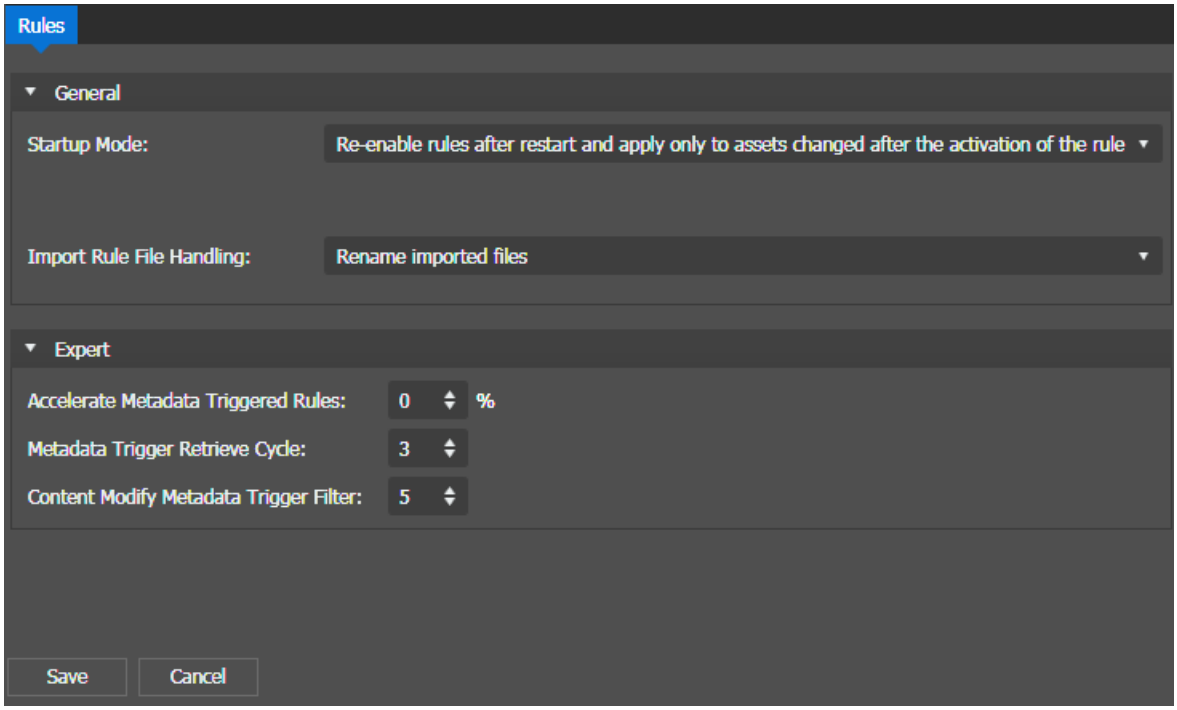


Setting or button	Description
Working Directory	The directory in which the Workflow Engine temporarily places files while exporting an asset to a FTP destination. First a K2 system exports the asset into the working directory, then an FTP transfer places the asset to the next destination. The working directory must have enough capacity for your largest concurrent exports. The directory must be accessible from the K2 system, GV STRATUS Render Engine, and the GV STRATUS server(s) running the Workflow Engine. The `GVAdmin` user must have access to the directory. ***NOTE: The location of working directories for the Workflow Engine and Xcode Control Engine must be on the same share, but configured on different sub-folders.***
E-Mail Server	Settings for the email server the GV STRATUS system uses to send emails triggered by GV STRATUS Rules.
DMZ Share	Used for Digital Media Platform workflow. The access from the GV STRATUS system to the server machine running in the DMZ hosting an IIS. Must be a UNC path such as `\\192.168.200.15\brightcove`.
DMZ External Access URL	Used for Digital Media Platform workflow. The HTTP address for access to fetch files from the Brightcove site.
Brightcove URL	Used for Digital Media Platform workflow. The Brightcove URL to register the files.

Rules engine settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Core | Engines | Rules | Modify**



Setting or button	Description
Startup Mode	**Re-enable rules after restart and apply only to assets changed after the activation of the rule**: When the GV STRATUS system starts up, rules are enabled but the Rules Engine does not take action on existing assets. Rather, it waits until an asset changes and then evaluates the asset to take action. **Re-enable rules after restart and apply to all applicable assets**: When the GV STRATUS system starts up, rules are enabled and the Rules Engine immediately evaluates existing assets and takes action accordingly. ***NOTE: Take care when using this setting. Assets for which the rule action successfully completed before the restart can have the rule action applied again after the restart, resulting in a large amount of unnecessary rule activity.*** **Do not re-enable rules after restart**: When the GV STRATUS system starts up, rules are disabled. You must manually re-enable rules.
Import Rule File Handling	**Rename imported files**: Assets are renamed if imported via rules conditions by the Rules Engine. **Create side-car files**: Assets are not renamed during import, but side-car files are created for each imported asset. The side-car file is in XML format with information such as the import start time, end time, import status, and import destination.

Setting or button	Description
Accelerate Metadata Triggered Rules	Setting to define the percentage of metadata triggers out of all enabled cyclic trigger rules in the Rules Condition Checker so that metadata triggered rules can be executed earlier. The default is set to 0%. ***NOTE: Do not change this setting except under advice of Grass Valley Support personnel.***
Metadata Trigger Retrieve Cycle	Setting of the cycle of time to read metadata change notices from the GV STRATUS core services. The default value is set to 3 seconds, but you can change the duration of time if desired. ***NOTE: Do not change this setting except under advice of Grass Valley Support personnel.***
Content Modify Metadata Trigger Filter	Setting to filter change notices of modified contents in metadata triggered rules. The default value is currently set to 5, so only every 5th polling cycle will pass these notices, while all other notices will be skipped. ***NOTE: Do not change this setting except under advice of Grass Valley Support personnel.***
Save	Restarts the Rules engine and applies changes.
Cancel	Reverts to previously saved setting.

Consider the Rules Engine setting Startup Mode and the Confirm Activation option when you enable a rule, as the behavior is similar. With the Rules Engine setting you specify the behavior of all currently enabled rules when the Rules Engine starts up. With the Confirm Activation option, you specify the behavior of an individual rule when you manually enable the rule.

Related Topics

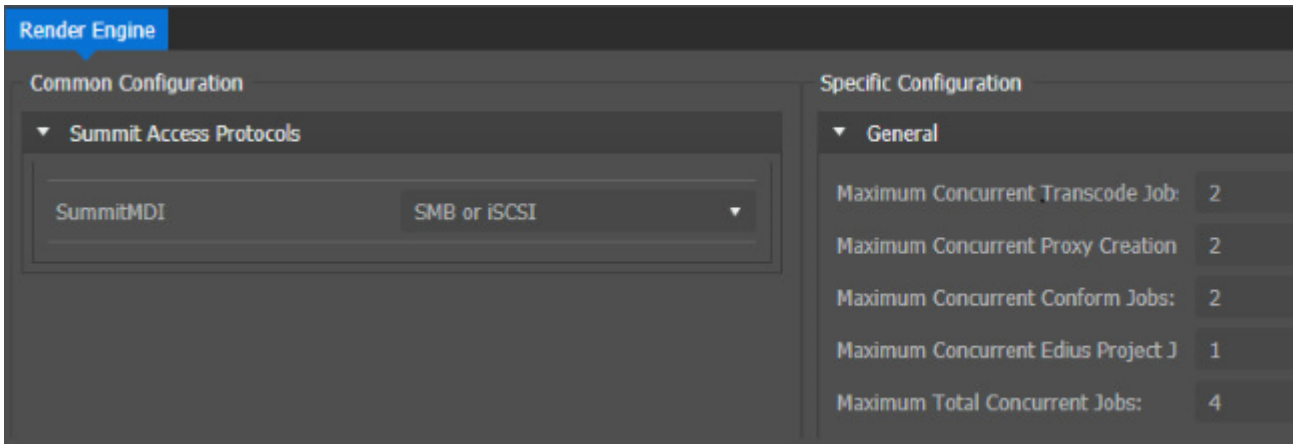
Enabling and disabling rules on page 636

About Control Panel, SiteConfig, and K2Config settings on page 433

Render Engine Settings

These settings are required on GV STRATUS systems.

To locate these settings, in GV STRATUS Control Panel click **Core | Engines | Render Engine | Modify**



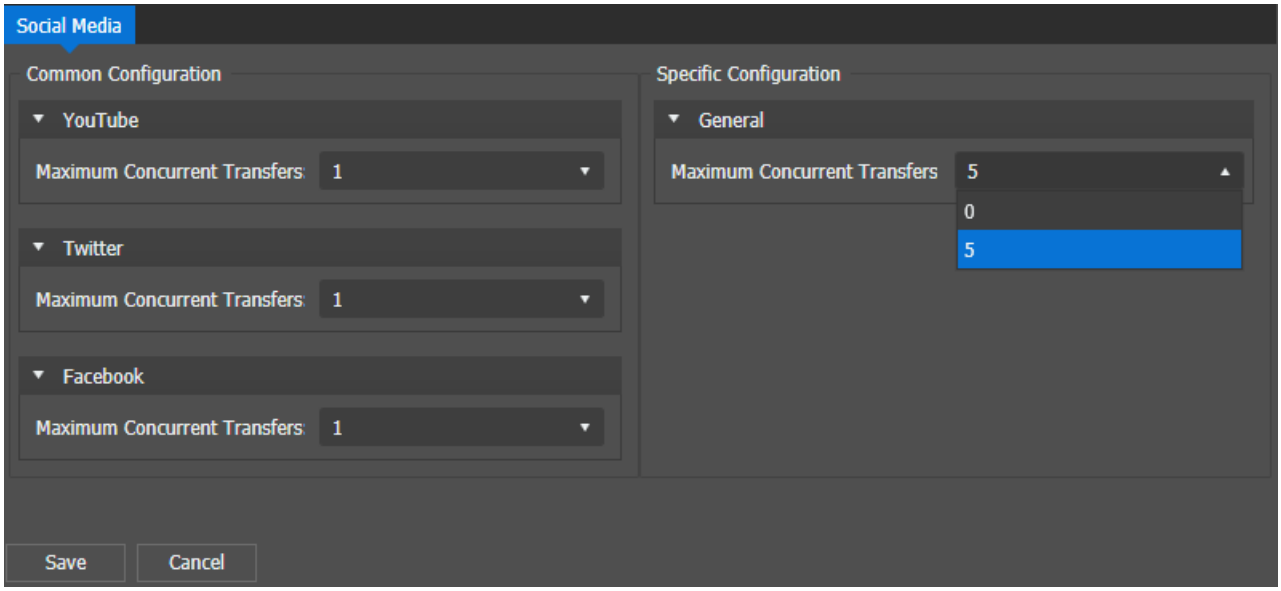
Setting or button	Description
Summit Access Protocols	The Summit Access protocol is a common configuration that must be the same for all GV Render Engine servers. Different K2 Summit servers might be accessed via different protocols. Select the Summit Access Protocol for your Render Engine server from the following: • **FTP**: Setting for FTP protocol to be used by Render Engine to access K2 Summits. • **SMB or iSCSI**: Setting for SMB or iSCSI protocol to be used by Render Engine to access K2 Summits. ***NOTE: When a Render Engine accesses high-res media on a standalone K2 Summit or a K2 Central server, FTP is ALWAYS the preferred method. It is recommended to use iSCSI with K2 SAN configurations, and SMB with Isilon shared storage configurations.***
Maximum Concurrent Transcode Jobs	Setting to specify the maximum number of concurrent transcode jobs allowed on the Render Engine server.
Maximum Concurrent Proxy Creation Jobs	Setting to specify the maximum number of concurrent proxy encoder jobs allowed on the Render Engine server.
Maximum Concurrent Conform Jobs	Setting to specify the maximum number of concurrent conform jobs allowed on the Render Engine server.
Maximum Concurrent EDIUS Project Jobs	Setting to specify the maximum number of concurrent EDIUS project jobs allowed on the Render Engine server.
Maximum Total Concurrent Jobs	Setting to specify the maximum number of total concurrent jobs allowed on the Render Engine server. ***NOTE: The maximum number for the setting is up to 4 concurrent jobs in total.***

NOTE: The total number of maximum concurrent jobs is limited by the number of available simultaneous connections with K2 Summits. If set to zero, the Render Engine does not process jobs of that type. Use these settings to balance resource load on the system hosting the engine.

Social Media engine settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Core | Engines | Social Media | Modify**



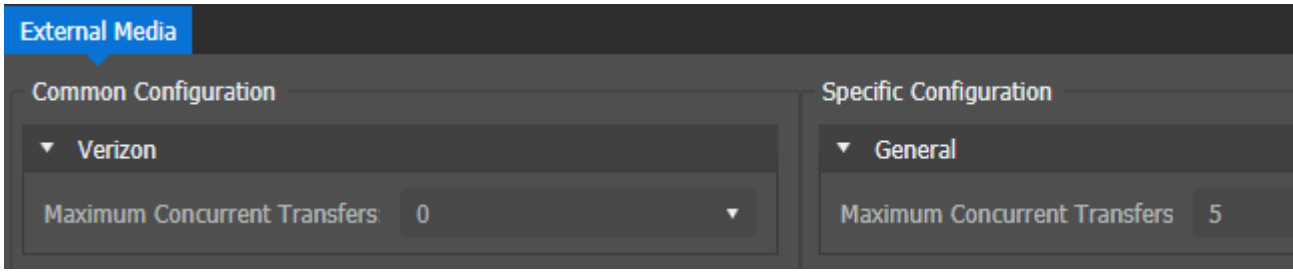
Setting or button	Description
YouTube : Maximum Concurrent Transfers	Limits the number of simultaneous transfers performed by the Social Media engine on your configured YouTube account. You can configure the number of maximum concurrent transfers between 0-10 per Social Media Platform type. This setting is set to “0” if the YouTube site license is not installed.
Twitter : Maximum Concurrent Transfers	Limits the number of simultaneous transfers performed by the Social Media engine on your configured Twitter account. You can configure the number of maximum concurrent transfers between 0-10 per Social Media Platform type. This setting is set to “0” if the Twitter site license is not installed.
Facebook : Maximum Concurrent Transfer	Limits the number of simultaneous transfers performed by the Social Media engine on your configured Facebook account. You can configure the number of maximum concurrent transfers between 0-10 per Social Media Platform type. This setting is set to “0” if the Facebook site license is not installed.
General: Maximum Concurrent Transfers	Limits the number of simultaneous transfers performed by the Social Media engine for all social media platforms. Use to balance resource load on the system hosting the engine. If the engine is deployed without a Social Media Engine license, this setting is set to “0” and cannot be configured. ***NOTE: Five (5) maximum concurrent transfers are supported with each Social Media Engine license.***

Setting or button	Description
Save	Restarts the Social Media engine and applies changes. ***NOTE: The resource status can also be monitored via the Resource Monitor in* GV STRATUS Control Panel.**
Cancel	Reverts to previously saved setting.

External Media engine settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Core | Engines | External Media | Modify**



Setting or button	Description
Verizon : Maximum Concurrent Transfers	Limits the number of simultaneous transfers performed by the External Media engine on your Verizon CMS system account. You can configure the number of maximum concurrent transfers between 0-10 per Social Media - CMS platform. This setting is set to “0” if the Verizon site license is not installed.
General: Maximum Concurrent Transfers	Limits the total number of simultaneous transfers performed by the External Media engine for all Social Media CMS platforms. Use to balance resource load on the system hosting the engine. If the engine is deployed without an External Media Engine license, this setting is set to “0” and cannot be configured. You can set up to 5 maximum concurrent transfers for each External Media Engine volume license.

Use these settings to balance resource load on the GV STRATUS server hosting the engine.

NOTE: One volume license for the External Media Engine limits the maximum concurrent jobs to five (5). It is possible to deploy more than one Engine per system for a larger operation. Each Engine must have its own license.

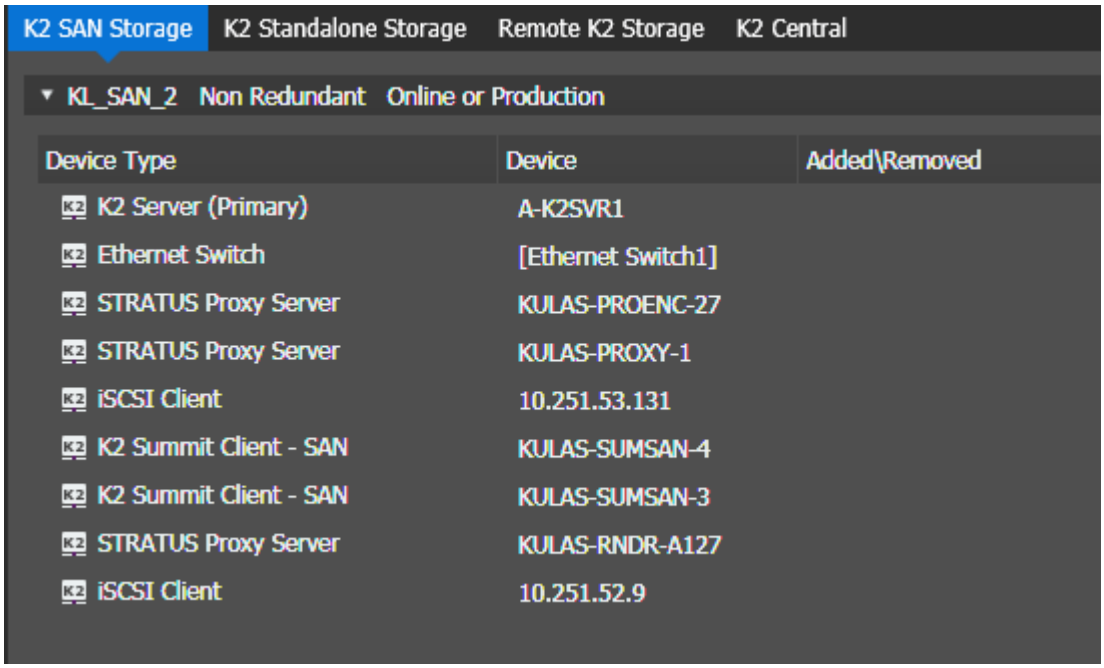
K2 Storage settings

K2 Storage settings verify that your K2 Summit/SAN systems are available for configuration. Access these settings in the GV STRATUS Control Panel application.

K2 SAN Storage settings

These settings and/or K2 Standalone Storage settings are required on all GV STRATUS systems.

To locate these settings, click **Core | K2 Storage | K2 SAN Storage**



Setting or button	Description
List	The K2 SANs found in K2Config information.
Refresh	Updates the list.

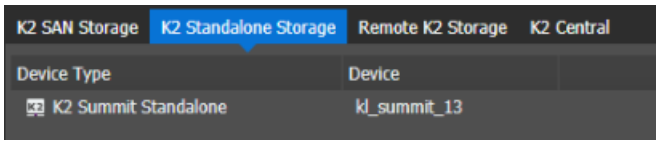
Related Topics

About redundant K2 SANs on page 419

K2 Standalone Storage settings

These settings and/or K2 SAN Storage settings are required on all GV STRATUS systems.

To locate these settings, click **Core | K2 Storage | K2 Standalone Storage**



Setting or button	Description
List	The list of K2 standalone systems found in SiteConfig information.
Refresh	Updates the list.

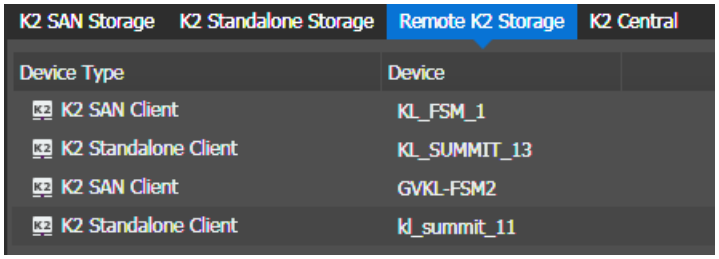
Remote K2 Storage settings

These settings are optional on GV STRATUS systems.

These settings affect the following:

- Send Destination, when sending from a local site to a remote site

To locate these settings, click **Core | K2 Storage | Remote K2 Storage**

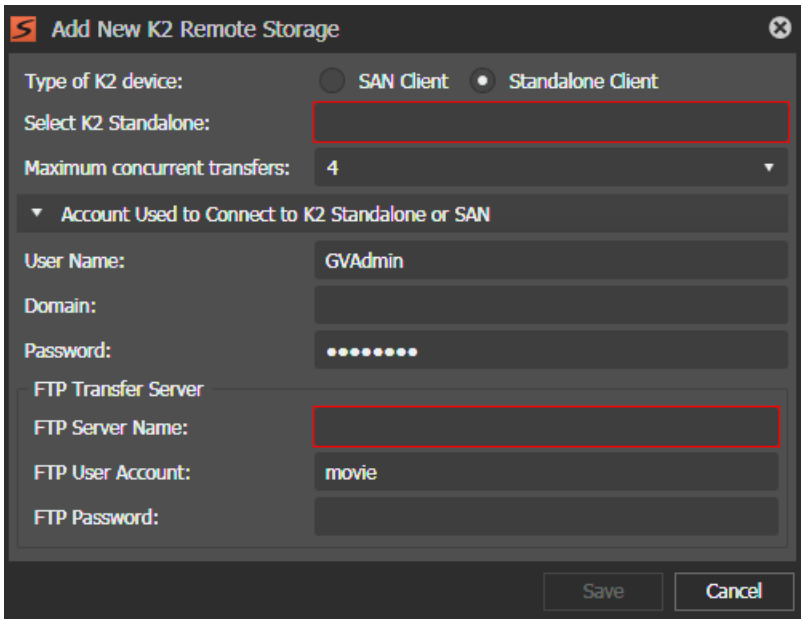


Setting or button	Description
Add	Opens the **Add new K2 remote storage** dialog box for you to add a remote K2 storage device. You can use the **Add** button repeatedly to add multiple remote K2 storage devices.
Modify	Opens the **Edit K2 remote storage** dialog box to modify settings of the selected remote K2 storage device.
Remove	Removes the selected remote K2 storage.

Remote K2 Storage Add/Modify settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Core | K2 Storage | Remote K2 Storage | Add** or **Modify**



Setting or button	Description
Type of K2 device	Select **Standalone Client** for your Standalone K2 Summit system or SAN-attached K2 Summit system. ***NOTE: Do not select the SAN Client option for your SAN-attached K2 Summit system.***
Select K2 Standalone	Do the following: • For a Standalone K2 Summit system, enter the host name of the remote K2 Summit system. • For a SAN-attached K2 Summit system, enter the name of the primary FTP server designated to be the managed device for the entire K2 SAN storage system.
Maximum concurrent transfers	The maximum number of concurrent transfers allowed. The maximum is set in K2Config. You may select the maximum or a lesser number as designed for your system. The number of concurrent transfers as well as the device status can be checked once the system is configured in Resource Monitor of the GV STRATUS Control Panel.
User Name	The user name to access the remote K2 Summit system. This is the internal system account, which by default is GVAdmin.
Domain	If on a domain, the domain that manages the account that accesses the remote K2 Summit system.
Update Password	The password to access the remote K2 Summit system. ***NOTE: Do not enter a domain or otherwise modify account settings except under the supervision of qualified Grass Valley Support personnel. Extensive system configuration is required to achieve a working GV STRATUS system.***
FTP Server Name	The FTP server name for the remote K2 Summit system. For the typical system where there is a separate FTP network, this is the name of the K2 SAN's FTP server with the `_he0` suffix added. The `_he0` suffix specifies the FTP network.
FTP User Account	The FTP user name for the remote K2 Summit system. This must be a valid account on the local and remote site, such as `gvservice\gvadmin`. Do not use the "movie" account.
Update FTP Password	The FTP password for the remote K2 Summit system.

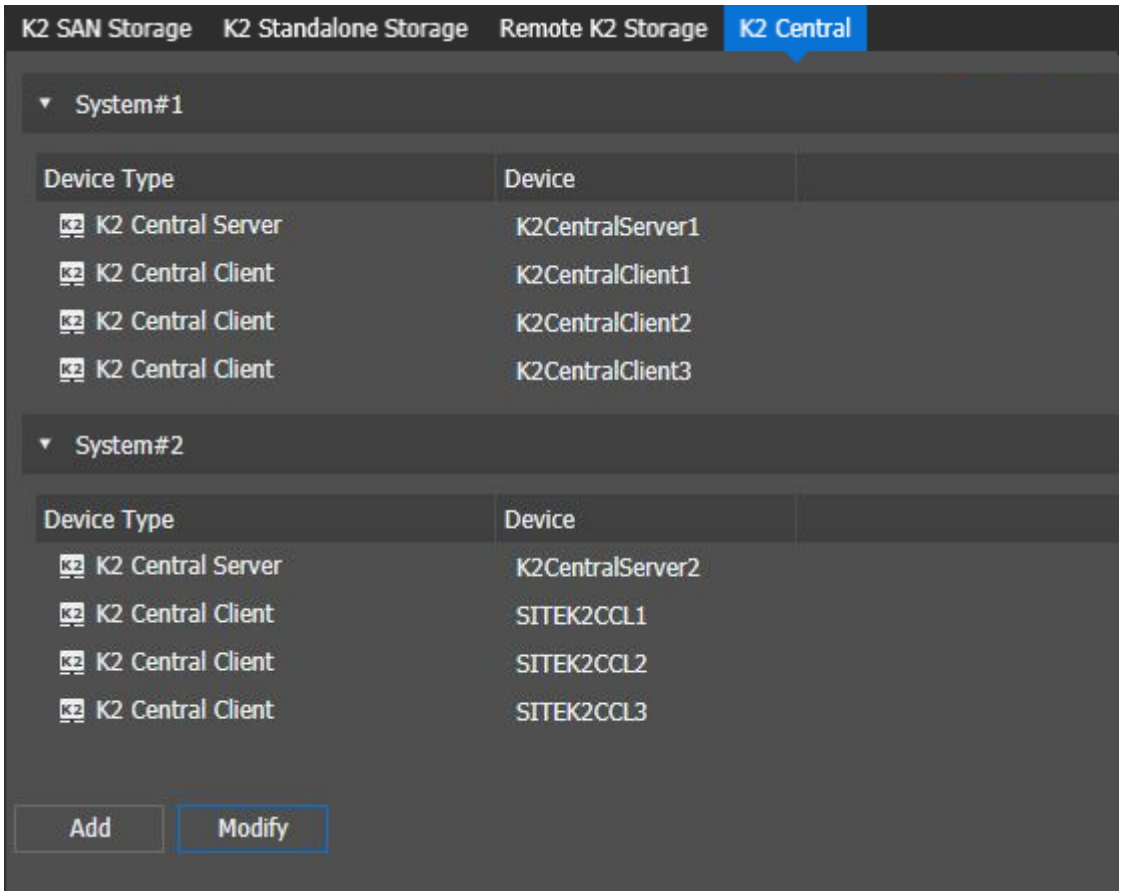
Related Topics

Remote and multiple site configuration on page 473

K2 Central settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Core | K2 Storage | K2 Central**



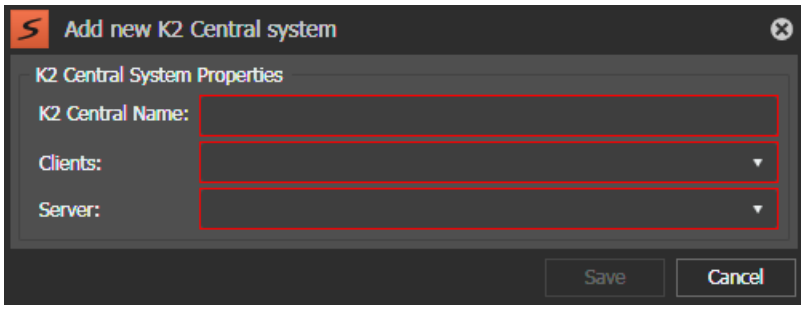
Setting or button	Description
Add	Opens the **Add new K2 Central system** dialog box for you to add the new K2 Central system in your operation. You can use the **Add** button repeatedly to add multiple K2 Central storage devices.
Modify	Opens the **Modify K2 Central system** dialog box to modify settings of the selected K2 Central system.

K2 Central Add/Modify settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Core | K2 Storage | K2 Central | Add** or **Modify**

***NOTE: It is required that any K2 config files be deleted, and services restarted on the GV STRATUS core server, if originally K2 Central devices had been manually added to these files before configuring K2 Central systems in the* GV STRATUS Control Panel.**



Setting	Description
K2 Central Name	The name of the K2 Central system in your operation. The name of the K2 Central system must not be empty and cannot be a duplicate of an already existing K2 Central system.
Clients	Select K2 Summit clients from the drop-down list for your K2 Central system. ***NOTE: Only 1 to 5 clients can be selected for any one K2 Central system.***
Server	The name of the K2 Central server in your system. A K2 Central server must be available and already configured in the Grass Valley Media Server MDI SAN settings.

Related Topics

GV STRATUS Control Panel configuration for K2 Central on page 937

Proxy Config settings

These settings are required on all GV STRATUS systems.

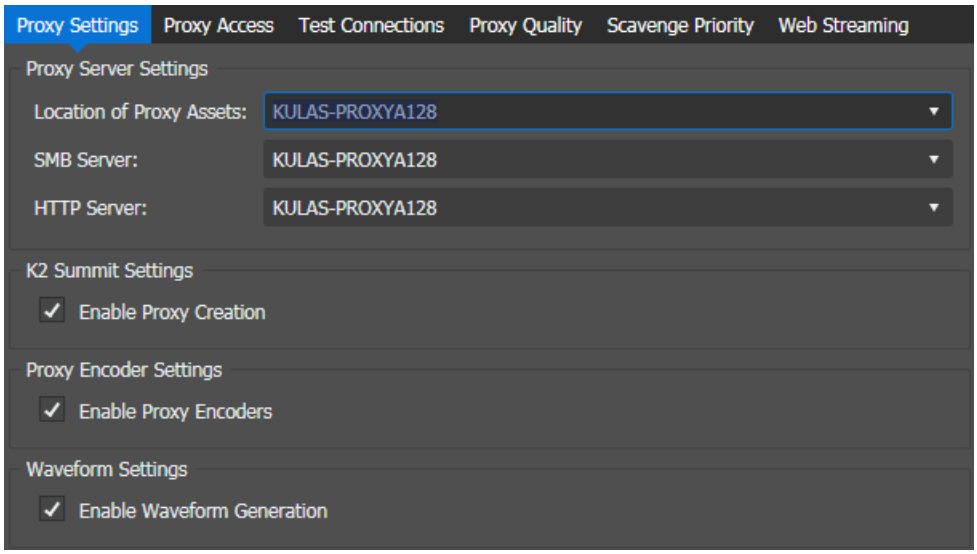
If you received your system pre-configured from Grass Valley, your Proxy Config settings are already configured so you can skip these tasks. Otherwise, work through this section sequentially to configure your Proxy Config settings.

Access these settings in the GV STRATUS Control Panel application.

Proxy Settings

These settings are required on all GV STRATUS systems.

To locate these settings, click **Core | Proxy Config.**



Setting or button	Description
Location of Proxy Assets	The name of the system that stores proxy files generated by K2 Summit and GV STRATUS systems, as follows: • For proxy stored on the GV STRATUS Lite PC, this is the network name of the GV STRATUS Lite PC. • For proxy stored on the GV STRATUS Express server, this is the network name of the server with role GV STRATUS Core Server Express, as configured in SiteConfig. • For proxy stored on the K2 SAN (A1), this is the name of the K2 SAN, as named in K2Config. • For proxy stored on the dedicated Proxy Storage system (B1, C1), this is the name of the Proxy Storage system, as named in K2Config.
SMB Server	The network machine name of the device hosting the server to which proxy files are written, as follows: • For proxy stored on the GV STRATUS Lite PC, this is the network name of the GV STRATUS Lite PC. • For proxy stored on the GV STRATUS Express server, this is the network name of the server with role GV STRATUS Core Server Express, as configured in SiteConfig. • For proxy stored on the K2 SAN (A1), this is the network name of the GV STRATUS Proxy server attached to the K2 SAN, as configured in K2Config. • For proxy stored on the dedicated Proxy Storage system (B1, C1), this is the network name of the GV STRATUS Proxy Storage file system server, as configured in K2Config.
HTTP Server	The network machine name of the device hosting the server from which GV STRATUS clients read proxy files. Typically the SMB Server and the HTTP Server are hosted by the same device.

Setting or button	Description
K2 Summit Settings: Enable Proxy Creation	Centralizes the location of proxy storage based on the Proxy Server Settings.
Proxy Encoder Settings: Enable Proxy Encoders	Enables or disables the automatic creation of proxy for high resolution clips. Does not affect the ability to manually create proxy from within the GV STRATUS application for a high resolution clip. Applies only to GV STRATUS systems with Render Engines that are properly configured and licensed.
Waveform Settings: Enable Waveform Generation	Enables or disables the creation of waveform cache (*.ewc2) files together with proxy files for the use in EDIUS application. This setting is enabled by default. Deselect the check-box if you do not want waveform cache files to be generated with proxy files.

Related Topics

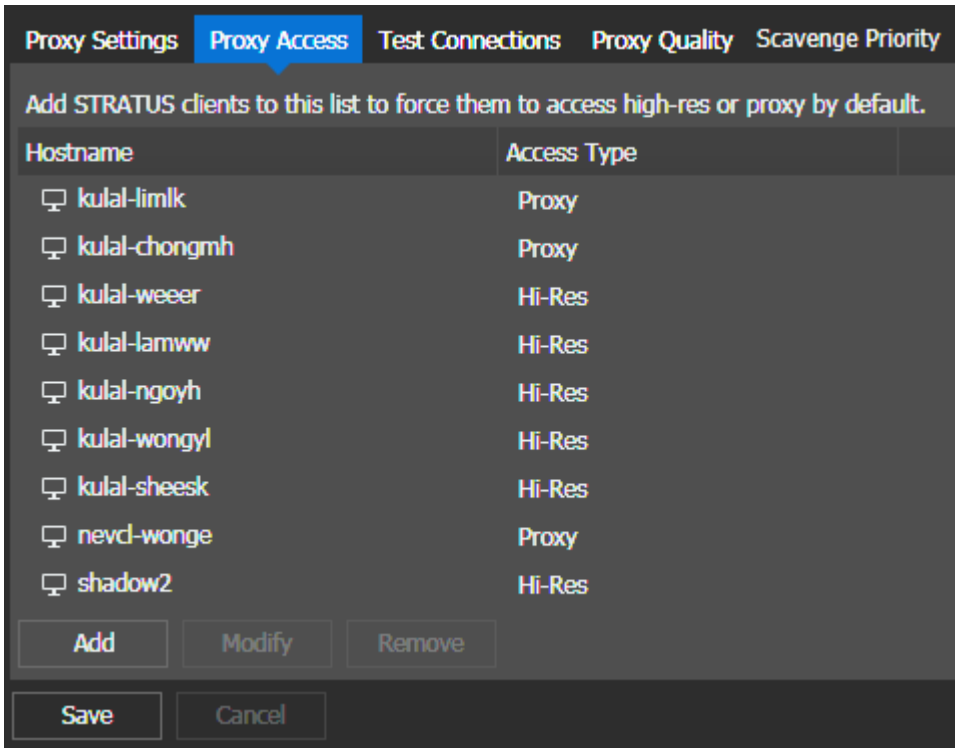
Configuring Proxy Config settings: Required on page 788
Custom Metadata settings on page 318
HTTP server overview on page 226
CIFS storage configuration

Proxy Access settings

These settings are required on all GV STRATUS systems.

These settings specify the GV STRATUS client PCs that use a high-resolution media workflow, rather than a proxy media workflow. By default, the GV STRATUS application and the EDIUS XS application access low-resolution live streaming and proxy media. If the PC is set to high-resolution in GV STRATUS Control Panel Proxy Access settings, the GV STRATUS application accesses high-resolution media. This also requires a high-resolution license.

To locate these settings, click **Core | Proxy Config | Proxy Access.**



Setting or button	Description
Add	Opens the Add Host Proxy Access dialog box.
Modify	Opens the Modify Host Proxy Access dialog box for the selected client.
Remove	Removes the selected client.

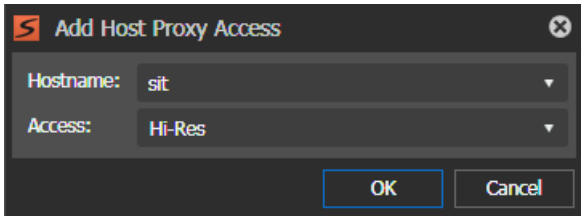
Related Topics

Set up RMI PC access to high-resolution assets on page 557
RMI settings on page 396
Set GV STRATUS client PC to high-resolution on page 293

Host Proxy Access Add/Modify settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Core | Proxy Config | Proxy Access | Add** or **Modify**

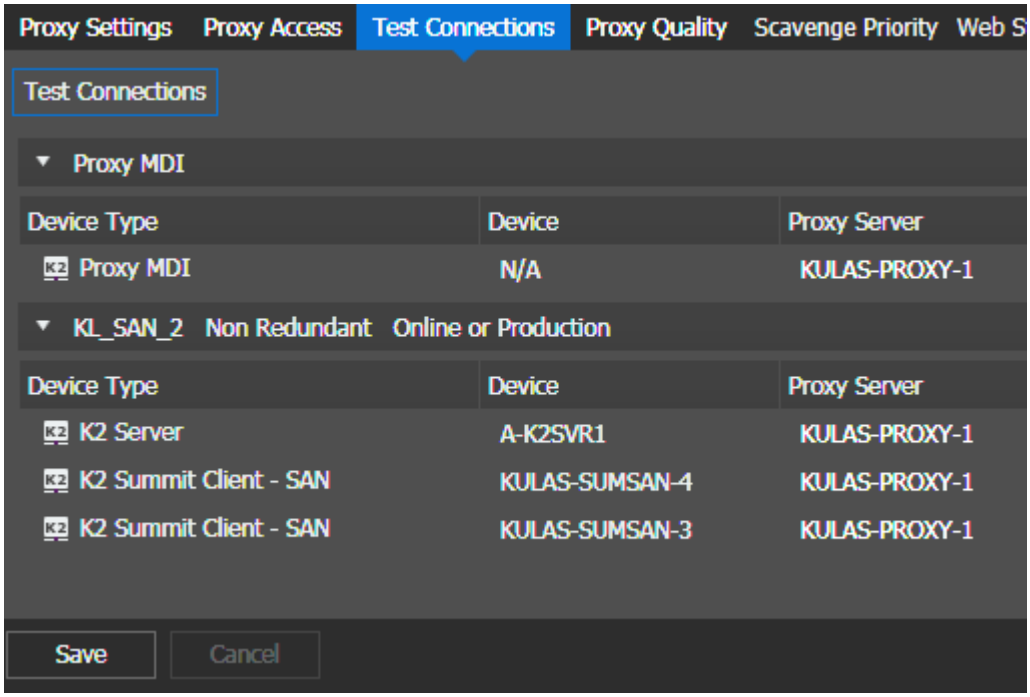


Setting or button	Description
Hostname	The network name of the client device.
Access	Sets the type of access for the client device.

Test Connections settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Core | Proxy Config | Test Connections**



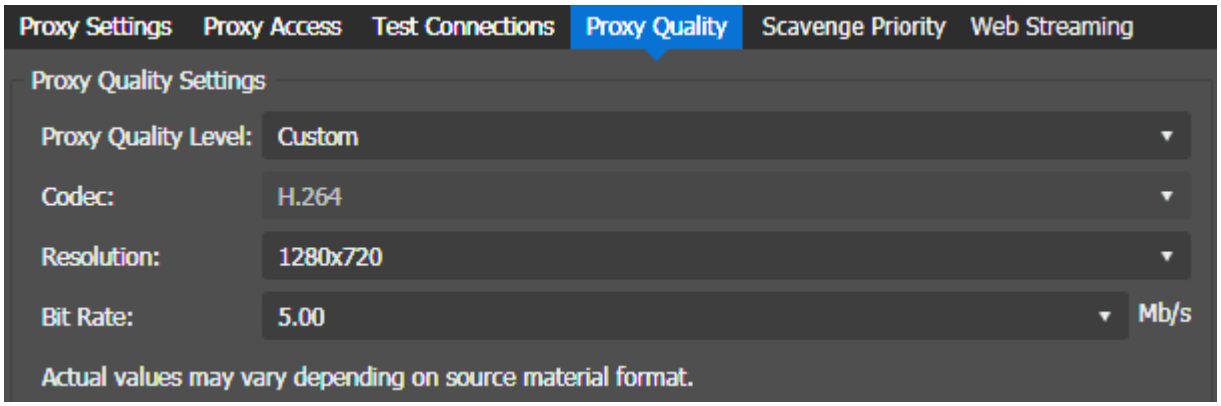
1. Click the **Test Connections** button. The system repopulates device connections in GV STRATUS application.
2. Verify that the list is correct and all devices are connected.

Proxy Quality settings

These settings are optional on all GV STRATUS systems.

These settings specify the quality of the proxy assets created by the GV STRATUS Render Engine. These settings do not affect proxy assets created by K2 Summit systems.

To locate these settings, click **Core | Proxy Config | Proxy Quality.**



Setting or button	Description
Proxy Quality Level	Sets the quality to Low, Medium, High, or Custom. Sets to Low by default. The **Custom** option lets users customize the resolution and bit rate of proxies. Consider proxy storage capacity, network bandwidth, and proxy creation speed. Increasing quality can impact system performance.
Codec, Resolution, Bitrate	Automatically configured, based on **Proxy Quality Level** setting. Values are displayed but cannot be changed. If the **Custom** proxy quality level is selected, you can configure the resolution and bit rate values.
Save	Saves current settings.
Cancel	Returns settings to their last saved state.

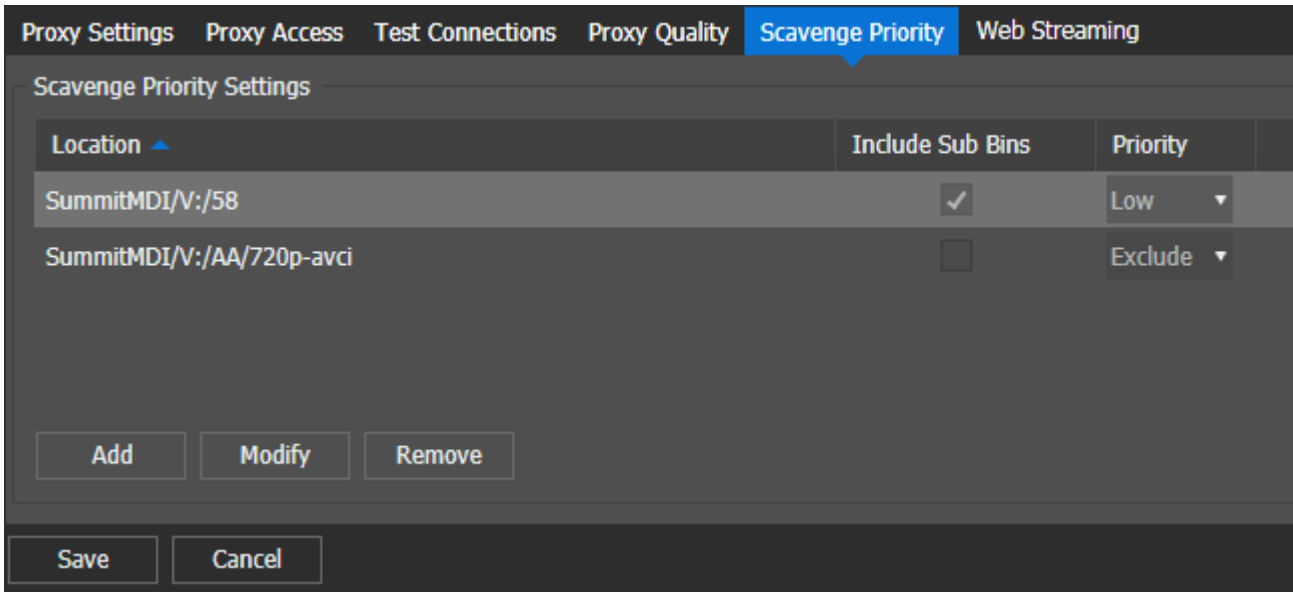
***NOTE: You must restart the GV STRATUS application each time you change proxy quality settings in the* GV STRATUS Control Panel.**

Scavenge Priority settings

These settings are optional on GV STRATUS systems.

These settings enable proxy scavenging based on device and/or location. Each location has an option to include sub bins and set the scavenge job priority. If an asset matches multiple location rules, the most specific location will be processed for the asset. You can also set specific locations to be excluded from proxy scavenging and no proxy will be generated for assets in those specified bins.

To locate these settings, click **Core | Proxy Config | Scavenge Priority.**

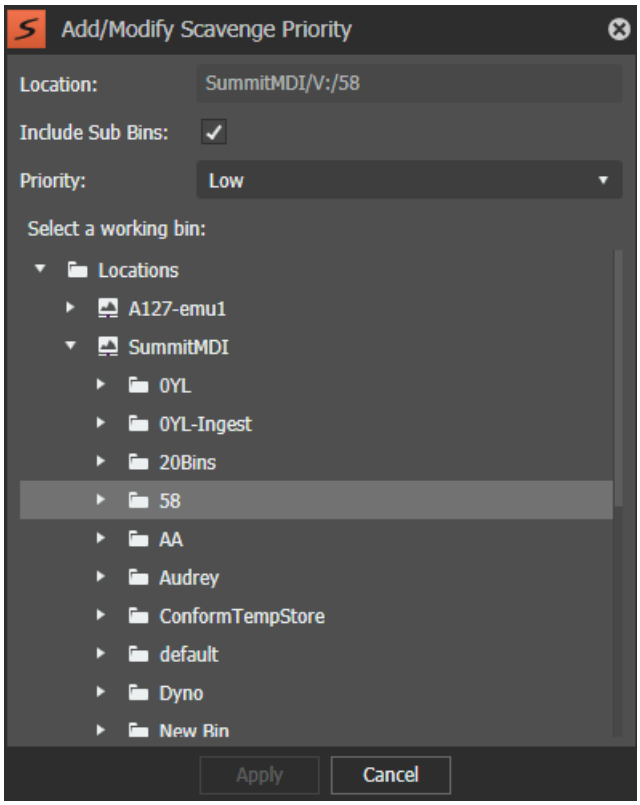


Setting or button	Description
Add	Opens the Add Scavenge Priority dialog box.
Modify	Opens the Modify Scavenge Priority dialog box for the selected location.
Remove	Removes the selected location.
Save	Saves the current settings.
Cancel	Discards any new settings and reverts to the last saved settings.

Scavenge Priority Add/Modify settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **General | Locations Config | Scavenge Priority | Add** or **Modify**



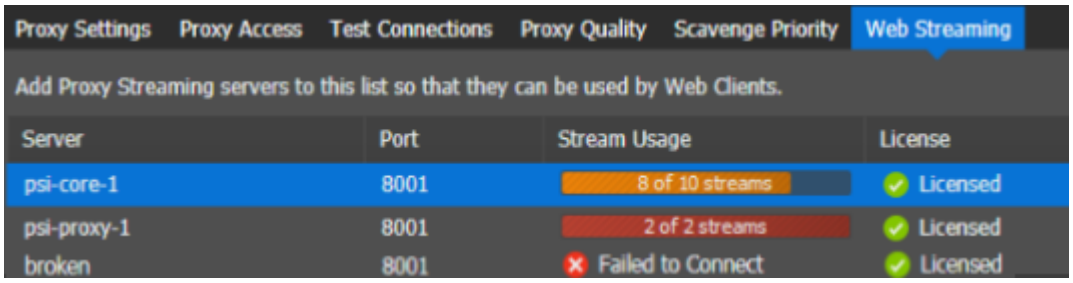
Setting or button	Description
Location	The location of proxy scavenge priority that is set in the GV STRATUS system.
Include Sub Bins	When selected, the proxy scavenge process includes sub bins of the specified location.
Priority	Specifies the scavenge priority to **High**, **Normal**, **Low**, or select **Exclude** to not generate proxy for assets in the specified location.
Select a working bin	The bin on the selected K2 system to which assets are set with the proxy scavenge priority.

Web Streaming settings

These settings are optional on GV STRATUS systems.

These settings enable the addition of proxy streaming servers to be used by GV STRATUS Web Clients. If there are more than one proxy streaming servers configured in this settings, the Web Client goes through the list randomly when initiating a connection. You can also set the port number for each proxy streaming server.

To locate these settings, click **Core | Proxy Config | Web Streaming**



Setting or button	Description
Add	Opens the Add Proxy Streaming Server dialog box.
Modify	Opens the Modify Proxy Streaming Server dialog box for the selected server.
Configure	Allows you to configure the maximum number of stream usage and add the SSL certificate for secure connection of web streams. Select the **Configure** button and select either **Set Certificate** or **Set Max Streams**. ***NOTE: The maximum stream count is up to 40 web streams per server.***
Remove	Removes the selected server.
Save	Saves the current settings.
Cancel	Discards any new settings and reverts to the last saved settings.

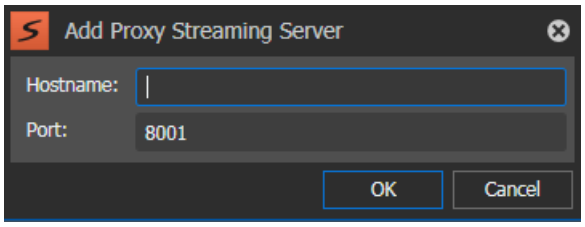
When the core services are initially installed they automatically generate a type of certificate called a “self-signed” certificate. This certificate offers basic encryption capabilities, but cannot be used to verify the server. By default browsers do no trust self-signed certificates as they can be created by anyone and offer no protection against imposters and middle-man attacks.

In order for the browser to trust the server and begin an HTTPS connection, it needs to validate a certificate. These certificates must come from a known organization called a certificate authority – one that the browser trusts to verify the server is who it says it is.

Web Streaming Add/Modify settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Core | Proxy Config | Web Streaming | Add** or **Modify**



Setting or button	Description
Hostname	The name of the proxy streaming server to be used by GV STRATUS Web Clients in your system.

Setting or button	Description
Port	Specifies the port number for the proxy streaming server. These ports are supported as below: • **8001** — This port is used for a specialized service for the transport of proxy streaming requests by the Proxy Streaming Gateway Service. By default, the service opens port 8001 for HTTP traffic. If the base port number is configured, this will be used as the HTTP port number. • **8002** — This port is used for a secure service for the transport of proxy streaming requests. The service must be configured with valid SSL certificates for browsers to successfully make use of WSS. By default, the service opens the port number incrementally after the HTTP port (e.g. if the HTTP port is 8001, the HTTPS port will be 8002). Except if the HTTP port is set to 80, the standard HTTPS will use port 443. • **8003** — This port is used by a web browser to assist with the setup of peer-peer WebRTC connections in complex network scenarios. By default, the service opens the port number incrementally after the HTTPS port (e.g. typically 8003). Except if the HTTP port is configured as 80, the standard STUN port of 3478 will be used.

Resource Management settings

These settings apply to all GV STRATUS systems.

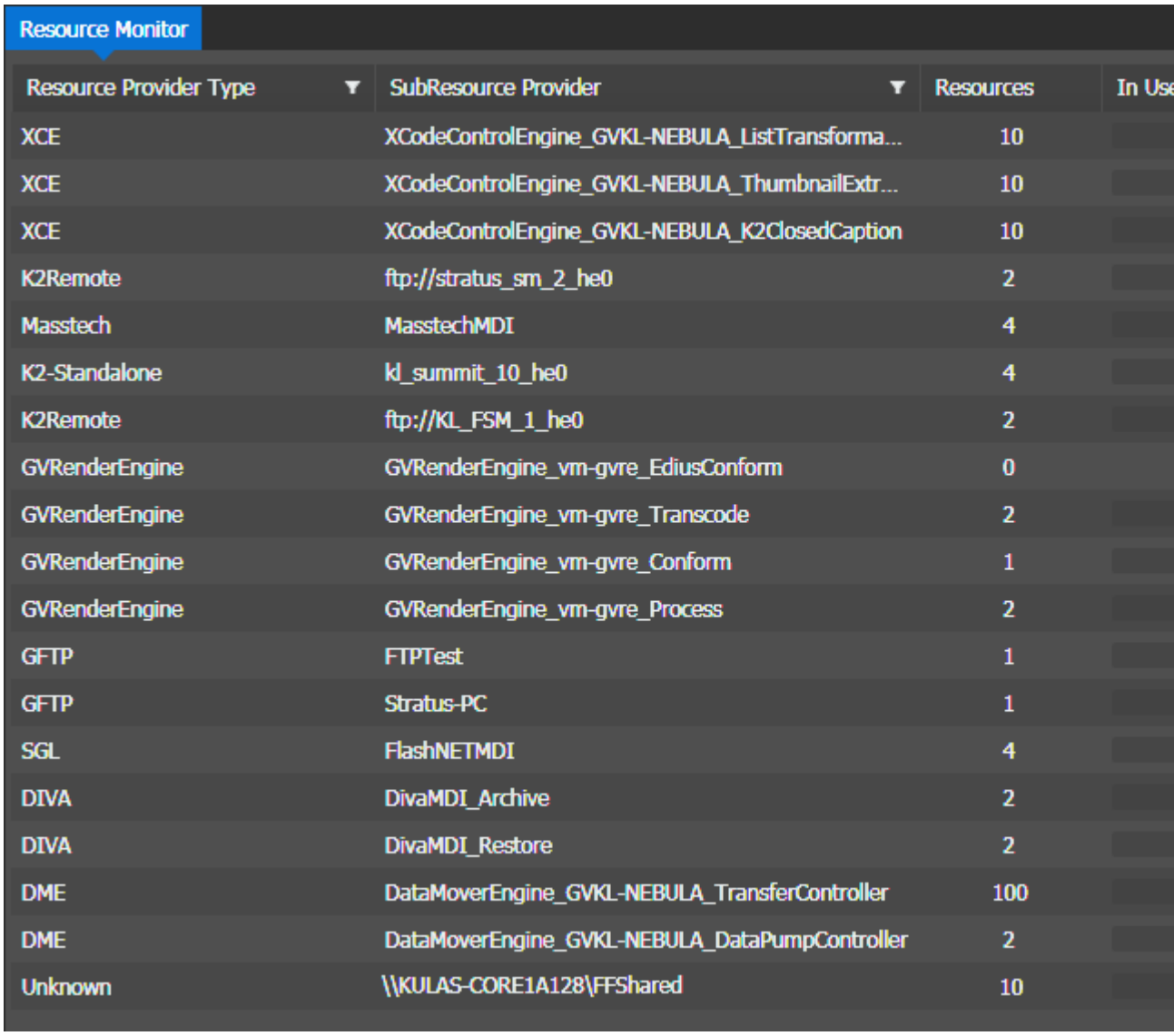
The Resource Monitor displays the name and type of Resource Providers and SubResource Providers, the amount of available resources, the number of resources in use, the online status, and enabled status of all resources. The Resource Monitor display refreshes every 60 seconds, but a **Refresh** button is also available for you to trigger the refresh manually.

The number of available resources can be configured within the individual MDI, Render Engine, DataMover Engine, and Xcode Control Engine settings in the GV STRATUS Control Panel. For GV Render Engine, the maximum number of resources for conform, proxy creation, EDIUS jobs, and total concurrent jobs can be configured by selecting **Core | Engines | Render Engine | Modify**. For unmanaged resources with connections via SMB or FTP protocol, the Resource Provider Type displays as **Unknown** on the Resource Monitor. The default is set to 10 for unmanaged resources, but you can configure up to 50 resources via right-click and select **Set Resource Count** for unmanaged resources with huge bandwidth. For unmanaged resources with smaller bandwidth, you can configure the **Set Resource Count** setting to one (1) or two (2) in the Resource Monitor.

The "In Use" status is updated whenever a resource is utilized. Usually all devices are “Online” and the status can be viewed in the Resource Monitor. In case a device is “Offline”, the administrator should investigate and set the device online again. The reason why a resource is "Offline" might be one of the following: an engine was stopped, a Windows Service was stopped, the MDI was not properly configured, or the network connectivity is interrupted.

Access these settings in the GV STRATUS Control Panel application.

To locate these settings, click **Core | Resource Management | Resource Monitor**.



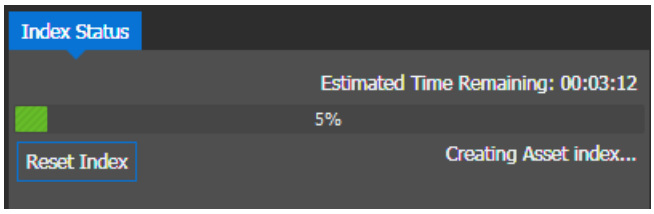
Setting or button	Description
Refresh	Updates resource status of all listed resources instantly in the **Resource Monitor** when the button is pressed.

Search Index Config settings

These settings apply to all GV STRATUS systems, but use only as advised by Grass Valley.

Access these settings in the GV STRATUS Control Panel application.

To locate these settings, click **Core | Search Index Config.** .



Setting or button	Description
Reset Index	Recreates all GV STRATUS search indexes. This can take several hours, depending on the size of your GV STRATUS database. The progress bar does not only show the progress of recreating search indexes, but also displays the progress of index updates. ***NOTE: Once the progress bar reached 100% to mark the completion of recreating asset indexes, the progress bar will return to 0% to indicate the on-going process of index updates.*** Under normal operating conditions resetting the index is not necessary. Use only as advised by Grass Valley.

Audio Tag Management settings

These settings are optional on GV STRATUS systems.

You can configure audio profiles by assigning tags to each audio channel in the **Profiles** setting. Audio tags can be created and customized in the **Audio Tags** setting.

You can view or assign audio tags to assets via the **Audio Tags** tab in the Inspector panel. Audio tags are only configurable if you have the Media Manager role or assigned with the Write permission for Audio Tags in **Core | Metadata | Permissions**.

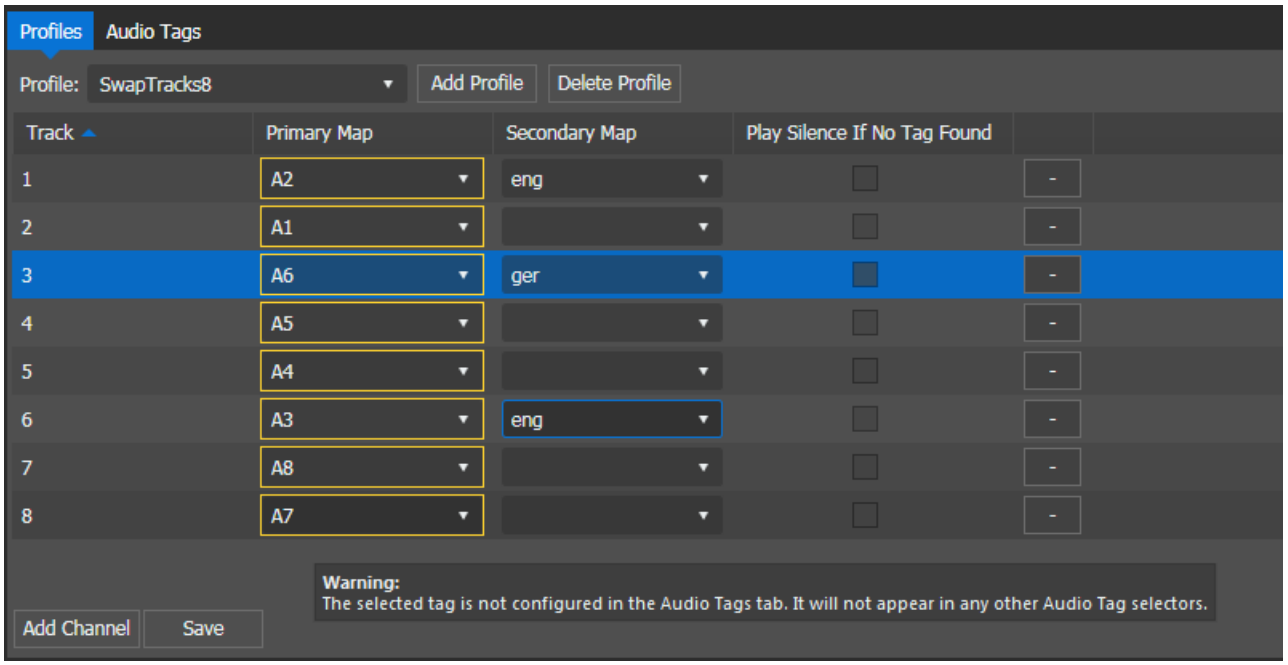
To locate these settings, click **General | Audio Tag Management**

Profiles settings

These settings are optional on GV STRATUS systems.

Audio mapping profiles are used for the Rules Engine and K2 FTP sessions.

To locate these settings, click **General | Audio Tag Management | Profiles**



Setting or button	Description
Profile	Provides the list of configured audio profiles. Profiles can be configured for single audio channels or stereo channels. ***NOTE: Audio groups of three or more channels are currently not supported.***
Add Profile	Opens the New Profile dialog to create and name a new audio profile.
Add Channel	Launches a new row to map audio tag settings for the audio track.
Track	Adds a track number sequentially each time an audio channel is added.
Primary Map	Lists all available audio tags to be mapped as the primary audio. Audio channels can be mapped by name as well as by the input number. Combo boxes in this setting are editable to allow you to enter values (such as audio input numbers) that are not configured in the Audio Tags tab. If no audio tags have been specified, audio tracks can be mapped via the input number as A1, A2, etc. (for Mono) or A1/2, A3/4, etc. (for Stereo). ***NOTE: A yellow outline displays around the combo box and a warning tooltip appears if the entered value is not in the Audio Tags tab.***

Setting or button	Description
Secondary Map	Lists all available audio tags to be mapped as the secondary audio. Audio channels can be mapped by name as well as by input number. Combo boxes in this setting are editable to allow you to enter values (such as audio input numbers) that are not configured in the Audio Tags tab. The Secondary Map, if configured, determines how audio channels in the Primary Map are grouped, either Mono or Stereo. ***NOTE: A yellow outline displays around the combo box and a warning tooltip appears if the entered value is not in the Audio Tags tab.***
Play Silence If No Tag Found	Mutes the channel when no audio tag is found, if this check box is selected. **The Play Silence If No Tag Found** option must match the grouping pattern set by the Secondary Map as well. (e.g.: You cannot have mismatched check boxes for a Stereo pair.)
-	Removes a track from the audio mapping profile.
Delete Profile	Deletes the selected audio mapping profile.
Save	Saves the audio mapping profile.

Once saved, an audio mapping XML file is created and sent to K2 Summit to this location: `C:\profile\config`.

You can also find the audio mapping XML file in the GV STRATUS Core Server at this location: `C:\ProgramData\Grass Valley\ConfigurationDataFiles\Audio Mapping`

NOTE: GV STRATUS does not support simultaneous use of separate Control Panel instances. When another user hits the save button, the source of record and all copies are overwritten. This can lead to lost audio mapping data of the previous user.

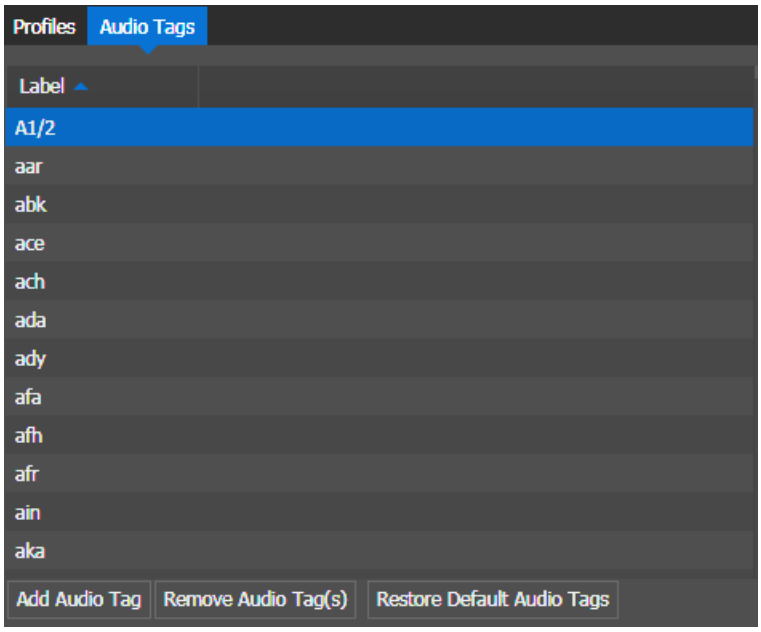
For K2 Central servers, you must start the GV STRATUS K2 Configuration Service manually if the audio mapping file does not exist in K2 Central at this location: `C:\profile\config`

Audio Tags settings

These settings are optional on GV STRATUS systems.

You can create, customize, and remove audio tags in this settings. You can also restore default audio tags, if needed.

To locate these settings, click **General | Audio Tag Management | Audio Tags**



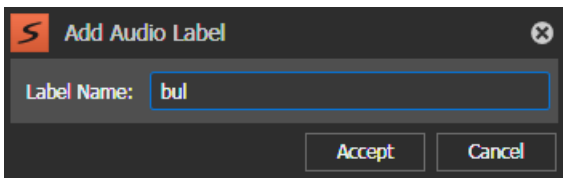
Setting or button	Description
Label	List of label name for Audio Tags.
Add Audio Tag	Opens the Add Audio Label dialog box to create a new audio tag.
Remove Audio Tag(s)	Opens the Remove Tag(s) dialog box to confirm the removal of the selected audio tag.
Restore Default Audio Tags	Restores default audio tags into the Audio Tags list. ***NOTE: Existing assets persist with customized audio tags when already assigned in the* GV STRATUS *application, even after default audio tags are restored in this setting.***

NOTE:* GV STRATUS *applications must be restarted for any changes in the Audio Tag Management settings to be available in the system.

Audio Tag Add/Modify settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **General | Audio Tag Management | Audio Tags | Add Audio Tag**



Setting or button	Description
Label Name	Name of an Audio Label to be added into the Audio Tags setting. ***NOTE: A yellow outline displays if the Label Name does not conform to the ISO639-2 standard. Otherwise, the Label Name field has a blue outline.***
Accept	Adds the new Audio Label into the list of Audio Tags. ***NOTE: The* GV STRATUS *application must be restarted for new audio tags to be available in the system.***
Cancel	Cancels the process and closes the Add Audio Label dialog.

Channels settings

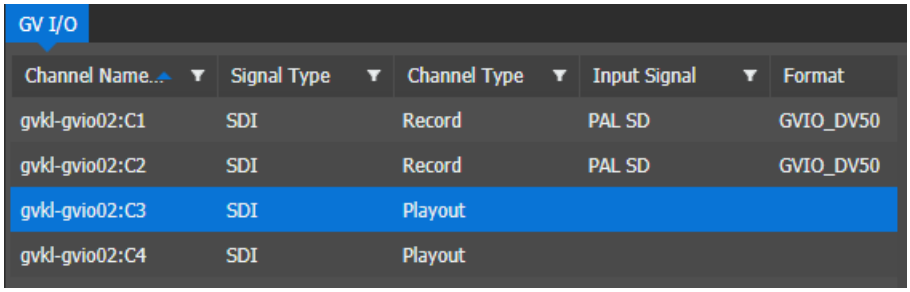
Channels settings let you configure channel formats and audio tracks for the GV I/O Live Ingest & Playback Servers.

To locate these settings, click **General | Channels**

GV I/O settings

These settings are optional on GV STRATUS systems, and only applicable to the GV I/O Live Ingest and Playback Server.

To locate these settings, click **General | Channels | GV I/O**



On the **GV I/O** tab, each row represents a channel of the GV I/O Live Ingest and Playback Server. These channels can either be used to ingest or playback clips in the GV STRATUS system.

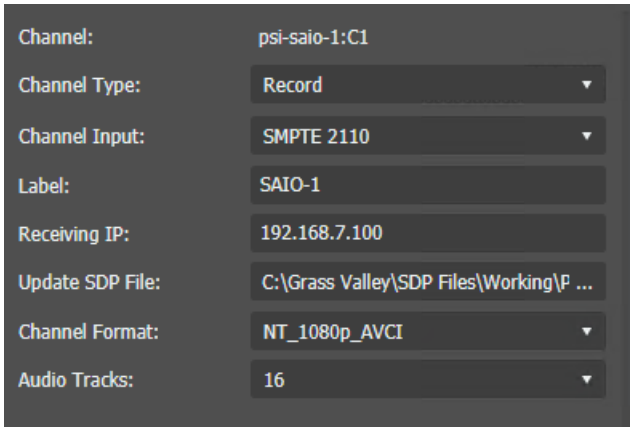
Setting or button	Description
Channel Name	The name of the channel as configured in the GV I/O Live Ingest and Playback Server. The channel name can only be edited or changed in the GV I/O Live Ingest and Playback Server.
Signal Type	The GV I/O Input signal type selected for the channel. Available inputs depend on sources configured in your system such as SDI, SMPTE 2110, SMPTE 2022-6, and Web Stream. ***NOTE: Only SDI signal type is supported for Playout.***

Setting or button	Description
Channel Type	The channel type that can be configured is either **Record** or **Playout** on the GV I/O Live Ingest and Playback Server.
Input Signal	The input signal connected to the channel as configured in the GV I/O Live Ingest and Playback Server. The input signal can only be changed at the GV I/O Live Ingest and Playback Server.
Format	The format of assets supported as configured in Format settings of GV STRATUS Control Panel.
Save	Saves the current configuration of the selected channel.

GV I/O Record Channel settings

These settings are optional on GV STRATUS systems, and only applicable to GV I/O record channels.

To locate these settings, click **General | Channels | GV I/O** and select a channel type configured to **Record**.



Setting or button	Description
Channel	The channel name as configured in the GV I/O Live Ingest and Playback Server.
Channel Type	The Channel Type selected is **Record** for the GV I/O Live Ingest and Playback Server. ***NOTE: The* GV STRATUS *desktop application needs to be restarted after changing a GV I/O channel type from Playout to Record or from Record to Playout in order to see updated configuration options in the Channel Panel tool.***

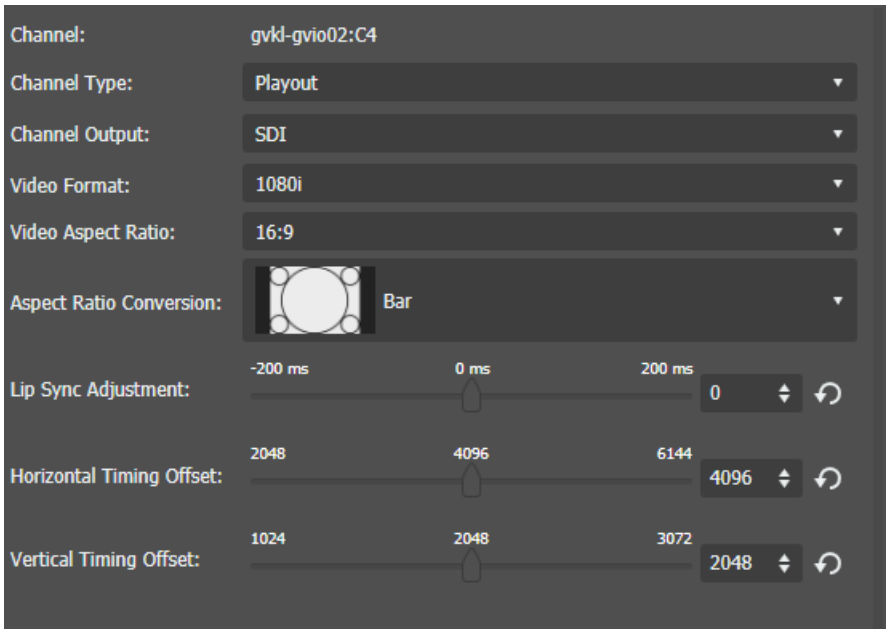
Setting or button	Description
Channel Input	Input signal that has been connected to the channel at the GV I/O Live Ingest and Playback Server. Available input signals are in the list below: • **SDI** - Allows the channel to use the hardwired AJA SDI input. Requires the GVIO-SVR-SDI license. • **SMPTE 2110** - Uncompressed video over IP with Video, Audio, Anc data all on separate routable streams, and allows for .sdp import. Requires the GVIO-SVR-IP license. • **SMPTE 2022-6** - Uncompressed video over IP with Video, Audio, Anc data all of the same stream, and allows for a single rdp entry. Requires the GVIO-SVR-IP license. • **Web Stream** - Allows a Web Stream channel to record. Requires the GVIO-SVR-WEB license.
Label	Enter a name to label the channel configuration.
Receiving IP	Enter the IP address of the Ingest server.
Update SDP File	Select the location to import the SDP file from. This is only applicable to SMPTE 2110 option as it requires an import of data from a .sdp file for the GV I/O configuration. Upon updating the .sdp file and clicking **Save**, or after clicking another SMPTE 2110 channel, the field becomes blank and does not display the existing SDP file configuration. ***NOTE: If you changed a channel input to SMPTE 2110 from either SDI, SMPTE 2022-6, or Web Stream, after previously saving a different SMPTE 2110 channel, you must set the SDP file for the current channel before saving your settings. If not, the channel will be configured with an incorrect SDP file from another SMPTE 2110 channel.***
IP Stream / Web Stream	If already configured with an IP Stream, the current IP value from K2 Summit will be populated.
Channel Format	Select a format for the channel from the drop-down list. Available formats are as configured in Format settings in the GV STRATUS Control Panel.
Audio Tracks	Select the number of audio tracks supported for recordings via the channel. You can select up to 16 audio tracks for each channel.

Click **Save** to save the current settings. If you click **Revert**, the application discards any new settings and reverts to the last saved settings.

GV I/O Playout Channel settings

These settings are optional on GV STRATUS systems, and only applicable to GV I/O playout channels.

To locate these settings, click **General | Channels | GV I/O** and select a channel type configured to **Playout**.



Setting or button	Description
Channel	The channel name as configured in the GV I/O Live Ingest and Playback Server.
Channel Type	The Channel Type selected is **Playout** for the GV I/O Live Ingest and Playback Server. ***NOTE: The* GV STRATUS *desktop application needs to be restarted after changing a GV I/O channel type from Playout to Record or from Record to Playout in order to see updated configuration options in the Channel Panel tool.***
Channel Output	Output signal type for the selected channel of the GV I/O Live Ingest and Playback Server. • **SDI** - Allows the channel to use the hardwired AJA SDI output. Requires the GVIO-SVR-SDI license. • **Unassigned** - No other settings are configurable when this option is selected.
Video Format	Select a format of 480i (NTSC), 576i (PAL), 720p, 1080i, or 1080p.
Video Aspect Ratio	Select an available aspect ratio of either 4:3 or 16:9. The default aspect ratio is set to 16:9. Only the 16:9 aspect ratio is available if HD video format is selected.
Aspect Ratio Conversion	Select an aspect ratio conversion for the playout channel from the list below: • Bar • Half Bar • Crop • Stretch

Setting or button	Description
Lip Sync Adjustment	Move the slider bar between -200ms to +200ms to adjust the lip sync of clip audio relative to the video rendering during playout. You can also enter a value manually or click the **Revert to Default** button to load the default value.
Horizontal Timing Offset	Move the slider bar to adjust the horizontal timing of the SDI signal output relative to the External Sync present in the AJA card. You can also enter a value manually or click the **Revert to Default** button to load the default value.
Vertical Timing Offset	Move the slider bar to adjust the vertical timing of the SDI signal output relative to the External Sync present in the AJA card. You can also enter a value manually or click the **Revert to Default** button to load the default value.

Click **Save** to save the current settings. If you click **Revert**, the application discards any new settings and reverts to the last saved settings.

Format settings

These settings are required on all GV STRATUS systems.

Format settings let you configure video and audio settings. The GV STRATUS application uses these settings as follows:

Conform When the Render Engine conforms a complex asset, such as a GV STRATUS sequence, into a simple clip, the Format settings define the format of the simple clip.

EDIUS XS Format settings are inherited by EDIUS XS when the application is launched and a new project is created.

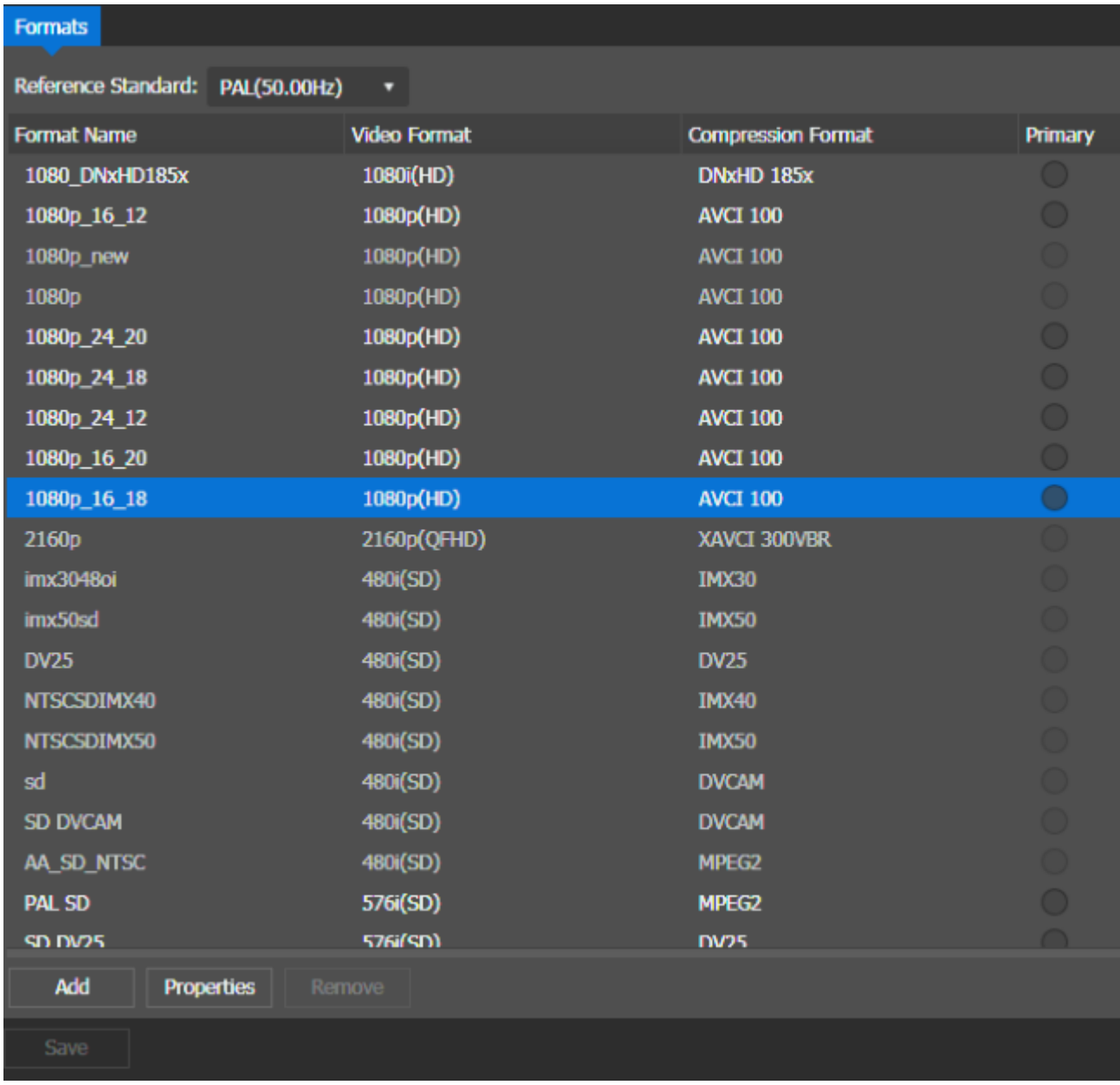
GV STRATUS Rundown Format settings define the video standard settings, such as PAL or NTSC.

GV I/O Appliance Format settings define the valid format for configured channels and ingested assets.

Storyboard and Source Viewer Format settings define the video standard, audio reference, etc.

Access these settings in the GV STRATUS Control Panel application.

To locate these settings, click **General | Format | Formats**



Setting or button	Description
Reference Standard	Sets the GV STRATUS formats available according to their Reference Standard, to match the current Reference Standard on the K2 system. Formats that do not match this setting are disabled in the list. When changing and saving this setting, a corresponding primary format must be selected.
Format Name, Video Format, Compression Format, etc	Format settings, as configured in the **Format Settings** dialog box.

Setting or button	Description
Primary	The default format for configuration. For example, when configuring a Send Destination, the primary format is set by default, but a different format can be selected if desired. ***NOTE: A primary format must be selected. Multiple primary formats are not allowed.***
Locked	Indicates if a format name can be modified. A format that is currently configured in a Send Destination displays a closed lock icon. A dialog box prompts for confirmation before a locked format name can be modified.
Add	Opens the **Format Settings** dialog box for you to add formats.
Properties	Opens the **Format Settings** dialog box for you to view properties of the selected format.
Remove	Removes the selected format. The format currently selected as the primary format can not be removed.
Save	Saves the current configuration of added formats and their order.

Clicking column heads and/or arrow buttons on the right reorders the list of formats.

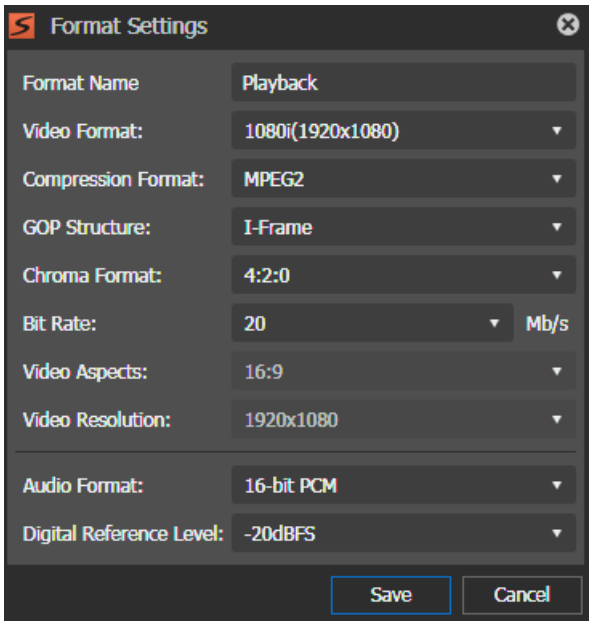
Related Topics

K2 - Send Destination settings on page 370
Send Destination Add/Modify settings on page 372
Configuring Format settings: Required

Format Add settings

These settings are required on all GV STRATUS systems.

To locate these settings, click **General | Format | Formats | Add**



Setting or button	Description
Format Name	The desired name of the video format. The name must be unique, not considering upper/lower case. The Save button is disabled if invalid characters are entered.
Video Format	The list of available video formats. The SD format available depends on the Formats Reference Standard setting.
Compression Format	The list of available compression formats.
GOP Structure	The GOP Structure setting is only enabled when the selected video format is 720p or 1080i, and the selected compression format is MPEG2.
Chroma Format	The list of available chroma formats.
Bit Rate	The list of available bit rates.
Video Aspects	The list of available video aspects.
Video Resolution	The list of available video resolutions.
Audio Format	The list of available audio formats.
Digital Reference Level	The list of available digital reference levels.

License Management settings

These settings are required on all GV STRATUS systems.

License Management settings assign the STRATUS licenses you have purchased from Grass Valley to different user groups and the roles associated with those licenses to users. Access these settings in the GV STRATUS Control Panel application.

Related Topics

About groups and users on a GV STRATUS system on page 37

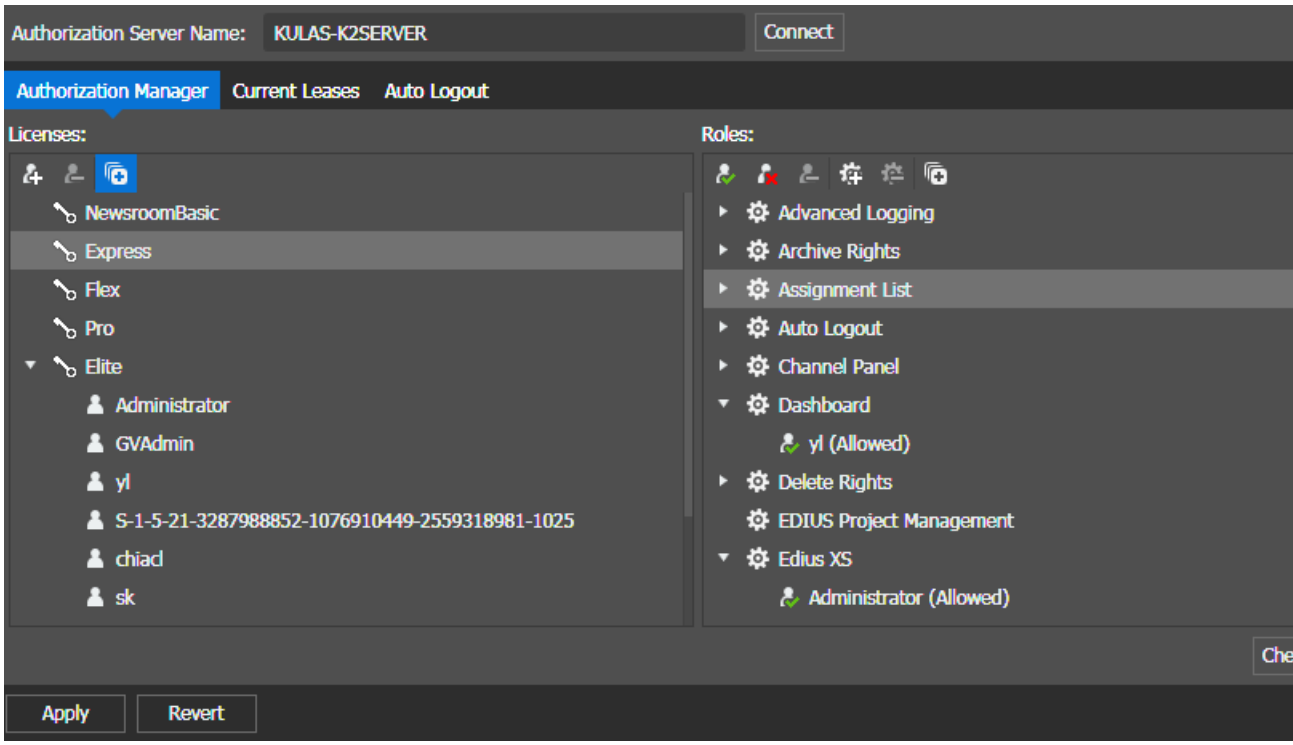
About Newsroom Basic on page 466
About Archive/Restore roles on page 465
GV STRATUS roles matrix on page 37
GV STRATUS roles matrix on page 37
Adding a custom role on page 466

Authorization Manager settings

These settings are required on all GV STRATUS systems.

If on a network Workgroup, to configure Authorization Manager settings, you must be running GV STRATUS Control Panel on the GV STRATUS Core server.

To locate these settings, click **General | License Management | Authorization Manager**



Setting or button	Description
Authorization Server Name	The name of GV STRATUS server with role of Common Services.
Connect	Connects to the GV STRATUS server and populates settings. If the Connect button is disabled, it means you are already connected.
Licenses	Settings to assign licenses to user groups. When you select a license and click **Assign**, you can use standard Windows operating system processes to assign a group to the license. This can be either Workgroup or Domain, as appropriate for your site's user accounts. When you first assign a license to a group, all users in the group are assigned all of that license's roles. These are floating license so you may over-assign. If you over-assign you must ensure that the number of licenses checked out at any one time does not exceed the number of licenses available.

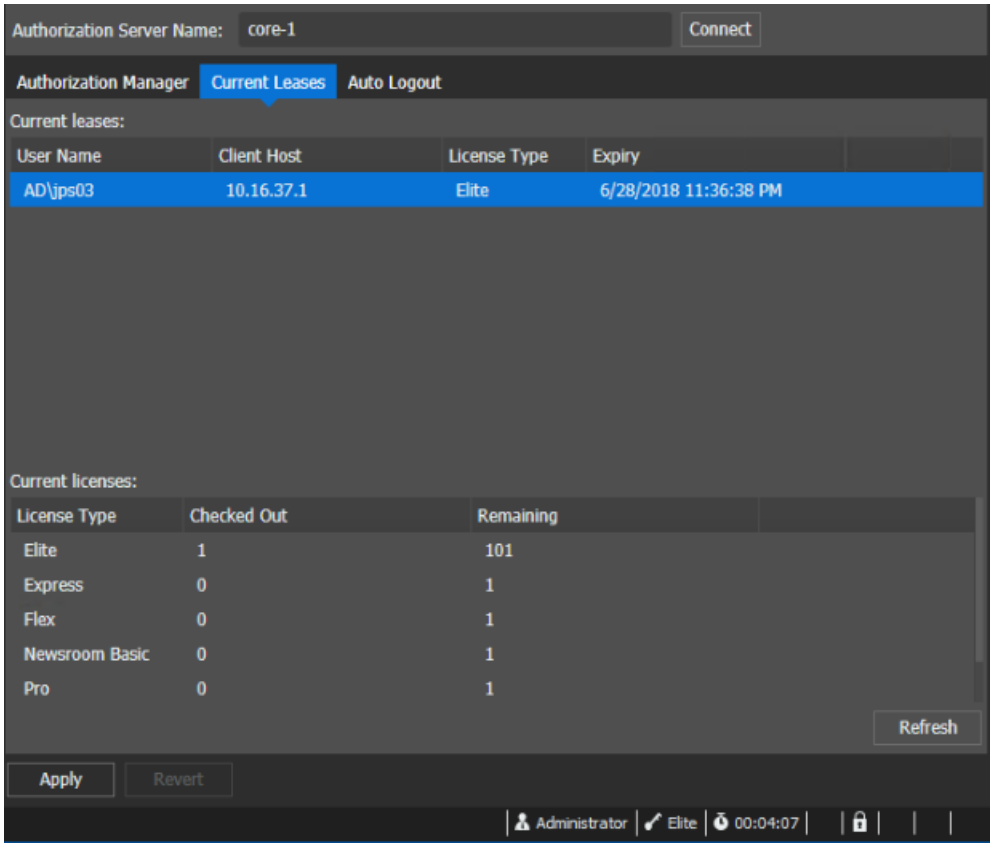
Setting or button	Description
Roles	Settings to assign tools and other functionality to users or groups. When you expand a node and select one of its groups or users, you can allow or deny the group or user the use of that operation. You can also remove the group or user from the node. If a tool is not assigned to a user, when that user logs into the GV STRATUS application, the tool does not appear in the GV STRATUS application. If a new version of GV STRATUS software adds a role to a license, make sure it is assigned correctly to existing users.
Check User	Allows you to check for the selected user or group in your Windows operating system accounts.
Apply	Saves current settings.
Revert	Returns settings to their last saved state.

Related Topics

GV STRATUS roles matrix on page 37
Adding a custom role on page 466

Current Leases settings

To locate these settings, click **General | License Management | Current Leases**



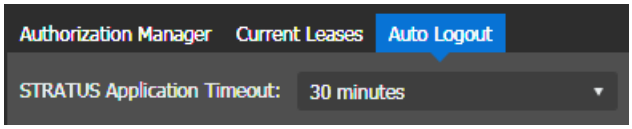
Setting or button	Description
User Name	A user with a license currently checked out. Right-click a row to revoke the lease.
Client Host	The network machine name of the system on which the user has the license checked out.
License Type	The type of license that is checked out.
Expiry	The date the license is automatically checked in, if the user has it continuously checked out until that time.
Checked Out	The number of licenses that are currently checked out.
Remaining	The number of remaining licenses that are available and not currently checked out.
Refresh	Detects licenses currently checked out and updates the tables with any new information.

Related Topics

Revoking a GV STRATUS license lease on page 471

Auto Logout settings

To locate these settings, click **General | License Management | Auto Logout**



Setting or button	Description
STRATUS Application Timeout	The length of time the PC that hosts the GV STRATUS application must sit idle, with no activity, before that PC's GV STRATUS license is released.

The auto logout process applies only to GV STRATUS user accounts with the role of Auto Logout.

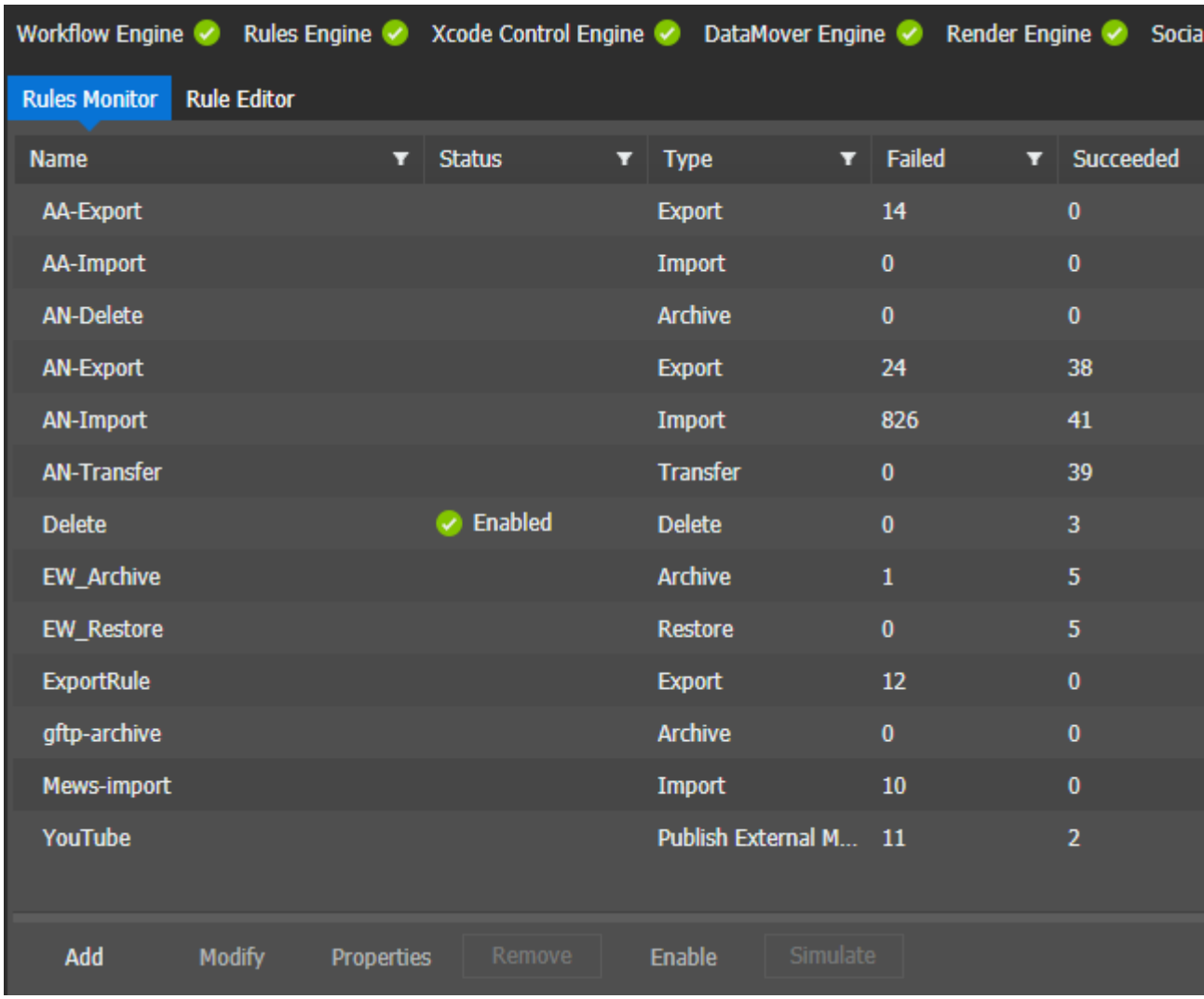
Related Topics

About Auto Logout on page 207

Rules settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **General | Rules | Rules Monitor**



Icons indicate Engine status:

- - The Engine is licensed and related rules can be enabled.
- - The Engine is not running and inaccessible, therefore related rules cannot be enabled.

Setting or button	Description
Add	Opens Rule Editor settings to create a new rule.
Modify	Opens Rule Editor settings to modify the selected rule.
Properties	Opens Rule Editor settings to view properties of the selected rule.
Remove	Removes the selected rule.
Enable/Disable	Enables or disables the selected rule.
Simulate	Simulates the selected rule to list assets affected by the rule.
Refresh	Updates the list of rules and their information.

Above settings can also be accessed via the context menu, by right-clicking on each rule or multiple rules.

You can also right-click and select **Reset Counters** from the context menu to reset values in the Failed and Succeeded columns back to zero. The reset is allowed for single and multiple rules at the same time on enabled and disabled rules.

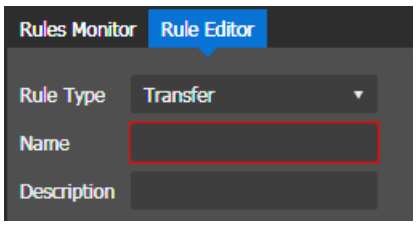
Related Topics

Configuring Rules on page 577

Rule Editor configuration settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **General | Rules Rule Editor | Add** or **Modify** or **Properties**.



Setting or button	Description
Rule Type	A list of the types of rules available to configure. Depending on the type selected, other settings are available for configuring rules.
Name	The name of the rule. This can be any text. Up to 200 characters are supported for the rule name.
Description	The description of the rule. This can be any text.

Related Topics

Configuring Rules on page 577

Locations Config settings

These settings are optional on GV STRATUS systems.

Locations Config settings configure locations that are referenced by features throughout the system, such as the destination of assets that need to be sent for playback or the destination of an export rule. Access these settings in the GV STRATUS Control Panel application.

To locate these settings, click **General | Locations Config**.

Related Topics

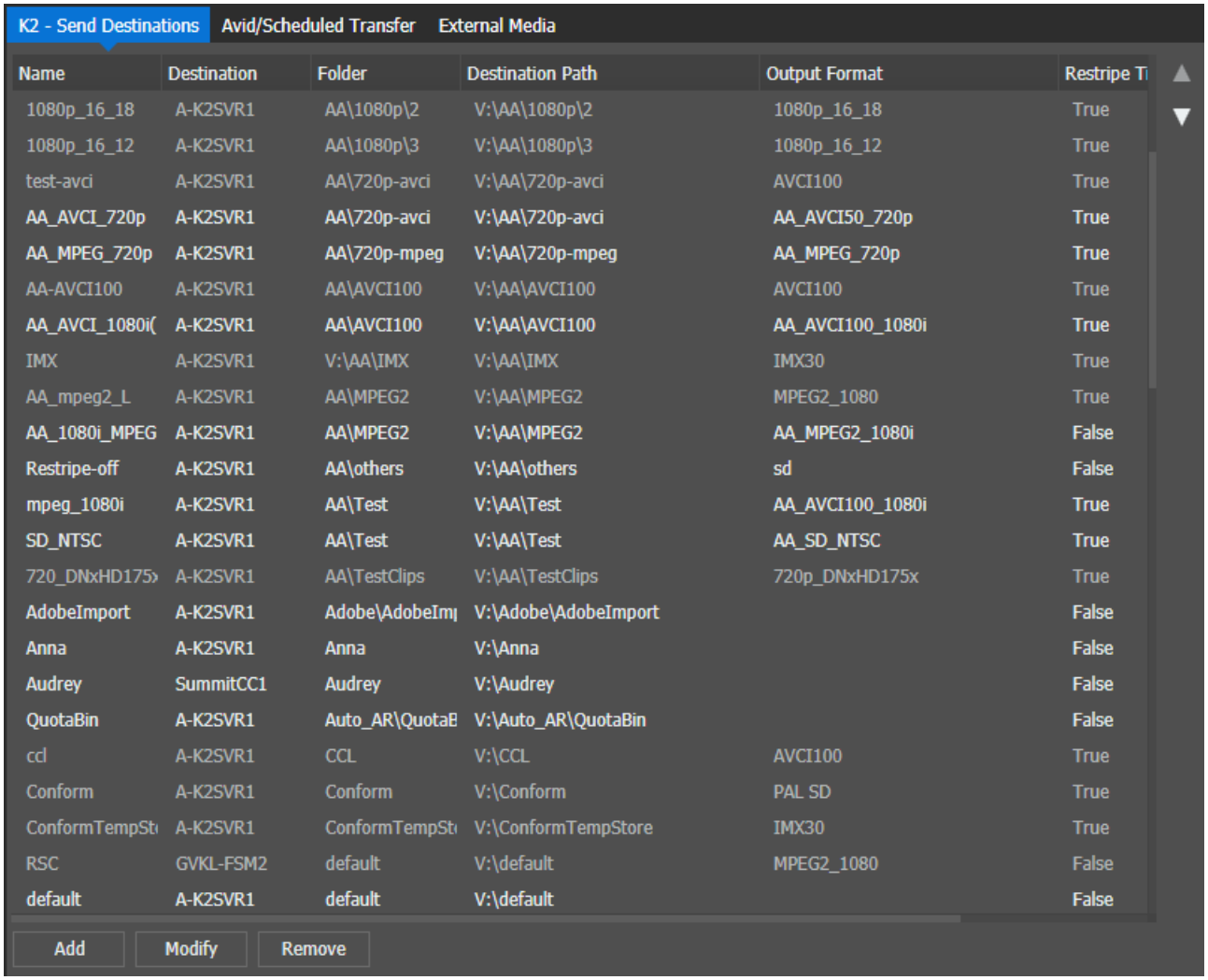
Remote and multiple site configuration on page 473

K2 - Send Destination settings

These settings are optional on GV STRATUS systems.

K2 - Send Destinations settings configure the destination of assets that need to be sent for playback. These assets will then be copied to the destination bin. Access these settings in the GV STRATUS Control Panel application.

To locate these settings, click **General | Locations Config | K2 - Send Destinations**.



Setting or button	Description
Add	Opens Send Destination Configuration dialog box
Modify	Opens the Send Destination Configuration dialog box for the selected destination. The only formats available are those compatible with the Reference Standard currently configured in Format settings.
Remove	Removes the selected destination. The only formats available are those compatible with the Reference Standard currently configured in Format settings.

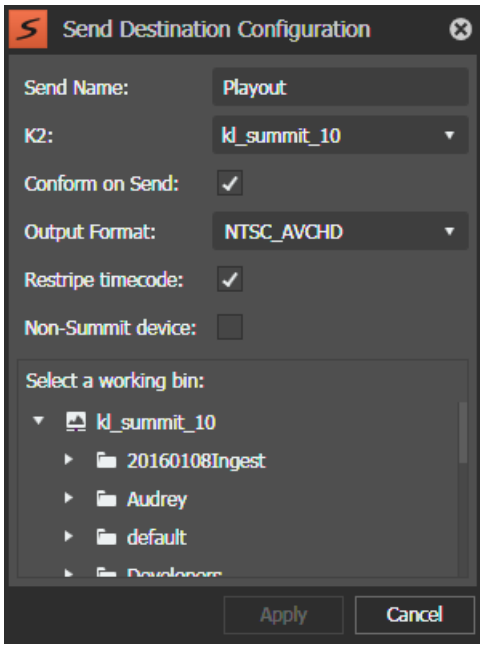
Related Topics

Format settings on page 161

Send Destination Add/Modify settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **General | Locations Config | K2 - Send Destinations | Add** or **Modify**



Setting or button	Description
Send Name	The name of the destination, as it appears in the Send Destinations list in the GV STRATUS application. This can be any name, as appropriate for your workflow.
K2	The destination system to which the asset is sent. If the destination is a K2 Summit/SAN system, it must be configured in K2 Storage , K2 SAN Storage, K2 Standalone Storage, or Remote K2 Storage settings. If the destination is a redundant K2 SAN system, the same send locations must to be configured for both primary and backup systems. If the destination is specified to use a separate FTP network (typically designated with the `_he0` suffix), that FTP network must be accessible when configuring these settings. If the destination is not a K2 Summit/SAN system, **Non-Summit device** must be selected.
Conform on Send	Triggers the Render Engine software component to render a complex asset as a simple clip. It is recommended that the Send Name indicate that the destination is configured for conform.

Setting or button	Description
Output Format	**Conform on Send** must be selected to populate this setting. This is the output format to which sent assets are conformed. Output formats on the list are configured in Format settings. The only formats available are those compatible with the Reference Standard currently configured in Format settings.
Restripe timecode	When selected, the start timecode of the conformed clip is set according to the EDIUS **Start Timecode** setting in GV STRATUS Control Panel. This setting is automatically selected when the **Conform on Send** box is checked. If not selected, the start timecode of the conformed clip is preserved according to original timecode. ***NOTE: The Restripe timecode option is only supported for same-format conforms (e.g.: 720p to 720p).*** For mixed-format conforms (e.g.: combination of 720p and 1080i), the resultant clip always consists of restriped timecode according to EDIUS **Start Timecode** setting regardless of selection for this option.
Non-Summit device	Identifies the destination system as one on which K2 Summit/SAN services are not running. When selected, an **Enter working bin** field opens. This is the bin on the destination system to which the asset is sent. The bin name must be entered manually, as only systems running K2 Summit/SAN services can populate a list of available bins/directories. ***NOTE: When this option is selected, the settings applied for the destination system name and working bin name must be valid and accessible on the network. The GV STRATUS system does not attempt to validate the settings and does not provide any messages if not valid when applied.***
Select a working bin	The bin on the selected K2 system to which the asset is sent. This list of available bins does not appear if **Non-Summit device** is selected.

Related Topics

Format settings on page 161

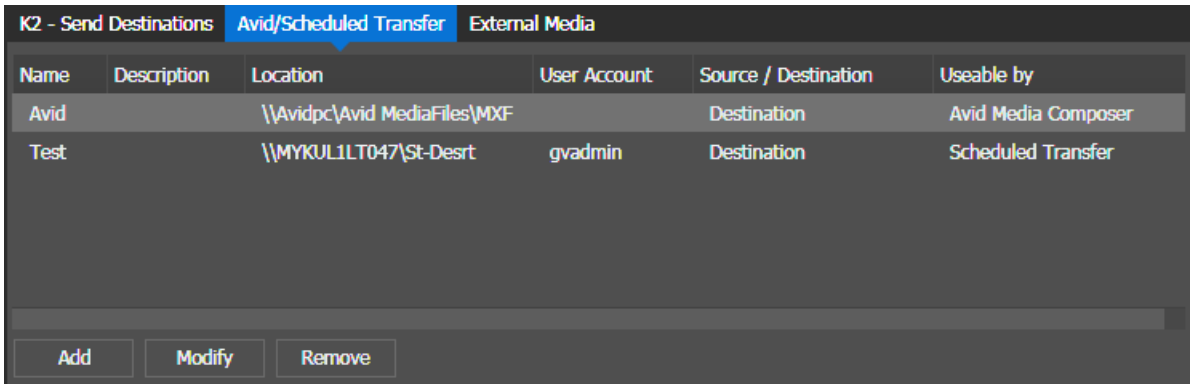
Remote Sites settings on page 298

Avid/Scheduled Transfer location settings

These settings are optional on GV STRATUS systems.

Avid/Scheduled Transfer configuration settings configure locations that are referenced by features throughout the system; such as Send to Avid destinations, Transfer to Avid rule destinations, and location of destinations for the Scheduled Transfer tool. Access these settings in the GV STRATUS Control Panel application.

To locate these settings, click **General | Locations Config | Avid/Scheduled Transfer**



Setting or button	Description
Add	Opens Avid/Scheduled Transfer Configuration dialog box
Modify	Opens the Avid/Scheduled Transfer Configuration dialog box for the selected location
Remove	Removes the selected location

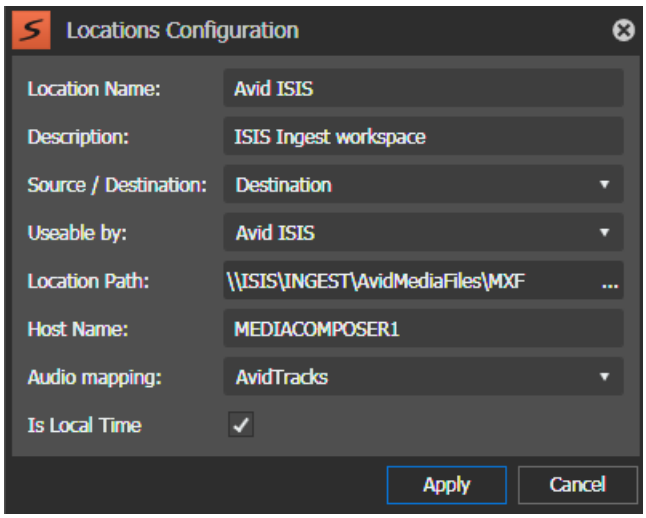
Related Topics

Configure Avid Media Composer send destinations on page 666
Configure Avid ISIS send destinations on page 668
Configure Avid Interplay send destinations on page 671
Configure Scheduled Transfer send locations on page 402

Locations Configuration Add/Modify settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **General | Locations Config | Locations Configuration | Add** or **Modify**



Setting or button	Description
Location Name	The name of the location, as it appears in the application. This can be any name, as appropriate for your workflow.
Description	Your description of the location.
Source / Destination	Specifies whether the destination is a source, a destination, or both.
Usable by	Specifies the system features and components that can use the location.
Location Path	The path to the location, which can be accessible through SMB, FTP, or HTTP. You can click the browse icon to launch the Windows dialog and select a specific location in your network.
Location Path Credentials	The credentials required to access the location.
Host Name	The host name of the Avid ISIS storage location. This setting is only applicable when Avid ISIS system is selected.
Audio mapping	This setting is only applicable when Avid Media Composer, Avid ISIS, or Avid Interplay system is selected. Specifies the audio track mapping of assets to be exported into Avid system. Audio track profiles can be created via the Audio Tag Management setting in the GV STRATUS Control Panel. Those audio profiles are then selectable in the **Audio Mapping** drop-down list when configuring export into the Avid system.
Is Local Time	Specifies the date and time of metadata fields for Avid in local time, instead of UTC. This setting is only applicable when Avid Media Composer, Avid ISIS, or Avid Interplay system is selected.

Related Topics

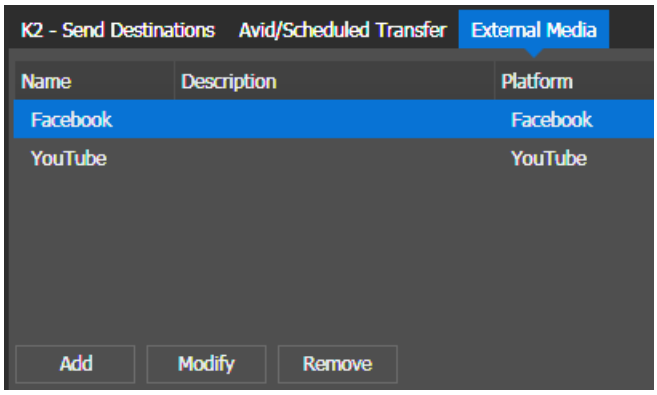
Configure Avid Media Composer send destinations on page 666
Configure Avid ISIS send destinations on page 668
Configure Avid Interplay send destinations on page 671
Configure Scheduled Transfer send locations on page 402

External Media locations configuration settings

These settings are optional on GV STRATUS systems.

The External Media locations configuration settings configure specific locations for Social Media transfer destinations of each social media platform (if licensed) such as YouTube, Twitter, Facebook, and Social Media CMS-System such as Verizon. You must access these settings with an administrator account in the GV STRATUS Control Panel application.

To locate these settings, click **General | Locations Config | External Media**



Setting or button	Description
Add	Opens a new External Media Locations Configuration dialog box.
Modify	Opens the External Media Locations Configuration dialog box for the selected location.
Remove	Removes the selected location.

For more information, refer to the *GV STRATUS Social Media Locations Configuration video*.

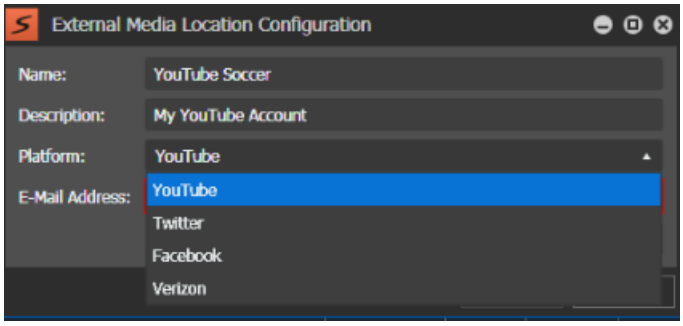
Related Topics

Configure and authenticate Facebook location on page 809
Configure and authenticate Twitter location on page 812
Configure and authenticate YouTube location on page 815
Configure and authenticate Verizon location on page 825

External Media Locations Configuration Add/Modify settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **General | Locations Config | External Media | Add** or **Modify**



Setting or button	Description
Name	The name of the location, as it appears in the application. This can be any name, as appropriate for your workflow.
Description	Your description of the location.

Setting or button	Description
Platform	Specifies whether the social media destination is for YouTube, Twitter, Facebook, or Verizon.
Email Address	Specifies the e-mail address of the social media account.
Register	Click the **Register** button to enter your credentials for the social media account to gain access of the transfer location.
Apply	Saves and applies changes to the location configuration settings.
Cancel	Reverts to previously saved settings.

Related Topics

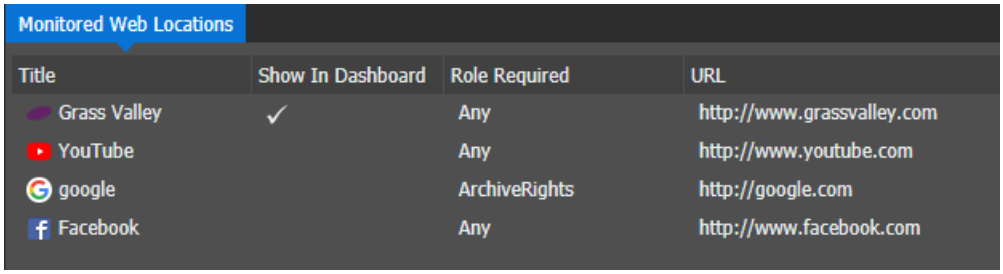
Configure and authenticate YouTube location on page 815
Configure and authenticate Twitter location on page 812
Configure and authenticate Facebook location on page 809
Configure and authenticate Verizon location on page 825

Web Monitor Config settings

These settings are optional on GV STRATUS systems.

Web Monitor Config settings let you assign web addresses for display in the Web Monitor tool. Access these settings in the GV STRATUS Control Panel application.

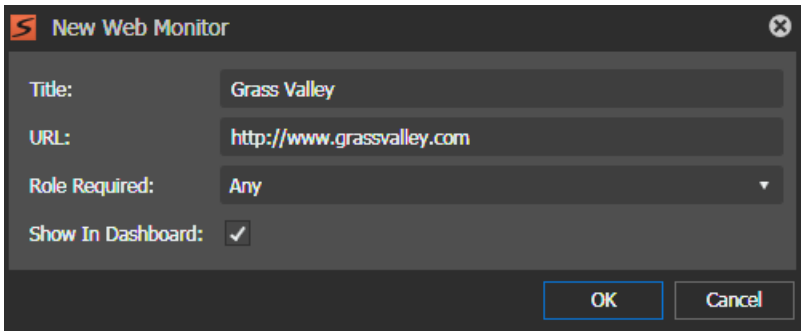
To locate these settings, click **General | Web Monitor Config**.



Setting or button	Description
Add	Opens New Web Monitor dialog box
Modify	Opens the Web Monitor dialog box for the selected Web Monitor URL
Remove	Removes the selected Web Monitor URL

Web Monitor Add/Modify settings

To locate these settings, click **General | Web Monitor Config | Add** or **Modify**

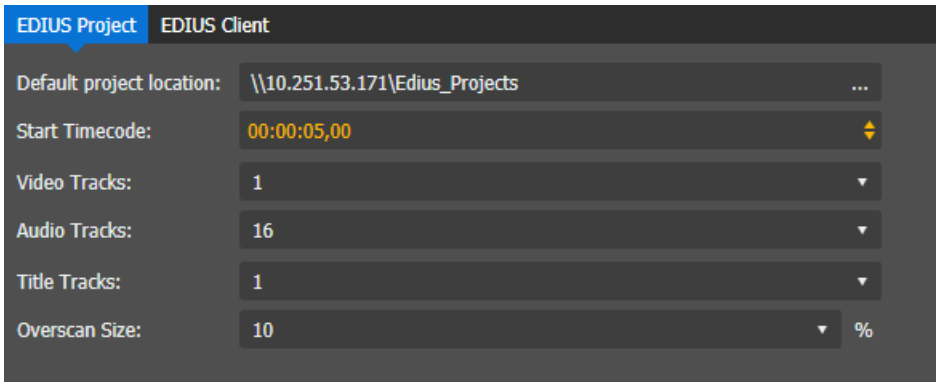


Setting or button	Description
Title	The name of the Web Monitor, as displayed in the Navigator panel of GV STRATUS application.
URL	The web address of the web page displayed in the Web Monitor panel.
Role Required	If selected, only users with the specified role could view the configured Web Monitor.
Show in Dashboard	When the checkbox is selected, the configured Web Monitor displays as a tab on the Dashboard panel only. If not selected, the configured Web Monitor displays in the Navigator panel of GV STRATUS application.

EDIUS Settings

These settings are only required on GV STRATUS systems with EDIUS.

To locate these settings, in GV STRATUS Control Panel click **Applications | EDIUS | EDIUS Project**



Setting or button	Description
Default project location	The default location for your EDIUS projects. The location is a folder on K2 storage. Make sure this path uses the standard convention of UNC path with hostname (not drive letter) for EDIUS access to K2 storage.
Start timecode	The start timecode of your project or conformed asset. The default is set to 00:00:00,00.

Setting or button	Description
Video Tracks	The number of video tracks for your project.
Audio Tracks	The number of audio tracks for your project.
Title Tracks	The number of title tracks for your project.
Overscan Size	The percentage ratio of overscan size for your project. Set to 0 if you are not using the overscan feature.

Format settings define the format of projects.

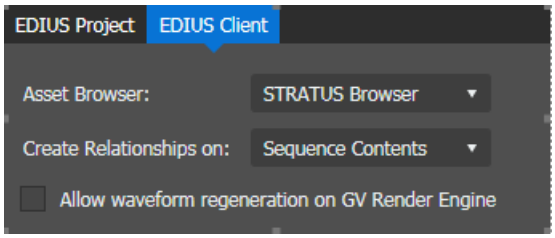
Related Topics

Format settings on page 161
If you have trouble launching EDIUS XS on page 169
Access K2 storage for EDIUS using standard convention on page 282
Access K2 storage for EDIUS using standard convention on page 282

EDIUS Client Settings

These settings are only required on GV STRATUS systems with EDIUS clients.

To locate these settings, in GV STRATUS Control Panel click **Applications | EDIUS | EDIUS Client**



Setting or button	Description
Asset Browser	The asset browser to be used in the EDIUS application. Select one from the following: • **STRATUS App** - utilizes GV STRATUS ActiveX panel in the EDIUS application. • **STRATUS Browser** - utilizes STRATUS browser in the EDIUS application to browse and search GV STRATUS assets.
Create Relationships on	Associates GV STRATUS assets in the EDIUS application. Select one from the following: • **Project Contents** - associates all assets used in the EDIUS project; including those loaded in the project bin only. • **Sequence Contents** - only associates assets used in sequences on the timeline of the EDIUS project.

Setting or button	Description
Allow waveform regeneration on GV Render Engine	Enables or disables the re-creation of waveform cache (*.ewc2) files in proxy server for the use in EDIUS client. Waveform cache files are usually generated in EDIUS when users expand audio tracks on the timeline.

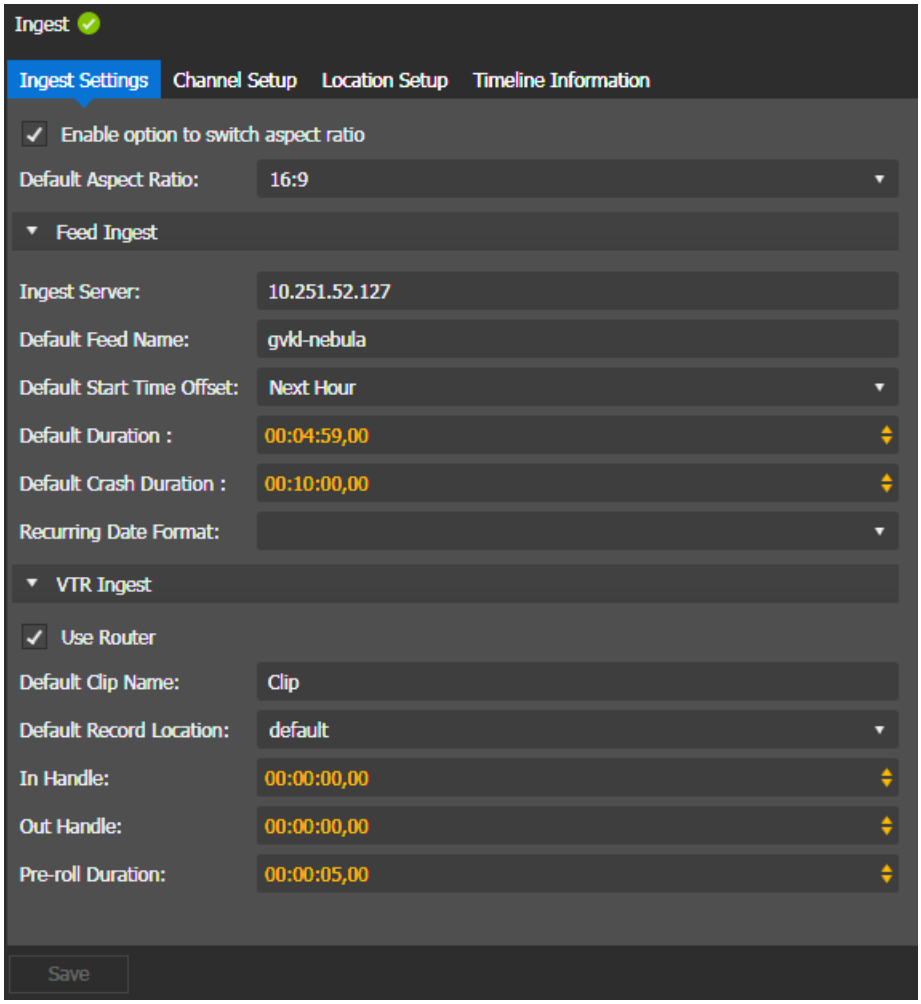
Ingest settings

Ingest settings let you configure feed ingest settings for the Scheduler, VTR ingest settings for the GV STRATUS VTR Ingest, set up K2 system channels to record clips, and set up record locations. These settings are persistent in their control of K2 system channels and cannot be overridden by K2 AppCenter or other GV STRATUS application tools, such as Channel Panel. Access the Ingest settings in the GV STRATUS Control Panel application.

Ingest settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Applications | Ingest | Ingest Settings**



Setting or button	Description
Enable option to switch aspect ratio	The aspect ratio can only be changed if you are recording to an SD channel.
Default Aspect Ratio	Default aspect ratio for ingests. The default aspect ratio is set to 16:9.
Ingest Server	IP address or machine name where Core Services Server resides. The Ingest Server is automatically populated if you install using Site Config.
Default Feed Name	Default feed name for events in Scheduler unless you enter a specific name for the event in the Channel panel or event properties.
Default Start Time Offset	Default start time offset from the time you schedule the event. The minimum offset is 1 minute and the maximum offset that you can set is 1 hour from the current time.
Default Duration	Default duration for any feed event that you want to schedule. The default duration is set to 59 minutes and 50 seconds.
Default Crash Duration	Default duration for crash records. The default duration is set to 59 minutes and 50 seconds.
Recurring Date Format	Specific date format for your recurring event.
Use Router	Enable ingest operation for GV STRATUS VTR Ingest to be done via a router, if selected.
Default Clip Name	Default clip name for assets ingested via the GV STRATUS VTR Ingest application, if you don't enter specific clip names for those assets.
Default Record Location	Default record location for assets ingested using the GV STRATUS VTR Ingest application, if you don't enter specific location for those assets.
In Handle	Duration to be added before the ingested asset. Handles allow you to have additional frames to use while editing.
Out Handle	Duration to be added after the ingested asset.
Pre-roll Duration	Duration of pre-roll to be set before ingest operation starts.

Ingest Service status indicator — Shows the connection status between Ingest core service, Scheduler tool, and GV STRATUS VTR Ingest application.

— Connected

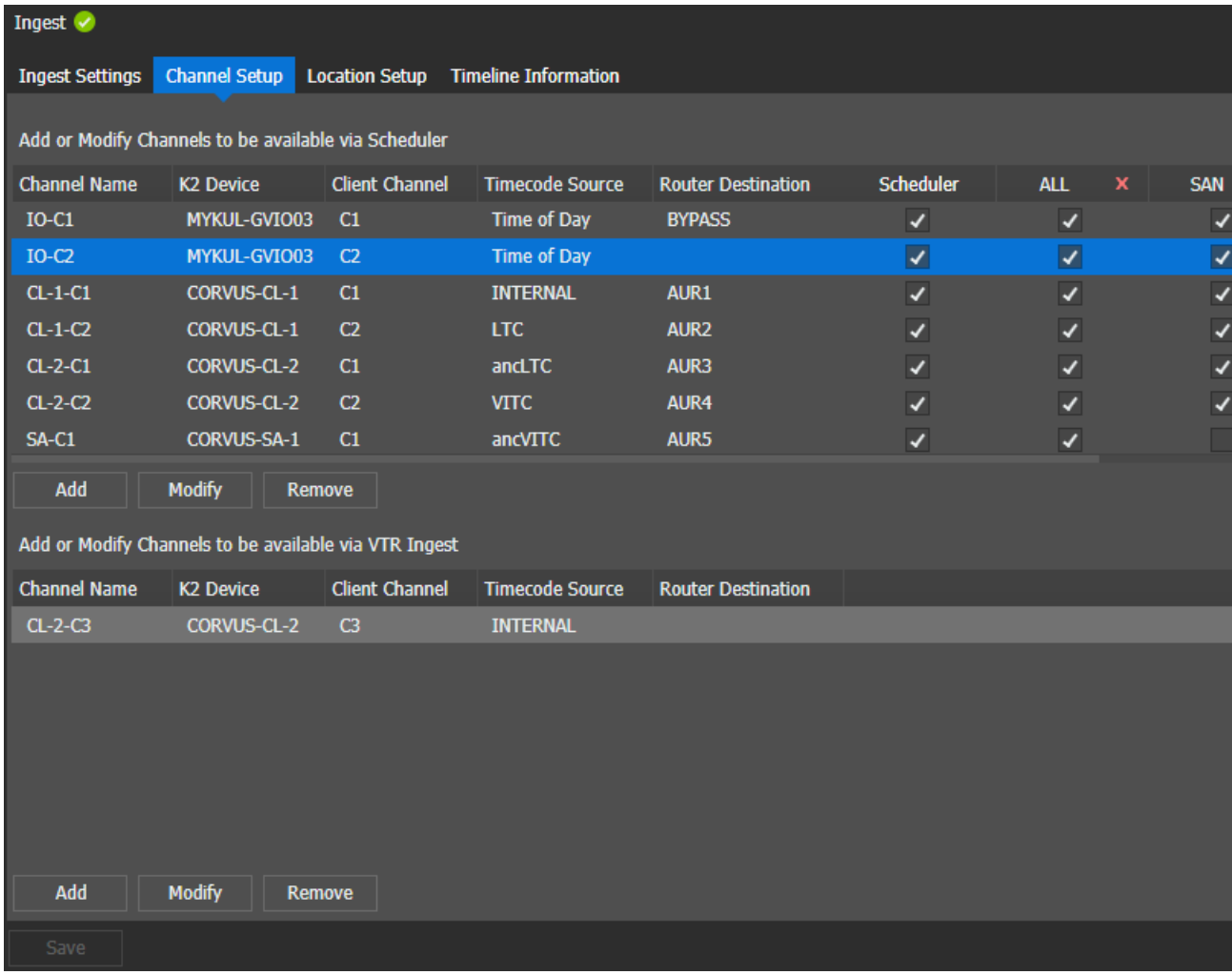
— Disconnected

— Ingest core service is not ready for recording yet. Users can only start recording after the status changes to **Connected**.

Channel setup settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Applications | Ingest | Channel Setup**



In the Scheduler section, you can add and organize Scheduler tool channel groups. In GV STRATUS Navigator, channel groups are displayed as individual Scheduler tools under the parent Scheduler tool. Each channel group can be launched as a Scheduler tool and can be configured to display a sub-set of Scheduler channels.

- Each row represents a Scheduler channel. Channels can be reordered higher/lower using up/down arrows.
- Each column on the right-hand side of the **Scheduler** column represents a channel group. Added channel groups can be reordered left/right using drag-and-drop. The left-right order is displayed as a top-bottom order in GV STRATUS Navigator.

Setting or button	Description
Channel Name, K2 Device, etc	Channel settings, as configured in the Add/Modify Channel dialog box.
Scheduler	Rows selected in the column define the channels displayed in the Scheduler tool. If a channel is not selected, it is not displayed in the parent Scheduler tool or in any channel groups. This column cannot be removed or its position altered.

Setting or button	Description
+	Opens the **Add Channel Group** dialog box, which defines and adds a new channel group. Rows selected in the column define the channels displayed on the added channel group.
X	Removes an added column.
Add	Opens the Add Channel dialog box for you to add channels for Scheduler or GV STRATUS VTR Ingest.
Modify	Opens the Modify Channel dialog box for the selected channel.
Remove	Removes the selected channel. ***NOTE: Events set to Auto-Assign in the channel must be removed prior to the channel's removal.***
Save	Saves the current configuration of added channels and their order.

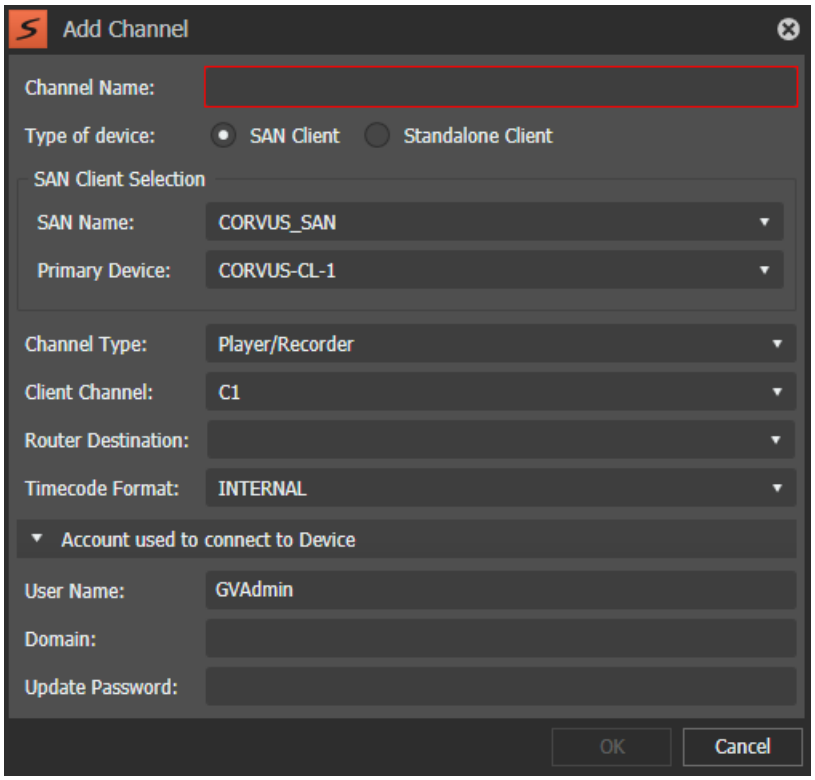
Arrow buttons on the right reorder selected channels. The channel order is displayed in the Scheduler tool. The channel order is not displayed in GV STRATUS VTR Ingest. The **Save** button must be clicked to save a new configuration. A prompt to save settings and restart ingest services opens to implement the change.

NOTE: Stop ingest operations before services restart. Scheduled feed recordings or GV STRATUS VTR Ingest operations can be affected while services restart.

Ingest Channel Add/Modify settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Applications | Ingest | Channel Setup | Add** or **Modify**



Setting or button	Description
Channel Name	Name for channel, as displayed in the GV STRATUS application. This can be any text, as desired to support your workflow.
Type of device	The type of device that you can choose is either SAN client or Standalone client.
SAN Name	The K2 SAN system name, if you chose SAN client. For GV I/O Device, select the K2 SAN name if you use K2 SAN for media storage or select the SMB storage name if you use SMB storage in your system.
Primary Device	The primary device in the K2 SAN that you want to use with the Scheduler tool. For GV I/O Device, the primary device is the GV I/O Live Ingest and Playback Server that you want to use with the Scheduler tool.
Select Standalone	The Standalone system name, if you chose Standalone Client.
Channel Type	Sets the type of channel, either Player/Recorder or Multicam, on the K2 Summit system and provides the appropriate number of video inputs available per channel in the Scheduler tool. For GV I/O Device, the channel type can only be set to Recorder when GV I/O Live Ingest and Playback Server is selected as the Primary Device.

Setting or button	Description
Client Channel	The channel you are using to record. Select a channel from the drop-down list such as C1, C2, C3, C4, etc. Ensure that the channel will not be in Continuous Record mode when you are using it for Scheduler record. This setting is persistent in its control of K2 system channels and cannot be overridden by K2 AppCenter or other GV STRATUS application tools, such as Channel Panel. For GV I/O Device, only 4 client channels are supported per GV I/O server.
Router Destination	The router destination for the channel. If you haven't configured your router sources or are not using a router in your operation, the drop-down list is empty. If Channel Type is Multicam, two router destinations are available.
Timecode Format	The timecode source for the channel. You can choose from Internal, LTC, ancLTC, Time of Day, VITC, and ancVITC as appropriate for the HD/SD configuration of the channel. ***NOTE: For a* GV STRATUS VTR Ingest *channel, the timecode format should be the same with your timecode setting in* GV STRATUS VTR Controller.** For GV I/O Device, the timecode format can only be set to Time of Day.
Account used to connect to Device	User name, domain, and password to connect to the device, if required to do so. ***NOTE: Do not enter a domain or otherwise modify account settings except under the supervision of qualified Grass Valley Support personnel. Extensive system configuration is required to achieve a working GV STRATUS system.***

Related Topics

Characters not allowed in router source and destination IDs on page 557
About timecode source and clock synchronization on page 422
Setting up control for Scheduler channels in the K2 AppCenter on page 385
Fully qualified domain configuration on page 913

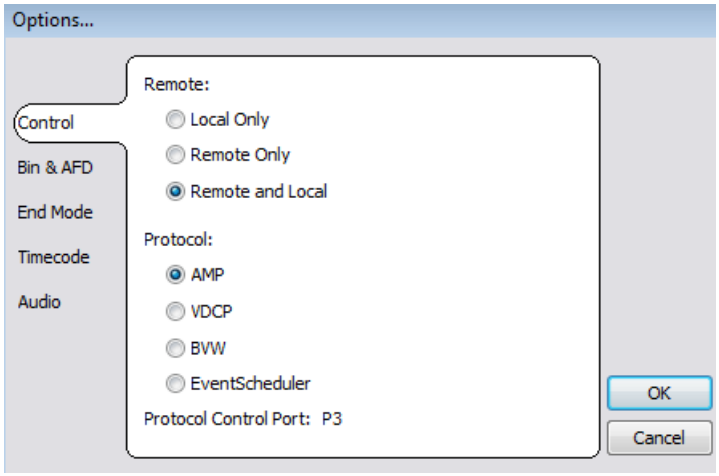
Setting up control for Scheduler channels in the K2 AppCenter

The Scheduler tool uses the K2 Summit API to communicate with K2 Summit channels. You must set K2 Summit channels to be controlled remotely and used as Scheduler channels in the GV STRATUS application.

1. In the K2 AppCenter, click on the channel that you want to specify for the Scheduler tool.

2. Select **Control | Options**.

   The Options dialog box displays. If it is not already displayed, select the **Control** tab.



3. Select a Remote setting either one from the list below:

Option	Description
Remote Only	Allows you to control the record channel remotely.
Remote and Local	Allows you to control the record channel locally as well as remotely.

   If you have GV STRATUS Rundown in your system, it is recommended to select **AMP** in the Protocol setting.

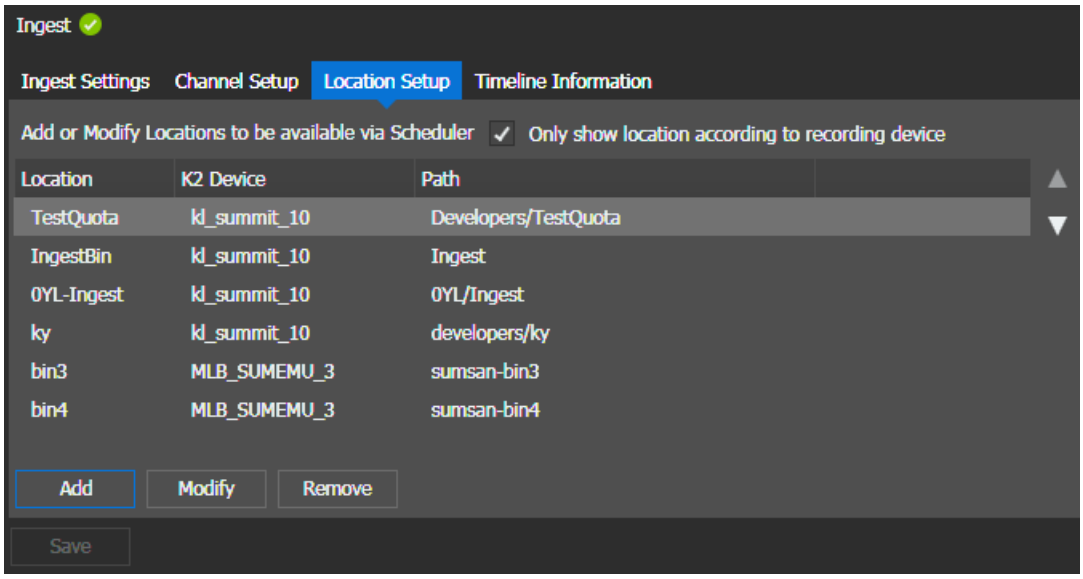
4. Click **OK**.

Repeat this procedure for each K2 Summit channel that will be controlled remotely via the Scheduler tool.

Ingest Location Setup settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Applications | Ingest | Location Setup**



Setting or button	Description
Only show location according to recording device	Displays only the bins of K2 system where the Ingest channel is configured. If this setting is not selected, all configured locations are available. ***NOTE: This setting is unchecked by default. The check-box must be selected to only display recording locations that are in the same K2 system as the configured Ingest channel.***
Add	Opens the Add Location dialog box.
Modify	Opens the Modify Location dialog box for the selected location.
Remove	Removes the selected location.

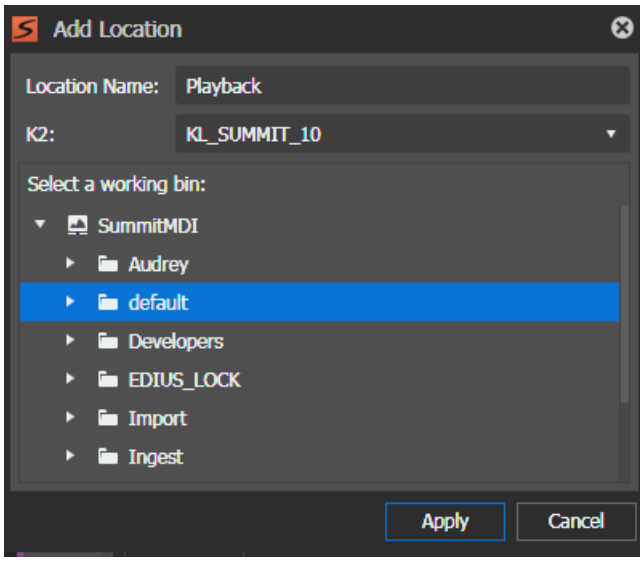
If you want to reorder the location list, select a location and click arrow buttons on the right to move up or down. Then, click **Save** to save the new configuration. Ingest services will be restarted to implement the change.

NOTE: While Ingest services restart, scheduled feeds may not start on time. Therefore, check* Scheduler *before modifying locations to ensure that no events are scheduled to start immediately.

Ingest Location Add/Modify settings

These settings are optional on GV STRATUS systems.

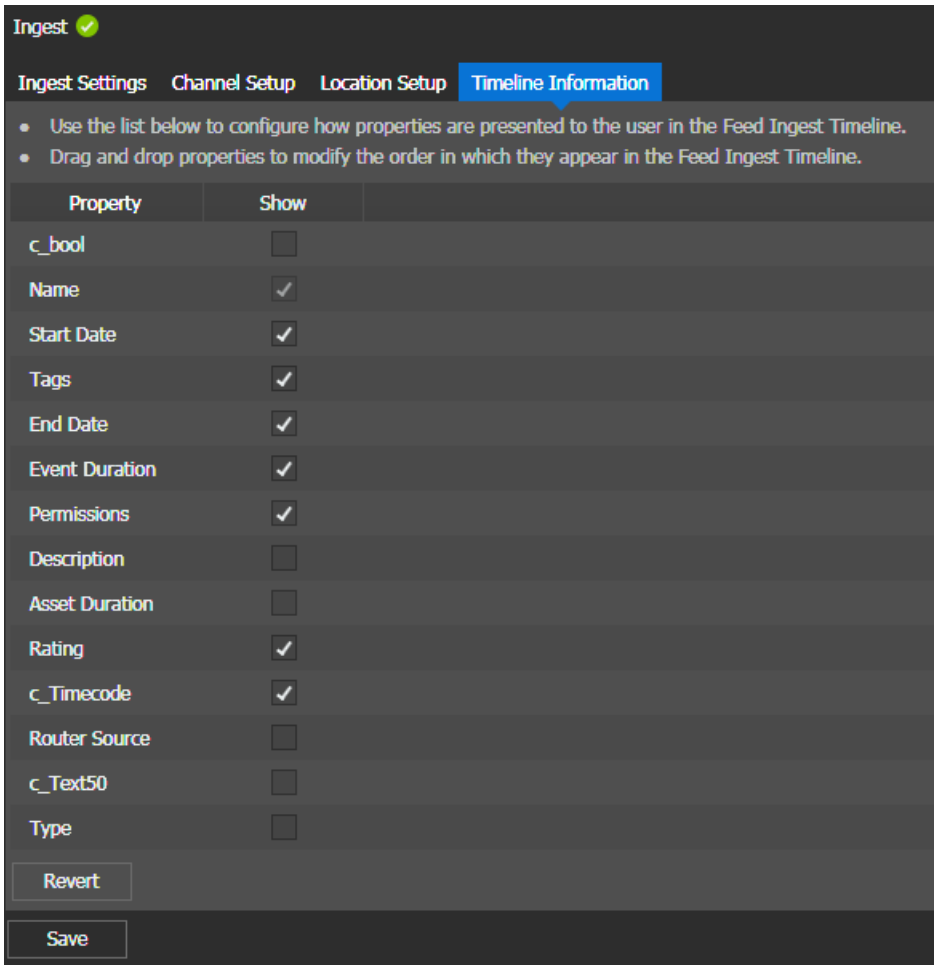
To locate these settings, click **Applications | Ingest | Location Setup | Add** or **Modify**



Setting or button	Description
Location Name	Location name on the K2 system that you want to store your recording into.
K2	The K2 system that you want to store your recording into. Only K2 standalone system or K2 SAN-attached system that have been configured in your operation can be selected from the drop-down list.

Timeline Information settings

To locate these settings, click **Applications | Ingest | Timeline Information**.



You can select specific properties to be displayed on scheduled events and tooltips in the Scheduler timeline. However, those selected properties are only available for display on the Track View of the Scheduler Tool.

The **Name** property is a mandatory field and cannot be disabled. If configured in the Metadata section and given full permissions, custom metadata can be selected and displayed on scheduled events and tooltips.

You can also drag and drop properties in this setting to reorder the display. To sort properties based on entries of the column, click a column head. To reverse the sort order, click the column head again.

NOTE: Scheduler supports the display up to 8 fields of properties for single camera recordings, and 6 fields of properties for Multicam recordings.

Setting or button	Description
Property	The list of property fields to be selected for display.
Show	Select fields in this column to customize the display on Scheduler timeline for event properties and tooltips in the Track View mode.
Save	Saves the current settings. Ingest services will be restarted each time users saved the settings.

Setting or button	Description
Revert	Discards any new settings and reverts to the last saved settings.

Rundown settings

Rundown settings configure the Simple Database (SDB) Server, XMOS Server, and K2 systems for the purpose of playout. The GV STRATUS application supports GV STRATUS Rundown for news broadcast operations. GV STRATUS Rundown server component settings are automatically populated if you install using SiteConfig. Access these settings in the GV STRATUS Control Panel application.

Format settings define the video standard.

You must install GV STRATUS Control Panel on SDB Server / XMOS Server, and run the GV STRATUS Control Panel application in order to make changes to Rundown settings.

If you change any Rundown settings, you must restart the SDB server. A restart of the Newsroom Computer system might also be required.

If you change the GV STRATUS Database Server setting in the GV STRATUS Core Services settings, you must do the following to propagate the change for GV STRATUS Rundown operations:

1. Launch and save settings.
2. Restart the SDB server.

Refer to related topics in the this Topic Library to configure playout channels in the GV STRATUS Rundown application.

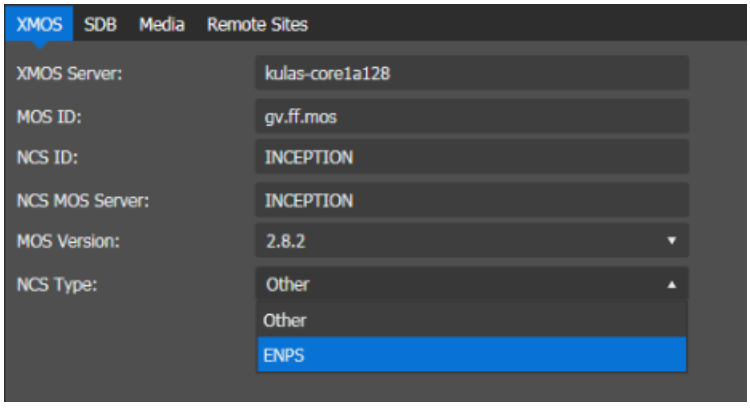
Related Topics

Format settings on page 161

XMOS Server settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Applications | Rundown | XMOS**

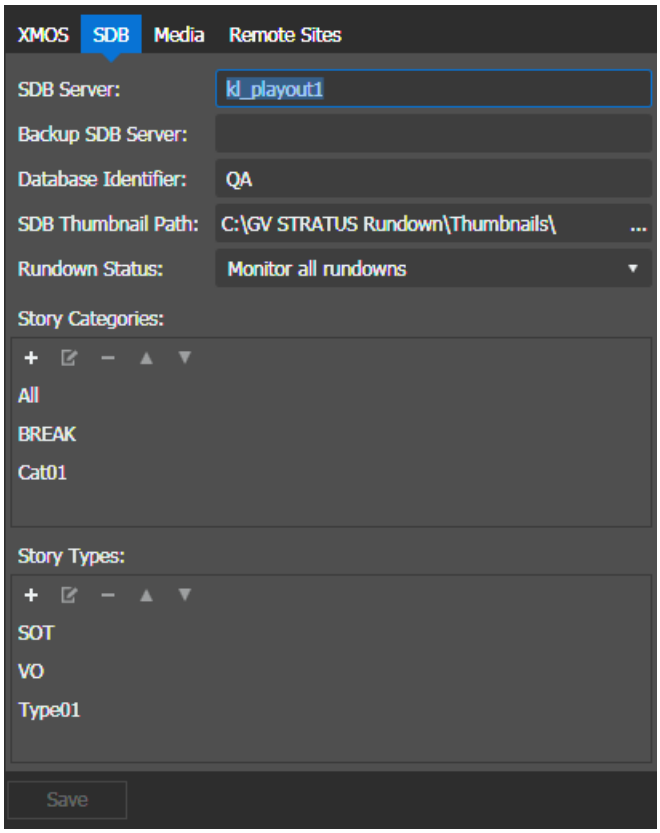


Setting or button	Description
XMOS Server	IP address or machine name where the XMOS Server resides. The XMOS Server is automatically populated if you install using Site Config. ***NOTE: The* GV STRATUS Control Panel *application must be installed on the XMOS Server.***
MOS ID	The MOS ID that you use in your operation. In ENPS, see ENPS | System Maintenance | MOS Configuration in the ID column. In iNEWS, this value matches the <mos> value within the configuration file on the iNEWS MOS Gateway at C:/Program Files/Avid/MOS Gateway/mosconfig.xml. In Octopus, see Admin | MOS | Devices.
NCS ID	Name of the machine hosting your newsroom computer system: For ENPS, the name of the ENPS Server. If you have an ENPS Buddy server, you need to enter both the main and buddy server names in both the NCS ID and NCS MOS Server fields, in the format "MAIN,BUDDY". For iNEWS, the name of the iNEWS Server. For Octopus, see Admin | MOS | Devices.
NCS MOS Server	Name of the machine hosting the NCS MOS Server component: For ENPS, the same value you entered for the NCS ID. For iNEWS, the name of the iNEWS MOS Gateway machine. For Octopus, the name of the Octopus Server machine.
MOS Version	The version number of MOS you are using. Refer to compatible versions in this Topic Library. If your version is unknown, leave the setting at the default value.
NCS Type	**ENPS** must be selected in this drop-down list if you are using ENPS version 8.2 and above with the GV STRATUS ActiveX Plug-in. If not selected, you cannot drag/drop placeholders and assets from the GV STRATUS ActiveX panel into ENPS.

SDB Server settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Applications | Rundown | SDB**



Setting or button	Description
SDB Server	IP address or machine name where the SDB Server resides. The SDB Server is automatically populated if you install using Site Config. ***NOTE: The* GV STRATUS Control Panel *application must be installed on the SDB Server.***
Backup SDB Server	IP address or machine name that hosts the backup SDB Server, if available.
Database Identifier	ID for the database, up to 4 characters, such as your station call letters. All clip IDs will begin with this identifier.
SDB Thumbnail Path	The path where clip thumbnails are stored. You can click the browse icon to launch the Windows dialog and select a specific location in your network.
Rundown Status	Display of rundown status; either **Monitor all rundowns** or **Monitor open rundowns only**.
Story Categories	Story categories are used to sort and assign placeholders in the Assignment List.
Story Types	The story type for placeholders. Default story types are SOT (Story on Tape) and VO (Voice Over).

Media settings

These settings are optional on GV STRATUS systems.

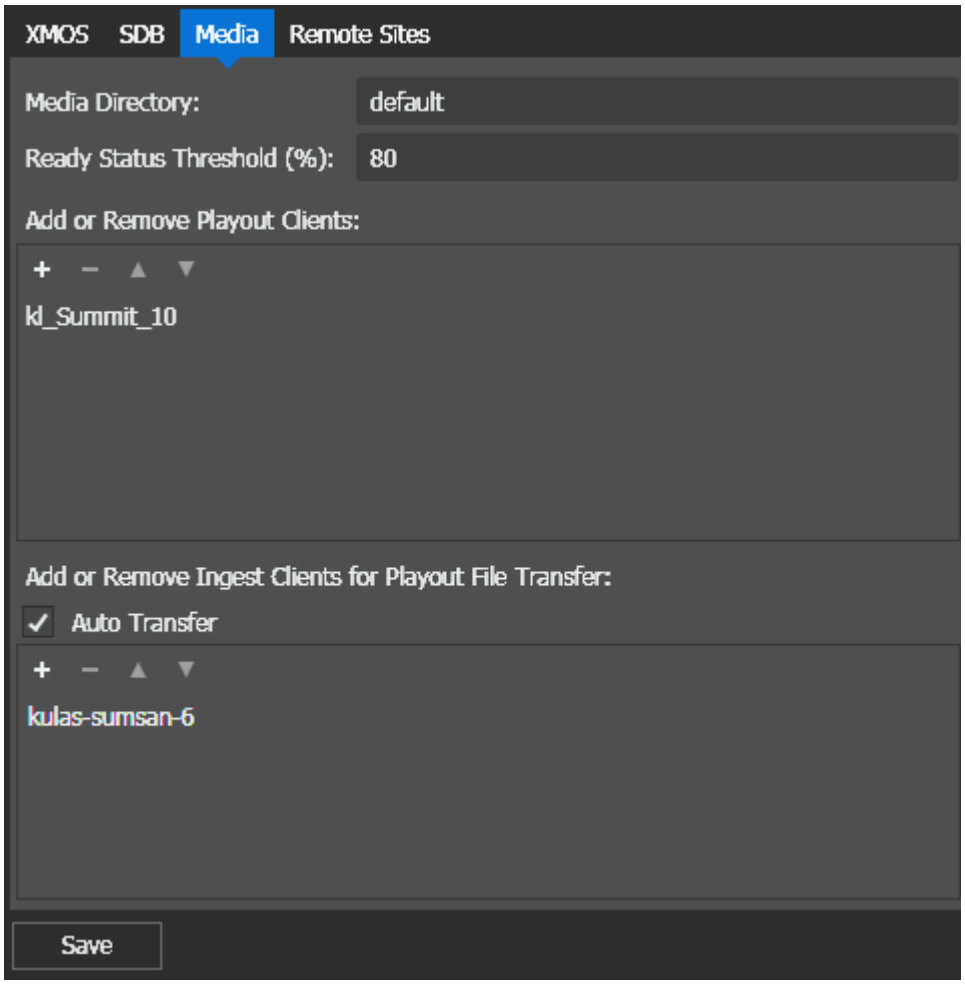
You can set the Media Directory for the operation with GV STRATUS Rundown.

You can also set the threshold percentage value of clip transfer progress for the status of linked growing clip to change to **Ready**.

When selecting the ingest client for Playout File Transfer, you have the option to use the **Auto Transfer** feature to automatically transfer media from a source (ingest) server to a destination (playout) server.

For the MOS Redirection workflow with ENPS, you must select the **Auto Transfer** feature and add K2 media servers for Playout File Transfer.

To locate these settings, click **Applications | Rundown | Media**



Setting or button	Description
Media Directory	Name of the default folder where playout media is sent to.

Setting or button	Description
Ready Status Threshold (%)	Defines the threshold (in percentage value) of clip transfer progress before the status of a linked growing clip changes to **Ready**. This setting is only applicable to clip transfers via Send Destinations (**F11**) and Move/Copy operation from a non-playout bin to playout bin after linking the clip to a placeholder. For other methods of ingesting clips that are not tracked by the GV STRATUS Jobs Monitor such as scheduled ingests, removable media interface (RMI) ingests, and imports/recordings via the K2 Summit AppCenter, placeholders which have a linked clip in the playout media bin with a Duration property greater than 0 (zero) will be set to **Ready** status and is not affected by the **Ready Status Threshold (%)** setting. In such cases, the placeholder status will only remain as **Not Ready** as long as the clip's duration value is still 0 (zero).
Add (+)	Opens the Add media server dialog. It lets you either define the playout server or ingest server that accommodates Playout File Transfer. For the MOS Redirection workflow with ENPS, the K2 media server must be configured and added for Playout File Transfer.
Remove (-)	Removes the selected media server.
Auto Transfer	Auto Transfer lets you automatically transfer assets from an ingest server to a playout server. The Auto Transfer takes place only when assets recorded on the ingest server is associated with a placeholder that is part of a MOS active rundown. ***NOTE: A media server can only be either a source or destination for Auto Transfer, so the same media server should never be added to both the playout and ingest sections.*** For the MOS Redirection workflow, the Auto Transfer checkbox must be selected to enable transfer of media between machines and locations automatically via ENPS. When MOS Redirection is triggered and stories with linked placeholders containing media are moved from one location to another, ENPS automatically transfers the media contained in those stories. This workflow supports automatic transfer of media between servers within a single newsroom, or between multiple newsrooms and servers in different locations. For stories with unlinked placeholders, only the placeholder gets created at the other location.

Related Topics

Configuring MOS Redirection workflow with ENPS on page 1345

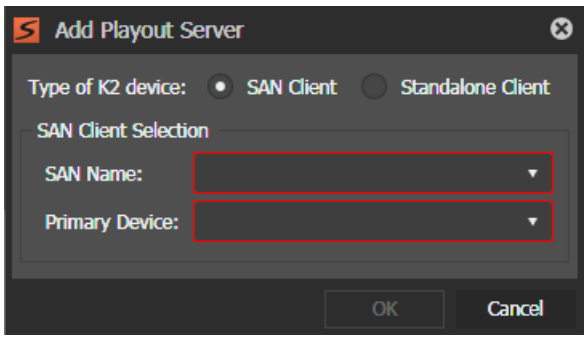
Rundown Add/Modify Server settings

These settings are optional on GV STRATUS systems.

A K2 system that is a playout or ingest client must have a Grass Valley Media Server MDI configured in GV STRATUS Control Panel. Refer to related topics in this Topic Library.

For the MOS Redirection workflow with ENPS, the K2 media server must be configured and added for Playout File Transfer.

To locate these settings, click **Applications | Rundown | Media | Add or Remove Playout Clients / Ingest Clients for Playout File Transfer | +**



Setting or button	Description
Type of K2 device	You can choose either SAN Client or Standalone Client in your operation.
SAN Name	Name of the K2 SAN-attached system if you chose SAN Client.
Primary Device	Name of the primary device in the SAN that you want to use.
Select K2 Standalone	Name of the K2 Standalone device if you chose Standalone Client.

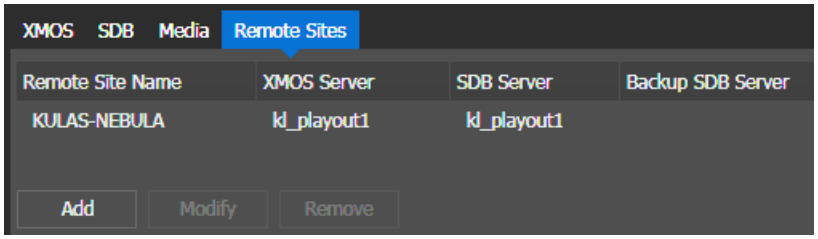
Related Topics

Grass Valley Media Server MDI standalone settings on page 304
Grass Valley Media Server MDI SAN settings on page 306

Rundown Remote Sites settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Applications | Rundown | Remote Sites**



Setting or button	Description
Add	Opens the **Add Remote Site** dialog box for you to add a playout remote site. You can use the **Add** button repeatedly to add multiple remote sites.

Setting or button	Description
Modify	Opens the **Edit Remote Site** dialog box to modify settings of the selected remote site.
Remove	Removes the selected remote site.

Related Topics

Remote and multiple site configuration on page 473

Rundown Add/Modify Remote Site settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Applications | Rundown | Remote Sites | Add** or **Modify**

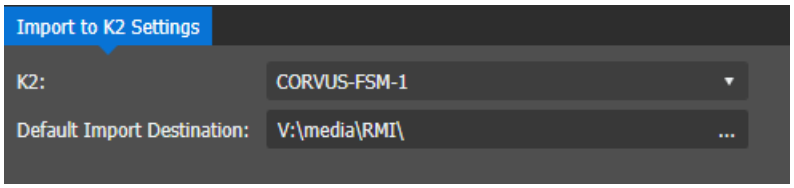
Setting or button	Description
Remote Site Name	Customizable name that has been set for your remote site. Only remote sites that have been configured in GV STRATUS Core Services Remote Sites settings can be selected from the drop-down list. Select **None** if there is no GV STRATUS Core Services server at the remote site.
XMOS Server	The IP address or machine name where the remote XMOS Server resides.
SDB Server	The IP address or machine name where the remote SDB Server resides.
Backup SDB Server	The IP address or machine name that hosts the backup of remote SDB Server, if available.
Save	Saves current settings.
Cancel	Returns settings to their last saved state.

After remote sites have been configured, you can see these remote sites in the Assignment List and Link to Placeholder tab of the Inspector and Send Destinations dialog box.

RMI settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Applications | RMI | Import to K2 Settings**



Setting or button	Description
K2	Name of K2 Summit/SAN system to import RMI clips directly into.
Default Import Destination	The default import destination for your RMI clips. If GV STRATUS security is enforced, the destination must allow write permissions for user accounts that import assets.

There are connection and configuration requirements for the GV STRATUS client PC on which the RMI tool is used. Refer to related topics in this Topic Library.

Related Topics

Set up RMI PC access to high-resolution assets on page 557

Proxy Access settings on page 345

Fully qualified domain configuration on page 913

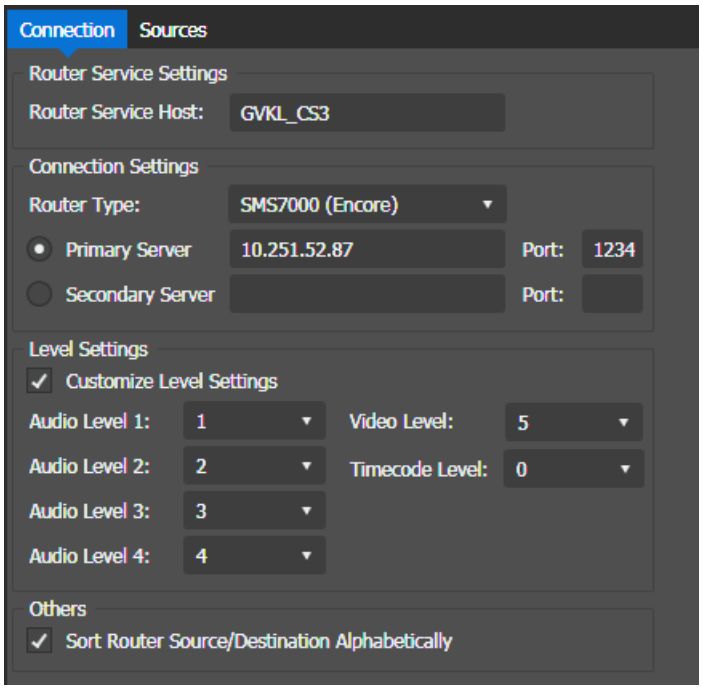
Router settings

Router settings configure the router connection and associate router sources, such as Encore, SMS7000, and Jupiter routers. Access these settings in the GV STRATUS Control Panel application.

Router Connection settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Applications | Router | Connection**



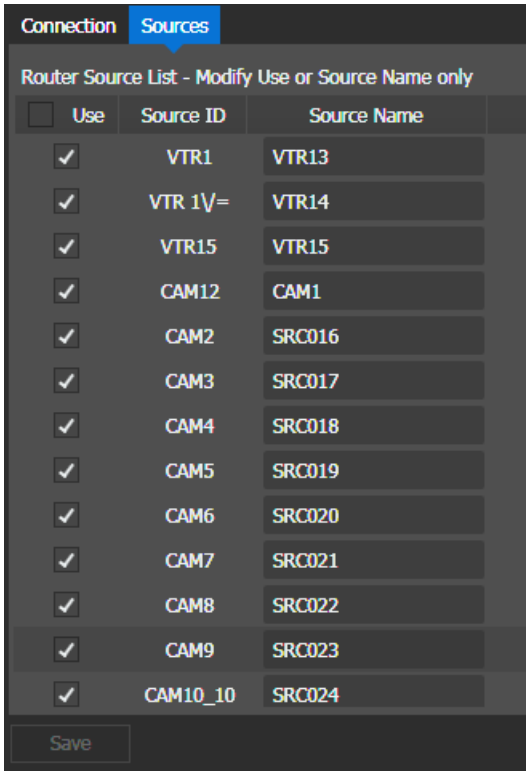
Setting or button	Description
Router Service Host	IP address or computer name that hosts the Router Service. This is populated automatically if you use SiteConfig for installation.
Router Type	Router types include Encore, SMS7000, and Jupiter. However, you need to select **Encore/SMS7000** from the Router Type drop-down list if you use Jupiter with the AccuSwitch application.
Primary server	IP address or the primary server of the router, if you chose Encore/SMS7000.
Port	Port number that the router needs to connect to.
Secondary Server	IP address or the secondary server of the router, if available.
COM Port	COM port number that Jupiter needs to connect to if you choose Jupiter on the Router Type drop-down list. ***NOTE: You need to enter "COM1", "COM2", or any other COM port number in this setting depending on which COM port that you want to use.***
Customize Level Settings	Level settings of the router can be customized. If checked, select the appropriate level from drop-down lists for video, audio and timecode. Select 0 (zero) for the video level if video is the first level in your router control system, 1 if it is the second level and so on.
Audio Level	4 audio level settings can be customized for the router.
Video Level	The video level setting can be customized for the router.
Timecode Level	The timecode level setting can be customized for the router.

Setting or button	Description
Sort Router Source/Destination Alphabetically	If selected, router sources and destinations are displayed alphabetically in the settings for **Ingest | Channel Setup** and in the Scheduler tool.

Router Sources settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Applications | Router | Sources**



Setting or button	Description
Use	Any particular router sources can be selected to be used.
Source ID	Source ID is automatically populated for each router source.
Source Name	Each router source can be given a source name. Once you have entered them, Source Names appear instead of Source IDs in the router source list.

You can also sort the Source ID and Source Name in alphabetical order by clicking the column head. To reverse the sort order, click the column head again.

NOTE: Changes made to source and destination values within the router itself will not be seen within the GV STRATUS Control Panel router configuration settings until the 'GV STRATUS Router Controller' service is restarted.

Related Topics

Characters not allowed in router source and destination IDs on page 557

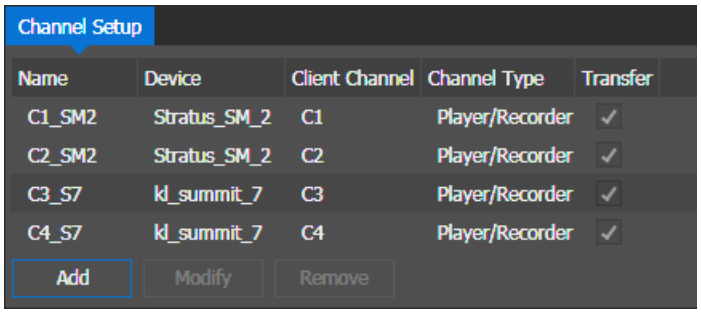
TX Scheduler settings

TX Scheduler settings let you configure event transfer settings for the Scheduled Transfer tool. Access the TX Scheduler settings in the GV STRATUS Control Panel application.

Channel setup settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Applications | TX Scheduler | Channel Setup**



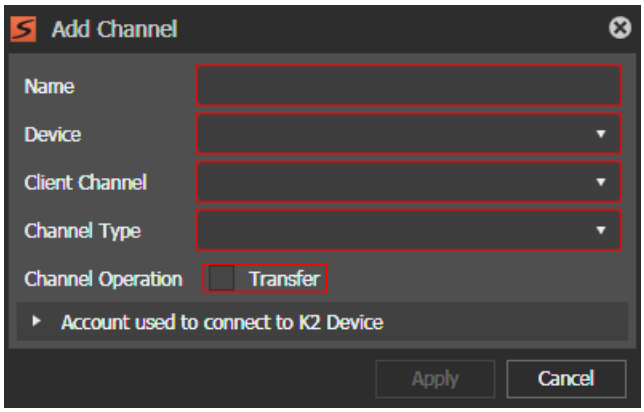
Each row represents a Scheduled Transfer channel that you configured.

Setting or button	Description
Channel Name, Device, etc	Channel settings, as configured in the Add/Modify Channel dialog box.
Add	Opens the Add Channel dialog box for you to add channels for the Scheduled Transfer.
Modify	Opens the Modify Channel dialog box for the selected channel.
Remove	Removes the selected channel.
Save	Saves the current configuration of added channels and their order.

TX Scheduler Channel Add/Modify settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Applications | TX Scheduler | Channel Setup | Add** or **Modify**.



Setting or button	Description
Name	Name for channel, as displayed in the GV STRATUS application. This can be any text, as desired to support your workflow.
Device	The type of K2 device that can be selected including K2 Summit Standalone client, K2 Media Server, or K2 Central Shared Storage, if configured in your operation.
Client Channel	The channel you are using to record, such as C1, C2, C3, etc. Ensure that the channel will not be in Continuous Record mode when you are using it for Scheduled Transfer record. This setting is persistent in its control of K2 system channels and cannot be overridden by K2 AppCenter or other GV STRATUS application tools, such as Channel Panel. ***NOTE: The timecode source of the channel must be set to Time of Day, or to LTC/VITC sources that had been synchronized to Windows system clock.***
Channel Type	Sets the type of channel, either Player/Recorder or Multicam, on the K2 Summit system and provides the appropriate number of video inputs available per channel in the Scheduled Transfer tool.
Channel Operation	Sets the operation of a channel for asset transfer.
Account used to connect to K2 Device	User name, domain, and password to connect to the K2 device, if required to do so. ***NOTE: Do not enter a domain or otherwise modify account settings except under the supervision of qualified Grass Valley Support personnel. Extensive system configuration is required to achieve a working GV STRATUS system.***

Once the channel is added, it appears automatically in the **Source Channel** drop-down list for event properties in the Inspector, and on the Scheduled Transfer timeline.

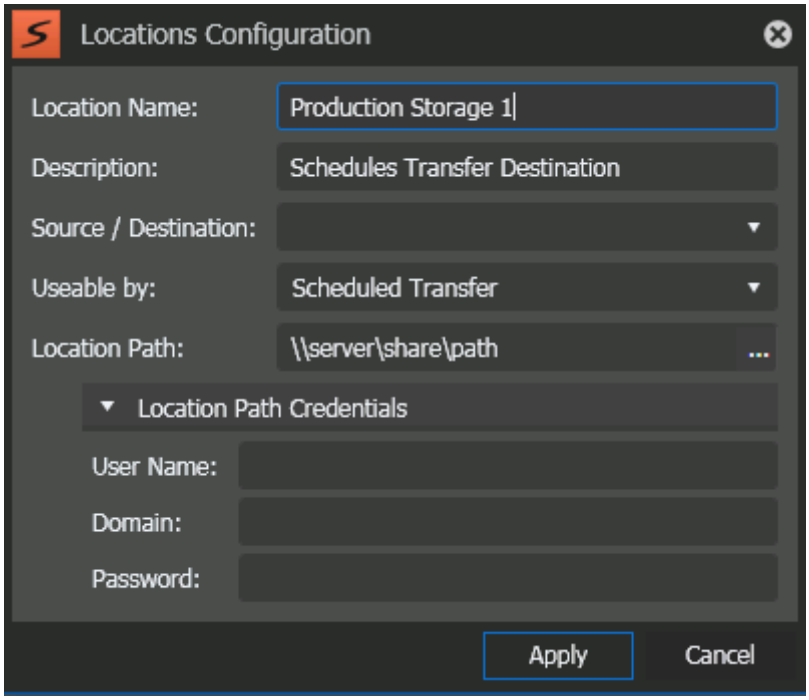
Configure Scheduled Transfer send locations

Only systems that transfer assets via the Scheduled Transfer tool require this process.

- To use the Scheduled Transfer tool, you must log on with a user account to which the Scheduled Transfer role is assigned. If the role is not assigned, the Scheduled Transfer tool is not available.

For the Scheduled Transfer tool, configure a location as follows:

1. In GV STRATUS Control Panel, navigate to **General | Locations Config | Locations Configuration | Add**.



2. Configure as follows:

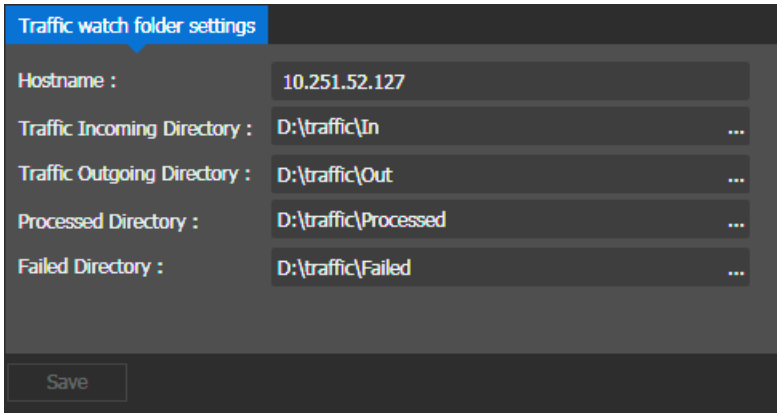
Setting or button	Description
Location Name	The name of the location, as it appears in the application. This can be any name, as appropriate for your workflow. This identifies the Scheduled Transfer location when creating the transfer event in the Inspector.
Description	Your description of the location.
Source / Destination	Set to **Destination**.
Usable by	Set to **Scheduled Transfer**.
Location Path	The UNC path to the folder for the transfer location. You can click the browse icon to launch the Windows dialog and select a specific location in your network.
Location Path Credentials	The credentials required to access the location.

3. Click **Apply**.

Segmentation settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Applications | Segmentation | Traffic watch folder settings**



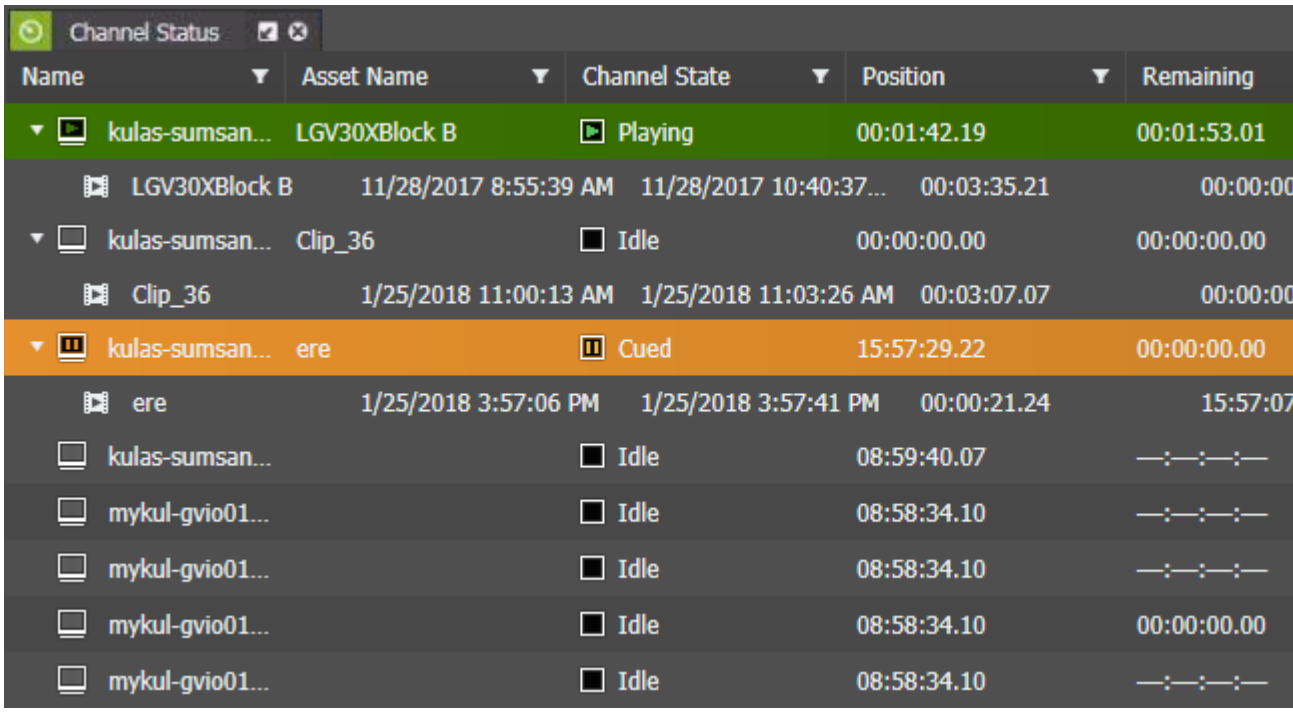
Setting or button	Description
Hostname	Name or IP address of the GV STRATUS server with GV STRATUS Traffic Gateway service.
Traffic Incoming Directory	The path of traffic watch folder for incoming BXF files.
Traffic Outgoing Directory	The path of traffic watch folder for outgoing BXF files.
Processed Directory	The folder path to processed BXF files.
Failed Directory	The folder path to BXF files with failed status.

The Dashboard tool

The Dashboard tool allows you to view information about the current activity on the GV STRATUS system.

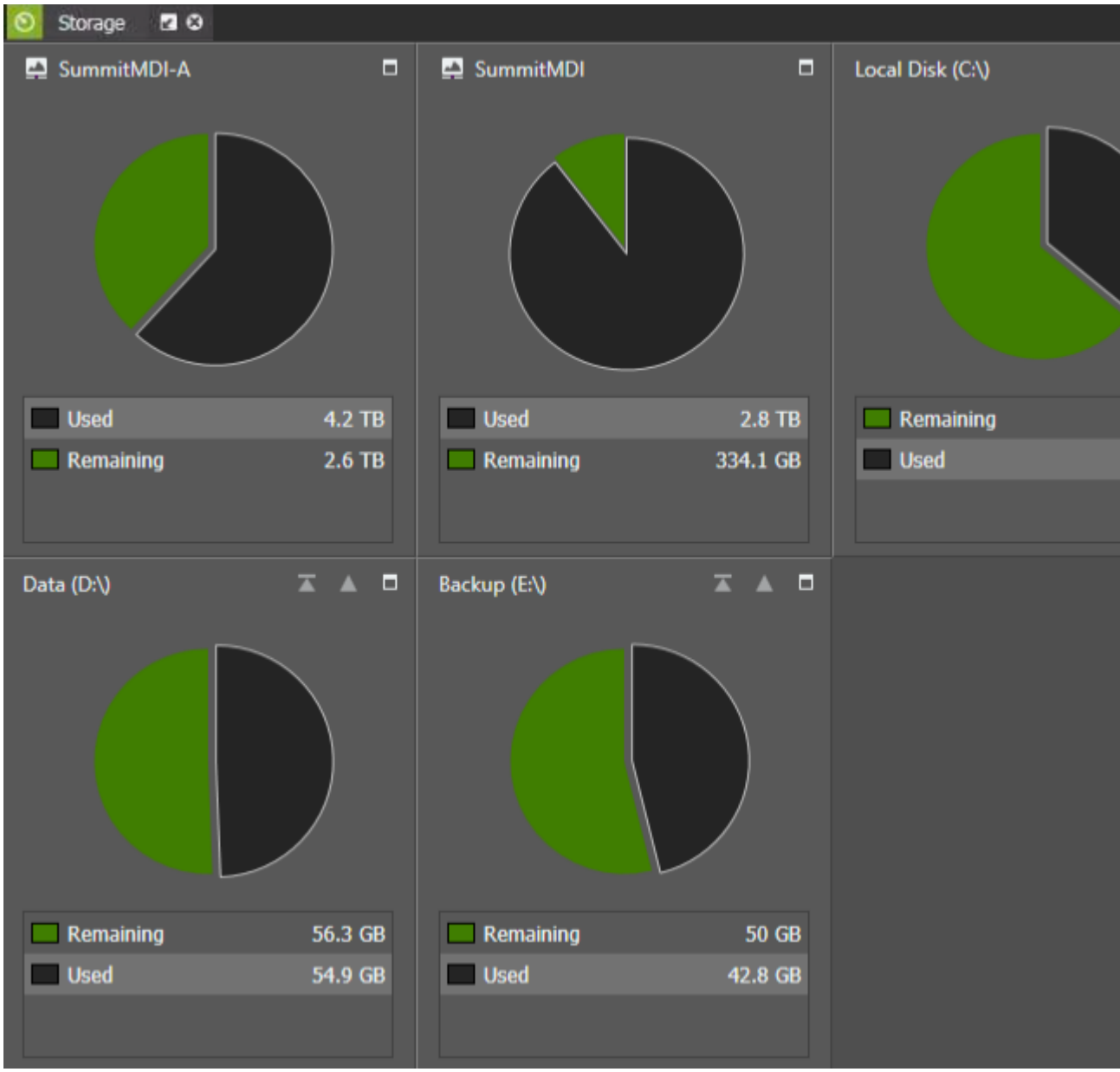
You can view the Dashboard tool either in the GV STRATUS application or the GV STRATUS Control Panel. You can also drag and drop any Dashboard panel into the **Favorites** section in the Navigator to easily access your Dashboard status. If you are assigned with appropriate roles in the GV STRATUS Control Panel, these options are available for the Dashboard tool under the Monitors node.

The Channel Status displays channel state and usage information when selected. You must be assigned with the **Dashboard** and **Dashboard - Channel Status** roles in order to view the panel. You can customize the display of list items, similar to Asset List items, with features such as sort, filter, and add/remove columns.

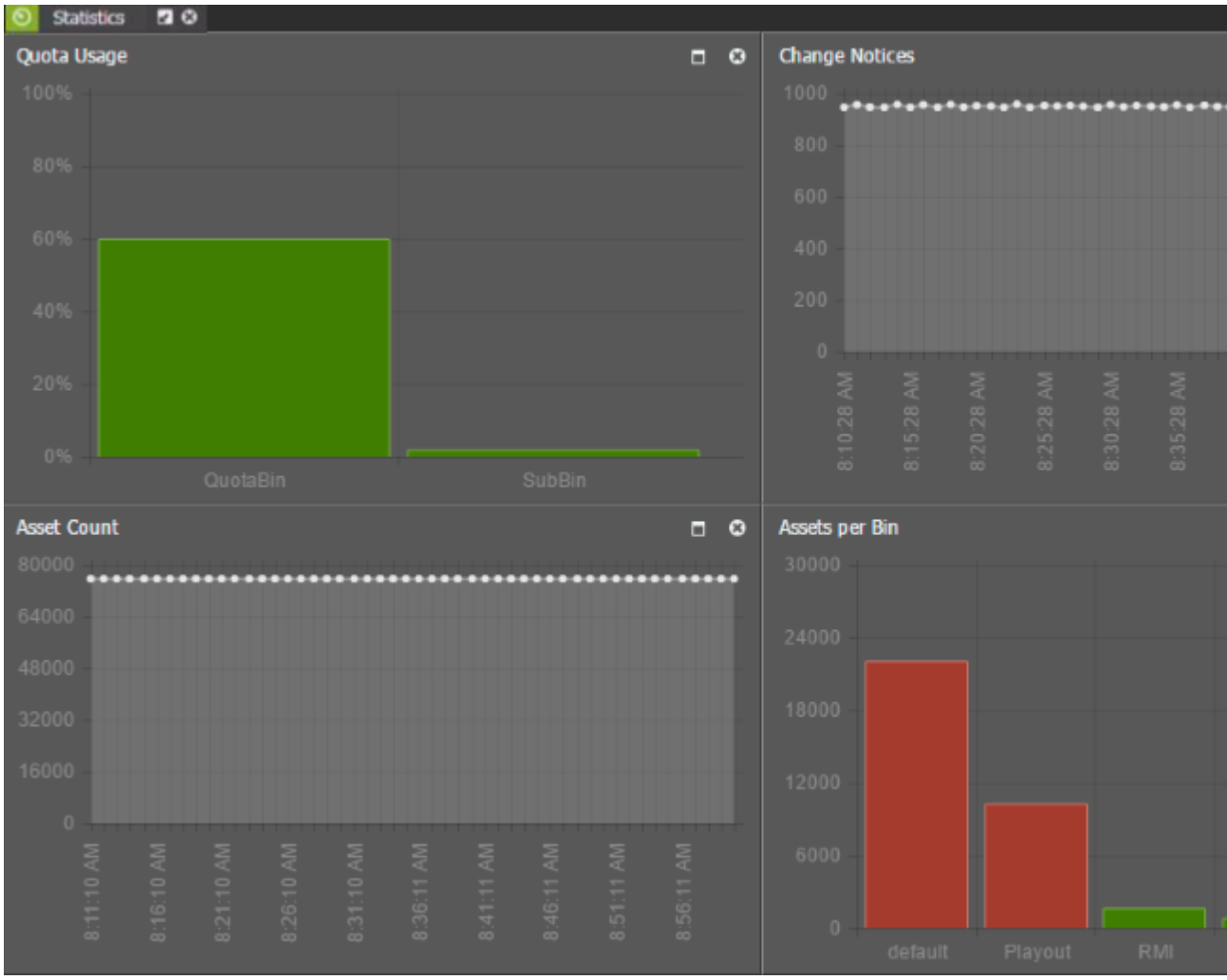


When a channel has an asset loaded, the asset details display in an expandable, separate line below the channel. You can also view the status of each channel whether it's idle, recording, or cueing assets.

The Storage panel reports storage capacity available on K2 devices and the local GV STRATUS PC. K2 storage displayed in the Storage dashboard panel now reflects 100% of its volume instead of the previous value of approximately 95%. You must be assigned with the **Dashboard** and **Dashboard - Storage** roles in order to view the panel. You can right-click on the **Used** report to explore storage levels further. Those storage reports can also be viewed via an internet browser at:
http://<coreservername>/webapps/statistics/?mode=storage

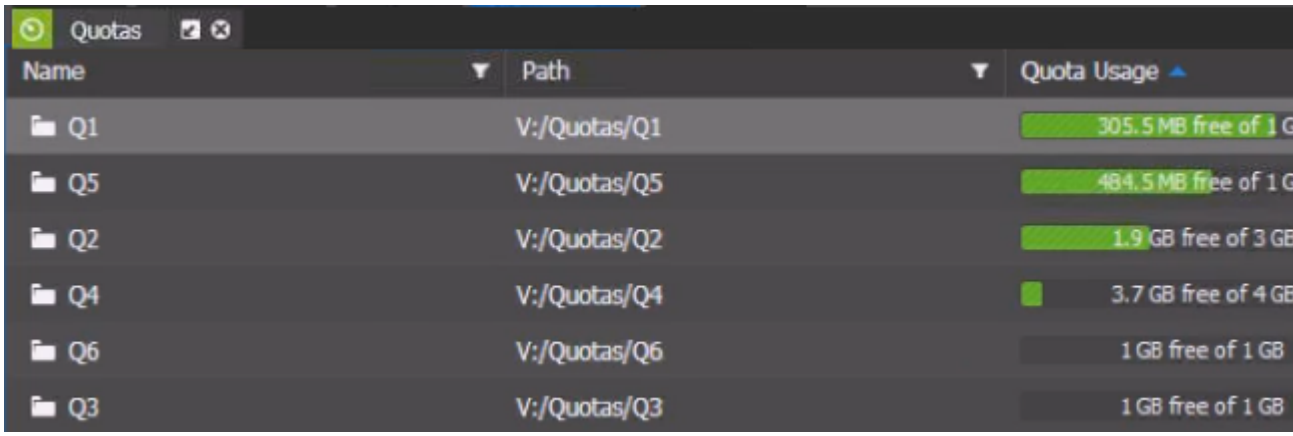


The Statistics panel displays data in graphical form for change notices, asset count, user sessions, system sessions, quota usage, and top 5 of assets per bin in the GV STRATUS system. In order for the Statistics panel to display via the Dashboard, the **GV STRATUS Web Apps** SiteConfig role must be installed on the GV STRATUS Core server. You must also be assigned with the **Dashboard** and **Dashboard - Statistics** roles in order to view the panel. Alternatively, those statistics can be viewed via an internet browser at: `http://<coreservername>/webapps/statistics/`

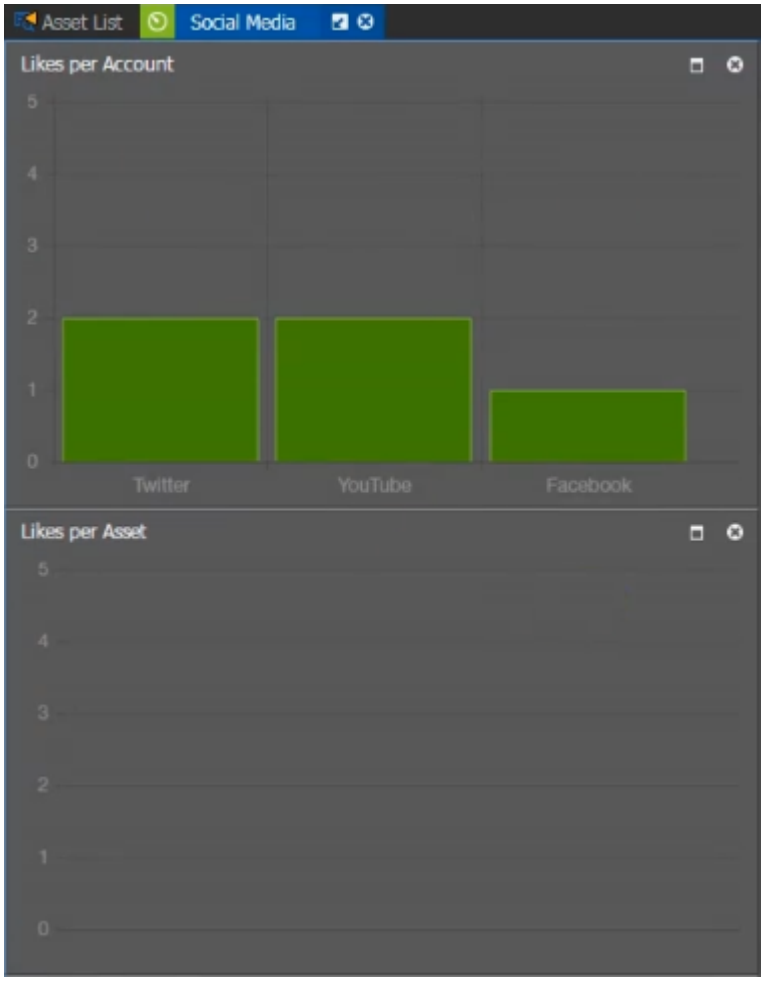


The Quotas panel displays the amount of disk space that the GV STRATUS system reserved for specific bins and the current quota usage. You must be assigned with the **Dashboard** and **Dashboard - Quotas** roles in order to view the panel. The quota of each bin is configurable via the StorNext Administration application on K2 Summits. The quota display turns orange when the disk space is less than 100MB of the limit, and turns red when it reaches the limit. The Quota Status icon displays on the status bar when the quota limit is reached. You can click the icon to launch the status viewer panel and view the quota limit.

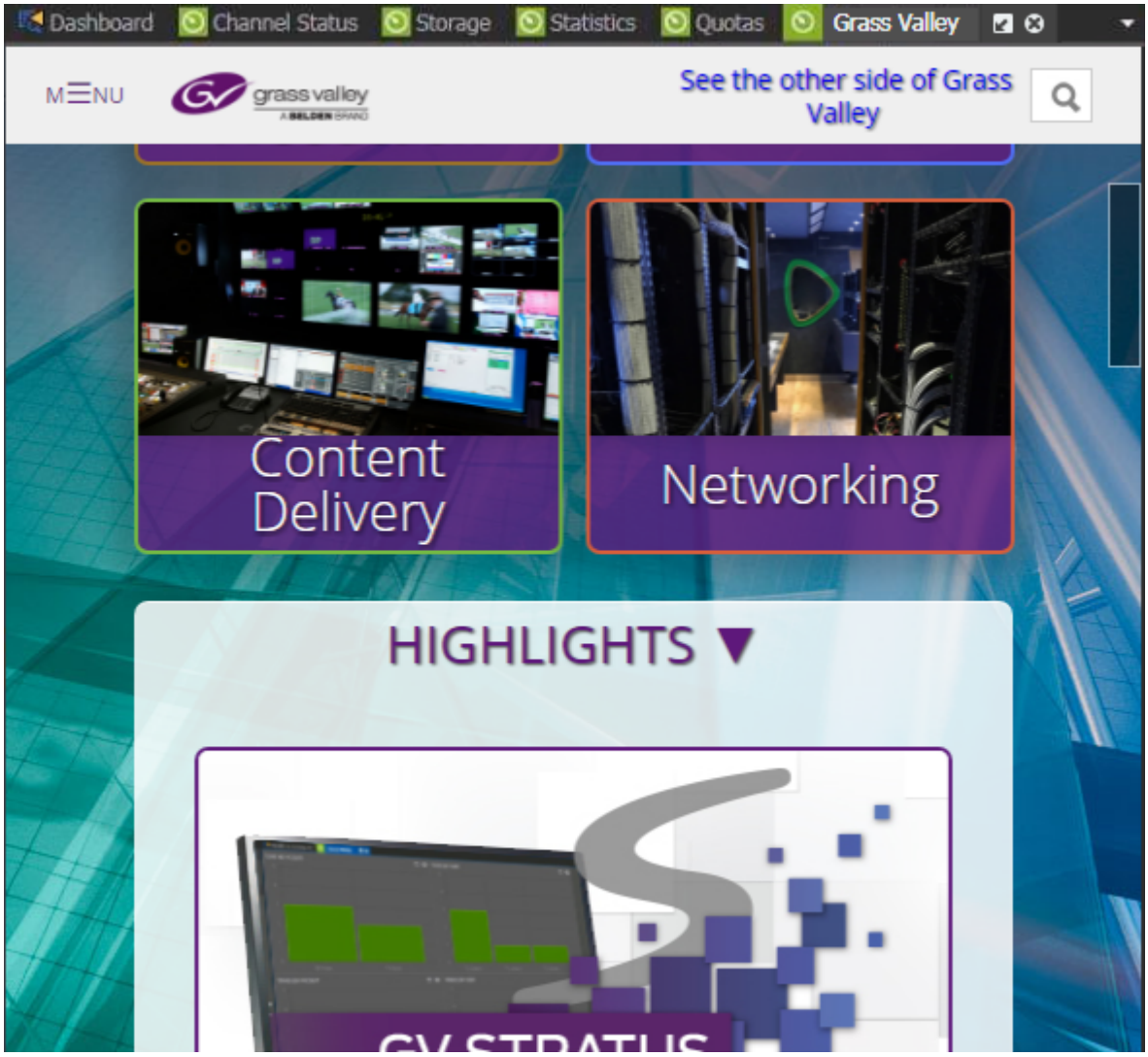
NOTE: The quota limit on K2 Summit system is only supported for K2 SAN media folders.



The Social Media panel displays data in graphical form for statistical information of all Social Media platforms. You must be assigned with the **Dashboard** and **Dashboard - Social Media** roles in order to view the panel. Once an asset is published via the configured social media account, it is possible to gather statistical data such as (View-, Like- and Share-) counts from the social media platform. In addition to the display via the Dashboard tool, those statistics can also be viewed via an internet browser at: `http://<coreservername>/webapps/statistics/?mode=social-media`



If a webpage is configured in GV STRATUS Control Panel for display in the Dashboard tool, you can select the webpage under Dashboard options and view the display on a separate panel.

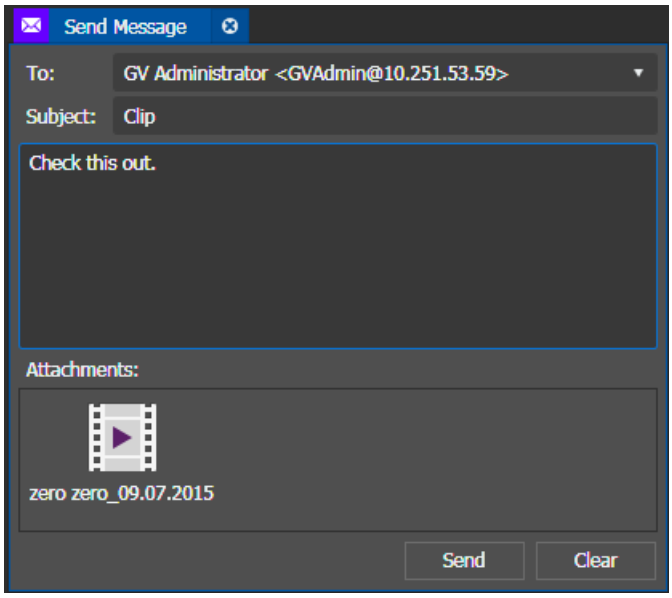


Related Topics

Web Monitor Add/Modify settings on page 377

The Send Message tool

The Send Message tool allows you to send and receive messages with attachments. If you are logged on to a GV STRATUS application you can send a message to another person that is currently logged on to a GV STRATUS application and on the same network subnet. The Send Message tool appears in the GV STRATUS application and in the GV STRATUS Control Panel application when you launch it from the Navigator panel.



Send Message tool features are as follows:

- To field — Specifies the GV STRATUS user to whom the message is sent. Select a user from the drop-down list.
- Subject field — Contains the title of the message.
- Message field — Contains the message.
- Attachments field — Provides a field to which you drag attachments.
- Send button — Sends the message.
- Clear button — Clears all fields in the Send Message panel.

You can attach the following:

- Clips
- Playlists
- Saved searches
- Workspaces
- Bins
- Logging buttons
- Button Panels
- Advanced Logging Tool composite panel
- Tools
- Devices
- Locations
- Monitors
- Channel Panels
- Drives

When you send an attachment, you are actually sending a link to the attachment, rather than the attachment itself.

When you receive a message, a Message dialog box opens and displays the message. If the message has an attachment, you can do the following:

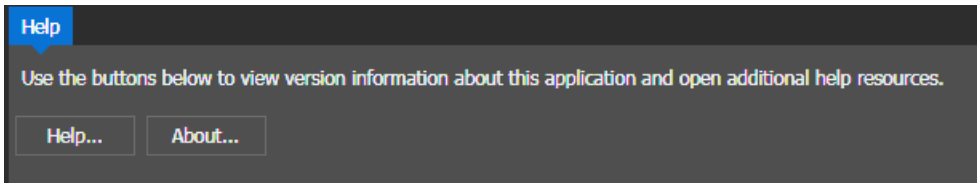
- Open the attachment by double-clicking it.
- Create a copy of the attachment in the Navigator panel or drag it to other panels in the GV STRATUS application. Consider the size of the attachment before creating a copy.

The Send Message tool is more similar to Instant Messaging than it is to E-mail, as there is no Outbox or Inbox functionality to store messages. If a person is not logged on to a GV STRATUS application you can not send them a message. Likewise, if you are not logged on to a GV STRATUS application you can not receive a message.

The Help tool

The Help tool allows you to view the **About GV STRATUS Control Panel** dialog box and **GV STRATUS Control Panel Help Topics**. The **About GV STRATUS Control Panel** dialog box consists of version information, while **GV STRATUS Control Panel Help Topics** display a compilation of resources for the application.

To locate this information, click **Help | Help** .



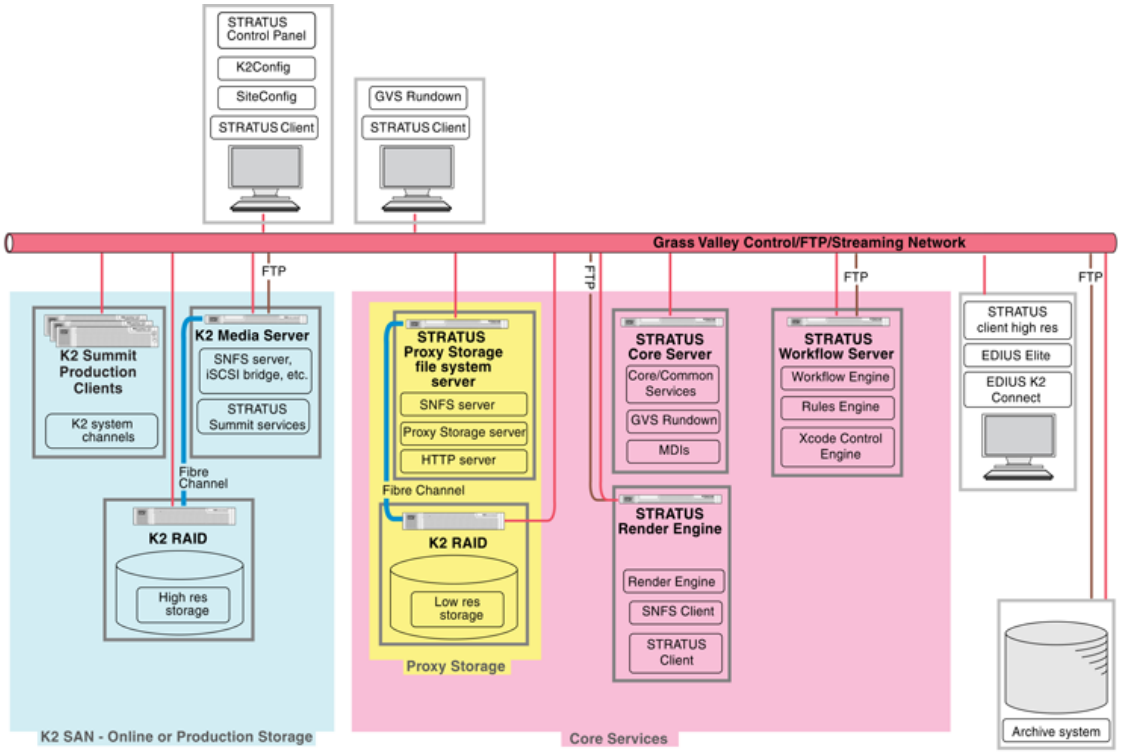
Button	Description
Help	Opens the **GV STRATUS Control Panel Help Topics**.
About	Opens the **About GV STRATUS Control Panel** dialog box.

Understanding system concepts

Understanding networks

Read the topics in this section for a better understanding of your system.

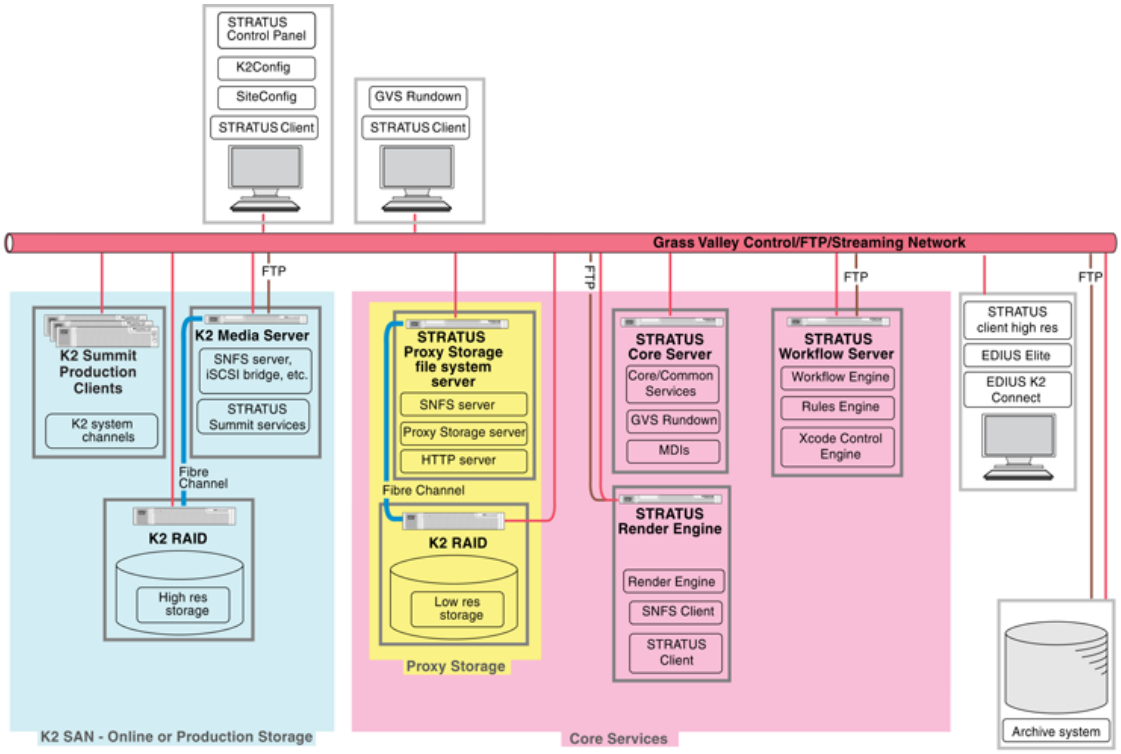
Control network description



The control network is for communication between devices and components. It does not have real-time media traffic or streaming/FTP media traffic. The control network traffic must be separated from the streaming/FTP network traffic and the media (iSCSI) network traffic. This separation may be provided by different subnets, VLANs, or physical switch fabrics. The control network and the streaming/FTP network, if on different subnets, may be on the same VLAN. The control network and the media (iSCSI) network must not be on the same VLAN. Static IP addresses with name resolution via host files are recommended for the control network.

The control network also carries low-resolution traffic, both live streaming (multicast) and proxy file access.

Streaming/FTP network description



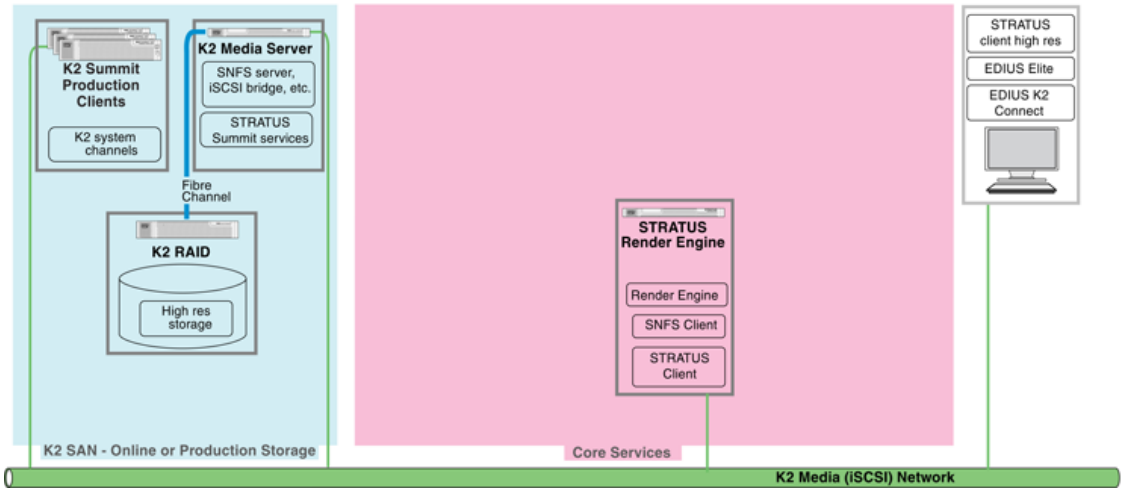
The streaming/FTP network is for media transfers and FTP traffic. The streaming/FTP network network traffic must be separated from the control network traffic and the media (iSCSI) network traffic. This separation may be provided by different subnets, VLANs, or physical switch fabrics. The control network and the streaming/FTP network, if on different subnets, may be on the same VLAN. The control network and the media (iSCSI) network must not be on the same VLAN. Static IP addresses with name resolution via host files are recommended for the streaming/FTP network. Hostnames of network adapters that are dedicated to the streaming/FTP network must be aliased in the hosts file with the `_he0` suffix. This directs the streaming traffic to the correct port.

The streaming/FTP subnet does not carry low-resolution traffic, such as live streaming (multicast) and proxy file access. That traffic is on the control subnet.

In a GV STRATUS system, if you use generic FTP for archive, the streaming/FTP network carries the archive traffic. Dedicated connections to the streaming/FTP network are required on the following GV STRATUS servers:

- Express server
- Core server
- Render Engine server

Media (iSCSI) network description



The media network is exclusively for real-time iSCSI traffic on a K2 SAN. It must be on a different subnet than the control network and the streaming/FTP network. Furthermore, its traffic is kept physically separate from that of other networks. This separation is provided by dedicated ports, cables, and by a dedicated VLAN on the Ethernet switch or by separate switches. Static IP addresses are required for the media network. Name resolution is not necessary, so media network IP addresses are not required in host files.

Corporate LAN network description

The Corporate LAN is the external customer LAN. GV STRATUS client PCs that use a low-resolution media workflow are typically on the corporate LAN. If so, the GV STRATUS server(s) with role of Core Server and role of Proxy Server must have network access to the corporate LAN.

If GV STRATUS clients are on the corporate LAN, the network carries low-resolution traffic, both live streaming (multicast) and proxy file access.

Related Topics

About the corporate LAN and SiteConfig on page 439

Networking tips

- Before configuring any devices for networks, determine the full scope of IP addresses and names needed for the all the machines in your system. Work with the network administrator at your facility to have IP addresses and names available for your use.
- It is recommended that you use the patterns offered in SiteConfig by default to establish a consistent convention for machine names and IP addresses. You can plan, organize, and enter this information in SiteConfig as you develop a system description. You can do this even before you have devices installed and/or cabled.

- On 64-bit devices, configure IPv4 addresses. Disable the IPv6 interface of the Control and FTP interfaces. SiteConfig always configures IPv4 addresses for 64-bit devices.

Network considerations and constraints

- If your GV STRATUS system is on a domain, all servers and client PCs on that system that have any interaction with Grass Valley components must be logged on to Windows with a domain user account. Do not use a local user account.
- Do not use any 10.1.0.n or 10.2.0.n IP addresses. These are used by the K2 RAID maintenance port and must be reserved for that purpose. If these addresses are otherwise used, maintenance port communication errors occur.

Network load balancing

Large GV STRATUS systems can require network load balancing to support workflow requirements.

Use standard Microsoft network load balancing techniques, as referenced by the links below, to support the requirements of your GV STRATUS system.

- *Overview of Network Load Balancing*
- *Installing Network Load Balancing*
- *Creating a Network Load Balancing Cluster*
- *Adding a host to a Network Load Balancing Cluster*

About host files

The hosts file is used by the control network and the streaming/FTP network for name resolution, which determines the IP address of a device on the network when only the device name (hostname) is given. The hosts file is located at `C:\Windows\system32\drivers\etc\hosts` on Windows XP and later operating systems. The hosts file must be the same on all network devices. It includes the names and addresses of all the devices on the network.

For FTP transfers on a K2 SAN, transfers go to/from K2 Media Servers that have the role of FTP server. No transfers go directly to/from the shared storage K2 clients that are on the K2 SAN. To support FTP transfers, in the hosts file the K2 Media Server hostname must have the `_he0` extension added at the end of the name and that hostname must be associated with the K2 Media Server's FTP/streaming network IP address.

Here is an example of IP addresses and names associated in a hosts file:

```
192.168.100.11   root_server_1
192.168.101.11   root_server_1_he0
192.168.100.21   root_server_2
192.168.101.21   root_server_2_he0
192.168.100.31   root_server_3
192.168.101.31   root_server_3_he0
192.168.100.41   root_server_4
192.168.101.41   root_server_4_he0
```

```
192.168.100.51   root_raid_1
192.168.100.61   root_gige_1
```

In this example 192.168.100.xx is the control network and 192.168.101.xx is the streaming/FTP network. Each K2 Media Server has its hostname associated with its control network IP address. In addition, each K2 Media Server (that has the role of FTP server) has its *_he0* hostname associated with its streaming/FTP network address.

Use SiteConfig to define your networks and devices. When you do so, SiteConfig creates the correct hosts file and copies the hosts file to each network device. This enforces consistent hosts files across networks and reduces errors introduced by editing and copying hosts files on individual devices. You can also view hosts files from SiteConfig for troubleshooting purposes.

About GV STRATUS client PCs

Depending on your site's system design and licensing, customer-supplied GV STRATUS client PCs are connected for media access as follows:

- Low-resolution client PC on the corporate LAN — This is the typical setup to access the GV STRATUS application and the EDIUS XS application from a standard PC desktop. The applications accesses proxy media via the corporate LAN to support the workflow, so the only connection required is the PC's existing connection to the corporate LAN. By default, the GV STRATUS application and the EDIUS XS application access low-resolution live streaming and proxy media, so no configuration in Control Panel Proxy Access settings is necessary. GV STRATUS and EDIUS XS authorization and licenses for the client PC are assigned and managed by the GV STRATUS server with role of Common Server.
- High-resolution client PC on K2 media (iSCSI) network — This setup is for high-resolution workflows, such as those that integrate with a high-resolution editor such as EDIUS Workgroup. The GV STRATUS application accesses the high-resolution assets via the media network to support the workflow. Two connections are required: one to the control network and one to the media network. The PC must be set to high-resolution in GV STRATUS Control Panel Proxy Access settings to enable the GV STRATUS application to access high-resolution media. A GV STRATUS high-resolution license is also required for the client PC. The high-resolution license is not managed by the GV STRATUS server with role of Common Server. The EDIUS license is installed on the PC and is managed by EDIUS license management. Other authorization and licensing is identical to the client PC on the corporate LAN.
- Client PC with SMB mount connection to K2 storage — This setup is for high-resolution workflows, such as those that integrate with a high-resolution editor such as EDIUS Workgroup. The GV STRATUS application accesses the high-resolution assets via a SMB mount, typically to the *V:* drive, to support the workflow. Two connections are required: one to the control network and one to the Grass Valley storage. The PC must be set to high-resolution in GV STRATUS Control Panel Proxy Access settings to enable the GV STRATUS application to access high-resolution media. A GV STRATUS high-resolution license is also required for the client PC. The high-resolution license is not managed by the GV STRATUS server with role of Common Server. The EDIUS license is installed on the PC and is managed by EDIUS license management. Other authorization and licensing is identical to the client PC on the corporate LAN.

- Client PC on control network only — This setup is supported for cases where it is convenient to connect to the control network rather than to the corporate LAN. All functionality is identical to the client PC on the corporate LAN.

Related Topics

Client PC set up process on page 253
GV STRATUS client on page 229
Install/configure for SiteConfig support on client PC on page 261
Set up RMI PC access to high-resolution assets on page 557

About the GV STRATUS Assets view

In the Navigator panel, the Assets node provides a view that is based on the information available in the GV STRATUS Database. This allows the GV STRATUS application to provide you with flexibility for viewing and organizing your assets. You can configure bins and folders based on users, projects, events, or other parameters to suit your particular workflows.

Under the Assets node are the following nodes:

- Groups — Provides a view of folders that can contain assets from any location in the GV STRATUS system. This allows you to create folders and group assets without being constrained by the locations of the assets. The folders you create are visible and accessible by everyone on the GV STRATUS system. The folders exist in the GV STRATUS Database but not in K2 Summit/SAN storage. In previous Grass Valley products, Groups were known as "Collections".
- Locations — Provides a view of bins in K2 Summit/SAN storage. When you create a bin, it is created in K2 Summit/SAN storage.
- EDIUS Projects — Provides a view of bins in the EDIUS Projects folder. The EDIUS Projects node appears under the Assets node only if logged-in users have the EDIUS Project Management role assigned to them. While an EDIUS project is being edited, the project and its included sequences and clips are locked in the GV STRATUS application.

The Navigator panel also provides a Devices node. Under the Devices node you find the local computer on which the GV STRATUS application is installed. Archive servers configured in GV STRATUS Control Panel are also shown under the Devices node if you have the Archive Rights or Restore Rights roles.

If you have the role of Media Manager, as configured in GV STRATUS Control Panel, the Navigator panel also provides the following:

- The Groups view includes the Lost and Found folder, which you can check for assets that do not have a location or that might not be otherwise accessible in the Assets view.
- Permission is granted to move assets from an archive system to the GV STRATUS system. Without this permission, assets may be copied but not moved.

The GV STRATUS Database controls both the Assets view and the Devices view. The database keeps the operations you perform in synchronization with the GV STRATUS/K2 system overall. The GV STRATUS Database also associates extended metadata with each of your assets, as well

as keeps track of relationships between assets. You can use this metadata as search criteria with the advanced search tool.

Related Topics

About the Lost and Found folder on page 469

About GV STRATUS system databases

The GV STRATUS system has an SQL database, which contains the following databases:

GV STRATUS Database	The database that provides the core asset management functionality to the GV STRATUS system. The database contains a repository of media asset management information about the GV STRATUS system. Other components in the system refer to the GV STRATUS Database for necessary information during configuration or while the system is operating. This is a SQL database. The SQL database name is MediaFrame.
License Management Database	The database for the assignment of GV STRATUS licenses and roles to groups and users This is a SQL database. The SQL database name is LicenseManager.
Ingest Database	The database for the Scheduler tool. This is a SQL database. The SQL database name is ISDB.
SDB	SDB is the acronym for Simple Database, which is the database server component for GV STRATUS Rundown. It provides status on clips and on playlists associated with NCS rundowns.
Workflow Database	The database for the workflow engine. Stores the workflow templates. This is a SQL database. The database name is MediaFlow.
WfPersistence Database	The database for the runtime data of the workflow engine. Stores the current state of running workpackages. This is a SQL database. The database name is WfPersistence.
Rules Engine Database	The database for the Rules Engine. Stores the rules and the current state of the active rules. This is a SQL database. The database name is RulesEngine.

On the GV STRATUS Core server or standalone Database Server, default directories for SQL database-related files are as follows:

- Database Engine user databases — `D:\SQL`
- Database Engine user database logs — `C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Data`
- Database Engine TempDB files — `D:\SQL`
- Database Engine TempDB log files — `C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Data`
- Database Engine backup files — `C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Backup`

About redundant K2 SANs

If your GV STRATUS system accesses a redundant K2 SAN, it introduces some considerations for operation and maintenance. A redundant K2 SAN has two K2 Media Servers (FSMs) that have the role of media file system server. These are redundant servers, so either server can be primary and either server can be backup. At any given time, one operates as the primary server and the other operates as the backup server. All K2 SAN media access takes place via the primary server, with the backup server online in a standby mode. Should a fault occur on the primary, a failover event occurs in which the backup becomes primary and the former primary shuts down.

In the GV STRATUS application you do not see the two K2 Media Servers in the Navigator tree-view. Instead, you see the K2 SAN represented as one location in the Assets view. Regardless of which redundant server is currently primary, you see no difference in your view of assets. This view of the K2 SAN is defined when you configure the Grass Valley Media Server MDI in the GV STRATUS Control Panel application.

In the GV STRATUS Control Panel application, K2 Storage settings provide a view of your K2 SAN that reports the primary or backup status of K2 Media Servers. When you refresh the view the report of primary/backup status is updated.

In the GV STRATUS Control Panel application, the same send destination locations must be configured for both primary and backup servers in the redundant K2 SAN system. In the case of a failover event, send destination locations will still be available for GV STRATUS and EDIUS applications.

If a failover event occurs on the redundant K2 SAN, a proxy-workflow GV STRATUS application momentarily suspends access to assets on the K2 SAN. After the failover event is complete, you can repopulate Asset Lists and other views of assets to continue with your media operations. Refer to the "Installing and Servicing the K2 SAN" section of the K2 Topic Library for more information about K2 SAN failover and steps for recovery after a failover.

About GV STRATUS markers, Dyno markers, and the K2 database

Marker information is stored in the GV STRATUS database and in the K2/Summit/SAN database. You can configure the way the GV STRATUS system synchronizes marker information between the databases. If you use the K2 Dyno Replay Controller as part of your workflow, you must consider this synchronization, since a Dyno marker is in the K2 database and a GV STRATUS marker is in the GV STRATUS database.

Another consideration is the number of markers in the K2 database. A very large number of markers can exceed the capacity of the K2 database. You can check logs on the K2 Summit/SAN system for messages about the database size. If it exceeds 80MB, there is a risk of database errors. If all GV STRATUS markers are synchronized to the K2 database the risk of exceeding the capacity increases. Grass Valley recommends that you only synchronize GV STRATUS markers to the K2 database if required by your Dyno workflow and that you adopt policies to limit the number of markers in the K2 database.

Your options for marker synchronization are as follows:

- Partial — One-way marker creation from Dyno to GV STRATUS, then two-way marker modification and deletion. This is the default synchronization method, and is appropriate for most workflows.
- Full — Two-way creation, modification, and deletion between Dyno and GV STRATUS.

To further reduce the number of markers, the system limits markers in subclips. If configured for partial synchronization, markers in the parent clip are inherited by the GV STRATUS subclip but are not inherited by the Dyno subclip. If configured for full synchronization, markers in the parent clip are not inherited by the GV STRATUS subclip or by the Dyno subclip.

Depending on the synchronization option you select, when you perform operations the GV STRATUS system responds with behaviors as follows:

Table 13: Partial synchronization

Operation —>	Behavior —>	Operation —>	Behavior —>	Operation —>	Behavior
Create Dyno marker A.	Marker A synchronized to GV STRATUS.	Modify or delete GV STRATUS marker A.	Change to marker A synchronized to K2 database/Dyno.	Modify or delete Dyno marker A.	Change to marker A synchronized to GV STRATUS.
Create GV STRATUS marker B.	None. Marker B not synchronized to K2 database/Dyno.	Modify or delete GV STRATUS marker B.	None. Marker B not in K2 database/Dyno.	—	—
Create Dyno marker C in clip D.	Marker C synchronized to GV STRATUS.	Create GV STRATUS subclip D1 from a portion of clip D that includes marker C.	GV STRATUS subclip D1 includes marker C. Subclip D1 synchronized to K2 database/Dyno. Dyno subclip D1 does not include marker C.	Create Dyno subclip D2 from a portion of clip D that includes marker C.	Dyno subclip D2 does not include marker C. Subclip D2 synchronized to GV STRATUS. GV STRATUS subclip D2 includes marker C.
Create GV STRATUS marker E in clip F.	None. Marker E not synchronized to K2 database/Dyno.	Create GV STRATUS subclip F1 from a portion of clip F that includes GV STRATUS marker E.	GV STRATUS subclip F1 includes marker E. Subclip F1 synchronized to K2 database/Dyno. Dyno subclip F1 does not include marker E.	—	—

Table 14: Full synchronization

Operation —>	Behavior —>	Operation —>	Behavior —>	Operation —>	Behavior
Create Dyno marker A.	Marker A synchronized to GV STRATUS.	Modify or delete GV STRATUS marker A.	Change to marker A synchronized to K2 database/Dyno.	Modify or delete Dyno marker A.	Change to marker A synchronized to GV STRATUS.
Create GV STRATUS marker B.	Marker B synchronized to K2 database/Dyno.	Modify or delete Dyno marker B.	Change to marker B synchronized to GV STRATUS.	Modify or delete GV STRATUS marker B.	Change to marker B synchronized to K2 database/Dyno.
Create Dyno marker C in clip D.	Marker C synchronized to GV STRATUS.	Create GV STRATUS subclip D1 from a portion of clip D that includes marker C.	GV STRATUS subclip D1 does not include marker C. Subclip D1 synchronized to K2 database/Dyno. Dyno subclip D1 does not include marker C.	Create Dyno subclip D2 from a portion of clip D that includes marker C.	Dyno subclip D2 does not include marker C. Subclip D2 synchronized to GV STRATUS. GV STRATUS subclip D2 does not include marker C.
Create GV STRATUS marker E in clip F.	Marker E synchronized to K2 database/Dyno	Create Dyno subclip F1 from a portion of clip F that includes Dyno marker E.	Dyno subclip F1 does not include marker E. Subclip F1 synchronized to GV STRATUS. GV STRATUS subclip F1 does not include marker E.	Create GV STRATUS subclip F2 from a portion of clip F that includes GV STRATUS marker E.	GV STRATUS subclip F2 does not include marker E. Subclip F2 synchronized to K2 database/Dyno. Dyno subclip F2 does not include marker E.

Related Topics

STRATUS Core Services settings on page 296

About loop modes in K2, Dyno, and GV STRATUS

Support for loop modes varies on Grass Valley products.

Grass Valley products provide features for putting an asset into a loop mode. Products and their loop modes are as follows:

- K2 AppCenter:
  - Loop play: Allows the clip to play in a continuous loop until stopped.
  - Continuous record: Allows you to specify a fixed-length recording that records continuously. When the fixed length you specify is reached, AppCenter begins to erase the oldest media in 3 minute segments to make room for new media.
- GV STRATUS:
  - Loop play (Loop Playback): Loops the current asset between mark in to mark out.
- K2 Dyno:
  - Loop record (LoopRec): Same as K2 AppCenter Continuous record.

While the GV STRATUS application can access the same K2 Storage as K2 AppCenter and K2 Dyno, the GV STRATUS application does not support a recording loop mode. Therefore, in the GV STRATUS application, do not attempt to access an asset while it is in a loop record mode. The asset can be put into this type of loop mode by K2 Dyno or K2 AppCenter.

About custom fields

Custom fields enhance site-specific management of assets. In the GV STRATUS Control Panel application you can define a custom field to create an asset metadata-type that uniquely fits your site's workflow. In the GV STRATUS application you can then assign metadata to an asset by entering text or making a selection in the custom field. Adding custom fields is optional.

Related Topics

Custom Metadata settings on page 318

About timecode source and clock synchronization

Timecode is a continuous sequence of data embedded in a clip from beginning to the end in order to provide time reference for logging, synchronization, and tracking. It enables editing of a media file by identifying specific timeframe, and marking those in and out timecodes as reference points. There are several timecode sources depending on the recorder and timecode generator of the media file.

The GV STRATUS application supports these timecode sources:

Timecode Source	Description
AncVITC	Available on HD channels only. Timecode is read from ancillary VITC.

Timecode Source	Description
VITC	Available on SD channels only. Timecode is read from the VITC input for the channel.
LTC	Available on HD/SD channels. Timecode is read from the LTC input for the channel.
AncLTC	Available on HD channels only. Timecode is read from ancillary LTC.
Time of Day	Available on HD or SD recordings. Time of Day is an internal generator. You can select either LTC feeds or Windows system clock as the clock source to drive the generator. LTC feeds can be from Channels 1, 2, 3, or 4.
Start Time	Available in HD or SD. When Start Time is selected, you can specify the timecode to use when the recording starts. The drop frame option is enabled when the system timing is set to the 525 line standard (NTSC). Drop frame timecode allows the generator to operate as an accurate clock.

Clock synchronization is required on all GV STRATUS servers and K2 Summit/SAN systems. Ensure that K2 Summit/SAN systems are locked to house reference and clocks on all machines are kept in sync. This is especially important on systems with Ingest Scheduler and Scheduled Transfer tools, as they must be kept in sync with the GV STRATUS Core server and K2 Summit/SAN systems.

About advanced query syntax, advanced searches and custom expressions

A combination of search features provide flexibility in creating GV STRATUS searches. Entering text with advanced query syntax is available in both the Simple Search tool and the Advanced Search tool. The Advanced Search tool provides additional capabilities.

The advanced query syntax available when you enter text is as follows:

- If you search on one or more words (with no search syntax), the search returns assets that match all the words in any order. This is the Boolean "AND" operator. This is a change from previous versions, where this was a phrase search.
- Search syntax is as follows:
  - If you enter words surrounded by quotation marks, the search returns assets that match that exact phrase, with the words in the exact order.
  - Text surrounded by quotation marks is searched literally. Any search syntax or operators within the quotation marks are interpreted as plain text instead.
  - Simple boolean operators AND, OR and NOT are supported. Enter these operators in all capital letters.
  - Parenthesis control the precedence of the boolean operations.

The following are advanced query syntax examples. Each example is followed by the steps the GV STRATUS system goes through as it processes the search:

- “the quick brown” (fox OR dog) jumped over the NOT lazy cat

  1. Contains the phrase “the quick brown” AND
  2. Contains ‘fox’ or ‘dog’ AND
  3. Contains ‘jumped’ AND
  4. Contains ‘over’ AND
  5. Contains ‘the’ AND
  6. Does not contain ‘lazy’ AND
  7. Contains ‘cat’

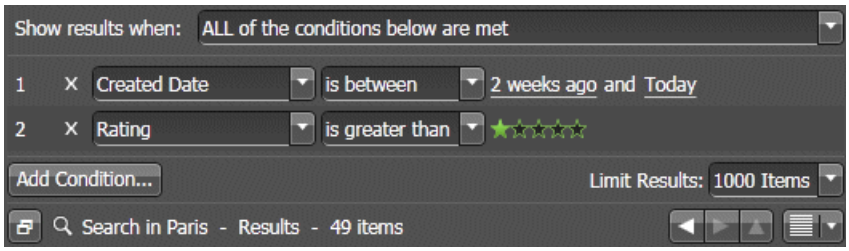
- abc AND (def OR ghi)

  1. Contains ‘abc’ AND
  2. Contains ‘def’ OR ‘ghi’

- abc AND def OR ghi

  1. Contains ‘abc’ AND ‘def’ OR
  2. Contains ‘ghi'

The **Advanced Search Toggle** button ... next to the Simple Search tool provides additional capabilities to the search tool.



You can search using multiple conditions. You define the type of search as follows:

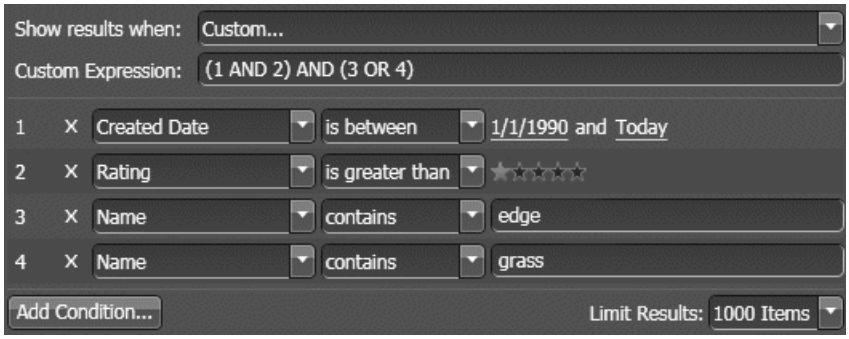
- ALL of the conditions below are met — This is the Boolean "AND" operator. The search returns assets that match all conditions. Only conditions with values (conditions that are not blank) are included in the search.
- ANY of the conditions below are met — This is the Boolean "OR" operator. The search returns assets that match any of the conditions. Only conditions with values (conditions that are not blank) are included in the search.

- Custom — You can enter text to create a custom expression using Boolean operators.

  In your custom expression, you use the condition numbers (1, 2, 3, 4, etc) to represent the condition on which you are searching. For example, if you have configured condition 1 as "Asset Name is basketball" and condition 2 as "Asset Created is Today", then entering custom expression "1 AND 2" finds assets named basketball created today.

  The "OR" and "AND" operators are at the same precedence, so for complex expression you use parentheses to group relationships. The following are examples of complex expressions:

  - (1 AND 2) OR (1 AND 3)
  - ((1 AND 4) OR 3) AND ((2 OR 4) AND 3)



You can use advanced query syntax in the Advanced Search tool. When you create a "contains" condition that searches a text field, you can enter text with advanced query syntax to search that field. The following is an example of this type of condition:

- Name | contains | guitar NOT rock

In this way a search in the Simple Search tool is equivalent to a "contains" search that searches multiple text fields by default. For a simple search you can enter text with advanced query syntax. Assets with names, tags, descriptions, comments, marker text, or custom text data that match the search are returned.

You can also search for custom metadata in the Advanced Search tool. In addition, the custom metadata search allows you to search for an empty field.

For an extended application of boolean logic in the Advanced Search tool, you can create multiple conditions that search text fields, each of which use advanced query syntax. Then you can combine those conditions as a custom expression.

Related Topics

Searching assets with the advanced search tool on page 992

Understanding credentials

Read the topics in this section for a better understanding of your system.

Related Topics

About credentials in SiteConfig on page 42

Passwords and security on Grass Valley systems

To provide a basic level of security, Grass Valley systems recognize three different security levels based on Windows users and groups, and the systems ship from the factory with accounts pre-configured accordingly. To access the system you must log on with the user name and password for one of the pre-configured accounts.

The following table shows the different types of users and their privileges.

	Windows administrator	Grass Valley product administrator	K2 product administrator	Grass Valley product user
User name	Administrator	GVAdmin	K2Admin	GVUser
AppCenter Configuration Manager	Full access	Full access	Full access	Can view
AppCenter	Full access	Full access	Full access	Full access; requires an account on the K2 Summit system
Storage Utility	Full access	Full access	Full access	Can't access
K2Config	Full access	Full access	Full access	Can't access
Server Control Panel	Full access	Full access	Can view	Can view
Windows Operating System	Full access	Full access	Limited access (based on Windows user account privileges).	Limited access (based on Windows user account privileges)

To support legacy FTP and security features, K2 systems also have *movie*, *mxfmovie*, *mpgmovie*, and *video_fs* accounts. Do not use these accounts to log in to the Windows operating system on K2 systems.

Related Topics

About credentials in SiteConfig on page 42
Set credentials on page 266
Changing passwords on page 710
GV STRATUS servers logon account on page 245

K2 and GV STRATUS security considerations

Access Control Lists (ACLs) specify individual user or group rights to specific system objects such as programs, processes, or files. K2 Summit systems enforce ACLs for security and permissions on K2 bins and channels, while the GV STRATUS system has its own mechanism for security. The

GV STRATUS system always accesses the K2 Summit system via the internal system account, which by default is GVAdmin, and the K2 Summit system is configured by default to allow full access to that account. This is an important consideration to allow the systems to operate together. Therefore you must not change the default configuration of security and permissions on your K2 Summit systems that are part of your GV STRATUS system. This includes Windows operating system ACL settings and K2 AppCenter security/permission settings on bins and channels. Changing these settings could prevent the GV STRATUS system from accessing the K2 Summit system. Configure security using GV STRATUS security only. Do not configure K2 Summit security.

About groups and users on a GV STRATUS system

If your GV STRATUS system is on a domain, all servers and client PCs on that system that have any interaction with Grass Valley components must be logged on to Windows with a domain user account. Do not use a local user account.

GV STRATUS licensing and roles are applied to Windows operating system groups and users. Any groups or users to which you assign GV STRATUS licenses or roles must be available for authentication on the GV STRATUS server with role of Common Services, which is typically the GV STRATUS Core server, and on all K2 devices that are part of your GV STRATUS system. This includes the following devices:

- GV STRATUS servers
- K2 Summit standalone systems
- K2 Summit SAN-attached systems
- K2 Media Servers

Groups and/or user accounts are not authorized on the GV STRATUS client PC itself. When you log on to an application from a client PC, you are authorized against the roles assigned to the accounts available on the GV STRATUS Core server as follows:

- GV STRATUS application — If you are using a domain, the log on accounts are on the domain server and are managed by the domain so the GV STRATUS Core server must be on the domain. If you are using a workgroup, the log on accounts must be a part of the workgroup on the GV STRATUS Core server.
- GV STRATUS Control Panel application — You must log on with Windows administrator credentials in order to have access to all the configuration settings in the GV STRATUS Control Panel application. The log on account must be a part of the local Windows administrator account on the GV STRATUS Core server. This is required whether you are using a domain or a workgroup. If you are using a domain, you can additionally add the log on account to the domain administrators group.

  If on a network Workgroup, to configure Authorization Manager settings, you must be running GV STRATUS Control Panel on the GV STRATUS Core server.

Understanding virus and security policies

Read the topics in this section for a better understanding of your system.

Windows operating system update policy

Grass Valley recognizes that it is essential to deploy Microsoft security patches to Windows operating system products as quickly as possible. As Grass Valley systems are used to meet the mission-critical requirements of your environment, it is imperative that these systems be kept up to date in order to maintain the highest level of security available. To that end, Grass Valley recommends that for standard-edition Windows operating system products, you install all important updates provided by Microsoft. In the unlikely event that one of these updates causes ill effects to a Grass Valley system, you are urged to uninstall the update and contact Grass Valley customer service as soon as possible. Grass Valley will investigate the incompatibility and, if necessary, provide a software update or work-around to allow the system to properly function with the Microsoft update in question.

Note that this policy applies to "Important" updates only. There are countless updates not classified as "Important" that are made available by Microsoft. If you believe that one or more of these other updates must be applied, contact Grass Valley prior to installation. This policy also applies to standard-edition (not embedded) operating systems only. Do not attempt to update an embedded Windows operating system in any way except as directed by Grass Valley for the specific product.

You should exercise common sense when applying updates. Specifically, do not download or install an update while a Grass Valley product is being used for mission-critical purposes such as play to air.

NOTE: If a computer does not have the Grass Valley* Embedded Security *solution one-time initial deployment process applied, do not install any Windows updates. Apply the one-time process before installing Windows updates.

Related Topics

Embedded Security modes and policies on page 718

Grass Valley anti-virus scan policy

Grass Valley systems are based on the Microsoft Windows operating system. It is important to defend this system against virus or Spyware attacks. However, you must use a strategy that allows you to scan Grass Valley systems without interrupting media access. The Grass Valley Embedded Security solution on K2 and GV STRATUS systems is a qualified strategy. If you use Embedded Security on a device, do not use other anti-virus strategies on that device. Contact Grass Valley Support to determine the strategy best suited to your environment.

Related Topics

Embedded Security modes and policies on page 718

Understanding system configuration tools

Read the topics in this section for a better understanding of your system.

About SiteConfig

SiteConfig is Grass Valley's tool for network configuration and software deployment. SiteConfig is a ProductFrame application. ProductFrame is an integrated platform of tools and product distribution processes for system installation and configuration.

You can use SiteConfig as a stand-alone tool for planning and system design, even before you have any devices installed or cabled. You can define networks, IP addresses, hostnames, interfaces, and other network parameters. You can add devices, group devices, and modify device roles in the system.

As you install and commission systems, SiteConfig runs on a designated PC. It discovers devices, configures their network settings, and manages host files. SiteConfig also manages software installations and upgrades and provides a unified software package with compatible versions for deployment across multi-product systems.

You should use SiteConfig for network configuration and software deployment at installation and throughout the life of the system in your facility. This enforces consistent policy and allows SiteConfig to keep a record of changes, which makes the system easier to maintain and aids in troubleshooting should a problem arise.

SiteConfig displays information from a system description file, which is an XML file.

K2Config

The K2 System Configuration application (K2Config) is the primary tool for configuring systems in the category of a K2 SAN, which include online or production K2 SANs, K2 Nearline systems, and GV STRATUS Proxy Storage systems. Once the devices of the storage system are cabled and are communicating on the control network, you can do all the configuration required to create a working K2 SAN using the K2Config application. When you use SiteConfig for network configuration, you can import the SiteConfig system description file into the K2Config application to get you started with your SAN configuration.

After your K2 SAN is initially installed and configured, if you need to reconfigure the system you should do so using SiteConfig and the K2Config application. This enforces consistent policy and sequencing for configuration tasks, which makes the system easier to maintain and aids in troubleshooting should a problem arise.

The K2Config application runs on a control point PC and accesses the devices of the K2 SAN via the control network. You can configure the devices of the K2 SAN as follows:

- SAN-attached K2/Summit systems and K2 Media Server — These devices are configured directly by the K2Config application.
- K2 RAID storage devices — The K2Config application launches a remote instance of Storage Utility, which configures RAID storage devices. Storage Utility components run on the K2 Media Server and the configuration actually takes place via the Fibre Channel connection between the K2 Media Server and the RAID storage device.
- Ethernet switches — The K2Config application can launch a switch’s web-based configuration application.

You can expand and select nodes in the tree view to view K2 SANs, individual devices, and configuration settings. The configuration file is saved on the V: drive, along with the media files in

the shared storage system. The configuration file is updated and saved whenever you change a configuration using the K2Config application. That is why you must always use the K2Config application to change settings on the storage system, so the most recently changed configurations will always be stored in the configuration file and displayed.

Grass Valley Recommended Deployment and Monitoring Solutions

To maximize up-time, a maintenance strategy must provide the ability to easily identify the root cause of an unanticipated hardware or software failure and to quickly compile failure data. The ability to proactively predict failures and to quickly notify those who can rectify them makes the maintenance strategy even more powerful. Grass Valley has a long history of building the necessary functionality into critical broadcast products. With Grass Valley's next generation tool, GV GUARDIAN, remote monitoring and proactive predictive failure analysis are important contributors to Grass Valley system solutions. GV GUARDIAN runs on commercial off-the-shelf server PCs, such as the K2 system control point PC, and is also available as an all-in-one turnkey product. Grass Valley and 3rd party devices report status via Window Messaging, Simple Network Management Protocol (SNMP), or syslog to GV GUARDIAN. The tool provides easy to use, fully autonomous remote monitoring to predict errors, provide proactive notifications, and centrally consolidate error logs and hardware failure information. With GV GUARDIAN you can maximize your up-time with less manpower, as compared to manual system monitoring. Watching for indicator lights, physically scanning logs, and other manual monitoring is far more time consuming, more error-prone, and much less accurate. Grass Valley recommends using GV GUARDIAN as your remote monitoring tool.

Windows Remote Desktop Connection

You can use the Microsoft Windows Remote Desktop Connection application to make a remote connection to a Grass Valley system that runs the Windows operating system.

Take the following into consideration when connecting to K2 systems:

- Before you can use the Remote Desktop Connection, you need network access and permissions to connect to the K2 system.
- You can use either the name or the IP address to access the K2 system.
- Do not use the Remote Desktop Connection to access the PC running the Control Point software or to access the AppCenter application; results may be unreliable.
- Take care when accessing an online K2 system on which media access is underway. The additional load on network and system resources could cause unpredictable results.
- Lack of robust video/graphic support can cause video display problems. Remote desktop connections can interrupt proxy and live streaming. AppCenter video monitoring is not supported through Remote Desktop Connection.

Accessing Remote Desktop Connection

1. Do one of the following:
   - Click the **Start** button on the Windows task bar
   - Press the Windows key on the keyboard.

2. Select **Programs | Remote Desktop Connection**.

   The Remote Desktop dialog box opens.

3. Enter the name or IP address of the system to which you are making the remote connection and click **Connect**.

   To enable Remote Desktop, type

   ```
   remote settings
   ```

   in the search box and select **Allow remote access to your computer**.

Accessing a device via Remote Desktop from SiteConfig

You can access a device via Remote Desktop if you have configured its network properties to allow communication over the control network.

- To initiate a Remote Desktop session, right-click on a device in the tree view and select **Remote Desktop**.

  SiteConfig opens a Remote Desktop session to the device in a new window and automatically logs on using either the global credentials or the overridden credentials (if any).

  If Remote Desktop does not log on to the device, check the credentials being used and check network connectivity to the device.

- Click the **visible dialog pending user input** link next to a deployment task.

  This link appears if a deployment task is underway and a dialog on the device requires your input. In this case SiteConfig can automatically launch a Remote Desktop session to the device. If a dialog is not visible on the screen, check for a Interactive Service Detection flashing toolbar button and use it to view the message. Provide user input as required for any dialogs or messages.

About SiteConfig and K2Config settings

Many settings and operations, such as network settings, adding/removing devices, and software versions, are managed by both the SiteConfig application and the K2Config application. Each application has its own XML file in which information is stored. You can keep the applications in synch by using an orderly task flow as you configure the K2 SAN.

When doing initial installation and configuration tasks, you can export/import system information from one application's XML file to the other application's XML file. You can also merge from K2Config into an existing SiteConfig system description. These export/import/merge features support a one-time process in which a system as described in the XML file of one application is imported into the XML file in the other application. The target XML must not already contain the system being imported.

When you change a setting in one application, it is not automatically updated directly in the other application. The applications do not communicate dynamically with one another. However, both applications can read settings as currently configured on the actual physical device and update their XML file accordingly. This is the method you must use to keep the applications in synch.

When you change a setting that is managed by both applications, you should change it first in SiteConfig, as a general rule. This application gives you the best context for the system as a whole and provides features to identify and verify changes. Once the change is implemented on the actual

physical device, you must then open the relevant page in the K2Config application. This causes the K2Config application to refresh its settings from the device and write the change to its XML file. It also allows you to verify your change within the context of the K2Config application.

The following table summarizes operations that involve interaction between SiteConfig and K2Config.

Operation	Task flow context and policies	Additional information
Import SiteConfig system description file into K2Config	Use this operation for initial install/commission (greenfield) sites. First define the site topology using SiteConfig and complete network configuration and software deployment. Then import the SiteConfig system description into K2Config and complete the K2 SAN configuration.	This operation creates a K2 SAN in K2Config with SiteConfig defined devices. Uses the site name to check if the K2 SAN already exists. The operation will not import if the K2 SAN exists with the same name. The operation can import all sites which are K2 SANs from a single system description file in a single import step.
Import K2Config XML into SiteConfig	Use this operation when you're running SiteConfig for the first time at a site with existing K2 SANs that have already been configured with K2Config. This allows you to seed the SiteConfig system description with device information that is already in the K2Config XML file. After you have done this operation for the first time, do not do it again.	This operation creates a SiteConfig site with K2Config defined devices. The operation removes all other sites.
Merge K2Config XML into SiteConfig system description	Use this operation when you've already defined some sites using SiteConfig and you later want to bring in another K2Config defined K2 SAN that doesn't exist in SiteConfig. Do not merge a K2Config XML that you've already merged. If you do so, it is likely that SiteConfig will create a new site with the same devices.	This operation creates a SiteConfig site with K2Config defined devices but leaves existing sites as is.
Rename Site\SAN	Rename first in SiteConfig. Then rename in K2Config. Do not import\merge into SiteConfig or K2Config.	—
Remove Site\SAN	Remove first in SiteConfig. Then remove in K2Config. Do not import\merge into SiteConfig or K2Config.	—
Remove device	Remove from both SiteConfig and K2Config.	—
Add device	Add in SiteConfig first, do network configuration and software deployment. Then, add in K2Config and configure using K2Config.	—
Create a new site\SAN	Use SiteConfig to create site, add devices, configure network and deploy software, then import into K2Config and configure each device	—

Operation	Task flow context and policies	Additional information
Change hostname	Perform hostname change using SiteConfig. Remove and re-add to K2Config. If changing the hostname of a media file system/metadata K2 Media Server, re-configure all clients on the K2 SAN using K2Config	—
Change IP address (except address of TOE on K2 Media Server)	Use SiteConfig for IP address changes. Then in K2Config, click on the changed device's network configuration node. This refreshes the K2Config view of IPs from the device.	—
Change IP address of TOE on K2 Media Server	For TOE IP changes and/or TOE card removal, use K2Config.	—
Modify K2 SAN redundancy - redundant to non-redundant or vice versa	Use SiteConfig to recreate the site using the appropriate redundancy models and configure network and deploy software. Remove K2 SAN from K2Config. Import site into K2Config. Configure using K2Config.	—

About Control Panel, SiteConfig, and K2Config settings

During system commissioning or system reconfiguration, the SiteConfig and K2Config applications are first used to set up or modify K2 SAN and network configurations. The GV STRATUS Control Panel application is then used to complete the setup of the GV STRATUS system-wide workflow components.

The GV STRATUS Control Panel application imports the configuration information and populates the GV STRATUS view of the available K2 systems. For example, information about K2 SANs comes from K2Config while information about standalone K2 Summit systems comes from SiteConfig. The information transfer is uni-directional, where the GV STRATUS Control Panel application imports the SiteConfig/K2Config generated configurations.

Use of the GV STRATUS Control Panel application requires the GV STRATUS Core server to be running, and Grass Valley recommends the GV STRATUS Control Panel is only configured on the Core server. If, during maintenance or commissioning, SiteConfig and K2Config are used to setup or modify systems while the GV STRATUS Core server is turned off, it is important to synchronize K2Config information to GV STRATUS Control Panel before attempting to use the GV STRATUS Control Panel application.

NOTE: While the* GV STRATUS Control Panel *application allows you to enter device names and other values as free-form text, it is not recommended for use at customer sites as manual entry can result in text errors.

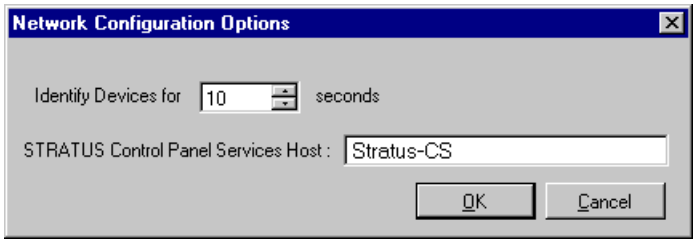
Related Topics

Synchronizing K2Config information to GV STRATUS Control Panel on page 523

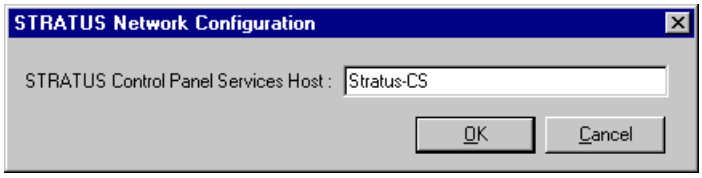
About the Control Panel Service host and applications

The GV STRATUS server with the SiteConfig role of Common Services hosts the Control Panel Service. Typically, this is the GV STRATUS Core server. To communicate configuration information, multiple applications must be configured to reference this GV STRATUS server.

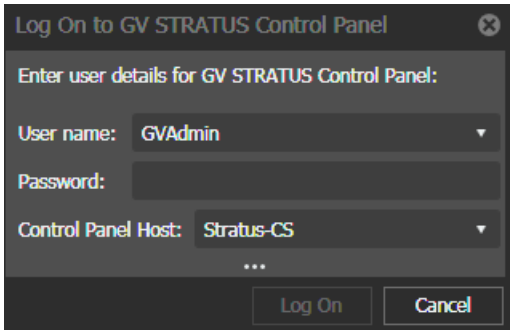
In the SiteConfig application, click **Tools | Options | Network Configuration**.



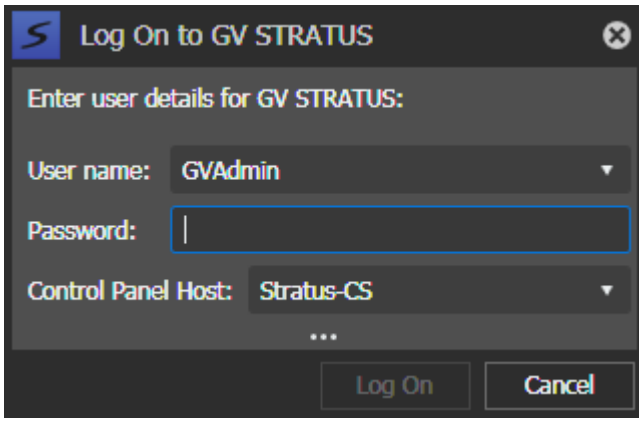
In the K2Config application, click **STRATUS | Network Configuration**.



In the GV STRATUS Control Panel application, configure the log in dialog box.



In the GV STRATUS application, configure the log in dialog box.



When you use SiteConfig to deploy the GV STRATUS application, SiteConfig configures the GV STRATUS Control Panel Host on each GV STRATUS client PC, providing the following prerequisites are in place:

- In the SiteConfig application, in **Tools | Options | Network Configuration**, the GV STRATUS Control Panel Services Host must be correctly configured.
- In the SiteConfig system description, the GV STRATUS client PC must have the role of GV STRATUS Application.

Related Topics

Logging on to the GV STRATUS Control Panel application on page 842
Synchronizing K2Config information to GV STRATUS Control Panel on page 523

Understanding and using SiteConfig

Read the topics in this section for a better understanding of your system.

Related Topics

Working with SiteConfig on page 485

About developing a system description

The SiteConfig system description includes the complete Grass Valley system, which includes K2, GV STRATUS, and other Grass Valley products. In most cases you install and test your K2 system first, so when you create your system description you start by adding your K2 systems, then you add GV STRATUS devices. The following taskflows provide examples:

- For a system in which all devices are new from Grass Valley with one or more K2 SANs, you first create a system description for your K2 SAN or SANs, then add GV STRATUS and Playout devices as appropriate. Refer to the *K2 SAN installation and Service Manual* for instructions on creating the system description.
- For a system in which all devices are new from Grass Valley with one or more standalone K2 Summit systems, you first create a system description and add your standalone K2 Summit systems, than add other devices as appropriate. Refer to the *K2 System Guide* for instructions on creating the system description and adding your standalone K2 Summit systems.

If you are using a different taskflow, use the topics in this manual as appropriate and refer to the *SiteConfig User Manual* or *SiteConfig Help Topics* for additional information.

Your devices must be in a SiteConfig system description in order to be managed by SiteConfig. When you already have a system description in place, you should use SiteConfig to modify this system description and add your devices. You can do this in your planning phase, even before you have devices installed or cabled. Your goal is to have the SiteConfig system description accurately represent all aspects of your devices and networks before you begin actually implementing any networking or other configuration tasks for those devices.

About device and host names

In SiteConfig, a device can have different names, as follows:

- Device name — This is a name for display in SiteConfig only. It is stored in the SiteConfig system description, but not written to the actual device. It is displayed in the device tree view and in the device list view. It can be a different name than the device's host name.
- Host name — This is the network name of the device. SiteConfig has a default naming convention for host names which you can use or override with your own host names.

In most cases it is recommended that the Device name and Host name be the same. This avoids confusion and aids troubleshooting.

The Device name can serve as a placeholder as a system is planned and implemented. During the install/commission process, when you reconcile a device's current and planned network interface settings, the Host name as configured in the system description can be overwritten by the host name on the actual device. However, the Device name configured in the system description is not affected. Therefore it is recommended that in the early planned stages, you configure the Device name to be the desired name for the device, but do not yet configure the Host name. Then, after you have applied network interface settings, you can change the Host name to be the same as the Device name. This changes the host name on the actual device so that then all names are in sync.

SiteConfig does not allow duplicate device names or host names.

Items in the tree view are automatically sorted alphabetically, so if you change a name the item might sort to a different position.

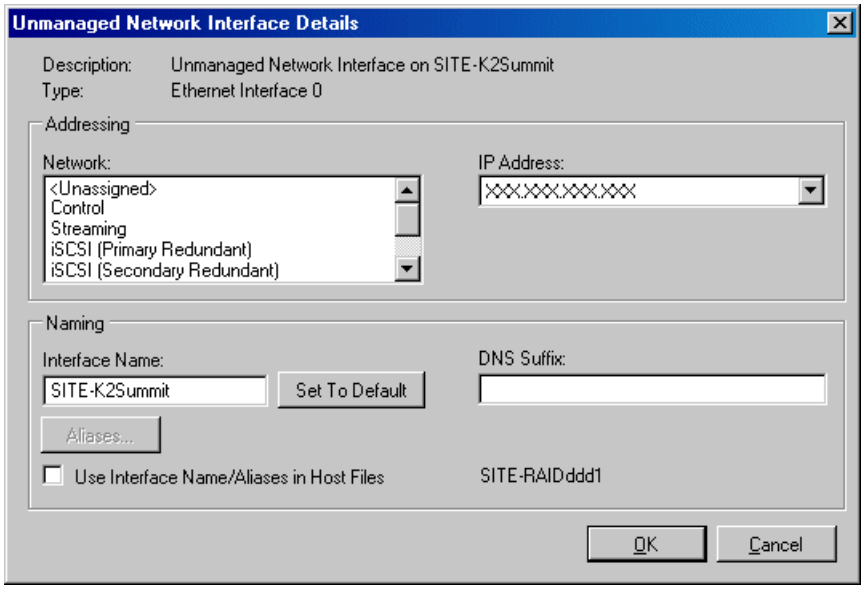
About IP configuration of network interfaces on devices

You can perform IP configuration of network interfaces when working with a placeholder device prior to discovery. When you add a device and choose a particular model, the model defines the number, type and usage characteristics of network interfaces to expect on such a device.

You can view and edit each network interface and set up IP configuration selecting an appropriate IP from the network to which each interface connects. The process for editing IP configuration varies, depending on the device's phase.

Placeholder device IP configuration

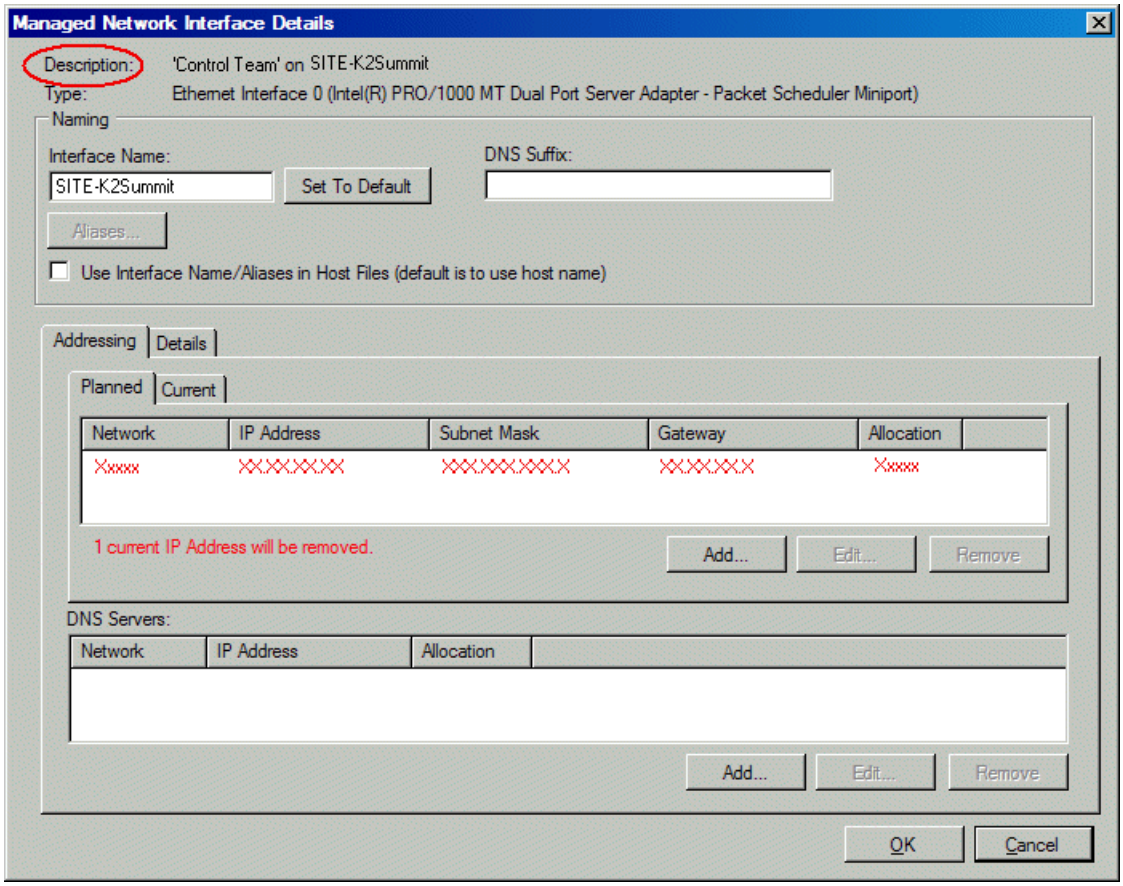
On a placeholder device, you edit network interfaces using the Unmanaged Network Interfaces dialog box.



The Unmanaged Network Interfaces dialog box allows you only to save changes to the system description.

Discovered device IP configuration

On a discovered device, you edit network interfaces using the Managed Network Interfaces dialog box.



The Managed Network Interfaces dialog box allows you to edit and save changes to the device.

About SiteConfig support on GV STRATUS devices

Before SiteConfig can be used to discover or manage a device, the device must meet the following requirements:

- The device must be a Microsoft Windows operating system device.
- The device must have Microsoft .NET version 3.5 installed, as reported in the Windows Add/Remove Programs control panel.
- The SiteConfig Discovery Agent service must be running on the device, as reported in the Windows Services control panel.

For GV STRATUS servers shipped new from Grass Valley, these requirements are pre-installed. These requirements are pre-installed on recovery images for these systems as well. Therefore, if you suspect a problem with these requirements, do not attempt to install SiteConfig support requirements. If you must restore SiteConfig support requirements, re-image the system.

GV STRATUS client PCs on the corporate LAN do not require the Discovery Agent because typically you do not use SiteConfig to discover or manage networking on these devices.

GV STRATUS client PCs on the control network do required the Discovery Agent.

Software that meets these requirements is bundled in various components and installation programs, some of which are available at your SiteConfig install location as follows:

- The `ConnectivityKit` folder contains Microsoft .NET. You can copy the contents of this folder to a device and then run `setup.exe` to install the software.
- The `DiscoveryAgent Setup` folder contains the SiteConfig Discovery Agent. You can copy the contents of this folder to a device and then run `setup.exe` to install the software.

Related Topics

Install/configure for SiteConfig support on client PC on page 261
About GV STRATUS client PCs on page 416
About software deployment on the corporate LAN on page 440

About credentials in SiteConfig

SiteConfig requires administrative privileges on devices in order to perform most of the network configuration and deployment tasks. For known devices types, SiteConfig has a default administrator account and password. These default credentials depend on the SiteConfig version, so check your SiteConfig Release Notes for any changes. When you add a device based on a known device type, SiteConfig references the default administrator account and password. Then, when you use remote desktop or perform software deployment to the device, SiteConfig automatically uses these credentials. These credentials are called "global" credentials for the device since the same credentials are used on all devices of that type in the system.

You can choose to override the default credentials for a given device type. For example, if you have specified a different administrator account or a different password on the devices when commissioning the system, then you want SiteConfig to use these modified credentials.

It is possible to also override the default credentials for a single device.

Related Topics

Understanding credentials on page 425
Changing passwords on page 710

About the corporate LAN and SiteConfig

GV STRATUS client PCs can be on the corporate LAN, which is considered an unmanaged network in SiteConfig. Since SiteConfig does not manage the network, you cannot use SiteConfig to configure network settings on those GV STRATUS client PCs. However, you must still configure your system description to include the corporate LAN, for the following purposes:

- A GV STRATUS client PC should be a SiteConfig managed device, so SiteConfig needs to know the connection for each network interface on the device, including the corporate LAN connection. Otherwise, SiteConfig displays error messages.
- If a GV STRATUS client PC uses a DNS server on the corporate LAN for name resolution, SiteConfig needs to reference that DNS server.

- You should use SiteConfig to deploy GV STRATUS application software to the client PC via the corporate LAN.

Related Topics

Corporate LAN network description on page 414

About software deployment on the corporate LAN

If you have GV STRATUS client PCs that are on a network that SiteConfig does not manage, such as your corporate LAN, you can configure your system description to allow software deployment to those devices. This method uses SiteConfig as a software deployment tool only, as you cannot configure network settings on the device or manage the device's network. With this method you create an unmanaged network in SiteConfig, add the DNS server(s) to the control point PC, then when you add the PC, edit the control interface and set it to the unmanaged network. This allows communication with the GV STRATUS client PCs. Then add a placeholder device for each of your GV STRATUS client PCs. With this method you do not use SiteConfig device discovery, and it is not necessary to install a discovery agent on the GV STRATUS client PC. Rather, you configure SiteConfig to look up the address via DNS or hosts file. This allows the GV STRATUS client PC to communicate as if it was a discovered device. SiteConfig can then deploy software to the device.

If necessary, get help from your IT department to ensure that the SiteConfig PC is configured to communicate with the PCs on the corporate network. If SiteConfig can ping the PC, SiteConfig can deploy software to the PC.

About hosts files and SiteConfig

SiteConfig uses the network information in the system description to define a hosts file and allows you to view the hosts file. SiteConfig can manage this hosts file on Windows operating system devices that are in the system description and that are part of a SiteConfig managed network.

When you have successfully assigned devices and applied planned network settings to interfaces, it is an indication that host table information, as currently captured in the system description, is valid and that you are ready to have SiteConfig assemble the host table information into a hosts file. Your options for placing this host table information on devices are as follows:

- If you do not want SiteConfig to manage your host table information, you can manage it yourself. This is typically the case if your facility has an existing hosts file that contains host table information for devices that are not in the SiteConfig system description. In this case, you can have SiteConfig generate a single hosts file that contains the host table information for the devices in the system description. You can then copy the desired host table information out of the SiteConfig hosts file and copy it into your facility hosts file. You must then distribute your facility hosts file to devices using your own mechanisms.
- If you want SiteConfig to manage all information in hosts files on devices, you can have SiteConfig copy its hosts file to devices. In so doing, SiteConfig overwrites the existing hosts files on devices. Therefore, this requires that all devices that have name resolution through the hosts file be configured accordingly in the SiteConfig system description.

If you choose to have SiteConfig write hosts files to devices, the process consumes system resource and network bandwidth. Therefore you should wait until you have verified the information for all

devices/interfaces in the host file, rather than updating hosts files incrementally as you discover/assign devices.

SiteConfig does not automatically deploy hosts files to managed devices as you add or remove devices. If you add or remove devices from the system description, you must re-deploy the modified hosts file to all devices.

Related Topics

Generating host tables using SiteConfig on page 276

Proxy/live streaming technical details

The K2 Summit system writes proxy files to the proxy location specified in the GV STRATUS Control Panel application. On the specified device the location is `V:\proxy\`. For each clip recorded, the K2 system creates a directory and names it with the asset GUID, which is a long, unique string of characters. These directory names do not correspond to clip names or other human readable information. The directory contains the proxy files, which include the proxy video and audio files, as well as thumbnails files and a scene change file. The proxy video file is a fragmented MPEG-4 file. For test purposes, you can open the proxy file in a video player application that supports fragmented MPEG-4.

The K2 Summit system multicasts the low-resolution live stream using Real-time Transport Protocol, with UDP ports for the MPEG video with timecode and UDP ports for audio tracks, as defined by the Session Description Protocol (SDP). For each channel, the K2 system generates a `*.sdp` file that contains the streaming media initialization parameters. The K2 system updates the file whenever you change the live streaming configuration. You can find these files on the K2 system at `V:\live streaming`. For test purposes, you can open a file in a text editor and read the IP addresses and ports assigned to the multicast session and other configuration information for the stream.

The K2 Summit system can also generate low-latency streaming media for use by DynoZoom and live monitoring. Refer to related topics in the "Configuring the K2 System" section of the K2 Topic Library.

The K2 Summit system generates for each of its channels the specific live streaming network ports and IP addresses based on a port base and an IP address base. The port base is the first UDP port address for elementary streams. The IP address base is the first two octets in the IP address, as specified by the Internet Assigned Numbers Authority (IANA). By default, the port base is 31820 and the IP address base is 239.192.0.0. With these default bases, the range of network ports is UDP 31820 to 31827 , and the range of IP addresses is 239.192.x.x to 239.195.x.x. Grass Valley recommends that you use these default settings. However, if necessary for your site's network policies, you can also change the K2 system's default settings. You can configure the port base and the IP address base. Only IP addresses specified by IANA for multicast are allowed. Do not attempt to edit the `*.sdp` files, as the K2 system generates them automatically whenever the system is restarted. If you change the IP address of the K2 system, you must restart in order to update the IP address in the `*.sdp` file.

The K2 Summit system hosts a simple web server over which it delivers the live stream via HTTP. For test purposes, you can access the live stream by entering a URL of the following convention in a standard web browser:

```
http://<httpservername>/live/<k2systemname>_<Cn>.sdp
```

For example, to view the live stream from channel four on a K2 system named Summit01, the URL is `http://Summit01/live/Summit01_C4.sdp`. The http server name is the same as the name of the K2 system.

MDI and Encoder logical names convention

As you configure your system you must create and enter logical names for the various software components (services) that provide functionality. These logical names provide a mapping of the functionality of the standard system services to the specific machines in your particular system. For this reason you should take care to create logical names that are easy to identify and interpret as they appear in the various configuration pages.

It is especially important that you distinguish between the logical name of a software component and the hostname of the machine to which the software component relates. For example, a convention could be that machine names are lower case and logical names are upper case.

The software components that require logical names are as follows:

- MDIs — The GV STRATUS system uses a Managed Device Interface (MDI) to manage a device that is not a platform for GV STRATUS software. Typically these are the machines on which media resides, such as K2 Summit/SAN systems and archive devices. Each type of device has its own MDI. The MDI software component is hosted on a GV STRATUS server, rather than being hosted on the same machine that it manages.
- Encoder services — The GV STRATUS system uses services to manage the scavenge encoder media processing. Typically these are a type of "transfer" service. This type of software component is hosted on the machine that it manages.

About archive MDIs

The archive MDI software component must be installed on a network connected computer. Archive MDIs can be configured to specify settings such as source and destination transfer locations. Similar to other MDIs, the archive MDI can be installed on the GV STRATUS Core server.

The archive MDI software component runs as a service. You can install the archive MDI software component from the SiteConfig application. The archive MDIs available are as follows:

- DIVA
- FlashNet
- Masstech
- Generic FTP
- Common RESTful

Related Topics

MDI and Encoder logical names convention on page 442

About roles

The concept of a "role" plays an important part in understanding system configuration, as follows:

- SiteConfig — When defining devices in SiteConfig, roles designate what system functions are carried out on which devices. Depending on the particular device model, SiteConfig provides typical roles and allows you to assign roles, within constraints appropriate for the device type. Depending on the roles assigned, SiteConfig then installs the appropriate software on the device.
- K2Config — Roles are applied to K2 Media Servers in K2Config. This defines how K2Config then configures the K2 media file system, K2 media database, services, and other K2 system components to create the K2 SAN.
- GV STRATUS Control Panel — User groups and accounts that are configured in the GV STRATUS Control Panel application are assigned roles. The roles correspond in a general sense to GV STRATUS application tools and other features. Depending on the roles assigned to the account used to log in to the GV STRATUS, tools and features are either displayed or hidden.

Related Topics

GV STRATUS roles matrix on page 37

Asset copies and deletions

When you copy an asset, different types of associations are created, depending on the K2 storage location and the type of asset copy, as follows:

- Shallow copy — When you copy assets and both copies are in the same K2 storage location, shallow copies are created. With a shallow copy, the high-resolution media files are not copied. Rather, the K2 media database and the GV STRATUS database contain a record for each shallow copy, and each record references the same media files. In the GV STRATUS system, this results in an asset with multiple references, similar to a subclip.
- Deep copy — When you copy assets and the copies are in different K2 storage locations, deep copies are created. With a deep copy, the high-resolution media files are copied. The K2 media database on each K2 system references its own media files. The GV STRATUS database references all the media files on all the different K2 storage locations and archive locations. In the GV STRATUS system, this results in an asset with multiple high-resolution associations.

When deleting assets, the following occurs:

- Assets with shallow copies — When the GV STRATUS system attempts to delete the shallow copy, the asset is not deleted. You must delete the referenced copy before you can delete the asset.
- Assets with deep copies — When you delete any one of the associated high-resolution assets, in any K2 storage or archive location, by default the GV STRATUS system deletes all the high-resolutions assets in all locations. Since it is one asset with multiple high-resolutions associations, the entire asset with all its associations is deleted. If you only want to delete a high-resolution association, you can do so on the **Associations** tab in the Inspector.

Take care when creating copies, considering your workflow in which copied assets are deleted. The GV STRATUS roles of **Delete Rights** and **Media Manager** can be assigned to user accounts to

implement the desired workflow. As part of the delete operation, Media Managers can specify online/archive deletion and choose whether to delete or conform referenced copy of assets.

Related Topics

Deleting assets on page 985

Deleting assets on page 985

Devices components: Roles, cab files, services, and licenses

The system components listed in these topics are related to GV STRATUS system functionality. Other components can be present, but if they are not specific to GV STRATUS system functionality they are not listed in these topics.

Related Topics

Ports and services mapping on page 715

Express server components

Description: The single server with all roles for a basic GV STRATUS system, including Proxy Server, to support a small GV STRATUS system.

Nomenclature:

- STRATUS-CS-EXPRESS

SiteConfig "Add Device":

- Family: GV STRATUS
- Device Type: GV STRATUS Server
- Model: GV STRATUS Core Server Express

SiteConfig Roles:

- GV STRATUS Ingest Services (Required)
- GV STRATUS Control Panel Service (Required)
- GV STRATUS Common Services (Required)
- License Manager (Required)
- GV STRATUS Data Mover Engine (Required)
- GV STRATUS Proxy Express Server (Required on Express server)
- GV STRATUS Control Panel (Required)
- GV STRATUS Core Services (Required)
- GV STRATUS Database (Required)
- GV STRATUS Summit MDI (Required)
- GV STRATUS Common RESTful Archive MDI (Optional)
- GV STRATUS Diva MDI (Optional)
- GV STRATUS FlashNet MDI (Optional)
- GV STRATUS Masstech MDI (Optional)
- GV STRATUS Generic FTP MDI (Optional)
- GV STRATUS Proxy Streaming Service (Optional)
- GV STRATUS Rules Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)

- GV STRATUS Scheduled Transfer Engine (Optional)
- GV STRATUS Scheduled Ingest Engine (Not used in this GV STRATUS release)
- GV STRATUS Scheduled Ingest Manager (Not used in this GV STRATUS release)
- GV STRATUS SocialMedia Engine (Optional)
- GV STRATUS ExternalMedia Engine (Optional)
- GV STRATUS Traffic Gateway (Optional)
- GV STRATUS Topic Service Bus (Not used in this GV STRATUS release)
- GV STRATUS Web Apps (Required. Must be assigned to Express/Core server to display Statistics panel via Dashboard)
- GV STRATUS Web Client (Optional)
- GV STRATUS Workflow Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
- GV STRATUS Xcode Control Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
- GV Log Manager (Required)
- GV Log Viewer (Required)
- GV STRATUS Rundown Server Components (Optional)
- GV STRATUS Application (Use for test purposes only)
- If optionally used as a Render Engine, these additional roles:
    - GV STRATUS Render Engine

K2Config Roles:

- None

SiteConfig cab files:

- *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
  - *GrassValley_STRATUS_IngestServices_x.x.x.cab*
  - *GrassValley_STRATUS_ControlPanelService_x.x.x.cab*
  - *GrassValley_STRATUS_CommonServices_x.x.x.cab*
  - *GrassValley_STRATUS_CoreServices_x.x.x.cab*
  - *GrassValley_STRATUS_ControlPanel_x.x.x.cab*
  - *GrassValley_STRATUS_Databases_x.x.x.cab*
  - *GrassValley_STRATUS_DataMover_x.x.x.cab*
  - *GrassValley_STRATUS_ExternalMedia_x.x.x.cab*
  - *GrassValley_STRATUS_HttpProxyServer_x.x.x.cab*
  - *GrassValley_STRATUS_Mediaflow_x.x.x.cab*
  - *GrassValley_STRATUS_CRArchive_MDI_x.x.x.cab*
  - *GrassValley_STRATUS_DIVA_MDI_x.x.x.cab*
  - *GrassValley_STRATUS_FlashNet_MDI_x.x.x.cab*
  - *GrassValley_STRATUS_Masstech_MDI_x.x.x.cab*
  - *GrassValley_STRATUS_GFTP_MDI_x.x.x.cab*
  - *GrassValley_STRATUS_Summit_MDI_x.x.x.cab*
  - *GrassValley_STRATUS_Proxy_MDI_x.x.x.cab*
  - *GrassValley_STRATUS_ProxyStreamingService_x.x.x.cab*
  - *GrassValley_STRATUS_RenderEngine_x.x.x.cab*
  - *GrassValley_STRATUS_Rules_x.x.x.cab*
  - *GrassValley_STRATUS_ScheduledTransferEngine_x.x.x.cab*
  - *GrassValley_STRATUS_SocialMedia_x.x.x.cab*
  - *GrassValley_STRATUS_Transcode_x.x.x.cab*
  - *GrassValley_STRATUS_TrafficGateway_x.x.x.cab*
  - *GrassValley_STRATUS_WebApps_x.x.x.cab*
  - *GrassValley_STRATUS_WebClient_x.x.x.cab*
  - *GrassValley_Sabretooth_Application_x.x.x.cab*
  - *GrassValley_DeviceKeyService_x.x.x.cab*
  - *GrassValley_LogManager_x.x.x.cab*
  - *GrassValley_LogViewer_x.x.x.cab*
  - *GV_STRATUS_Rundown_x.x.x.cab*
- *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:
  - *GrassValley_STRATUS_ControlPanel_x.x.x.cab*
  - *GrassValley_STRATUS_Application_x.x.x.cab* (Use for test purposes only)
- *GrassValley_K2system_x.x.x.cab* for K2 9.8.x systems.
- *GrassValley_K2Plus_x.x.x.cab* for K2 10.x systems.

Licenses:

- GV STRATUS licenses (Express/Flex/Pro/Elite) as appropriate for customer site.
- STRATUS-CONFORM (Optional) Includes XRE, Conform, and Proxy Encoder functionality.
- STRATUS-GVRE (Optional) Includes Conform and Proxy Encoder functionality. Only one license is needed per system, either the STRATUS-CONFORM or STRATUS-GVRE.

- STRATUS-PROXYSTREAMING for servers supporting proxy streaming via the Web Client.
- STRATUS-QFHD (Optional) only required for 4K/QFHD format to be supported in your operation.
- STRATUS-TRANSCODE (Optional) for generic transcoder functionality with GVRE.
- STRATUS-ARCHIVE (Optional) for archive and restore functionality.
- STRATUS-RULES (Optional)
- STRATUS-SMNSOCIALMEDIAENGINE (Optional)
- STRATUS-EMNEXTERNALMEDIAENGINE (Optional)
- STRATUS-SMNFACEBOOK (Optional)
- STRATUS-SMNTWITTER (Optional)
- STRATUS-SMNYOUTUBE (Optional)
- STRATUS-EMNVERIZON (Optional)
- STRATUS-XCODECONTROLCARBONCODER (Optional. Depends on STRATUS-RULES.)
- STRATUS-XCODECONTROLVANTAGE (Optional. Depends on STRATUS-RULES.)
- STRATUS-XCODECONTROLELEMENTAL (Optional. Depends on STRATUS-RULES.)
- STRATUS-MULTISITE (Optional)
- STRA-PREM-CONNECT (Optional)
- STRATUS-VTR-ING (Optional)
- STRATUS-WEB-CLIENT (Optional)
- STRATUS-XCODECONTROLMEWS (Optional)
- STRATUS-XCODECONTROLMEWSEXT

These are Sabretooth floating licenses, which means they are not restricted to single computer. GV STRATUS Control Panel assigns the licenses to user groups.

Contact your Grass Valley representative for a current list of available licenses.

Windows Control Panel Services:

- GV STRATUS ASK. Startup type: Automatic
- GV STRATUS Common Services. Startup type: Automatic
- GV STRATUS Control Panel Services. Startup type: Automatic
- GV STRATUS Data Mover Engine. Startup type: Automatic
- GV STRATUS Index Agent. Startup type: Automatic
- GV STRATUS Ingest Config. Startup type: Automatic
- GV STRATUS Ingest Core. Startup type: Automatic
- GV STRATUS Ingest DB. Startup type: Automatic
- GV STRATUS Maintenance Service. Startup type: Automatic
- GV STRATUS MDI Common RESTful Archive. Startup type: Automatic
- GV STRATUS MDI DIVA. Startup type: Automatic
- GV STRATUS MDI Flashnet. Startup type: Automatic
- GV STRATUS MDI Masstech. Startup type: Automatic
- GV STRATUS MDI GFTP. Startup type: Automatic
- GV STRATUS MDI Proxy. Startup type: Automatic
- GV STRATUS MDI Summit. Startup type: Automatic
- GV STRATUS MediaFlow Workflow Engine. Startup type: Automatic
- GV STRATUS Resolver. Startup type: Automatic
- GV STRATUS Router Config. Startup type: Automatic
- GV STRATUS Router Controller. Startup type: Automatic
- GV STRATUS Rules Engine. Startup type: Automatic

- GV STRATUS Rules Wizard. Startup type: Automatic
- GV STRATUS Scheduled Transfer Engine. Startup type: Automatic
- GV STRATUS Segmentation Config. Startup type: Automatic
- GV STRATUS Social Media Engine. Startup type: Automatic
- GV STRATUS External Media Engine. Startup type: Automatic
- GV STRATUS Traffic Gateway. Startup type: Automatic
- GV STRATUS Xcode Control Engine
- GV Device Key Service. Startup type: Automatic
- GV Proxy Streaming Gateway Service. Startup type: Automatic
- GV Log Manager. Startup type: Automatic
- ProductFrame Discovery Agent Service. Startup type: Automatic
- Sabretooth License Server. Startup type: Manual
- Sabretooth Protocol Service. Startup type: Manual
- If optionally used as a Render Engine, these additional services:
  - GV Render Engine. Startup type: Automatic (Delayed Start)
  - Grass Valley XRE Controller. Startup type: Automatic (Delayed Start)

Core Server components

Description: A server that has the role of Core Services on a GV STRATUS system with multiple GV STRATUS servers, including a different GV STRATUS server with role of Proxy Server.

Nomenclature:

- STRATUS-CS-A1, STRATUS-CS-B1, STRATUS-CS-C1

SiteConfig "Add Device":

- Family: GV STRATUS
- Device Type: GV STRATUS Server
- Model: GV STRATUS Core Server

SiteConfig Roles:

- GV STRATUS Ingest Services (Required)
- GV STRATUS Control Panel Service (Required)
- GV STRATUS Common Services (Required)
- License Manager (Required)
- GV STRATUS Control Panel (Required)
- GV STRATUS Core Services (Required)
- GV STRATUS Database (Required)
- GV STRATUS Data Mover Engine (Required)
- GV STRATUS Summit MDI (Required)
- GV STRATUS Common RESTful Archive MDI (Optional)
- GV STRATUS Diva MDI (Optional)
- GV STRATUS FlashNet MDI (Optional)
- GV STRATUS Masstech MDI (Optional)
- GV STRATUS Generic FTP MDI (Optional)
- GV STRATUS Proxy Streaming Service (Optional)

- GV STRATUS Rules Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
- GV STRATUS Scheduled Transfer Engine (Optional)
- GV STRATUS Scheduled Ingest Engine (Not used in this GV STRATUS release)
- GV STRATUS Scheduled Ingest Manager (Not used in this GV STRATUS release)
- GV STRATUS SocialMedia Engine (Optional)
- GV STRATUS ExternalMedia Engine (Optional)
- GV STRATUS Traffic Gateway (Optional)
- GV STRATUS Topic Service Bus (Not used in this GV STRATUS release)
- GV STRATUS Workflow Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
- GV STRATUS Xcode Control Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
- GV Log Manager (Required)
- GV Log Viewer (Required)
- GV STRATUS Web Apps (Required. Must be assigned to Express/Core server to display Statistics panel via Dashboard)
- GV STRATUS Web Client (Optional)
- GV STRATUS Rundown Server Components (Optional)
- GV STRATUS Application (Use for test purposes only)

K2Config Roles:

- None

SiteConfig cab files:

- *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
  - *GrassValley_STRATUS_IngestServices_x.x.x.cab*
  - *GrassValley_STRATUS_ControlPanelService_x.x.x.cab*
  - *GrassValley_STRATUS_CommonServices_x.x.x.cab*
  - *GrassValley_STRATUS_CoreServices_x.x.x.cab*
  - *GrassValley_STRATUS_ControlPanel_x.x.x.cab*
  - *GrassValley_STRATUS_Databases_x.x.x.cab*
  - *GrassValley_STRATUS_DataMover_x.x.x.cab*
  - *GrassValley_STRATUS_ExternalMedia_x.x.x.cab*
  - *GrassValley_STRATUS_CRArchive_MDI_x.x.x.cab*
  - *GrassValley_STRATUS_DIVA_MDI_x.x.x.cab*
  - *GrassValley_STRATUS_FlashNet_MDI_x.x.x.cab*
  - *GrassValley_STRATUS_Masstech_MDI_x.x.x.cab*
  - *GrassValley_STRATUS_GFTP_MDI_x.x.x.cab*
  - *GrassValley_STRATUS_Summit_MDI_x.x.x.cab*
  - *GrassValley_STRATUS_Proxy_MDI_x.x.x.cab*
  - *GrassValley_STRATUS_ProxyStreamingService_x.x.x.cab*
  - *GrassValley_STRATUS_Mediaflow_x.x.x.cab*
  - *GrassValley_STRATUS_Rules_x.x.x.cab*
  - *GrassValley_STRATUS_ScheduledTransferEngine_x.x.x.cab*
  - *GrassValley_STRATUS_SocialMedia_x.x.x.cab*
  - *GrassValley_STRATUS_Transcode_x.x.x.cab*
  - *GrassValley_STRATUS_TrafficGateway_x.x.x.cab*
  - *GrassValley_STRATUS_WebApps_x.x.x.cab*
  - *GrassValley_STRATUS_WebClient_x.x.x.cab*
  - *GrassValley_Sabretooth_Application_x.x.x.cab*
  - *GrassValley_DeviceKeyService_x.x.x.cab*
  - *GrassValley_LogManager_x.x.x.cab*
  - *GrassValley_LogViewer_x.x.x.cab*
  - *GV_STRATUS_Rundown_x.x.x.cab*
- *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:
  - *GrassValley_STRATUS_ControlPanel_x.x.x.cab*
  - *GrassValley_STRATUS_Application_x.x.x.cab* (Use for test purposes only)
- *GrassValley_K2system_x.x.x.cab* for K2 9.8.x systems.
- *GrassValley_K2Plus_x.x.x.cab* for K2 10.x systems.

Licenses:

- GV STRATUS licenses (Express/Flex/Pro/Elite) as appropriate for customer site.
- STRATUS-CONFORM (Optional) Includes XRE, Conform, Proxy Encoder functionality.
- STRATUS-GVRE (Optional) Includes Conform and Proxy Encoder functionality. Only one license is needed in a system, either STRATUS-CONFORM or STRATUS-GVRE.
- STRATUS-PROXYSTREAMING for servers supporting proxy streaming via the Web Client.

- STRATUS-QFHD (Optional) only required for 4K/QFHD format to be supported in your operation.
- STRATUS-TRANSCODE (Optional) for generic transcoder functionality with GVRE.
- STRATUS-ARCHIVE (Optional)
- STRATUS-RULES (Optional)
- STRATUS-SMNSOCIALMEDIAENGINE (Optional)
- STRATUS-EMNEXTERNALMEDIAENGINE (Optional)
- STRATUS-SMNFACEBOOK (Optional)
- STRATUS-SMNTWITTER (Optional)
- STRATUS-SMNYOUTUBE (Optional)
- STRATUS-EMNVERIZON (Optional)
- STRATUS-XCODECONTROLCARBONCODER (Optional. Depends on STRATUS-RULES.)
- STRATUS-XCODECONTROLVANTAGE (Optional. Depends on STRATUS-RULES.)
- STRATUS-XCODECONTROLELEMENTAL (Optional. Depends on STRATUS-RULES.)
- STRATUS-MULTISITE (Optional)
- STRA-PREM-CONNECT (Optional)
- STRATUS-VTR-ING (Optional)
- STRATUS-WEB-CLIENT (Optional)
- STRATUS-XCODECONTROLMEWS (Optional)
- STRATUS-XCODECONTROLMEWSEXT (Optional)

These are Sabretooth floating licenses, which means they are not restricted to single computer. GV STRATUS Control Panel assigns the licenses to user groups.

Contact your Grass Valley representative for a current list of available licenses.

Windows Control Panel Services:

- GV STRATUS ASK. Startup type: Automatic
- GV STRATUS Common Services. Startup type: Automatic
- GV STRATUS Control Panel Services. Startup type: Automatic
- GV STRATUS Data Mover Engine. Startup type: Automatic
- GV STRATUS Index Agent. Startup type: Automatic
- GV STRATUS Ingest Config. Startup type: Automatic
- GV STRATUS Ingest Core. Startup type: Automatic
- GV STRATUS Ingest DB. Startup type: Automatic
- GV STRATUS Maintenance Service. Startup type: Automatic
- GV STRATUS MDI Common RESTful Archive. Startup type: Automatic
- GV STRATUS MDI DIVA. Startup type: Automatic
- GV STRATUS MDI Flashnet. Startup type: Automatic
- GV STRATUS MDI Masstech. Startup type: Automatic
- GV STRATUS MDI GFTP. Startup type: Automatic
- GV STRATUS MDI Proxy. Startup type: Automatic
- GV STRATUS MDI Summit. Startup type: Automatic
- GV STRATUS MediaFlow Workflow Engine. Startup type: Automatic
- GV STRATUS Resolver. Startup type: Automatic
- GV STRATUS Router Config. Startup type: Automatic
- GV STRATUS Router Controller. Startup type: Automatic
- GV STRATUS Rules Engine. Startup type: Automatic
- GV STRATUS Rules Wizard. Startup type: Automatic

- GV STRATUS Scheduled Transfer Engine. Startup type: Automatic
- GV STRATUS Segmentation Config. Startup type: Automatic
- GV STRATUS Social Media Engine. Startup type: Automatic
- GV STRATUS External Media Engine. Startup type: Automatic
- GV STRATUS Traffic Gateway. Startup type: Automatic
- GV STRATUS Xcode Control Engine
- GV Device Key Service. Startup type: Automatic
- GV Proxy Streaming Gateway Service. Startup type: Automatic
- GV Log Manager. Startup type: Automatic
- ProductFrame Discovery Agent Service. Startup type: Automatic
- Sabretooth License Server. Startup type: Manual
- Sabretooth Protocol Service. Startup type: Manual

Proxy Server components

Description: The server that provides access to the proxy media on a GV STRATUS system with proxy media stored on an online or production K2 SAN.

Nomenclature:

- This server is a subcomponent of the STRATUS-CS-A1 nomenclature.

SiteConfig "Add Device":

- Family: GV STRATUS
- Device Type: GV STRATUS Server
- Model: GV STRATUS Proxy Server

SiteConfig Roles:

- GV STRATUS Proxy K2 SAN Server
- GV Log Manager
- StorNext File System Client

K2Config Roles:

- SNFS file system client

SiteConfig cab files:

- *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
  - *GrassValley_STRATUS_HttpProxyServer_x.x.x.cab*
  - *GrassValley_LogManager_x.x.x.cab*
- *GrassValley_STRATUSClient_x.x.x.cab*.
- For K2 9.8.x systems; use *GrassValley_K2system_x.x.x.cab*, which contains the following cab files that apply to this device:
  - *GrassValleyK2Server_x64_9.8.x.x.cab*
  - *SNFS_x64_4.7.x.xxx.cab*

- For K2 10.x systems; use *GrassValley_K2Plus_x.x.x.cab*, which contains the following cab files that apply to this device:
  - *GrassValleyK2Server_x64_10.x.x.cab*
  - *SNFS_x64_6.0.x.xxx.cab*

Licenses:

- None

Windows Control Panel Services:

- CvfsPM. Startup type: Automatic
- Grass Valley AppService. Startup type: Automatic
- Grass Valley Extent Manager Service. Startup type: Manual
- Grass Valley FTP Daemon. Startup type: Automatic
- Grass Valley Import Service. Startup type: Manual
- Grass Valley K2 Config. Startup type: Automatic
- Grass Valley MegaRaid Server. Startup type: Manual
- Grass Valley Performance Status. Startup type: Manual
- Grass Valley Performance Status Maker. Startup type: Manual
- Grass Valley SabreToothWS. Startup type: Automatic
- Grass Valley Server Monitor. Startup type: Automatic
- Grass Valley SNFS SetRtio. Startup type: Automatic
- Grass Valley Storage Utility Host. Startup type: Automatic
- GV STRATUS K2 Configuration Service. Startup type: Automatic
- ProductFrame Discovery Agent Service. Startup type: Automatic

Proxy Storage file system server components

Description: The server that provides access to the proxy media on a GV STRATUS system with a dedicated Proxy Storage system.

Nomenclature:

- This server is a subcomponent of the following nomenclatures:
  - STRATUS-CS-B1
  - STRATUS-CS-C1
  - STRATUS-CS-B1-FT
  - STRATUS-CS-C1-FT

SiteConfig "Add Device":

- Family: GV STRATUS
- Device Type: GV STRATUS Server
- Model: GV STRATUS Proxy Storage File System Server

SiteConfig Roles:

- GV STRATUS Proxy Storage Server
- GV Log Manager
- StorNext File System Server

- StorNext File System Client

K2Config Roles:

- SNFS file system server

SiteConfig cab files:

- *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
  - *GrassValley_STRATUS_HttpProxyServer_x.x.x.cab*
  - *GrassValley_LogManager_x.x.x.cab*
- *GrassValley_STRATUSClient_x.x.x.cab*.
- For K2 9.8.x systems; use *GrassValley_K2system_x.x.x.cab*, which contains the following cab files that apply to this device:
  - *GrassValleyK2Server_x64_9.8.x.x.cab*
  - *SNFS_x64_4.7.x.xxx.cab*
- For K2 10.x systems; use *GrassValley_K2Plus_x.x.x.cab*, which contains the following cab files that apply to this device:
  - *GrassValleyK2Server_x64_10.x.x.cab*
  - *SNFS_x64_6.0.x.xxx.cab*

Licenses:

- None

Windows Control Panel Services:

- CvfsPM. Startup type: Automatic
- Grass Valley AppService. Startup type: Automatic
- Grass Valley Extent Manager Service. Startup type: Manual
- Grass Valley FTP Daemon. Startup type: Automatic
- Grass Valley Import Service. Startup type: Manual
- Grass Valley K2 Config. Startup type: Automatic
- Grass Valley MegaRaid Server. Startup type: Manual
- Grass Valley Performance Status. Startup type: Manual
- Grass Valley Performance Status Maker. Startup type: Manual
- Grass Valley SabreToothWS. Startup type: Automatic
- Grass Valley Server Monitor. Startup type: Automatic
- Grass Valley SNFS SetRtio. Startup type: Automatic
- Grass Valley Storage Utility Host. Startup type: Automatic
- GV STRATUS K2 Configuration Service. Startup type: Automatic
- ProductFrame Discovery Agent Service. Startup type: Automatic
- Sabretooth License Server. Startup type: Manual
- Sabretooth Protocol Service. Startup type: Manual

Render Engine Server components

The system components listed in these topics are related to GV STRATUS system functionality. Other components can be present, but if they are not specific to GV STRATUS system functionality they are not listed in these topics.

Description: A GV STRATUS server that functions as a proxy encoder and as a conform server. As a proxy encoder, the server creates low-resolution proxy assets. If a high-resolution asset does not yet have associated proxy, the server creates it. The software that provides the proxy encoder functionality can run on a dedicated Render Engine server or on a GV STRATUS server that has other roles as well, such as a GV STRATUS Express server. As a conform server, the server hosts the Render Engine Service. The service renders a complex asset, such as a GV STRATUS sequence or a project created in EDIUS, into a simple clip.

Nomenclature:

- STRATUS-CS-RE

SiteConfig "Add Device":

- Family: GV STRATUS
- Device Type: GV STRATUS Server
- Model: GV STRATUS Render Engine

SiteConfig Roles:

- GV STRATUS Control Panel
- GV Log Manager
- StorNext File System Client
- GV Embedded Security Manager
- GV STRATUS Render Engine

K2Config Roles:

- None

SiteConfig cab files:

- *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
  - *GrassValley_STRATUS_RenderEngine_x.x.x.cab*
  - *GVEmbeddedSecurityManager_x.x.x.cab*
  - *GrassValley_Sabretooth_Application_x.x.x.cab*
  - *GrassValley_LogManager_x.x.x.cab*
- For K2 9.8.x systems; use *GrassValley_K2system_x.x.x.cab*, which contains the following cab files that apply to this device:
  - *GrassValleyK2Server_x64_9.8.x.x.cab*
  - *SNFS_x64_4.7.x.xxx.cab*
- For K2 10.x systems; use *GrassValley_K2Plus_x.x.x.cab*, which contains the following cab files that apply to this device:
  - *GrassValleyK2Server_x64_10.x.x.cab*
  - *SNFS_x64_6.0.x.xxx.cab*

- *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:
  - *GrassValley_STRATUS_Application_x.x.x.cab*
  - *GrassValley_STRATUS_ControlPanel_x.x.x.cab*

Licenses:

- None

Windows Control Panel Services:

- CvfsPM. Startup type: Automatic
- Grass Valley AppService. Startup type: Automatic
- Grass Valley Extent Manager Service. Startup type: Manual
- Grass Valley FTP Daemon. Startup type: Automatic (not required from GV STRATUS 4.5)
- Grass Valley Import Service. Startup type: Manual
- Grass Valley K2 Config. Startup type: Automatic
- Grass Valley MegaRaid Server. Startup type: Manual
- Grass Valley Performance Status. Startup type: Manual
- Grass Valley Performance Status Maker. Startup type: Manual
- Grass Valley SabreToothWS. Startup type: Automatic
- Grass Valley Server Monitor. Startup type: Automatic
- Grass Valley SNFS SetRtio. Startup type: Automatic
- Grass Valley Storage Utility Host. Startup type: Automatic
- Grass Valley XRE Controller. Startup type: Automatic (Delayed Start)
- GV Render Engine. Startup type: Automatic (Delayed Start)
- GV STRATUS K2 Configuration Service. Startup type: Automatic
- Microsoft iSCSI Initiator Service. Startup type: Automatic
- ProductFrame Discovery Agent Service. Startup type: Automatic
- Sabretooth License Server. Startup type: Manual
- Sabretooth Protocol Service. Startup type: Manual

Workflow Server components

Description: A GV STRATUS server dedicated to hosting the Workflow Engine Service, the Rules Engine Service, and the Xcode Control Engine Service. These services support rules-based operations.

Nomenclature:

- STRATUS-CS-WFE

SiteConfig "Add Device":

- Family: GV STRATUS
- Device Type: GV STRATUS Server
- Model: GV STRATUS Workflow Server

SiteConfig Roles:

- GV STRATUS Workflow Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
- GV STRATUS Rules Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)

- GV STRATUS SocialMedia Engine (Optional)
- GV STRATUS ExternalMedia Engine (Optional)
- GV STRATUS Xcode Control Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
- GV STRATUS Control Panel
- GV Log Manager

K2Config Roles:

- None

SiteConfig cab files:

- *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
  - *GrassValley_STRATUS_Mediaflow_x.x.x.cab*
  - *GrassValley_STRATUS_Rules_x.x.x.cab*
  - *GrassValley_STRATUS_SocialMedia_x.x.x.cab*
  - *GrassValley_STRATUS_ExternalMedia_x.x.x.cab*
  - *GrassValley_STRATUS_Transcode_x.x.x.cab*
  - *GrassValley_STRATUS_TrafficGateway_x.x.x.cab*
  - *GrassValley_Sabretooth_Application_x.x.x.cab*
  - *GrassValley_LogManager_x.x.x.cab*
- *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:
  - *GrassValley_STRATUS_ControlPanel_x.x.x.cab*
- *GrassValley_K2system_x.x.x.cab* for K2 9.8.x systems.
- *GrassValley_K2Plus_x.x.x.cab* for K2 10.x systems.

Licenses:

- STRATUS-RULES
- STRATUS-EMNEXTERNALMEDIAENGINE (Optional)
- STRATUS-SMNSOCIALMEDIAENGINE (Optional)
- STRATUS-EMNVERIZON (Optional)
- STRATUS-SMNFACEBOOK (Optional)
- STRATUS-SMNTWITTER (Optional)
- STRATUS-SMNYOUTUBE (Optional)
- STRATUS-XCODECONTROLCARBONCODER
- STRATUS-XCODECONTROLVANTAGE
- STRATUS-XCODECONTROLELEMENTAL

Windows Control Panel Services:

- GV STRATUS MediaFlow Workflow Engine. Startup type: Automatic
- GV STRATUS Rules Engine. Startup type: Automatic
- GV STRATUS Social Media Engine. Startup type: Automatic
- GV STRATUS External Media Engine. Startup type: Automatic
- GV STRATUS Xcode Control Engine
- ProductFrame Discovery Agent Service. Startup type: Automatic

- Sabretooth License Server. Startup type: Manual
- Sabretooth Protocol Service. Startup type: Manual

MEWS Server components

Description: A customer-supplied server dedicated to MEWS functionality. It hosts MewsService, which is a Grass Valley service.

Nomenclature:

- None. This is a customer-supplied device.

SiteConfig "Add Device":

- Family: GV STRATUS
- Device Type: GV STRATUS Server
- Model: GV STRATUS MEWS Server

SiteConfig Roles:

- GV STRATUS MEWS Engine
- GV Log Manager

K2Config Roles:

- None

SiteConfig cab files:

- *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
  - *GrassValley_STRATUS_MEWS_x.x.x.cab*
  - *GrassValley_LogManager_x.x.x.cab*

Licenses:

- STRATUS-XCODECONTROLMEWS
- STRATUS-XCODECONTROLMEWSEXT

NOTE: Multiple MEWS licenses of the same type are not supported in a* GV STRATUS *system.

Windows Control Panel Services:

- GV STRATUS MEWS Engine. Startup type: Automatic

GV STRATUS proxy client PC components

Description: A customer-supplied PC connected to the customer's corporate LAN or to the control network for a proxy media workflow.

SiteConfig "Add Device":

- Family: GV STRATUS
  NOTE: Do not select the EDIUS family.
- Device Type: GV STRATUS Client
- Model: GV STRATUS PC or GV STRATUS/EDIUS PC (if using EDIUS XS)

SiteConfig Roles:

- GV STRATUS Application
- EDIUS (Required for EDIUS XS)

K2Config Roles:

- None

SiteConfig cab files:

- *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:
  - *GrassValley_STRATUS_Application_x.x.x.cab*
  - *EDIUS_x.x.x.cab* (Required for EDIUS XS)

Licenses:

- GV STRATUS license assigned/managed by Core Services server with role of Common Services.

  NOTE: You must not have an EDIUS Workgroup license installed on the client PC. This is an EDIUS license, not a Sabretooth license. If the EDIUS Workgroup license is installed, the EDIUS application launches as high-resoluton EDIUS Workgroup, not low resolution (proxy) EDIUS XS. Running EDIUS XS and EDIUS Workgroup on the same client PC is not supported.

Windows Control Panel Services:

- None

GV STRATUS high-resolution client PC components

Description: A customer-supplied PC connected to the K2 media (iSCSI) network for a high-resolution media workflow.

SiteConfig "Add Device":

- Family: GV STRATUS

  NOTE: Do not select the EDIUS family.
- Device Type: GV STRATUS Client
- Model: GV STRATUS PC - SAN Client or GV STRATUS/EDIUS PC - SAN Client (if using EDIUS Workgroup)

SiteConfig Roles:

- GV STRATUS Application
- StorNext File System Client (non K2 only)
- Generic iSCSI Client (non K2 only)

  NOTE: First install StorNext File System Client, then install Generic iSCSI Client via SiteConfig for the following:

  - ***First installation of GV STRATUS application into a system.***
  - ***When there is an upgrade of the StorNext File System Client.***
- EDIUS (Required for EDIUS Workgroup)

K2Config Roles:

- SNFS file system client

SiteConfig cab files:

- *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:
  - *GrassValley_STRATUS_Application_x.x.x.cab*
  - *GenericISCSI_x64_ x.x.x.cab*
  - *SNFS_nonK2_x64_x.x.x.cab*
  - *EDIUS_x.x.x.cab* (Required for EDIUS Workgroup).

Licenses:

- GV STRATUS license assigned/managed by Core Services server with role of Common Services.
- GV STRATUS high-resolution also required for each high-resolution GV STRATUS client PC.
- EDIUS Workgroup (Required for EDIUS Workgroup). This is an EDIUS license, installed on the client PC, and managed by EDIUS license management.

Windows Control Panel Services:

- CvfsPM. Startup type: Automatic
- Grass Valley K2 Config. Startup type: Automatic
- Microsoft iSCSI Initiator Service. Startup type: Automatic
- ProductFrame Discovery Agent Service. Startup type: Automatic
- Sabretooth License Server. Startup type: Manual
- Sabretooth Protocol Service. Startup type: Manual

K2 systems components

K2 system

Description: The K2 devices that provide the high-resolution assets for the GV STRATUS system. This includes standalone K2 Summit systems and K2 Media Servers that are File System Managers (FSM) on K2 SANs.

SiteConfig "Add Device":

- Family: K2
- Device Type:

  K2 Summit Client - Standalone

  or

  K2 Server
- Model: As appropriate for the type of K2 system

SiteConfig Roles:

- GV STRATUS Summit Service

K2Config Roles:

- As appropriate for the type of K2 system

SiteConfig cab files:

- *GrassValley_K2system_x.x.x.cab*, which contains the following cab files that apply to this device:
  - *GrassValley_STRATUS_SummitServices_x.x.x.cab*

Licenses:

- On K2 Summit systems, K2 software license
- On K2 Summit systems, AppCenter Pro or Workgroup, as appropriate for the customer site. Either of these licenses enables proxy on the K2 Summit system.
- On K2 Media Servers, a license for bandwidth.

These are Sabretooth node-locked licenses, which means they are restricted to single computer.

Windows Control Panel Services:

- As appropriate for the type of K2 system. Refer to "K2 Summit Production Client Service Manual" or the "Installing and Servicing the K2 SAN" section of the K2 Topic Library.

GV STRATUS Rundown client PC components

Description: A customer-supplied PC that hosts the GV STRATUS Rundown application.

SiteConfig "Add Device":

- Family: GV STRATUS
- Device Type: GV STRATUS Client
- Model: GV STRATUS Rundown

SiteConfig Roles:

- GV STRATUS Rundown Application
- GV STRATUS Application
- License Manager

K2Config Roles:

- None

SiteConfig cab files:

- *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:
  - *GrassValley_STRATUS_Application_x.x.x.cab*
  - *GV_STRATUS_Rundown_x.x.x.cab*

    NOTE: If the target machine does not have Microsoft .NET installed, SiteConfig attempts to install it. This requires that Grass Valley Prerequisite Files be installed on the SiteConfig host PC, to provide the Microsoft .NET installation files.

- *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
  - *GrassValley_Sabretooth_Application_x.x.x.cab*
- *GrassValley_K2system_x.x.x.cab* for K2 9.8.x systems.

- `GrassValley_K2Plus_x.x.x.cab` for K2 10.1.x systems.

Licenses:

- GV STRATUS Elite
- Aurora GFX

GV STRATUS VTR applications client PC components

Description: A customer-supplied PC that hosts the GV STRATUS VTR Ingest and GV STRATUS VTR Controller application.

SiteConfig "Add Device":

- Family: GV STRATUS
- Device Type: GV STRATUS Client
- Model:
  - GV STRATUS VTR Ingest
  - GV STRATUS VTR Controller

SiteConfig Roles:

- GV STRATUS VTR Ingest
- GV STRATUS VTR Controller

K2Config Roles:

- None

SiteConfig cab files:

- `GrassValley_STRATUSClient_x.x.x.cab`, which contains the following cab files that apply to this device:
  - `GrassValley_STRATUS_VTRIngest_x.x.x.cab`

    NOTE: If the target machine does not have Microsoft .NET installed, SiteConfig attempts to install it. This requires that Grass Valley Prerequisite Files be installed on the SiteConfig host PC, to provide the Microsoft .NET installation files.

Licenses:

- STRATUS-VTR-ING

This is a Sabretooth floating license, which means it is not restricted to a single computer. You can use the license on multiple GV STRATUS VTR Ingest clients, one at a time.

GV STRATUS roles matrix

Key:

- AA = Automatically Added for a User or Group with that license (except during version upgrades).
- P = Possible to add for a User or Group with that license.
- X = Not available to be added for a User or Group with that license.

	News room Basic	Express	Flex	Pro	Elite	Enables a Group or User:
Advanced Editor	X	X	AA	AA	AA	Enables a Group or User: Access to Go! Web Client Editor.
Advanced Logging	X	X	X	AA	AA	Access to Advanced Logging tool.
Archive Rights	X	AA	AA	AA	AA	Ability to archive Assets.
Assignment List	AA	AA	AA	AA	AA	Access to Assignment List tool.
Auto Logout	AA	AA	AA	AA	AA	To be automatically logged off as part of Auto Logout scope.
Bin Creation Rights	AA	AA	AA	AA	AA	Ability to create Bins.
Change Thumbnail Rights	AA	AA	AA	AA	AA	Ability to upload, set, and delete Thumbnails.
Channel Panel	X	X	X	AA	AA	Access to Channel Panel tool.
Copy Metadata	AA	AA	AA	AA	AA	Ability to copy and paste Metadata.
Dashboard	X	P	P	P	P	Access to Dashboard node.
Dashboard - Channel Status	X	X	P	P	P	Access to Channel Status Dashboard (Dashboard Role Also Required).
Dashboard - Quotas	X	P	P	P	P	Access to Quota Dashboard (Dashboard Role Also Required).
Dashboard - Social Media	X	P	P	P	P	Access to Social Media Dashboard (Dashboard Role Also Required).
Dashboard - Statistics	X	P	P	P	P	Access to Statistics Dashboard (Dashboard Role Also Required).
Dashboard - Storage	X	P	P	P	P	Access to Storage Dashboard (Dashboard Role Also Required)
Delete Rights	AA	AA	AA	AA	AA	Ability to delete Bins, Assets, and Associations.
Edius Project Management	X	P	P	P	P	Access to EDIUS Projects node.

Edius XS	X	X	AA	AA	AA	Ability to launch Assets into EDIUS XS.
Export Rights	AA	AA	AA	AA	AA	Ability to export Assets.
Media Manager	X	P	P	P	P	See note below.
Missing Material List	P	P	P	P	P	GV Developer Use Only.
Move Rights	AA	AA	AA	AA	AA	Ability to move Assets (Locations and Groups) (Delete Rights Role Also Required).
Multisite Access	X	AA	AA	AA	AA	Access and search for remote Assets.
Playlist Editor	X	X	X	AA	AA	Access to Playlist Editor tool.
Queue Management	X	AA	AA	AA	AA	Ability to set job priority within Job Monitor.
Rename Asset Rights	AA	AA	AA	AA	AA	Ability to rename Assets.
Rename Bin Rights	AA	AA	AA	AA	AA	Ability to rename Bins in Locations node.
Restore Rights	X	AA	AA	AA	AA	Ability to restore Assets as copy.
RMI	X	X	X	AA	AA	Access to RMI tool.
Schedule Monitor	X	AA	AA	AA	AA	Access to Schedule Monitor under Monitors node.
Scheduled Transfer	X	X	X	X	P	Access to Scheduled Transfer tool.
Scheduler	X	X	X	X	AA	Access to Scheduler tool.
Scheduler (Read Only)	X	AA	AA	AA	P	Access to Read-Only Scheduler tool.
Security Manager	X	P	P	P	P	Bypass security/permissions, modify any Bin, Group, or Asset permissions, owner, and owner hint, plus all Media Manager functionality.
Segmentation	X	AA	AA	AA	AA	Access to Segmentation tool and House Number tool. Ability to make Segments in Web Client.
Send Message	X	AA	AA	AA	AA	Access to Send Message tool.

Simple Editor	X	AA	AA	AA	AA	Access to Simple Editor tool and Lost and Found group.
Source Viewer	X	AA	AA	AA	AA	Access to Source Viewer tool.
Storyboard Editor	X	AA	AA	AA	AA	Access to Storyboard Editor tool.
Trim Rights	AA	AA	AA	AA	AA	Ability to Trim and Untrim Assets.
Web Monitor	X	AA	AA	AA	AA	Access to Web Monitor tool for web pages.
Web Access	AA	AA	AA	AA	AA	Access to GV STRATUS Web Client shortcut nodes.

Notes:

Media Manager Role:

- Enables Archive Rights
- Enables Restore Rights as copy and also as move
- Enables Extended Delete Type Options (Delete Rights Role Also Required)
- Enables the ability to save Public Searches
- Enables access to the Lost and Found group
- Enables access to the Archives in Devices node
- Enables the ability to copy and paste Metadata even if Denied
- Enables an API account to create Custom Metadata for Markers and Keywords

The Deny Role option disables a role's functionality or tool(s) for a specific User or Group.

Example: Enable Delete Rights for Group X members, then Deny Delete Rights for User Y of Group X.

Related Topics

If you have trouble launching EDIUS XS on page 169

About Archive/Restore roles

Archive/Restore roles are enabled by a SabreTooth license that is installed on the GV STRATUS Core server. When installed, in GV STRATUS Control Panel, the following roles are enabled and can be assigned to groups and users.

- Archive Rights
- Restore Rights

In the GV STRATUS Navigator panel, Archive systems are located under the Devices node. These systems are visible only for those with Archive Rights and/or Restore Rights.

If the role of Media Manager is assigned, the following occurs:

- Archive Rights and Restore Rights roles are enforced. You cannot remove the Archive/Restore role of a Media Manager.

- Permission is granted to move assets from an archive system to the GV STRATUS system. Without this permission, assets may be copied but not moved.

If a Newsroom Basic license, Archive/Restore roles are disabled.

Related Topics

GV STRATUS roles matrix on page 37

About Move/Delete Rights roles

In GV STRATUS Control Panel, the following roles can be assigned to groups and users.

- Move Rights: Allows assets to be moved from one bin to another. This applies to K2 storage locations and to logical Asset Groups.
- Delete Rights: Allows assets to be deleted.

In most asset transfer cases, the Move Rights roles supersedes the Delete Rights role, as follows:

- Move operation: When you move an asset, by design it is deleted from the source location. Since this operation requires the Move Rights role, the Delete Rights role is not required.
- Overwrite: When an asset exists at the destination location that is named the same as the asset you are transferring, you have the option to overwrite (delete) the asset. If a move operation, since the Move Rights role is required, the Delete Rights role is not required. If a copy operation, the Move Rights role does not apply, so the Delete Rights role is required.

The Move Rights role is independent of the Archive Rights role. It is recommended that users with the Archive Rights role also have the Move Rights role, so that move operations to archive are allowed.

About Newsroom Basic

The Newsroom Basic license is for journalists that work with the GV STRATUS application as an ActiveX window within a Newsroom Computer System (NCS) application. For this workflow, only the Inspector panel and the Assignment List tool are typically required. The Newsroom Basic license provides this limited functionality as an economical solution. There is no access to the full range of GV STRATUS functionality and tools, as available with other licenses.

If your license type is changed from some other license to the Newsroom Basic license, some of your previously saved workspaces might not be available. Workspaces that contain tools for which the Newsroom Basic license has no access are not allowed. Load the Default Workspace if necessary.

Related Topics

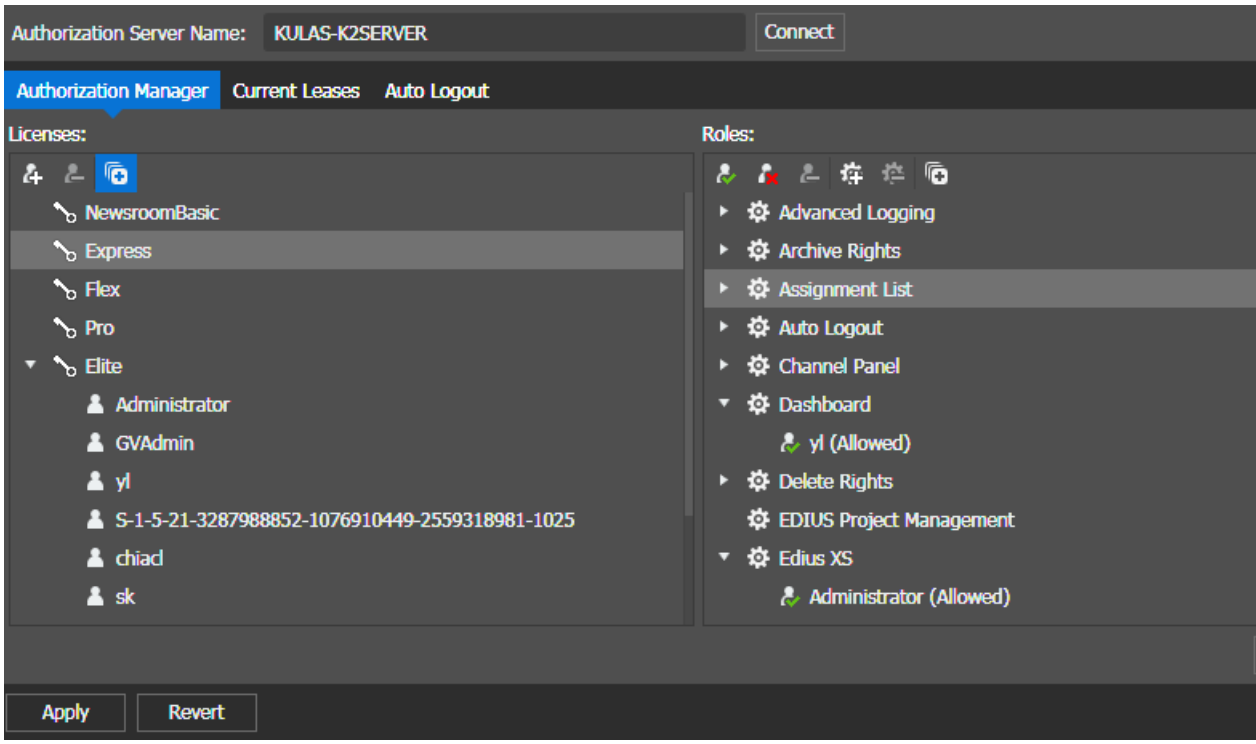
GV STRATUS roles matrix on page 37

Adding a custom role

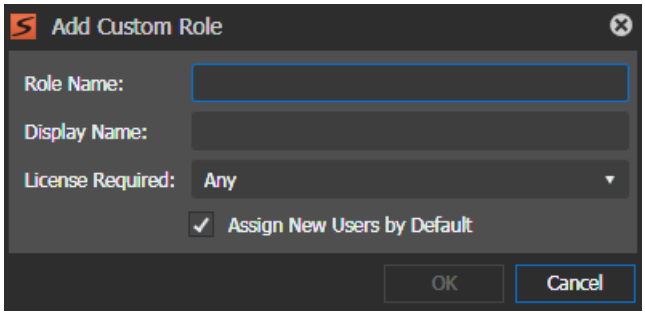
You can create custom roles in the GV STRATUS Control Panel, if desired. This is useful for license management of third party system users connected to the GV STRATUS application. If multiple

custom roles are created, you can assign tools and features to be displayed or hidden according to required licenses of these custom roles.

1. In GV STRATUS Control Panel, click **General | License Management | Authorization Manager**.



2. Click the **Add Custom Role** button.
   The Add Custom Role dialog box opens.



3. Enter details for the custom role as follows:

   - **Role Name**: The name of the newly created role.
   - **Display Name**: The custom role name to be displayed in GV STRATUS Control Panel application.
   - **License Required**: Select the required license for the custom role from the drop-down list.
   - **Assign New Users by Default**: Select the checkbox if you want to assign new users with this custom role by default.

4. Click **OK**.

The new custom role displays under the **Roles** section in the **Authorization Manager** tab.

If the custom role is not needed in future, you can remove it by clicking the **Remove Custom Role** button.

About Auto Logout

The purpose of the Auto Logout role is to release the GV STRATUS license that is assigned to a system that has been idle for a long period of time. This returns the license to the pool of available licenses and makes it available for use by another GV STRATUS application.

In GV STRATUS Control Panel, the Auto Logout role can be assigned to groups and users. When a user account with this role is logged on to the GV STRATUS application, the GV STRATUS system monitors the host PC for activity and triggers the auto logout process if appropriate. This process is configured in Auto Logout settings.

To locate these settings, click **General | License Management | Auto Logout**

The following setting specifies the timing of the auto logout process:

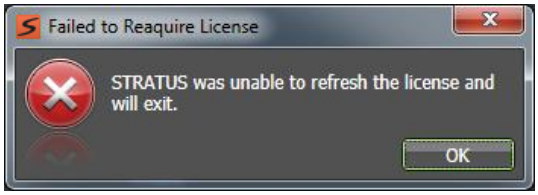
Setting or button	Description
STRATUS Application Timeout	The length of time the PC that hosts the GV STRATUS application must sit idle, with no activity, before that PC's GV STRATUS license is released.

The auto logout process occurs as follows:

1. Five minutes before the timeout, a dialog box opens with a message specifying the time the license is to be released.

2. If a user clicks **Continue** within five minutes, the auto logout process is discontinued and the timeout is reset.
3. If there is no interaction with the message dialog box within five minutes, the dialog box closes and another dialog box opens. This second dialog box displays a message that the license is released and provides options to log off the GV STRATUS application or to refresh the license.

4. The license used currently by the GV STRATUS application is returned to the pool of available licenses. Until an option is selected, the GV STRATUS application and the dialog box remain open. The GV STRATUS application is unusable, but current work is retained.
5. When the option to refresh the license is selected, if a license is available, the GV STRATUS application is licensed and becomes usable. If a license is not available, a dialog box opens with a message about the license. Clicking **OK** logs out and closes the GV STRATUS application.



Related Topics

Auto Logout settings on page 368

Administering and maintaining the GV STRATUS system

Configuring the GV STRATUS system

Topics in this section provide instructions for configuration and housekeeping tasks necessary for customizing and maintaining your site's workflows.

About the Lost and Found folder

If you have the role of Media Manager you will find a folder named **Lost and Found** under the **Groups** node in Navigator. This is the default folder for any asset that does not otherwise have a location, meaning that there is no folder under the Navigator **Groups | Locations** node that contains the asset. When the GV STRATUS application determines that an asset does not have a location, it automatically places the asset in the **Lost and Found** folder.

Examples of an asset with no location are as follows:

- An event scheduled by the Scheduler that does not yet have an associated location.
- An asset for which the high-resolution media no longer exists in the GV STRATUS system.

If an asset in the **Lost and Found** folder later acquires a location, the asset appears in that location and is removed from the **Lost and Found** folder.

You can manage assets in the **Lost and Found** folder the same as any other folder under the **Groups** node.

Related Topics

About the GV STRATUS Assets view on page 417

Configuring delete rights

- The groups and users for which you are configuring delete rights must be set up, either on a workgroup or on a domain, on the following:
  - The GV STRATUS server with role of Common Services.
- The GV STRATUS server with role of Common Services must have the site's GV STRATUS licenses installed.

If on a network Workgroup, to configure Authorization Manager settings, you must be running GV STRATUS Control Panel on the GV STRATUS Core server.

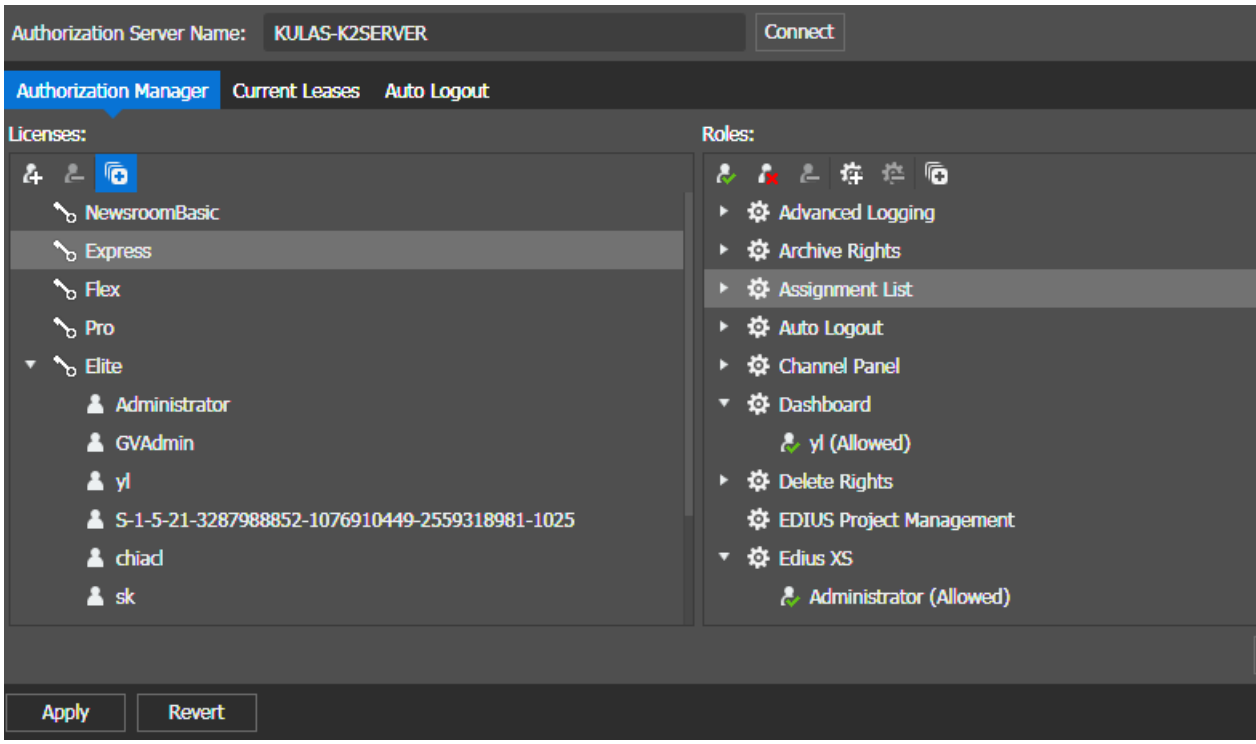
By default, all groups and users have permission to delete bins and assets. You can deny delete rights to some groups and users. When delete rights are denied, the following occurs:

- Bins and assets cannot be deleted from the GV STRATUS system.
- Delete menu items are disabled and delete keyboard shortcuts do not take effect.
- Under Favorites, bins and assets can still be removed, since doing so does not actually delete anything from the GV STRATUS system.

Delete rights apply to all licenses.

To locate these settings, click **General | License Management | Authorization Manager**

1. In the GV STRATUS Control Panel application, open **License Management** settings.



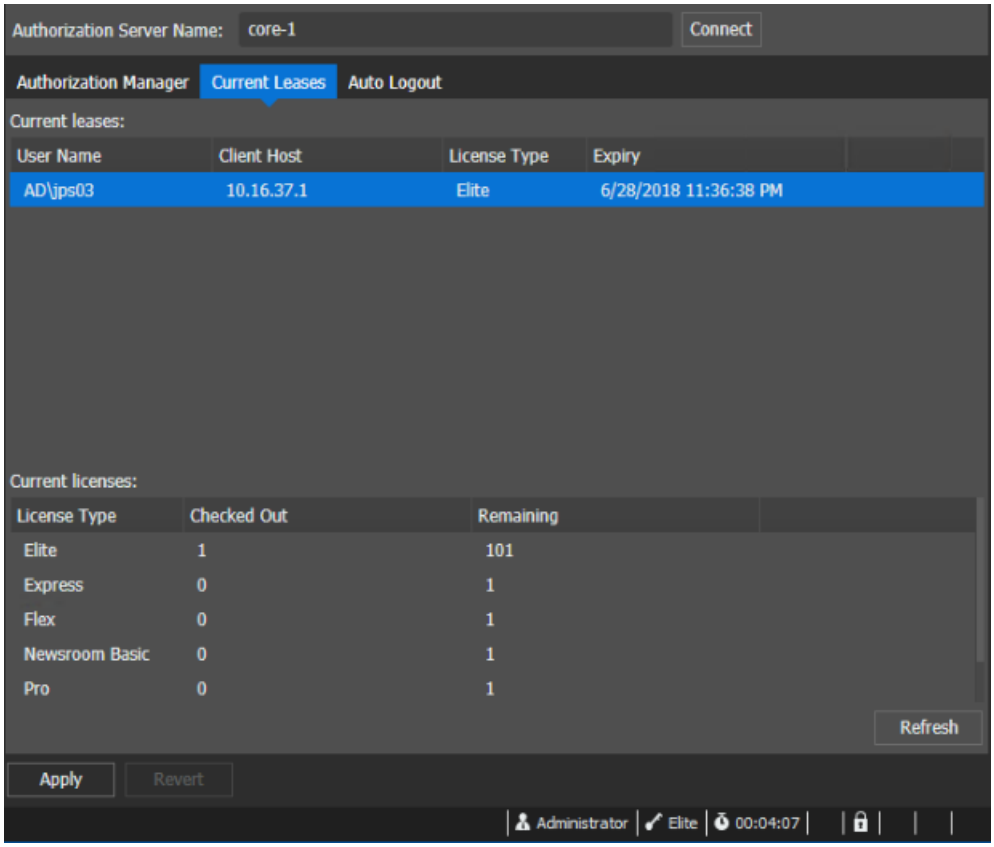
2. On the Authorization Manager tab, enter the following:
   - **Authorization Server Name**: The name of GV STRATUS server with role of Common Services.

3. Click the following:
   - **Connect**: Connects to the GV STRATUS server and populates settings. If the Connect button is disabled, it means you are already connected.
4. Under **Roles**, right-click **Delete Rights** and select one of the following:
   - **Allow Group or User**
   - **Deny Group or User**
5. Use standard Windows operating system procedures to specify the group or user.
6. Click **Apply** to save your current settings, or click **Revert** to return to the last saved settings.

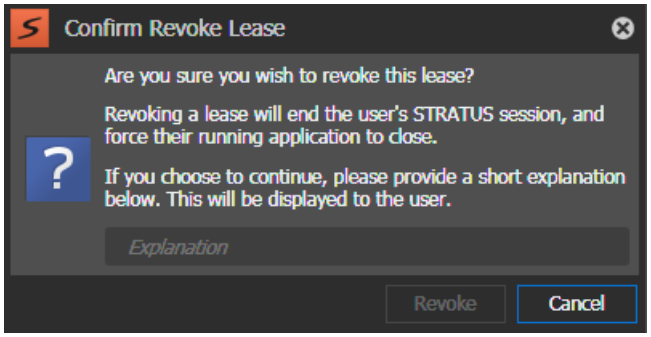
Revoking a GV STRATUS license lease

If a GV STRATUS user is currently using a license, you can revoke their lease on the license. This automatically closes the user's GV STRATUS application and makes the license available for a different GV STRATUS user to use.

1. In GV STRATUS Control Panel click **General | License Management | Current Leases**.



2. Under **Current leases**, right-click a row and select **Revoke Lease**.
   The Confirm Revoke Lease dialog box opens.



3. Enter a message to inform the user that their lease is to be revoked.
4. Click **Revoke**.
   The following occurs:
   - The license is immediately available to be used by another GV STRATUS user.
   - Within one minute, the message opens in front of the revoked user's GV STRATUS application.
   - 30 seconds after the revoked user clicks **OK** on the message, the revoked user's GV STRATUS application automatically closes.

Working with GV Log Viewer

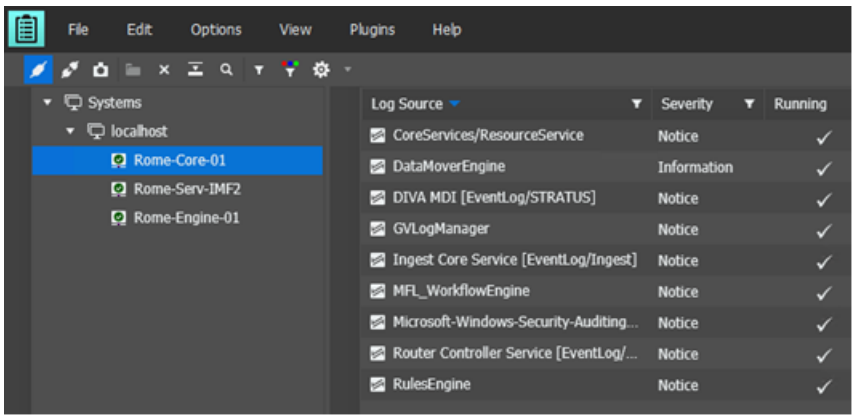
The GV Log Viewer application displays detailed information about significant events on your GV STRATUS system. Use the application only if you are a qualified system administrator or as directed by Grass Valley support.

The SiteConfig GV STRATUS Log Viewer role installs the application on GV STRATUS servers.

You can open GV Log Viewer to view event logs, save event logs as an xml file, or copy event logs into another application.

Launch the GV Log Viewer by doing one of the following:

- Double-click the **GV Log Viewer** shortcut on your desktop.
- Click **Start | All Programs | Grass Valley | GV Log Viewer**.



Remote and multiple site configuration

There are several different workflow configurations available for multiple GV STRATUS sites, to provide the level of access and functionality appropriate for your workflow requirements. The configurations are as follows:

- Browse and transfer — From your local GV STRATUS system, you can browse, search, view, and transfer assets to/from a remote GV STRATUS system.

  When you access multiple GV STRATUS sites, you do so from the context of your local site. Both local and remote GV STRATUS client PCs must be able to resolve the hostnames of local GV system servers, such as Core Server, Proxy Server, and K2 system. This local site is your primary site, where you do your normal workflow tasks, such as ingesting, editing, and playing out on channels. When you access a remote site, you can search and browse the remote assets, but you cannot edit or do other operations on remote assets. You must transfer the remote asset to your local site in order to apply the full range of GV STRATUS operations to the asset. Asset transfers are allowed both ways between your local and remote sites.

  Configure remote sites settings in the GV STRATUS Control Panel to access those sites in the GV STRATUS application. The setup includes the core server of the remote site and customizable name for the remote site.

- Browse, transfer, and send — In addition to the browse and transfer workflow, you can send assets from your local site to a remote site using the Send Destination feature.

  To use the Send Destination feature, configure Remote K2 Storage and Locations Config settings.

- Playout — In addition to the browse, transfer, and send workflow, you can use the GV STRATUS Rundown functionality at the remote site.

  To integrate with a playout system on a remote site, add your remote XMOS and SDB servers on the Playout Remote Sites tab in GV STRATUS Control Panel application. This allows you to view and select placeholders from your remote site.

- Send to K2 system — From your local GV STRATUS system, you can send assets to a remote K2 system that is not part of a GV STRATUS system, using the Send Destination feature.

  To use the Send Destination feature, configure Remote K2 Storage and Locations Config settings.

If you have remote sites configured in your system, the Navigator panel displays nodes for those sites. Only the **Assets** node is displayed under remote sites. Asset indicators identify assets on remote sites.

NOTE: When using multiple* GV STRATUS *sites, make sure all sites either have security enabled or disabled. Do not attempt to run mixed environments.

Configuring multisite browse and transfer workflow

- Both local and remote GV STRATUS systems must have multisite licenses.

- The FTP networks on the local and remotes sites must be able to communicate with each other.

Configure settings in the local site GV STRATUS Control Panel application.

Configure the remote site in **Remote Sites** settings.

Related Topics

Remote Sites settings on page 298

Configuring multisite browse, transfer, and send workflow

- Both local and remote GV STRATUS systems must have multisite licenses.
- The FTP networks on the local and remotes sites must be able to communicate with each other.

Configure settings in the local site GV STRATUS Control Panel application.

1. Configure the remote site in **Remote Sites** settings.
2. Configure one or more remote K2 systems in **Remote K2 Storage** settings.
3. Configure the remote K2 systems as Send Destination in **Locations Config**.

   Only those K2 systems configured in Remote K2 Storage are available for configuration as Send Destinations.

Related Topics

Remote Sites settings on page 298
Remote K2 Storage Add/Modify settings on page 340
Locations Config settings on page 370

Configuring multisite playout workflow

- Both local and remote GV STRATUS systems must have multisite licenses.
- The FTP networks on the local and remotes sites must be able to communicate with each other.
- GV STRATUS Rundown must be part of the remote GV STRATUS system.

Configure settings in the local site GV STRATUS Control Panel application.

1. Configure the remote site in **Remote Sites** settings.
2. Configure one or more remote K2 systems in **Remote K2 Storage** settings.
3. Configure the remote K2 systems as Send Destination in **Locations Config**.

   Only those K2 systems configured in Remote K2 Storage are available for configuration as Send Destinations.
4. Configure the remote GV STRATUS Rundown system in **Rundown | Remote Sites**.

Related Topics

Remote Sites settings on page 298
Remote K2 Storage Add/Modify settings on page 340
Locations Config settings on page 370
Rundown Remote Sites settings on page 395

Configuring multisite send to K2 system workflow

- The local GV STRATUS system must have a multisite license.

Configure settings in the local site GV STRATUS Control Panel application.

1. Configure one or more remote K2 systems in **Remote K2 Storage** settings.
2. Configure the remote K2 systems as Send Destination in **Locations Config**.

   Only those K2 systems configured in Remote K2 Storage are available for configuration as Send Destinations.

Related Topics

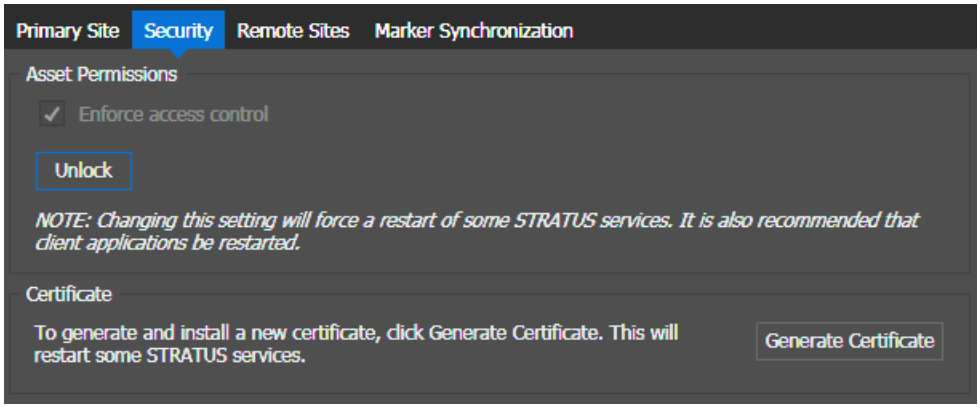
Remote K2 Storage Add/Modify settings on page 340
Locations Config settings on page 370

Security

GV STRATUS system security settings

These settings are required on all GV STRATUS systems.

In GV STRATUS Control Panel, to locate these settings, click **Core | STRATUS Core Services | Security**



Setting or button	Description
Enforce access control	When selected, the GV STRATUS system configures, retains, and enforces security settings on assets and bins. When not selected, the GV STRATUS system configures and retains, but does not enforce, security settings on assets and bins.
Lock/Unlock	Locks and unlocks the access control setting.
Generate Certificate	This creates a self-signed security certificate and installs it on the GV STRATUS Core server. Manually generating a certificate in this way is required only if the GV STRATUS Core server name changes, or if instructed to do so by Grass Valley Support. Otherwise, generating a certificate is handled automatically by GV STRATUS software installation.

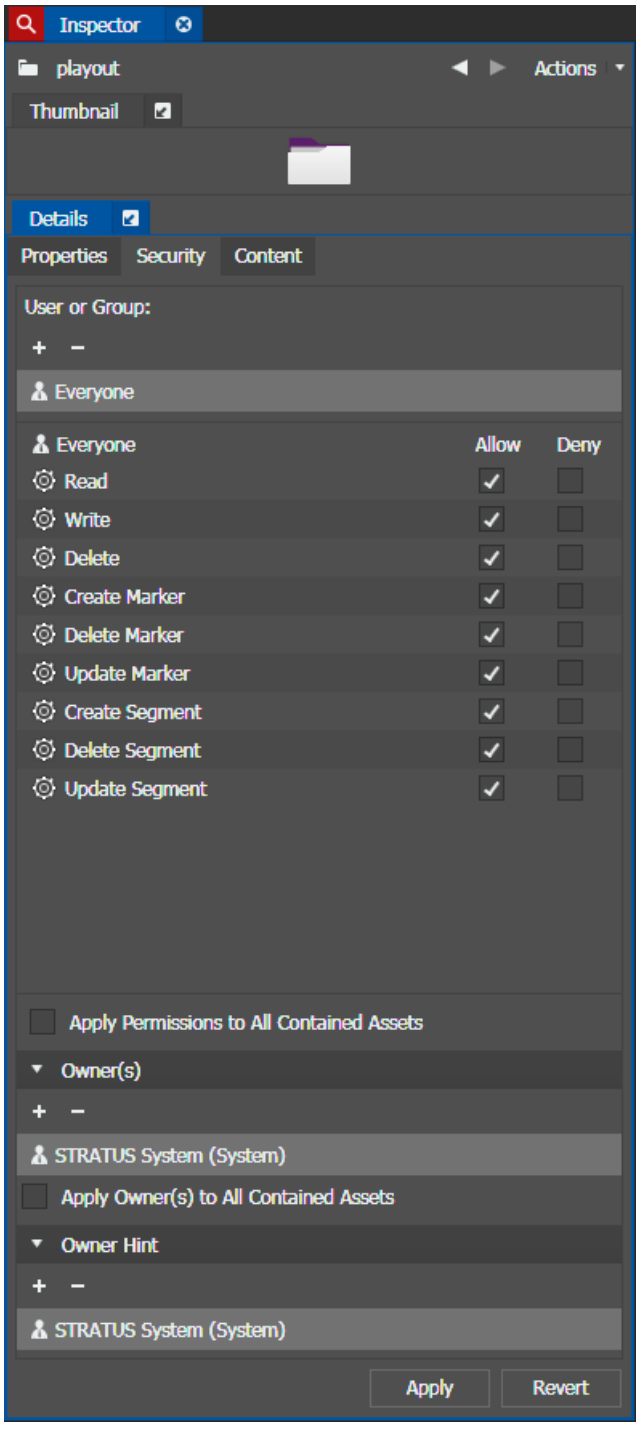
Setting or button	Description
Save	Saves current settings.
Cancel	Returns settings to their last saved state.

If settings are saved, GV STRATUS services are restarted automatically. All instances of the GV STRATUS currently open should be restarted manually.

Setting security in Inspector

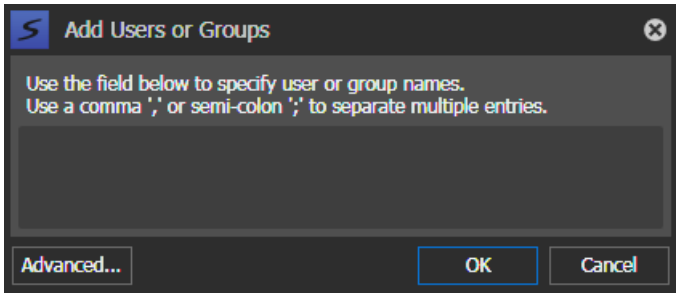
- To change security settings, you must log on to the GV STRATUS application with a user account to which the Security Manager role is assigned.

1. Load an asset or a bin into the Inspector panel and click the **Security** tab.



Security settings are displayed. If you are not logged on with a user account to which the Security Manager role is assigned, button and controls are not available for configuring settings.

2. Under **User or Group**, configure users or groups as desired.
   a) Click **+**.
      The **Add Users or Groups** dialog box opens.



   b) Enter user or groups, or if necessary click **Advanced** to open Windows operating system dialog boxes to find and validate users or groups.
3. Set permissions by selecting **Allow** or **Deny** as appropriate.
   Bins, assets, and metadata that do not have read permissions are not visible. Markers and segments permissions must be set to **Allow** in order to create, update, or delete markers and segments.
4. If a bin, select **Apply Permissions to All Contained Assets** to apply the configured permissions to assets already in the bin. This does not apply to sub-bins.
5. Under **Owner**, configure the list of owners of the asset or bin.
   Owners automatically have Read, Write, and Delete permissions. These permissions take precedence over any Allow or Deny permissions that might be set otherwise. Owners also have security options while copying/moving/sending assets and creating/deleting/updating markers and segments.
6. If a bin, select **Apply Owners(s) to All Contained Assets** to apply the configured owners to assets already in the bin. This does not apply to sub-bins.
7. If a bin, under **Owner Hint**, configure the list of owners that become the default owners of any newly arrived assets in the bin or newly-created sub-bins.
   If no owners are configured, a newly created asset or bin is owned by the user account that creates it.
8. Click **Apply** to save settings.

Related Topics

GV STRATUS security considerations on page 481
Security options while copying/moving/sending on page 482

Identifying security enforcement

You can identify security enforcement from the **Security Status** button display in the application Status bar of GV STRATUS and GV STRATUS Control Panel applications.

1. In the lower-right of GV STRATUS or GV STRATUS Control Panel application Status bar, click the **Security Status** button.

   The Notification pop-up panel opens to show details of the security enforcement.

   If the security enforcement is not enabled, the **Security Status** button is not displayed on the application Status bar.

2. To close the Notification pop-up panel, click the down-arrow on the top edge of the panel or click the **Security Status** button again.

Related Topics

GV STRATUS system security settings on page 298

Identifying asset permissions

You can identify security permissions on assets in several ways.

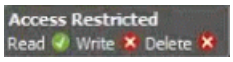
In Inspector, the **Permissions** property is displayed.

In an Asset List, you can add the **Permissions** column to display the permissions of all the assets in the list.

If your access to an asset is restricted, the **Access Restricted** icon is displayed.

The icon can be displayed as an overlay.

When you hover over the **Access Restricted** icon for an asset in an **Asset List**, asset permissions are displayed as in the example below:



Related Topics

GV STRATUS security considerations on page 481

GV STRATUS security considerations

Take the following into consideration when configuring GV STRATUS security.

- If the permission on an asset does not allow you to read the asset, the GV STRATUS system hides the asset from you and does not return the asset in your search results. This behavior is different than the Windows operating system, in which a file is visible even if no permissions are allowed.
- Bins inherit permissions as follows:
  - When creating a bin, the bin automatically inherits the permissions of its parent bin.
  - When changing permissions on a bin, permissions are not recursive. Sub-bins do not inherit the changed permissions of parent bins. This is true even if **Apply Permissions to All Contained Assets** is selected.
- Deny permissions take precedence over Allow permissions. Use Deny permissions sparingly as they can cause confusion with group permissions. For example, if a specific user is assigned Deny permissions, then those permissions override the permissions that are otherwise allowed for the group to which the user belongs. This then requires the system administrator to manage access control for specific users, rather than being able to manage access control for groups, which is a recommended best practice.
- Owners automatically have Read, Write, and Delete permissions. These permissions take precedence over any Allow or Deny permissions that might be set otherwise. Owners also have security options while copying/moving/sending assets and creating/deleting/updating markers and segments.
- If you want to copy assets, read permissions on the (source) asset and write permissions on the destination are required.
- Consider the tools and workflow required for user accounts affected by changes in security settings. If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets, and metadata that do not have read permissions are not visible. Markers and segments permissions must be set to **Allow** in order to create, update, or delete markers and segments.
- The following roles allow user operations similar to the way GV STRATUS system access permissions allow user operations:
  - Delete Rights
  - Move Rights
  - Rename Bin Rights
  - Rename Asset Rights

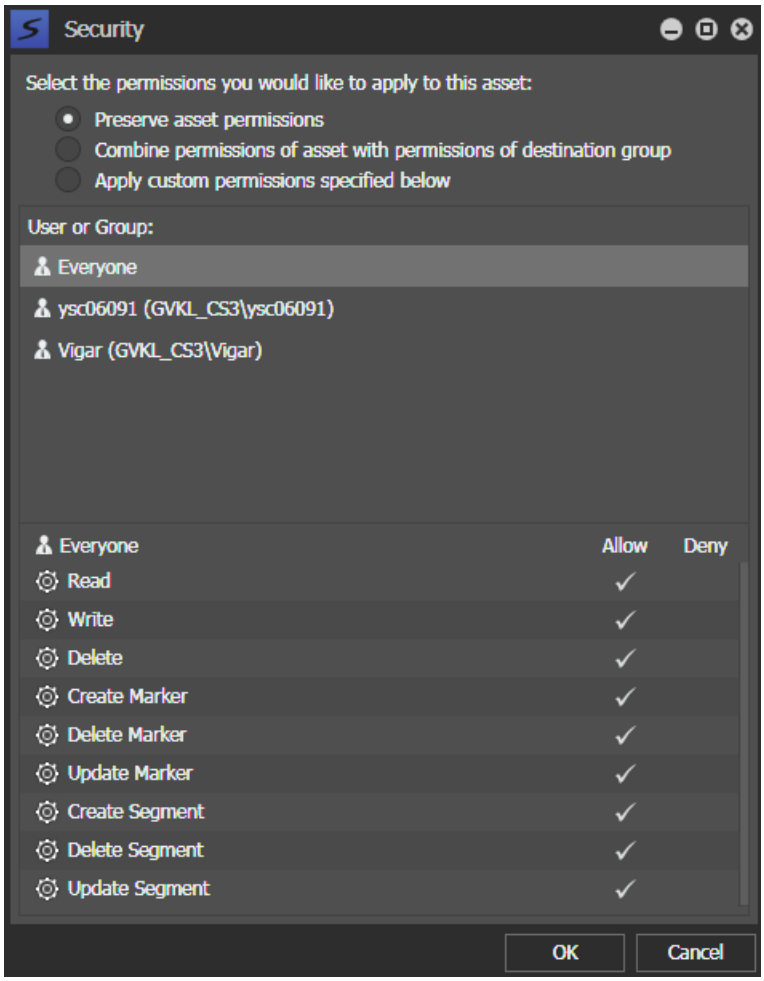
  To allow/deny user operations using access permissions only, ensure that all user accounts are assigned the above roles.

- Access to assets on a remote site is limited to read-only, regardless of other permission settings. Therefore, only read not allowed or read denied effect access to remote assets. Modify and delete permissions have no effect.

Security options while copying/moving/sending

When you copy, move, or send assets, you are working with source assets and destination assets. A source asset is the original asset from which you initiate the copy, move, or send operation. A destination asset is the result of the operation and is a new asset and/or is an asset in a different location. When security access control is enforced for your GV STRATUS system, your site's policies might require that security settings be configured for destination assets. If not, destination assets will always inherit the security settings of the destination bin.

For operations on a local GV STRATUS system, you make security settings for destination assets in the **Security** dialog box. If the account you use to log in to the GV STRATUS application has the role of Security Manager, the widest range of options are displayed.



Security options are as follows:

1. **Preserve asset permissions**: Destination assets have the same security settings as source assets. When this option is selected, the resultant security settings cannot be modified. If a single asset, security settings are displayed. If multiple assets, security settings are not displayed.
2. **Combine permissions of asset with permission of destination group**: Destination assets have the same security settings as source assets. If destination bins have security settings, security settings from all destination bins and all assets are combined and applied uniformly to all bins and assets. When this option is selected, the resultant security settings cannot be modified. If a single asset, security settings are displayed. If multiple assets, security settings are not displayed. Do note that Deny permissions take precedence over Allow permissions.
3. **Apply custom permissions specified below**: Regardless of current security settings on assets or on bins, settings can be configured as desired. When this option is selected, security settings can be modified.

Security options apply to assets found in GV STRATUS Navigator under Locations, Groups, and Favorites.

Depending on the account you use to log in to the GV STRATUS application, the **Security** dialog box displays as follows:

- Security Manager: If the account you use to log in to the GV STRATUS application has the role of Security Manager, option 1, 2, and 3 are displayed.
- Owner: If you are the asset owner, options 1 and 2 are displayed.
- Common: If you are neither a Security Manager nor the asset owner, the **Security** dialog box is not available.

If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets, and metadata that do not have read permissions are not visible. Markers and segments permissions must be set to **Allow** in order to create, update, or delete markers and segments.

About the GV STRATUS system user

The GV STRATUS system account is the account that the GV STRATUS services use to act as system user. The GV STRATUS system user is a "super-user" who can do everything regardless of any access control settings that have been set in the GV STRATUS system. The purpose is to protect your GV STRATUS system if other users made changes that affect everyone who uses the system. In the case it happens, the GV STRATUS system user can override those changes.

The GV STRATUS system user logon account must be the GV STRATUS internal system account.

Related Topics

Internal system/domain account considerations on page 914

GV STRATUS security and access from other applications

The GV STRATUS system accesses assets on K2 Summit/SAN media storage. The management of asset security for this access takes place in the GV STRATUS system only. GV STRATUS security does not change asset permissions on the K2 Summit/SAN media storage system. Therefore, when an application that is not GV STRATUS accesses assets directly on the K2 Summit/SAN media storage system, that access is not managed by GV STRATUS security. Take this into

consideration if you have workflows that are dependent on GV STRATUS security. Access to assets without management by GV STRATUS security can interfere with those workflows.

The following are examples of applications that can access assets directly on the K2 Summit/SAN media storage system, without being managed by GV STRATUS security:

- K2 Summit AppCenter
- Connected editors, such as the following:
  - EDIUS Workgroup
  - Adobe® Premiere® Pro CC
  - Avid Media Composer®
  - Apple Final Cut Pro

The following is an example of how accessing assets without management by GV STRATUS security can affect a workflow that depends on security.

1. There are three bins, A, B, and C, in the GV STRATUS system.
2. GV STRATUS security allows a user to have write and delete permission on bins A and B, but does not allow write or delete permission on bin C. From the GV STRATUS system, the user cannot add, remove, or modify assets in bin C.
3. From a connected editor with direct access to K2 storage, the user exports assets to the three bins. The asset exports successfully to bin C, since the user's access is not managed by GV STRATUS security.
4. The GV STRATUS system detects the presence of the newly arrived assets and adds them to the GV STRATUS database. As it does so, it applies GV STRATUS security to the asset references.
5. In the GV STRATUS application, the user attempts to move the assets in the three bins to other bins. The move is successful for assets in bins A and B but unsuccessful for the asset in bin C. This is because GV STRATUS security does not allow the user to remove assets from bin C.

In this example, the user's workflow is blocked. Since the export to all three bins was successful, the user expects to then be able to move those assets using the GV STRATUS application. But because of their GV STRATUS security settings on bin C, they can view the asset but they can't complete the intended workflow for the asset.

To prevent problems with security dependent workflows, access assets using GV STRATUS security management only. If an application has an embedded GV STRATUS panel or plugin, where you use GV STRATUS Navigator and other GV STRATUS features to access assets, then that access is managed by GV STRATUS security. For example, Newsroom Computer Systems access assets in this way. Some applications, such as high-resolution EDIUS Workgroup, can access assets both ways: via a GV STRATUS panel and also directly on the K2 Summit/SAN media storage system via the EDIUS K2 Browser. If your workflows depend on GV STRATUS security, Grass Valley recommends that you access assets only with the GV STRATUS application or with a GV STRATUS panel/plugin embedded in another application.

Working with SiteConfig

Topics in this section provide instructions for using the SiteConfig application.

Related Topics

Understanding and using SiteConfig on page 435

Installing SiteConfig

All system require this process.

If you have a control point PC supplied by Grass Valley with SiteConfig already installed, you can skip this task.

Work through the following topics to install the SiteConfig application.

About installing SiteConfig

SiteConfig uses a protocol that involves sending Ethernet broadcast messages to discover and configure devices. To enable this protocol to work correctly, there must be unrestricted network access between the PC that hosts SiteConfig and the devices to be discovered.

This is achieved if control network interfaces are all connected to the same switch or to multiple switches interconnected with ISLs/trunks. If your site requires that other switches and/or routers be in the network path, you must make sure that no restrictions are in place that block SiteConfig protocols.

Also, do not install SiteConfig on a PC on which a drive from a managed device is mapped as an administrative share (C$). For example, if you have a PC set up to run anti-virus software and for this purpose you have network drives set up on the PC mapped to C$ shares on devices, then do not use that PC to host SiteConfig and manage those devices.

For a given system, there should be just one instance of SiteConfig managing the system.

Related Topics

System requirements for GV STRATUS client PC on page 52

Installing/upgrading SiteConfig

- The PC on which you are installing SiteConfg must meet system requirements.
- The PC must be connected to the LAN on which all the devices to be managed are connected.
- There must be no routed paths to the devices to be managed.

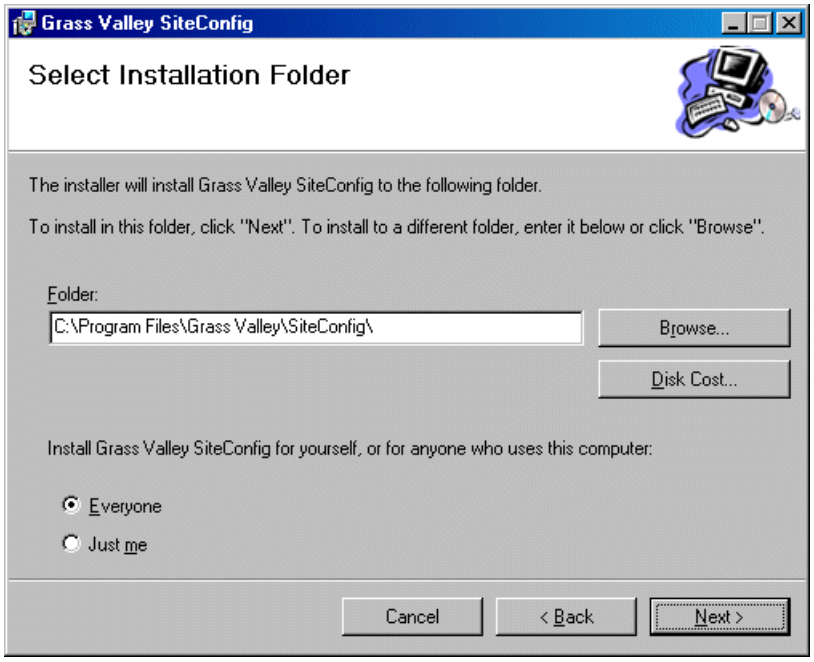
1. Procure SiteConfig installation files from the Grass Valley website or via other distribution mechanisms.

   The following directory and files are required to install SiteConfig:

   - `DotNetFx` directory
   - `ProductFrameUISetup.msi`
   - `setup.exe`

2. If you already have a version of SiteConfig installed, go to Windows **Add/Remove Programs** and uninstall it.
3. Double-click `setup.exe`.

   The installation wizard opens.
4. Work through the wizard pages, clicking **Next** and **Finish**.



   If the PC does not have the appropriate version of Microsoft .NET, the SiteConfig installation programs installs it.
5. Open the Windows operating system Services control panel on the PC and look for an entry called " ProductFrame Discovery Agent".

   The Discovery Agent must be installed on the SiteConfig PC so that the PC can be discovered by SiteConfig and added to the system description as a managed device. This is necessary to ensure name resolution in SiteConfig's hosts file.

   The Discovery Agent is also known as the Network Configuration Connect Kit. For example, in Windows Add/Remove Programs, it can be displayed as either Network Configuration Connect Kit or SiteConfig Discovery Agent.
6. Proceed as follows:

   - If the Discovery Agent is not installed, navigate to the SiteConfig install location's Discovery Agent Setup subdirectory and double-click the `DiscoveryAgentServiceSetup.msi` file. This launches the setup program and installs the Discovery Agent. Follow the setup wizard to complete installation. A restart is required after installation. Then continue with the next step in this procedure.
   - If the Discovery Agent is already installed, continue with the next step in this procedure.

7. If not already configured, configure the SiteConfig PC with a valid Ethernet IP address for the LAN using Windows Network Connections.
8. If you are not going to be using SiteConfig to manage system hosts files, put the system hosts file on the SiteConfig PC.

Related Topics

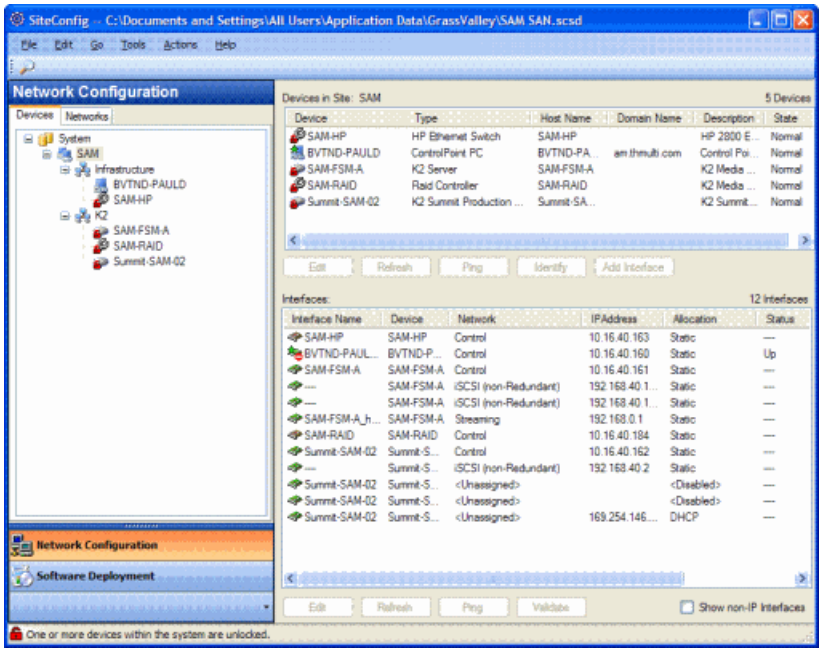
System requirements for GV STRATUS client PC on page 52

Opening SiteConfig

1. Do one of the following: Use the SiteConfig shortcut on the Windows desktop or in the Start menu to open SiteConfig.
   - On the Windows desktop, click the **Grass Valley SiteConfig** shortcut.
   - On the Windows **Start** menu, in the **Grass Valley** folder, click the **SiteConfig** shortcut.
2. SiteConfig opens as follows:
   - If you have previously opened SiteConfig, the SiteConfig main window opens with the most recently used system description loaded.
   - If you have not previously used SiteConfig or if SiteConfig does not have access to a system description file, you are prompted to create a new system description or to import an existing system description.
3. Respond as appropriate.

SiteConfig main window

The SiteConfig main window is as follows:



The left side of the screen shows the tree view of the currently loaded system description. The Network Configuration and Software Deployment buttons at the bottom of the tree view activate either the network configuration workspace or the software deployment workspace.

The network configuration workspace on the left has two tabs: a Devices tab to display the tree of devices in the system and a Networks tab to show the hierarchy of networks defined in the system.

The software deployment workspace also has two tabs: a Devices tab that displays the same tree view of devices but provides information about the software roles assigned to the devices and the software currently installed on devices. The Deployment Groups tab provides the interface to manage software deployment tasks.

Select an item in the tree and the view on the right side of the screen shows details about the item selected. Select a site or group to show information about all the items that fall under the selected item.

Right-click an item to access a context menu of operations.

Icon overlays on items and tooltips provide status and warning feedback.

Modifying unassigned (unmanaged) control network interface

- The system description must have a placeholder device for the computer with the control network connection.
- The placeholder device must have one or more unmanaged network interfaces.

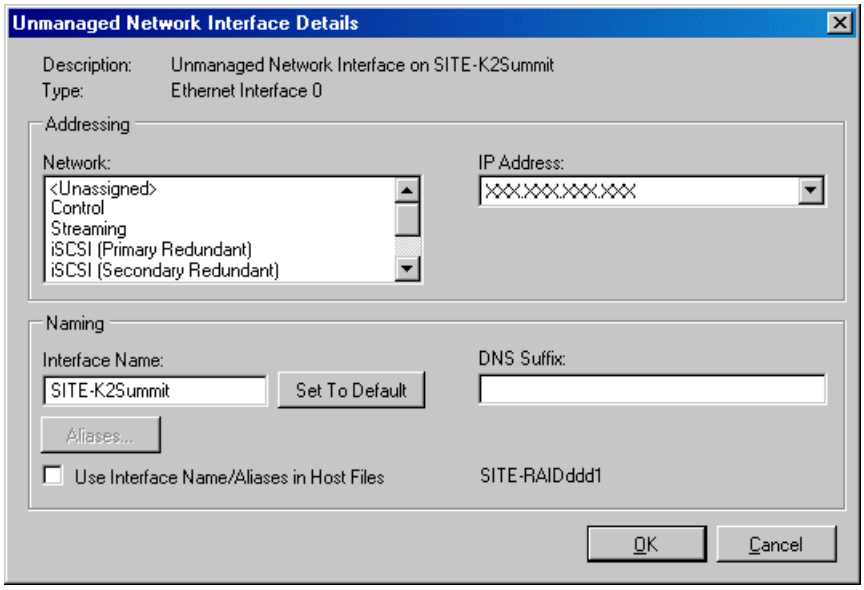
1. In the **Network Configuration | Devices** tree view, select the placeholder device for the computer with the control network connection.

   The interfaces for that device are displayed in the interfaces list view.

   Edit the control network interface first.

2. In the interfaces list view, right-click the control network interface and select **Edit**.

   The Unmanaged Network Interface Details dialog box opens.



3. Configure the settings for the interface as follows:

Setting...	For control network interface
Network	*Control* is required
IP Address	The IP address for this interface on the network. Required.
Interface Name	The device host name. Required.
Set to Default	Not recommended. Sets the interface name to SiteConfig default convention, based on the root Site name and device-type.
...use Interface Name/Aliases in Host Files...	*Unselected* is required. Since not selected, the default behavior occurs, which is to use the device host name in the hosts file.
Aliases	Not allowed
DNS Suffix	Allowed, if applicable to the network. The DNS suffix is added to the interface name.

4. Click **OK** to save settings and close.

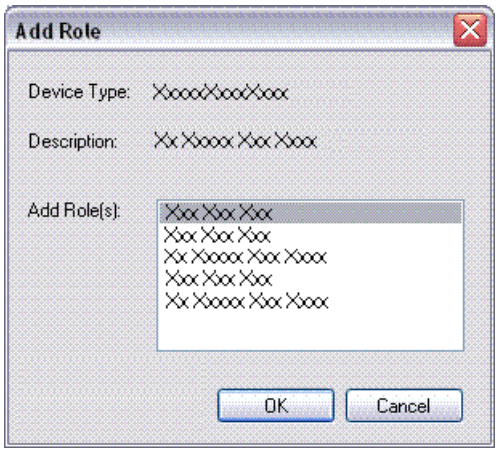
Related Topics

About IP configuration of network interfaces on devices on page 436
Adding a Proxy Storage file system server to the SiteConfig system description on page 740

Adding a software role to a device

1. In the **Software Deployment | Devices** tree view, right-click the device and select **Add Role**.

   The Add Role dialog box opens.



   The Add Role dialog box displays only those roles that SiteConfig allows for the selected device type.

2. Select the role or roles that you want to add to the device. Use Ctrl + Click or Shift + Click to add multiple roles.
3. Click **OK** to save settings and close.

   The new role or roles appear under the device in the tree view.

Removing a software role from a device

1. In the **Software Deployment | Devices** tree view, expand a device's node to expose the roles currently assigned to the device.
2. Right-click the role you want to remove and select **Remove**.

   The role is removed from the device in the tree view.

Adding a device to a network with SiteConfig

You can use SiteConfig to configure network settings on a device.

After you have added the device to the SiteConfig system description, work through the topics in this section to add the device to your network.

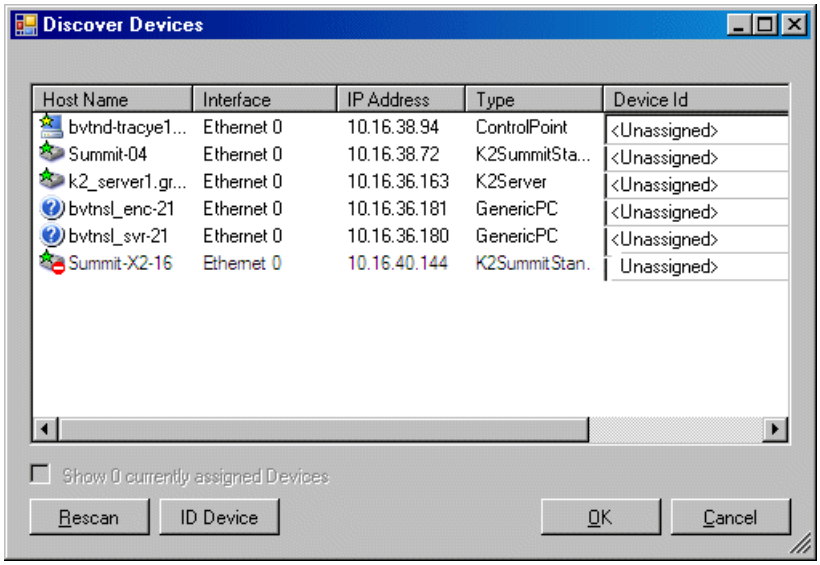
Discovering devices with SiteConfig

- The Ethernet switch or switches that support the control network must be configured and operational. If multiple switches, ISLs are connected and trunks configured.
- The PC that hosts SiteConfig must be communicating on the control network.
- There must be no routers between the PC that hosts SiteConfig and the devices to be discovered.

- Devices to be discovered must be Windows operating system devices, with SiteConfig support installed.
- Devices must be cabled for control network connections.

1. Open SiteConfig.
2. In the toolbar, click the discover devices button.

   The Discover Devices dialog box opens.



   A list of discovered devices is displayed.

3. Click **Rescan** to re-run the discovery mechanism. You can do this if a device that you want to discover has its network connection restored or otherwise becomes available. Additional devices discovered are added to the list.

Assigning discovered devices

- Devices must be discovered by SiteConfig
- Discovered devices must not yet be assigned to a device in the system description
- The system description must have placeholder devices to which to assign the discovered devices.

1. If the Discovered Devices Dialog box is not already open, click the discover devices button.

   The Discover Devices dialog box opens.

2. Identify discovered devices.

   - If a single device is discovered in multiple rows, it means the device has multiple network interfaces. Choose the interface that represents the device's currently connected control connection. This is typically Ethernet ... 0.
   - If necessary, select a device in the list and click **ID Device**. This triggers an action on the device, such as flashing an LED or ejecting a CD drive, to identify the device.

3. To also view previously discovered devices that have already been assigned to a device in the system description, select **Show … currently assigned devices**.

   The currently assigned devices are added to the list. Viewing both assigned and unassigned devices in this way can be helpful to verify the match between discovered devices and placeholder devices.

4. In the row for each discovered device, view items on the Device Id drop-down list to determine the match with placeholder devices, as follows:

   - If SiteConfig finds a match between the device-type discovered and the device-type of one or more placeholder devices, it displays those placeholder devices in the list.
   - If SiteConfig does not find a match between the device-type discovered and the device-type of a placeholder device, no placeholder device is displayed in the list.

5. In the row for a discovered device, click the Device Id drop-down list and select the placeholder device that corresponds to the discovered device.

   If there is no corresponding placeholder device currently in the system description, you can select **Add** to create a new placeholder device and then assign the discovered device to it.

6. When discovered devices have been assigned, click **OK** to save settings and close.
7. In the **Network Configuration | Devices** tree view, select each of the devices to which you assigned a discovered device.

Modifying managed control network interface

- The physical device you are configuring must be discovered and must be assigned to a device in the SiteConfig system description.
- SiteConfig must have communication with the device.
- The device must be defined in the system description with an appropriate network interface.

Use this task to modify managed the control network interface on a GV STRATUS server:

1. In the Interfaces list view determine the interface to configure, as follows:

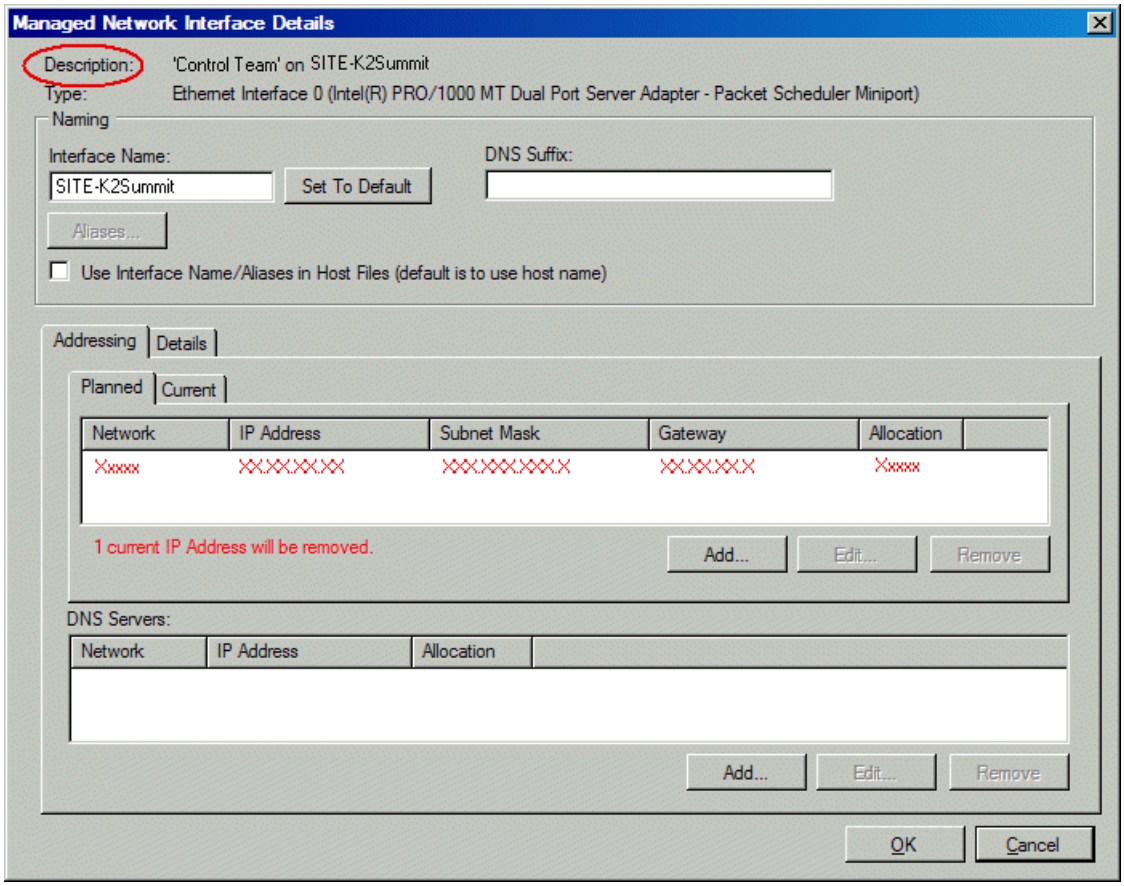
   - Identify the interface with which SiteConfig is currently communicating, indicated by the green star overlay icon. This should be the control network interface.
   - Verify that the interface over which SiteConfig is currently communicating is in fact the interface defined for the control network in the system description. If this is not the case, you might have the control network cable connected to the wrong interface port. The control connection should always be the first port on the motherboard, except when you have a loopback connection.
   - Configure the control network interface only. Other interfaces are not connected.
   - A server typically has multiple network interfaces that are not connected and are not required for system functionality. Give these interfaces a name such as "Unused" to aid identification.

2. In the Interfaces list view, check the icon for the interface you are configuring.

   If the icon has a red stop sign overlay, it indicates that current settings and planned settings do not match or that there is some other problem. Hover over the icon to read a tooltip with information about the problem.

3. In the Interfaces list view, right-click the control network interface and select **Edit**.

   The Managed Network Interface Details dialog box opens.



4. Identify the interface on the discovered device that you are configuring.

   - Identify Ethernet LAN adapters by their "Description" name. This is the Windows connection name. SiteConfig reads this name from the device and displays it at the top of this dialog box. This is the most accurate way to identify the network adapter on the discovered device that you are configuring.

   Make sure you are configuring the control network interface.

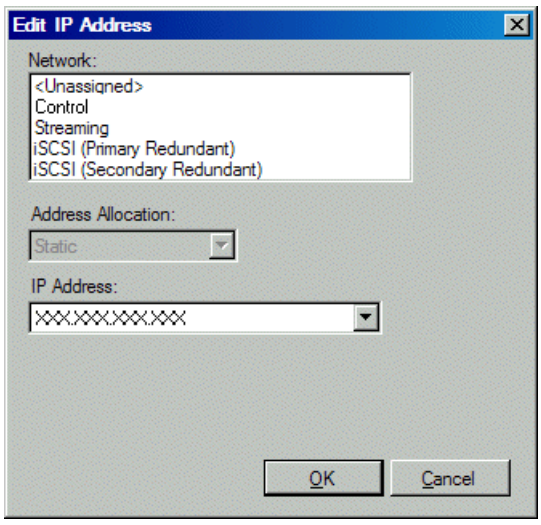
5. Configure naming settings as follows:

Setting...	For network interface Network Connection
Interface Name	The device host name. Required.
Set To Default	Not recommended
DNS Suffix	Allowed, if applicable to the network. The DNS suffix is added to the interface name.
Aliases	Not allowed
Use Interface Name/Aliases in Host Files	*Unselected* is required. Since not selected, the default behavior occurs, which is to use the device host name in the hosts file.

6. Evaluate settings on the Planned tab and change if necessary.
   - Compare settings on the Planned tab with settings on the Current tab.
   - If you want to keep the current settings as reported in the Current tab, click **Remove** to remove the planned settings.
   - Do not specify multiple IP addresses for the same interface. Do not use the Add button.

7. To modify planned settings, do the following:
   a) Select the network settings and click **Edit**.

      The Edit IP Address dialog box opens.



   b) Edit IP address settings as follows:

Setting...	For network interface Network Connection
Network	*Control* is required
Address Allocation	*Static* is recommended.
IP Address	The IP address for this interface on the network. Required.

      The networks listed in the Edit IP Address dialog box are those currently defined in the system description, with available settings restricted according to the network definition. If you require settings that are not available, you can close dialog boxes and go to the **Network Configuration | Networks** tab to modify network settings, then return to the Edit IP Address dialog box to continue.

8. When you have verified that the planned settings are correct, click **OK**, then **Yes** to apply settings to the device and close.

   A Contacting Device message box reports progress.

9. After configuring control network settings, do the following
   a) If a message informs you of a possible loss of communication, click **OK**.

      This message is normal, since this is the network over which you are currently communicating.

   b) In the Device list view, observe the device icon and wait until the icon displays the green star overlay before proceeding.

      The icon might not display the green star overlay for several seconds as settings are reconfigured and communication is re-established.

   c) In the Interface list view, right-click the interface and select **Ping**.

      The Ping Host dialog box opens.

      If ping status reports success, the interface is communicating on the control network.

Related Topics

About IP configuration of network interfaces on devices on page 436

Making the host name the same as the device name

1. Verify that the current device name, as displayed in the SiteConfig tree view, is the same as your desired host name.
2. In the **Network Configuration | Devices | Device** list view, right-click the device and select **Edit**.

   The Edit Device dialog box opens.
3. Identify the state of buttons as follows:
   - If the host name is different than the device name, the **Set to Device Name** button is enabled.
   - If the host name is the same as the device name, the **Set to Device Name** button is disabled.
4. If enabled, click **Set to Device Name**.

   This changes the host name to be the same as the device name.
5. Click **OK**.
6. When prompted, restart the device.

Pinging devices from the PC that hosts SiteConfig

- The devices you are pinging must be in the SiteConfig system description.

You can send the ping command to one or more devices in the system description over the network to which the SiteConfig host PC is connected. Typically this is the control network.

1. In the **Network Configuration** | **Networks** tree view, select a network, site, or system node.
2. In the Devices list view, select one or more devices. Use Ctrl + Click or Shift + Click to select multiple devices.
3. Right-click the selected device or devices and select **Ping**.

   The Ping Devices dialog box opens and lists the selected device or devices.

The Ping Devices dialog box reports the progress and results of the ping command per device.

Verify credentials

- The device you are verifying must be in the SiteConfig system description and must be communicating on the network.

  In the SiteConfig tree-view, right-click the device and select **Remote Desktop**, then proceed as follows:

  - If Remote Desktop opens without prompting you to log on, no further steps are necessary. SiteConfig credentials are set properly to allow access to the device.
  - If Remote Desktop prompts you to log on, check credentials in SiteConfig and on the device and reconcile as necessary.

Related Topics

About credentials in SiteConfig on page 42
Set credentials on page 266
Changing passwords on page 710

Generating host tables using SiteConfig

- Planned control network settings must be applied to control network interfaces and devices must be communicating on the control network as defined in the system description.
- Interfaces for networks that require name resolution via the hosts file, such as the FTP/streaming network, must have settings applied and must be communicating.
- Host names defined in the system description must be correct.
- The SiteConfig PC must be added to the system description so that it is included in the host tables generated by SiteConfig.

When you add or modify devices or their IP addresses in the SiteConfig system description, you should update host tables on all devices that use them.

1. In the **Network Configuration | Networks** tree view, select a network, site, or system node.
2. Click **View Hosts file**.

   A Hosts File Contents window opens that displays the contents of the hosts file as currently defined in the system description.

3. Verify the information in the hosts file.

4. Do one of the following:

   - If you are managing host table information yourself, click **Save As** and save a copy of the hosts file to a location on the control point PC. Then open the copy of the hosts file, copy the desired host table information from it, and paste it into your facility hosts file as desired. Then you can use your own process to distribute the facility hosts file to devices. Remember to distribute to the control point PC so that SiteConfig and other management applications such as K2Config can resolve network host names.
   - If SiteConfig is managing hosts files, do the following:

   NOTE: Writing hosts files to multiple devices consumes system resource and network bandwidth. Therefore it is recommended that you wait and do this after the system is complete and fully implemented, rather than updating hosts files incrementally as you discover/assign devices.

   a) In the **Network Configuration | Devices | Devices** list view, right-click a device to which you intend to write the hosts file and select **View Current Host File**.

      A Host File Contents window opens that displays the contents of the hosts file that is currently on that actual device.

   b) Verify that there is no information that you want to retain in the device's current hosts file that is not also in the hosts file as currently defined in the system description. If you need to save the device's current hosts file, click **Save As** and save to a different location.

   c) In the **Network Configuration | Devices | Devices** list view, right-click a device or use Ctrl + Click to select multiple devices, and select **Update Host File**.

      The current hosts file is overwritten with the hosts file as defined in the system description.

Related Topics

About hosts files and SiteConfig on page 440

Licensing a GV STRATUS system

Licenses are requested through email and managed through the SabreTooth License Manager, which is installed on the Grass Valley product with the Grass Valley software. The SabreTooth License Manager must be located on the Grass Valley product.

License information is stored in XML files that you can manage just like any other file on your system. Node-locked licenses are unique to the system for which they are requested and cannot be used on any other machine. A floating license can be used on multiple machines, one at a time. You should back up the license text files to a separate drive or as part of a recovery image.

Licenses are based on your system's unique identifier, which is partially derived from your system's Media Access Control (MAC) address. If you change your system's MAC address by performing operations such as changing the System Processor card, you must obtain a new license based on the new MAC address.

To license a GV STRATUS system, one or more licenses must be installed on the GV STRATUS server with role of Common Services. If the system has a server that does proxy encoding, one or more licenses for proxy encoding must be installed on that server as well.

Related Topics

Devices components: Roles, cab files, services, and licenses on page 444

Licensing GV STRATUS Rundown

If using GV STRATUS Rundown with GV STRATUS, you need the STRATUS-ELITE license installed on the GV STRATUS server with role of Common Services. The GV STRATUS Rundown application checks for the STRATUS-ELITE license in order for you to operate in both GV STRATUS and GV STRATUS Rundown environments.

Requesting a license

Features for your GV STRATUS system are enabled by SabreTooth licenses. For each server you are licensing, you must provide a generated unique ID to Grass Valley. Grass Valley uses the ID to create your unique license.

1. Refer to the license sheet that you received with your GV STRATUS license. The license sheet has the Sales Order number that you need.
2. Generate a unique ID of the device where you will install software, as follows:
   a) Double click on the License Manager icon on the Windows Desktop.
      The SabreTooth License Manager opens.
   b) Choose **File | Generate Unique Id** the License Manager.
   c) Click **Copy to clipboard** to copy the generated ID, and **OK** to exit.
3. Prepare an email that includes the following information:
   - Customer Name
   - Customer Email
   - Sales Order Number
   - Unique ID of the device where you will install software.
   - The license types you are requesting.
4. Send the email to GrassValleyLicensing@grassvalley.com.

The SabreTooth license number will be emailed to the email address you specified.

Next add the license to the SabreTooth License Manager.

Adding a license

Your software license, *Licenses_<SalesNumber>.txt*, is provided as a text file. Use the License Manager to add this file to your system and enable the desired feature.

1. Double click on the License Manager icon on the Windows Desktop.
   The SabreTooth License Manager opens.
2. Do one of the following:
   - Choose **File | Import License** and navigate to the file location to open the text file.
   - Drag and drop the text file onto the License Manager.

   You will now see the permanent license in SabreTooth, as well as any other licenses, permanent or temporary, that have been installed on this machine.

You should archive the permanent license to a backup system.

Deleting licenses

Deleting a license disables the feature that it enabled. You might want to delete a temporary license prior to its expiry if you have decided not to purchase the feature. You can delete a temporary license after the permanent license has been installed without disabling the licensed product.

1. Select the license in the SabreTooth License Manager.
2. Use the Delete key on your keyboard or right click with your mouse and select **Delete**.

Archiving licenses

You can archive your licenses to a secure external location. This allows you to quickly re-install a license should it be deleted or should you have to downgrade and then re-license the software. You can archive multiple licenses at the same time.

NOTE: If you downgrade to an earlier version of the licensed software, make sure to archive the licenses first.

1. In the SabreTooth License Manager, select the license or licenses.
2. Choose **File | Export License** to open the Save As dialog box.
3. Assign a meaningful name to the file, and save it to the desired location. Grass Valley recommends saving the license file to a USB drive or other external location.

Working with GV Log Viewer

Topics in this section provide instructions for using the GV Log Viewer application.

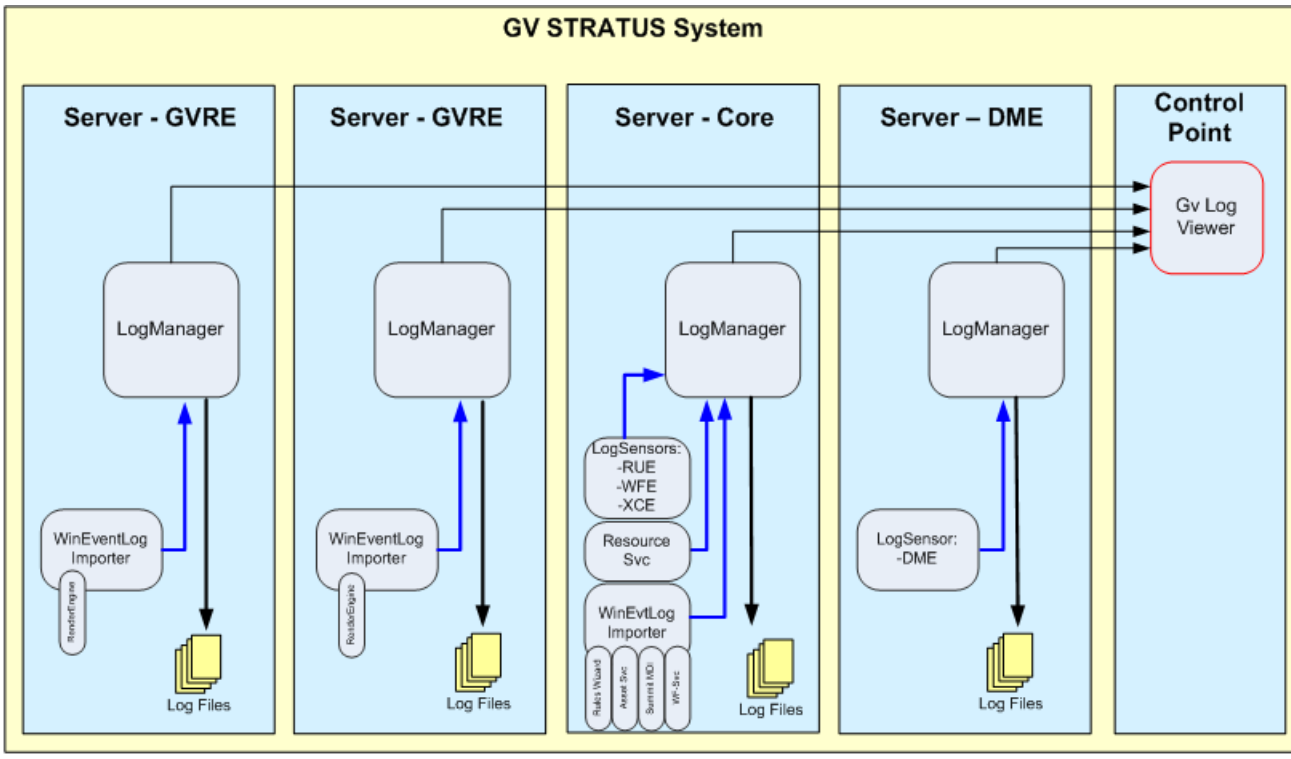
About GV Logging System

The GV Logging System consists of two main components, the GV Log Manager and the GV Log Viewer. All GV STRATUS software modules send log messages to the GV Logging System via the local GV Log Manager.

This is achieved if control network interfaces are all connected to the same switch or to multiple switches interconnected with ISLs/trunks. If your site requires that other switches and/or routers be in the network path, you must make sure that no restrictions are in place that block GV Logging System protocols.

On each GV STRATUS back-end machine, there should be a GV Log Manager running.

The diagram below provides an overview on the new GV Logging System concept.



About GV Log Manager

The GV Log Manager runs on all GV STRATUS back-end machines. It receives log messages from all local GV STRATUS software modules and store them in file(s) on the local disc.

All GV Log Managers are allowed to configure the amount of stored messages so that log files will not become too large. Furthermore, the Severity level per Log Source also can be configured. Thus, the GV Logging system provides the concept of adjusting the amount of messages to be limited at the root by setting a “Delivery Filter”.

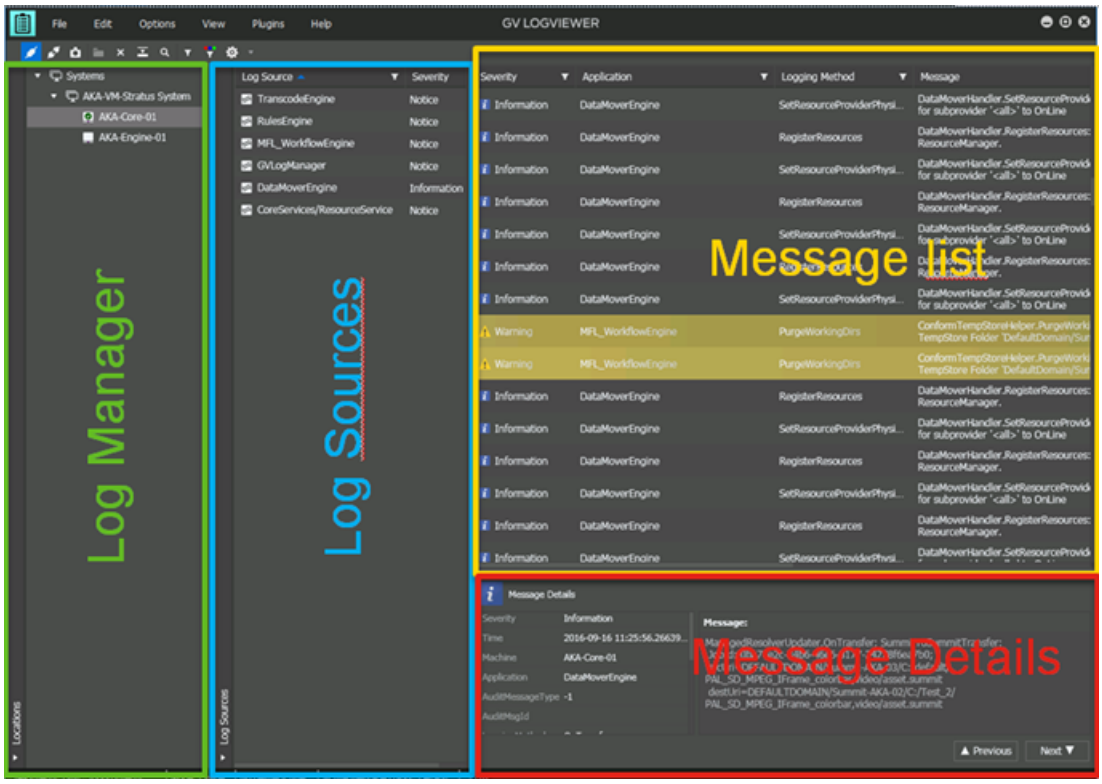
About GV Log Viewer

The GV Log Viewer allows us to connect to all machines in the GV STRATUS system. It provides the capability to view and monitor all back-end machines automatically.

The logging system extracts existing configuration data from the GV STRATUS Control Panel, including settings of the Core Server, Ingest server, Archive servers, and Engine servers such as MEWS, GV Render Engine, Xcode Control Engine, and Data Mover Engine.

The GV Log Viewer consists of these components to monitor the system:

- Log Manager
- Log Sources
- Message List
- Message Details



About GV Log Viewer controls

The toolbar lets you access GV Log Viewer controls.

Icon	Description
	Online mode: Allows you to switch to Online mode.
	Offline mode: Allows you to switch to Offline mode.
	Snapshot mode: Allows you to switch to Snapshot mode.
	Open file: Allows you to import messages from a file for Offline mode.
	Clear Messages: Allows you to clear all log messages.
	Auto scrolling: Allows you to toggle between enabling or disabling auto scrolling of messages.
	Find Messages: Allows you to search and find items in the messages.
	Delivery Filters: Allows you to filter messages based on pre-configured conditions.
	Message Colors: Allows you to define colors of messages in the Message List.
	Settings: Allows you to configure settings of the GV Log Viewer, such as configuration of the maximum number of messages, number of lines per log entry, and UTC timecode display.

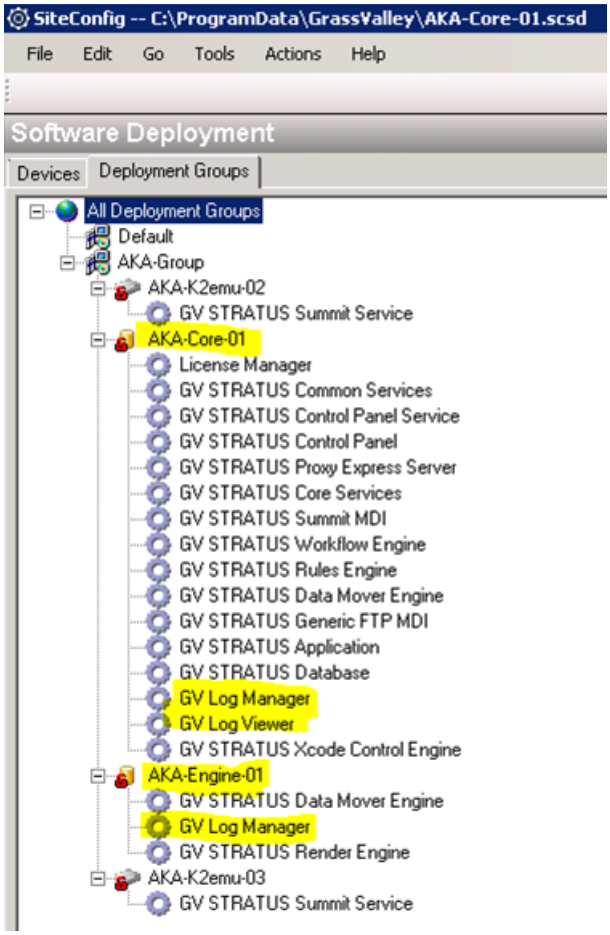
Installing GV Logging System

Use SiteConfig to install software on the GV STRATUS Express/Core Server and back-end machines.

- The server on which you are installing software is in the SiteConfig system description and communicating on the control network.
- The server on which you are installing software has its credentials set in SiteConfig to allow access.

1. Verify the SiteConfig roles currently assigned to the server. If the roles are not correct for your system design, add or remove roles accordingly. Roles are as follows:

   - GV Log Manager - on GV STRATUS Express/Core Server and all back-end machines.
   - GV Log Viewer - on GV STRATUS Express/Core Server.



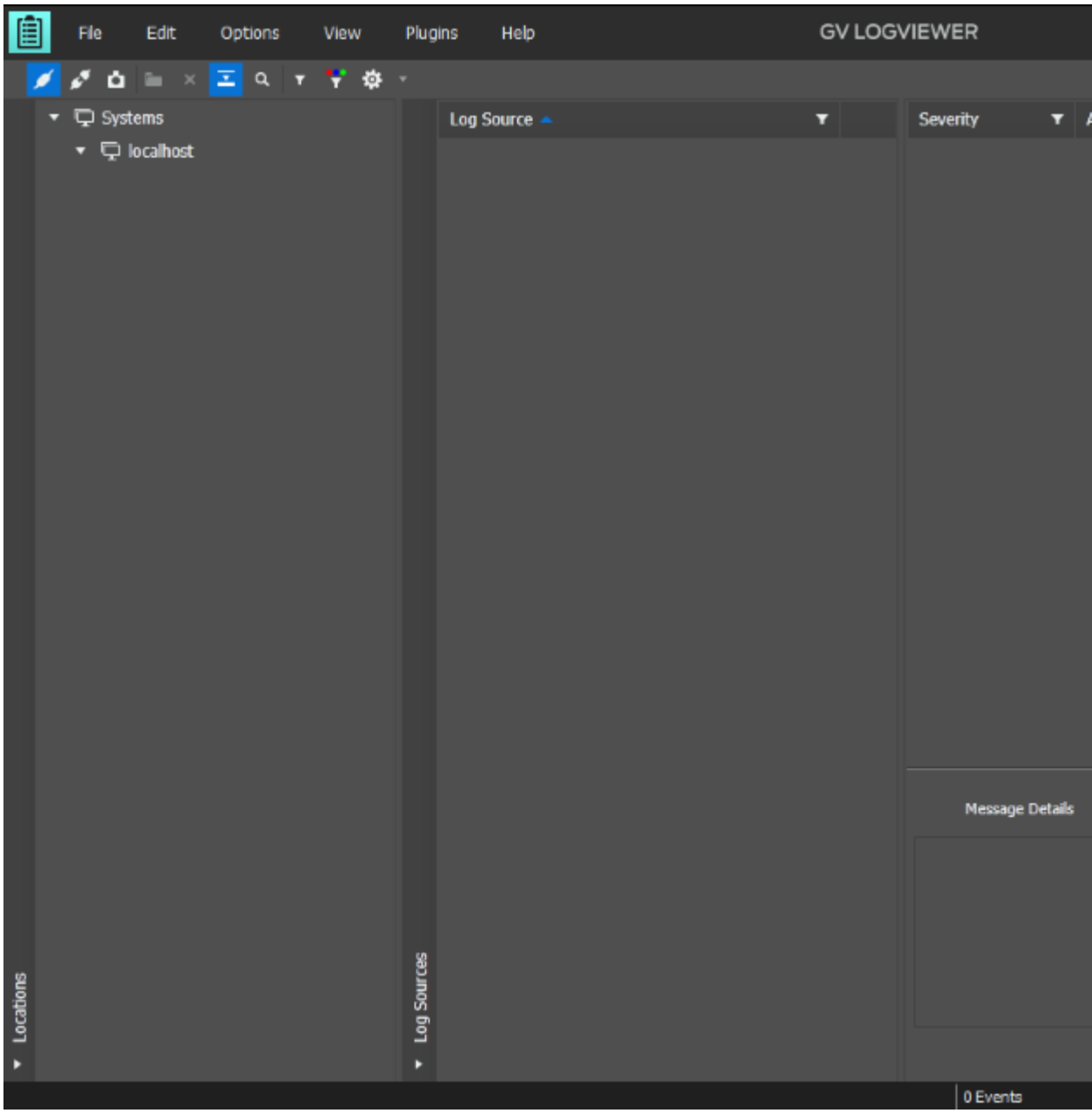
2. Add the following files to the deployment group:
   - For GV STRATUS Express/Core Server, add *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
     - *GrassValley_LogManager_x.x.x.cab*
     - *GrassValley_LogViewer_x.x.x.cab*
   - For all back-end machines, add *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab file that apply to this device:
     - *GrassValley_LogManager_x.x.x.cab*
3. Do the SiteConfig **Check Software** operation on the server.
4. Verify that deployment tasks are set to **Install** for the files listed above.
5. Deploy software to the server.
6. Restart as prompted.

Launching and connecting the GV Log Viewer

Once you have installed the GV Log Viewer on the GV STRATUS Express/Core server, you can launch it as follows:

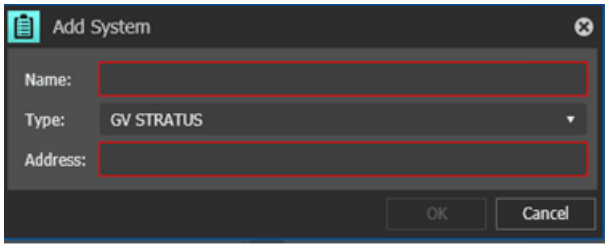
1. Click **Start | All Programs | Grass Valley | GV Log Viewer** .

   The GV Log Viewer opens.



2. Select **File | New** to add a new system.

   The Add System dialog opens.

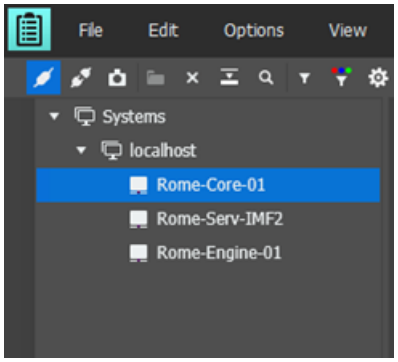


3. Enter details as below:

Setting or button	Description
Name	Name of the GV STRATUS Express/Core server or back-end machine to be monitored.
Type	Select the system type as **GV STRATUS**.
Address	Enter the IP address of the GV STRATUS Express/Core server or back-end machine.

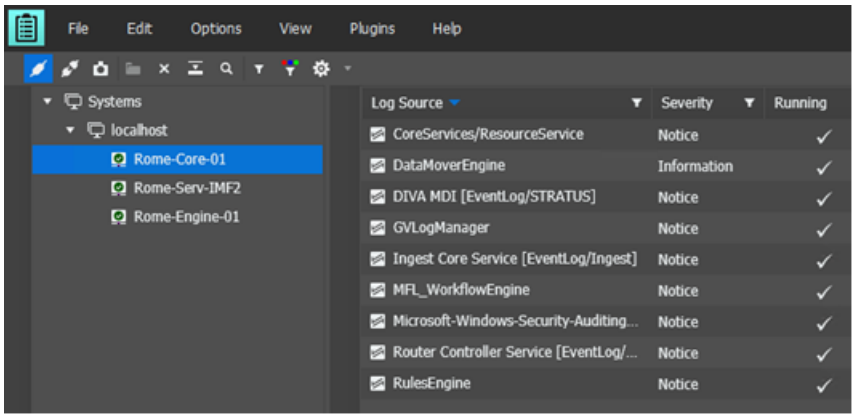
4. Click **OK**.
5. Repeat above steps to add other systems to the GV Log Viewer.

   The GV Logging System extracts configuration data of all back-end machines, such as Express/Core Server, Engine servers (MEWS, GVRE, XCE, DME) and lists all GV Log Managers installed in this GV STRATUS system.



6. Select a GV Log Manager from the list of back-end machines, right-click and select **Connect**.

   GV Log Viewer connects to the selected GV Log Manager and displays as connected with the green tick sign.

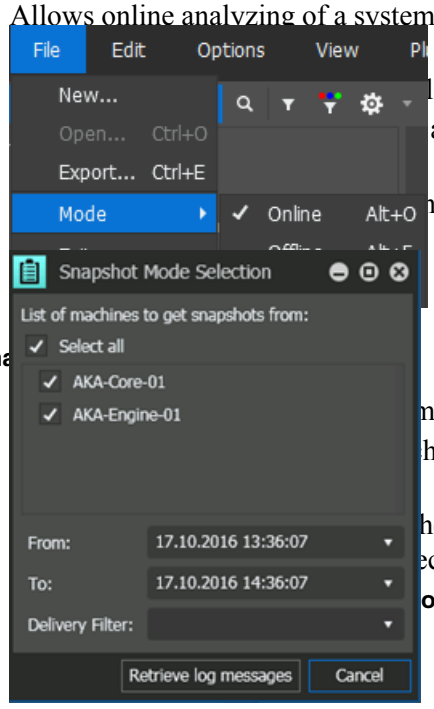


   By default, all Log Sources are set to the Severity Level - **'Notice'** and new messages will be listed when connected.

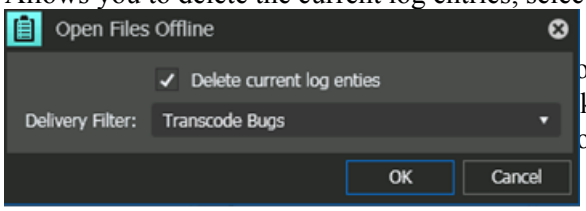
About logging modes in GV Log Viewer

The GV Logging System provides three type of logging modes: Online, Snapshot and Offline. Supported logging modes are as follows:

- **Online**:
  - Allows online analyzing of a system by live monitoring of the system behavior based on log
  - le GV LogManager(s) at the same time.
  - are displayed from the moment the operator started the
  - ns with the Online mode. If not, you can select **File | Mode**



- **Sna**
  - me in the past for log messages to be analyzed.
  - hine you are interested in and select a pre-configured
  - he particular machine and specific dates are listed allowing ecific time-frame when the failure happened.
  - **ot**, the dialog below appears for you to configure the

- **Offline**:
  - Allows you to load log files from a GV STRATUS system into the GV LogViewer to analyze log messages from a remote system.
  - Allows you to delete the current log entries, select a delivery filter, and select the log file(s)
  - 

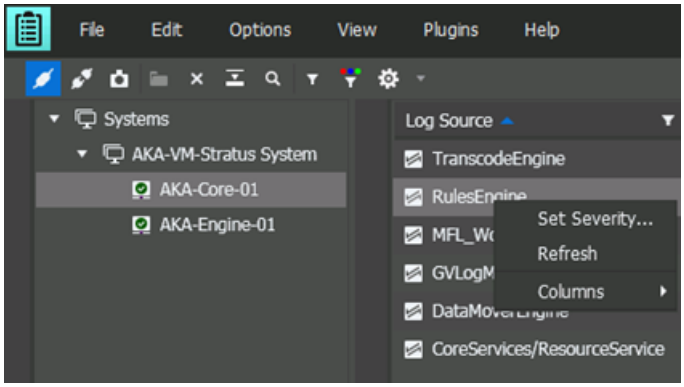
ow appears for you to configure the Offline king **OK**, another dialog appears for you to oad.

Since it is possible to configure the Severity level and Trace level for certain Log Sources, you can expect lots of log messages to be analyzed. These three different logging modes allow a service personnel to isolate the time-frame and specific system component he needs when searching through the log messages.

Configuring the Severity Level

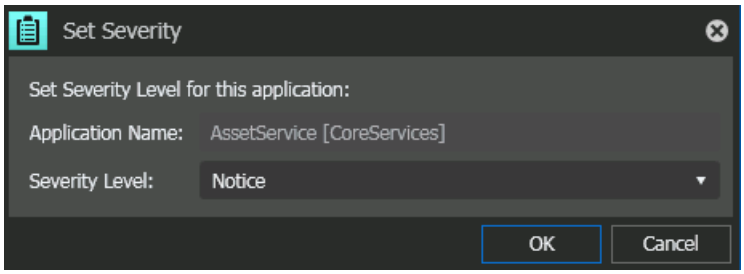
You can set the GV Log Viewer to display log messages according to the severity level. By this way, you can focus on relevant messages from specific software modules of GV STRATUS that require a deeper analysis.

1. Select a system in the Log Manager panel to display log sources in the Log Source panel.



2. Right-click on a Log Source and select **Set Severity**.

   The **Set Severity** dialog opens.



3. Select a Severity Level from the following:

Option	Severity Level
Disabled	0
Fatal	1
Error	2
Warning	3
Notice	4
Information	5
Debug	6
Cyclic	7
General	8

   The level zero (0) allows you to disable one or multiple log sources in the GV Log Viewer.

4. Click **OK**.

   GV Log Viewer displays log messages from that particular software module in the selected Severity level and above. For example if the default Severity level is set to Notice (4), then log messages from level 1-4 are stored and displayed in GV Log Viewer.

   NOTE: All GV STRATUS components are fully integrated into the GV Logging System, except a few components like the render engine for instance. These sources currently log into the Windows Event Log and can be identified by the information "EventViewer-Stratus" in the square brackets of the Log Source.

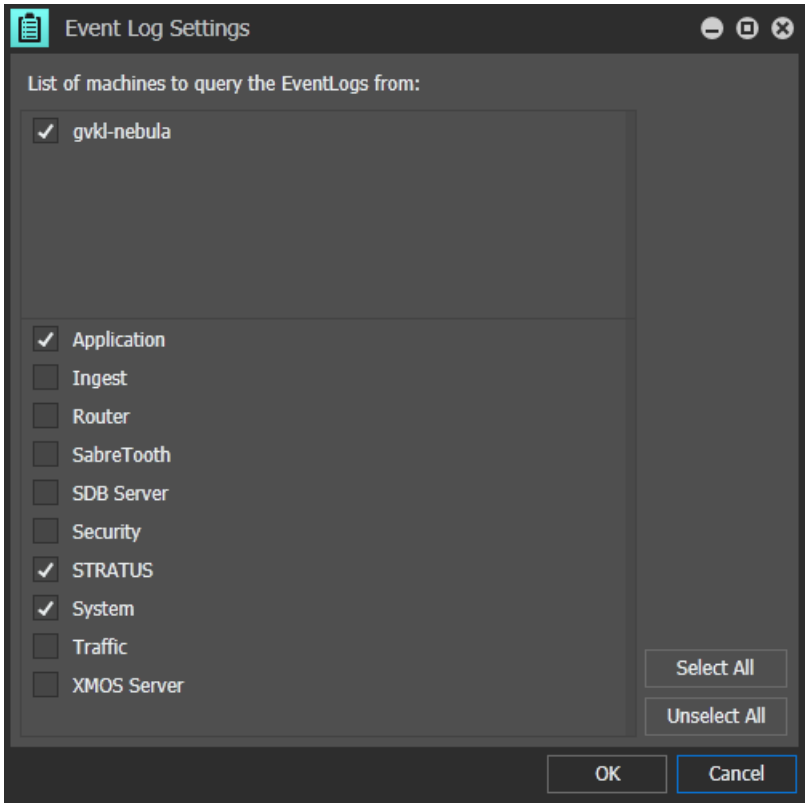
Viewing Windows Event Log in GV Log Viewer

You can configure Windows Event Log messages to be displayed via the GV Log Viewer. This allows you to import those messages, store them in GV Log files, and view them with all other messages from different Log Sources.

1. Select a GV STRATUS back-end machine in the Log Manager panel to retrieve its Event Log.

2. Right-click on the selected machine and select **Event Log Setting**.

   The **Event Log Settings** dialog opens.



   All applications running on that system are displayed.

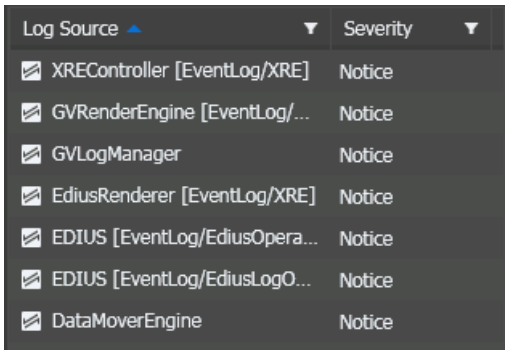
3. Select the applications you want to retrieve log messages from.

   You can click the **Select All** button to retrieve log messages from all applications.

   You can also click the **Unselect All** button to reset and deselect from all applications.

4. Click **OK**.

   Event Log messages from the selected applications are stored then by the GV Logging system and displayed from now on in the GV Log Viewer.



   Log Sources pulled from the Windows Event Log have their sources display in square brackets behind each Log Source name.

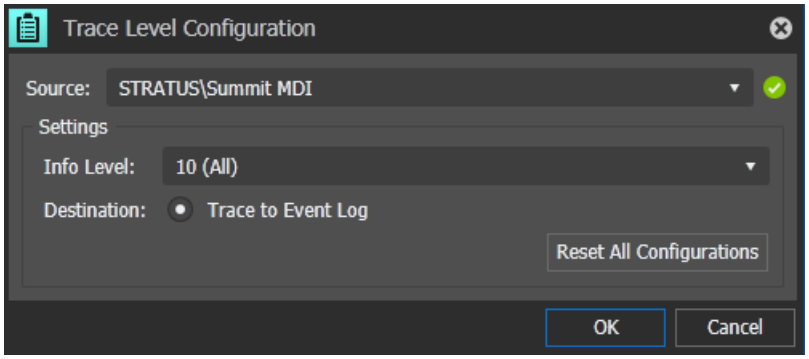
   NOTE: Log Sources from applications logging into the Windows Event Log are displayed the first time when they are producing log messages.

Configuring the Trace Level

Some GV STRATUS software modules are logging into the Windows Event Log. For those software modules, the configuration of the Trace Level provides the capability to adjust the amount of messages written into the Windows Event Log / GV STRATUS Log.

1. Click **Plugins | GV STRATUS | Trace Level Configuration**.

   The Trace Level Configuration dialog appears.



2. Select a Log Source from the **Source** drop-down list.

   The green tick sign displays if the log source is enabled to be traced.

3. Select an **Info Level** between **0 (None) - 10 (All)**.

   By default, the Destination is always set to **Trace to Event Log**.

   You can also click the **Reset All Configurations** button to disable and reconfigure all traces.

4. Click **OK**.

   All configured traces are sent to the Windows Event Log.

Since Trace Levels are stored in the systems registry, you must restart the affected GV STRATUS component to apply the Trace Level change.

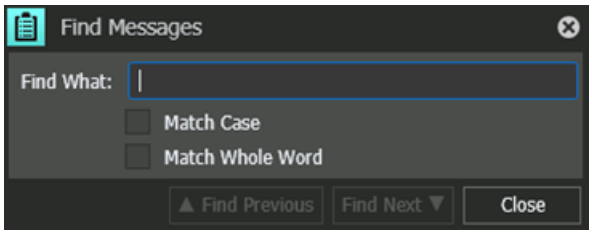
NOTE: A restart of a service or an MDI has an impact on the system operation. Therefore, ensure there is no important operation in progress before restarting the particular system.

Searching log messages

You can search for specific items in log messages via the Search function or using the Filter in columns.

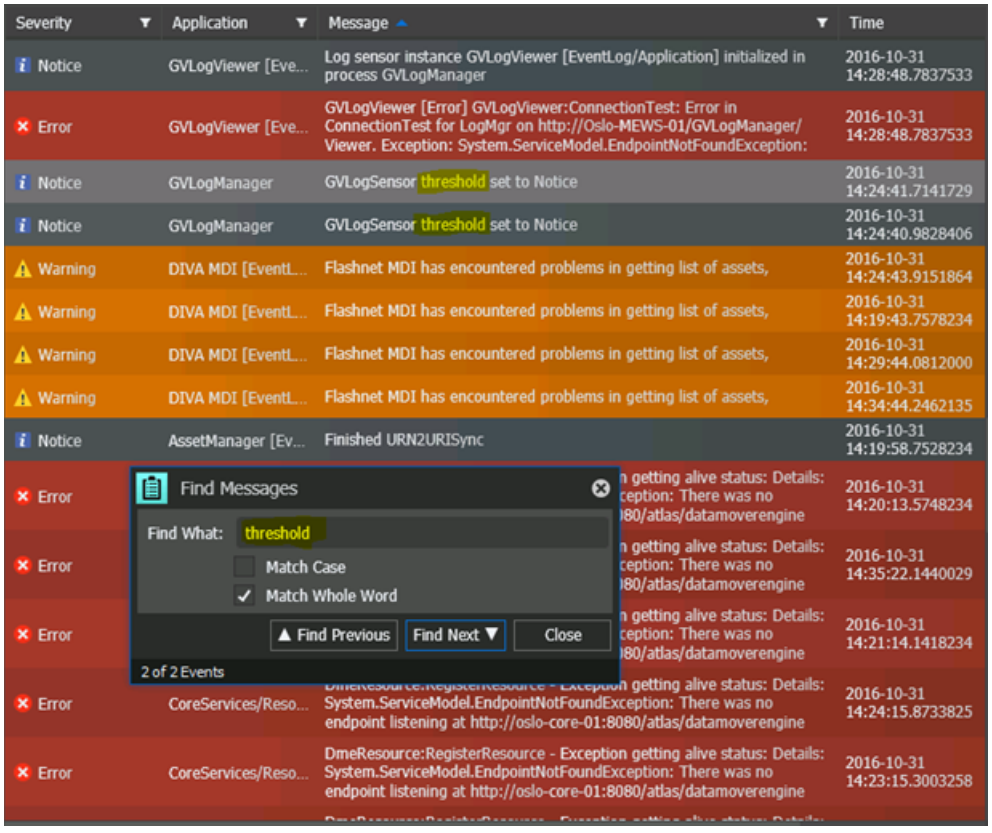
- To search via the Search function, do one from the following options:
  - Click the **Search** button on the toolbar.
  - On the main menu, select **Edit | Find Messages**.
  - Press **Ctrl + F** keys.

  The Find Messages dialog appears.



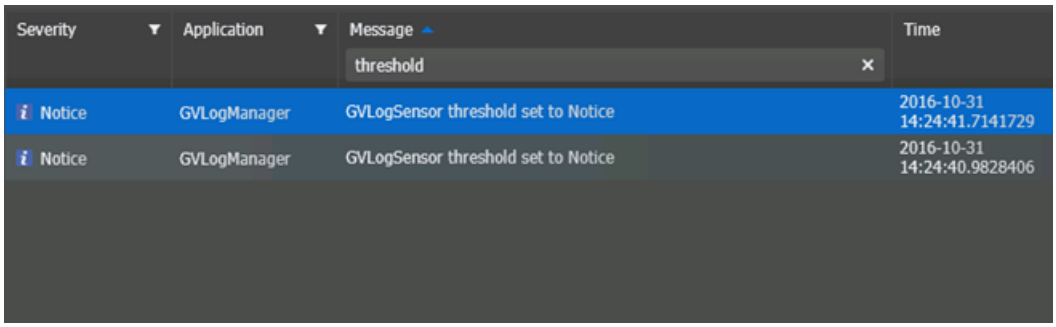
Enter the term that you want to search for, select whether you require the **Match Case** or **Match Whole Word** option, and press **Enter**.

The search results are highlighted in the Message List. Click **Find Next** or **Find Previous** button to keep searching the term throughout your log messages. Click **Close** to close the Find Messages dialog.



- To search via the column filter, click the **Filter** button at the head of a column. Enter the term that you want to search for, and press **Enter**.

  The search results appear in the Message List.

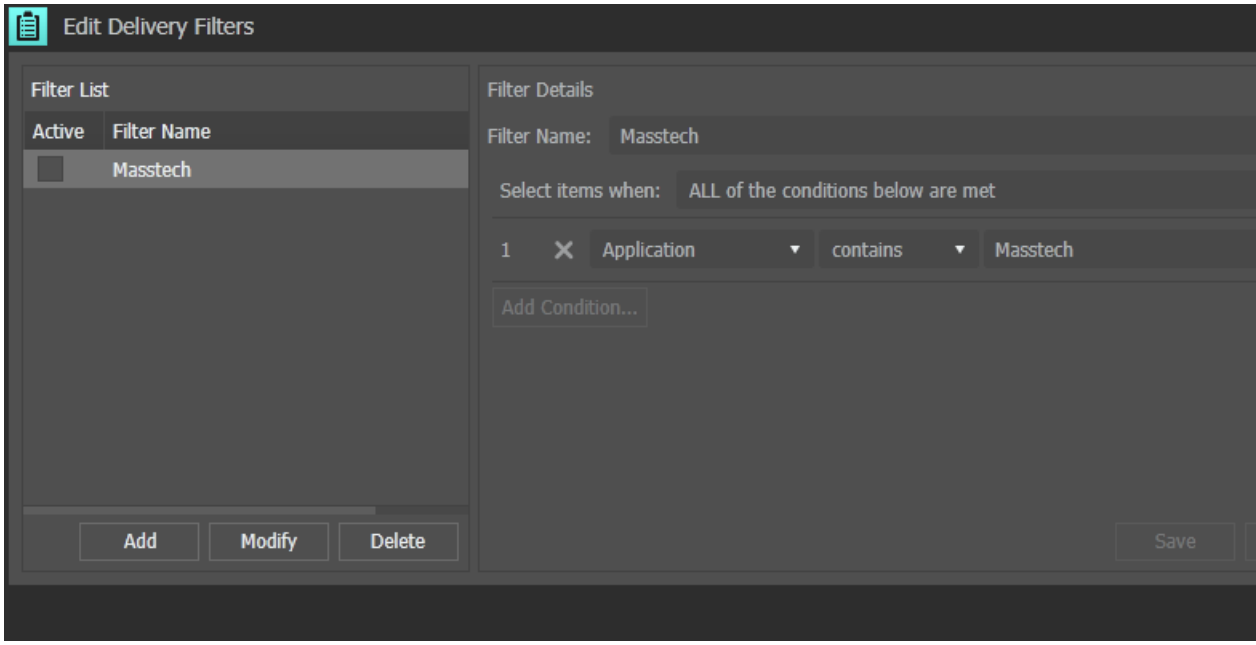


Creating a Delivery Filter

You can create delivery filters with specific conditions and find information easily within your log messages.

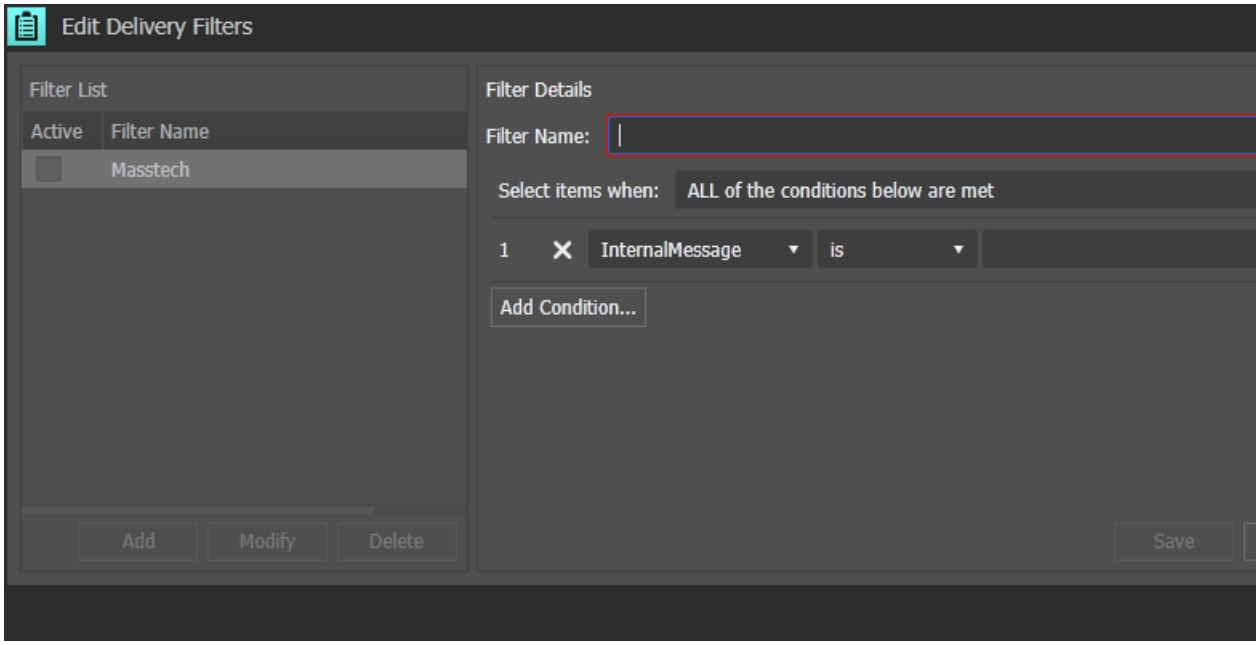
1. Do one from the following options:
   - On the toolbar, click the **Delivery Filter** button.
   - On the main menu, click **Options | Delivery Filter**.

   The Edit Delivery Filters window appears.



2. Click the **Add** button to create a delivery filter.

   The Filter Details section is enabled in the Edit Delivery Filters window.



3. Enter a name for the filter.
4. In the **Select items when** drop-down list, select one of the following:

   - **ALL of the conditions below are met**: For results that match all conditions.
   - **ANY of the conditions below are met**: For results that match any condition.

   Conditions and custom expressions are similar to those in GV STRATUS Advanced Search.

5. Configure conditions as follows:

   - For each condition (1, 2, 3, 4, etc) click the **Add Condition** button and select from lists to define the condition.
   - Click the **X** button to remove a condition from the list.

6. Click **Save**.

   The newly created filter appears in the Filter List.

   You also can select a filter in the Filter List and click **Modify** to edit the filter, or click **Delete** to delete the filter.

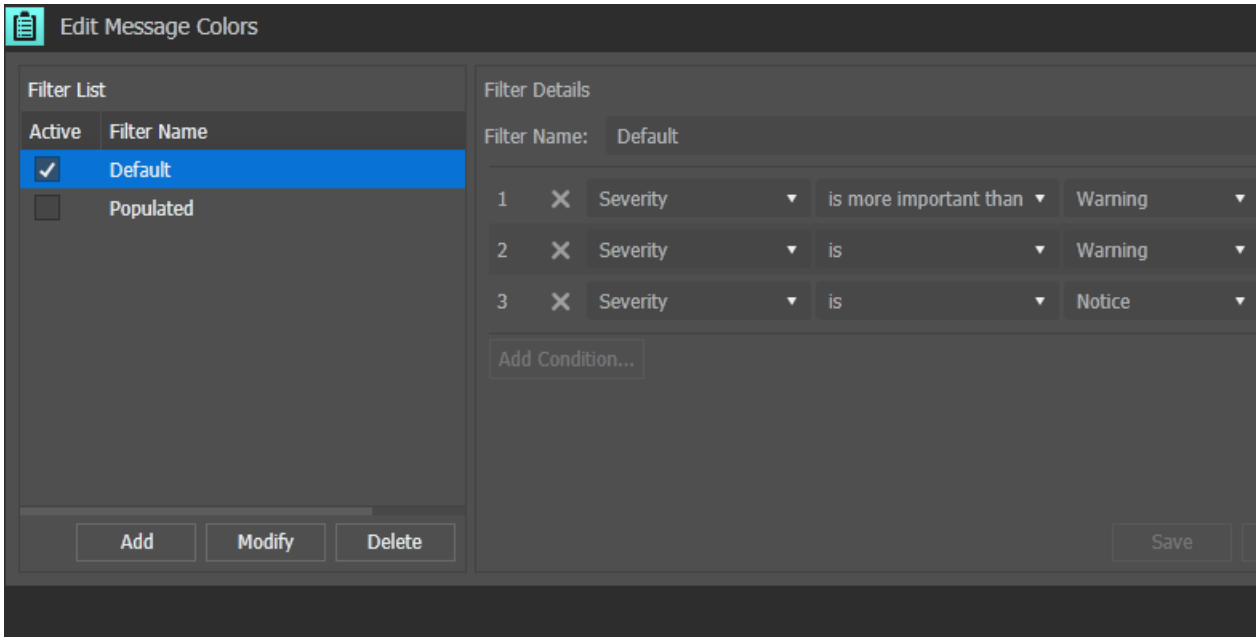
The Delivery Filter can be selected to filter log messages in both Snapshot and Offline modes.

Configuring colors for log messages

You can configure different colors for log messages display to find information easily at a glance.

1. Do one from the following options:
   - On the toolbar, click the **Message Colors** button.
   - On the main menu, click **Options | Message Colors**.

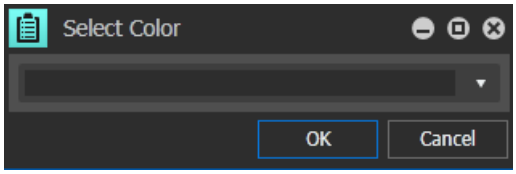
   The Edit Message Colors window appears.



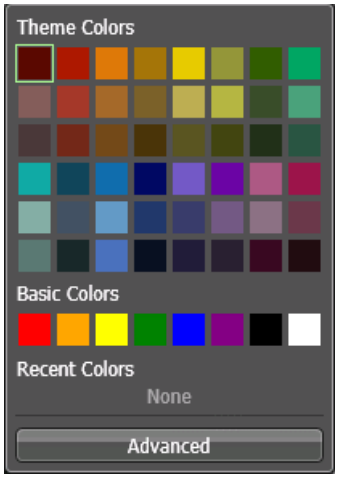
2. Click the **Add** button to configure colors for your log messages.

   The Filter Details section is enabled in the Edit Message Colors window.
3. Enter a name for the filter.
4. For each condition (1, 2, 3, 4, etc), select from drop-down lists to define the condition.
5. Click the **Color** button to assign a color to each condition.

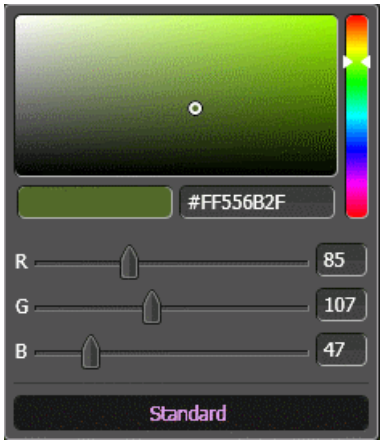
   The Select Color dialog appears.



6. Click the drop-down list to display the color palette, and do one of the following:
   - Select any theme or basic colors as provided.

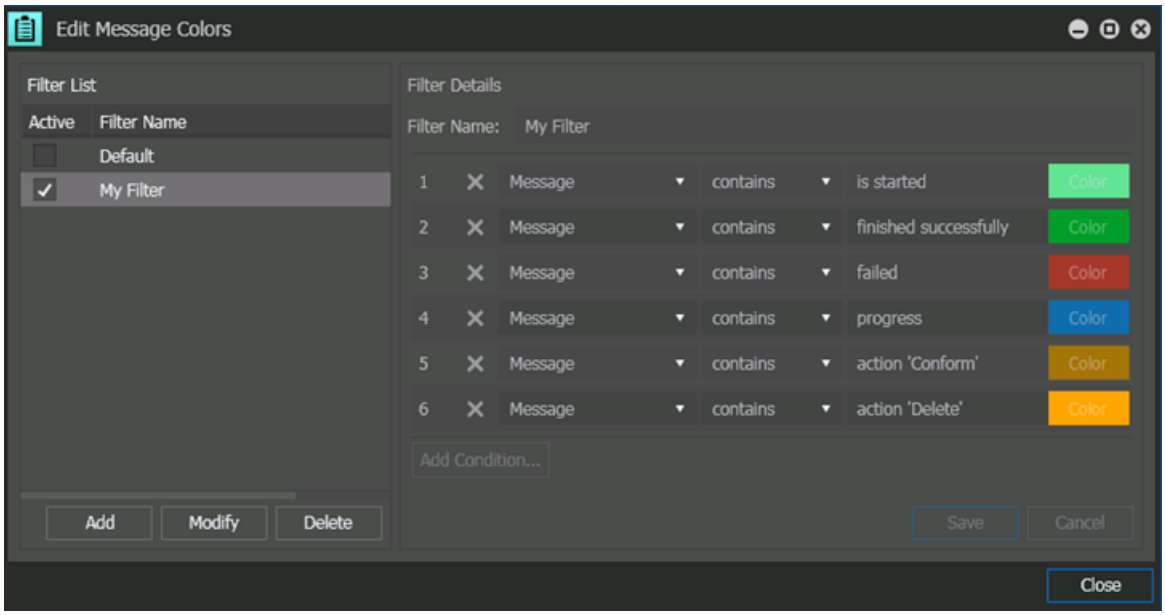


   - Click **Advanced** to define your own custom color and RGB values.



7. Click **OK** to save the selected color for the condition.

8. Click **Save** and **Close** after colors are configured for all conditions.



The newly created filter appears in the Filter List.

You also can select a filter in the Filter List and click **Modify** to edit the filter, or click **Delete** to delete the filter.

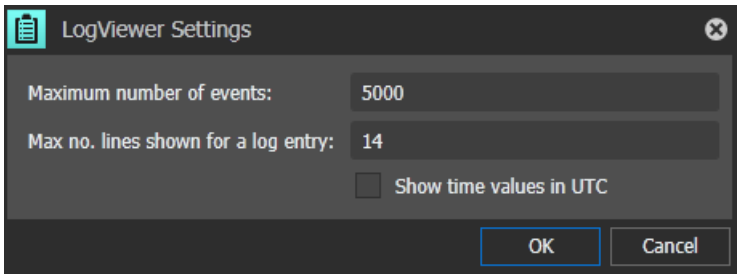
Log messages display according to selected colors in the Message List.

Configuring GV Log Viewer settings

In the GV Log Viewer settings, you can configure the maximum number of events or lines shown in a log entry and the UTC timecode display.

1. Do one from the following options:
   - On the toolbar, click the **Settings** button.
   - On the main menu, click **Options | Settings**.

   The Log Viewer Settings dialog appears.



2. Enter the maximum number of events to be displayed in the GV Log Viewer.
3. Enter the maximum number of lines shown for a log entry.
4. Select the check box if you want to display time values in UTC.

5. Click **OK**.

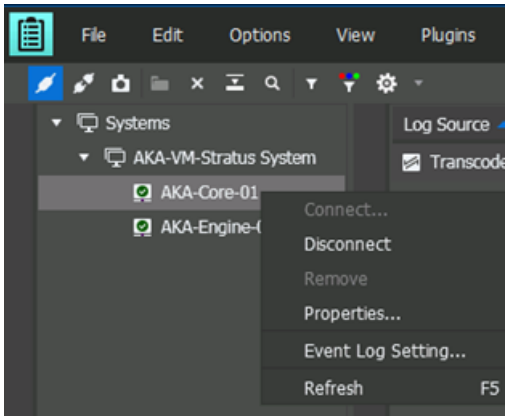
   GV Log Viewer updates the Message List according to the new settings.

Configuring GV Log Manager properties

For each connected system, you can configure these GV Log Manager properties below:

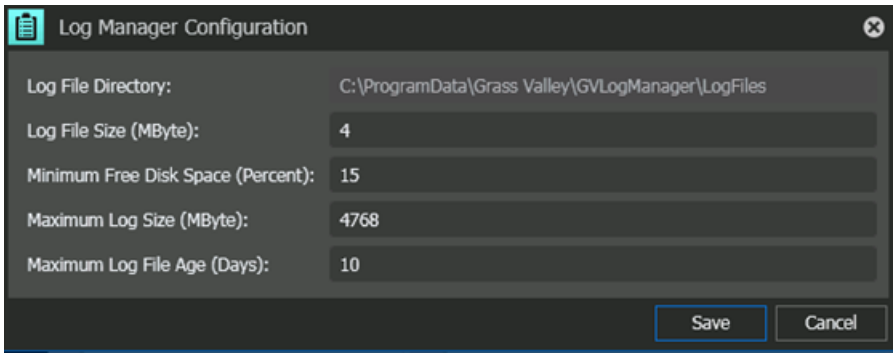
- Log File Size
- Minimum Free Disc Space
- Maximum Log Size
- Maximum Log File Age

1. Select a system in the Log Manager panel.



2. Right-click on the system and select **Properties**.

   The Log Manager Configuration dialog appears.



3. Enter the Log File Size.
4. Enter the minimum percentage of Free Disk Space to be assigned.
5. Enter the Maximum Log Size.
6. Enter the number of days for the Maximum Log File Age.
7. Click **Save**.

   GV Log Manager updates according to the new configuration.

Exporting log messages

- The selected system to export your log messages from must be in Online mode.

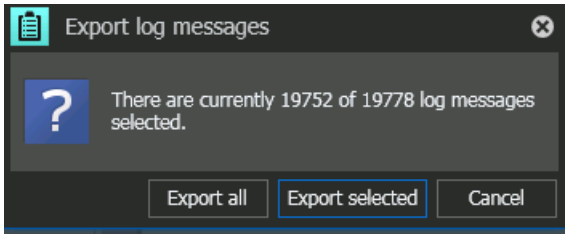
1. Select log messages that you want to export in the Message List.

   You can use Delivery Filters or column header filter to minimize the number of log messages displayed.

   To select multiple log messages, hold the **Shift** key down and select all between two selected messages; or hold the **Ctrl** key down and select messages randomly.

2. In the main menu, select **File | Export**.

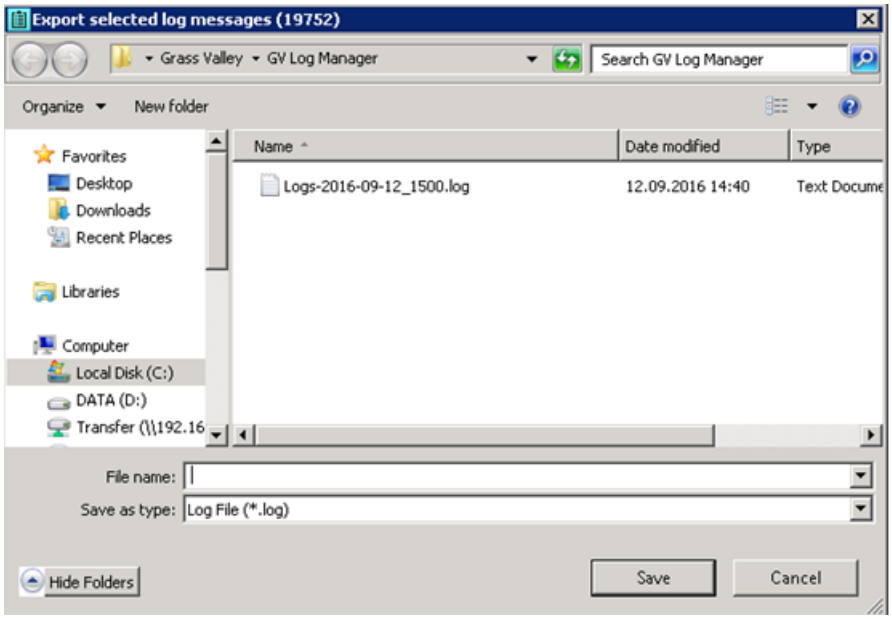
   The Export log messages dialog displays.



3. Click **Export selected** to export log messages that you selected earlier.

   You can also click **Export all** if you want to export all your log messages.

   The Export log messages window appears.



4. Browse to the location that you want to export into and click **Save**.

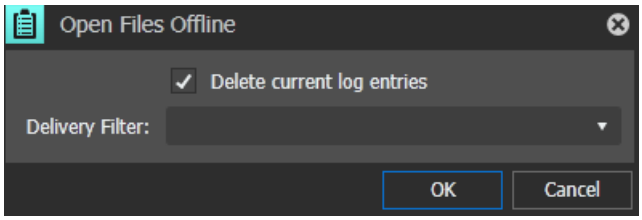
   Log messages are exported and saved in the `*.log` file format.

Importing log messages into GV Log Viewer

You can only import log messages in the Offline or Snapshot mode.

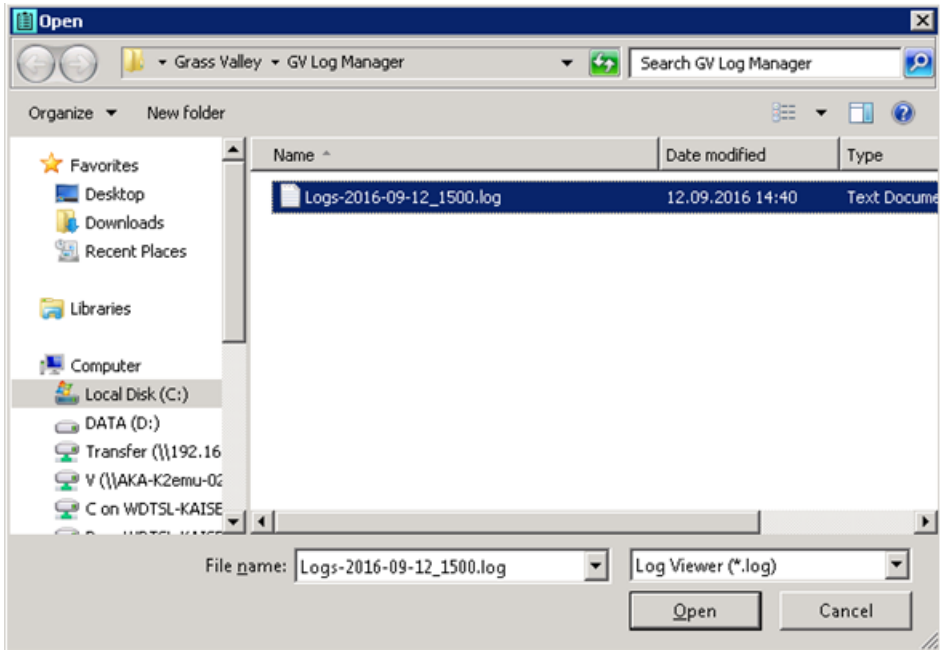
1. Do one of the following:
   - In the Snapshot mode, click the **Open** button or click **File | Open**.
   - Click the **Offline** button to change to Offline mode.

   The Open Files Offline dialog displays.



2. Deselect the **Delete current log entries** check box if you still need your current log messages.
3. Select a Delivery Filter from the drop-down list, if desired.
4. Click **OK**.

   The Open window displays.



5. Browse and select the log file that you want to import and click **Open**.
   The log file is imported and log messages from the file are displayed in the Message List.

Working with K2Config

Topics in this section provide instructions for using the K2Config application.

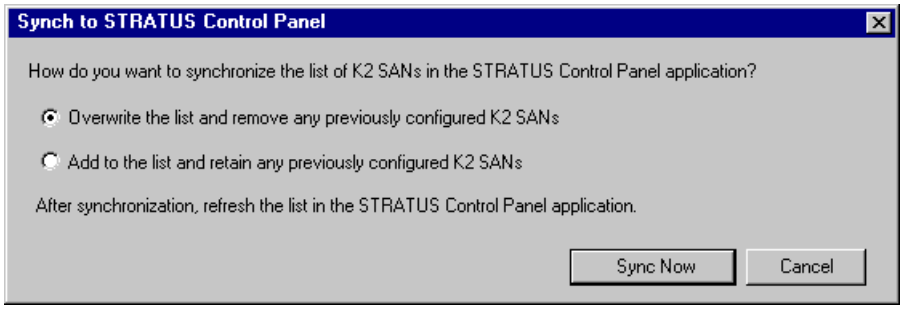
Synchronizing K2Config information to GV STRATUS Control Panel

The K2Config application writes its configuration file to the GV STRATUS server that hosts the Control Panel Service. Typically this is the GV STRATUS Core server. If the Control Panel Service is running, the K2Config application automatically does this whenever you change K2 SAN information. In most cases, this automatic operation should be sufficient. For example, when you add or remove a K2 SAN, the K2Config application adds or removes that K2 SAN in the configuration file that is on the Control Panel Service host. If the configuration file does not already exist on the Control Panel Service host, the file is created. If the file already exists, the K2 SAN is added or remove in the configuration file, but any information in the configuration file about other K2 SANs is not removed or modified.

However, if a situation arises in which you want to purge the information in the configuration file or otherwise control the rules for writing the K2Config information to the Control Panel Service host, you can do so as explained in this topic.

1. Make sure the GV STRATUS Core server is running.
2. Open the K2Config application.
3. In the K2Config application click **STRATUS | Network Configuration** and verify that the machine that hosts the Control Panel Service is correctly configured. Typically this is the GV STRATUS Core server.
4. Click **STRATUS | Sync to Control Panel**.

   The Synch to STRATUS Control Panel dialog box opens.



5. Select the synchronization option as follows:

   - Overwrite the list... — This overwrites the K2Config configuration file currently on the Control Panel Service host. Any K2 SAN information currently in the file is lost and replaced by the K2 SAN information currently in K2Config. Take care when selecting this option, especially if you previously configured a K2 SAN from a different instance of K2Config. This practice is not recommended, but if you are doing this, you could lose the information from that other K2Config instance.
   - Add to the list... — This is the same action that K2Config does automatically when you add a K2 SAN. The SAN's information is written to the configuration file on the Control Panel Service host, replacing any information for that same K2 SAN that is already in the configuration file. By selecting this option, you are triggering the same operation that would take place if you removed a K2 SAN from K2Config and then added the SAN back to K2Config.

6. Click **Sync Now** to write the K2 SAN information to the K2Config file on the Control Panel Service host.
7. Close the K2Config application.
8. Open the GV STRATUS Control Panel application and click **Core | K2 Storage | K2 SAN Storage.**

   K2 SAN Storage settings open.
9. Click **Refresh**.

   The Control Panel application reads the information from its local K2Config file and updates the list of K2 SANs.

Related Topics

About Control Panel, SiteConfig, and K2Config settings on page 433
About the Control Panel Service host and applications on page 434

Working with GV STRATUS servers

Use the procedures in this section when doing configuration or service work on a GV STRATUS server that is part of a GV STRATUS system.

Backup and Recovery Strategies

When you receive a GV STRATUS server from the factory, the machine has a generic image on the E: drive. The generic image is not specific to the individual machine. It is generic for all machines of that type. Some servers also have a system-specific image on the E: drive.

You receive a recovery CD with your server. This recovery CD does not contain a disk image. Rather, the recovery CD is bootable and contains the Acronis True Image software necessary to create and restore a disk image.

After your server is installed, configured, and running in your system environment, you should create new recovery disk images for the machine to capture settings changed from default. These “first birthday” images are the baseline recovery image for the machine in its life in your facility. You should likewise create new recovery disk images after completing any process that changes system software or data, such as a software upgrade. In this way you retain the ability to restore to a recent “last known good” state.

For the highest degree of safety, you should create a set of disk image recovery CDs, in addition to storing disk images on the E: partition. Since system drives are RAID protected, in most failure cases the disk images on the E: partition will still be accessible. But in the unlikely even of a catastrophic failure whereby you lose the entire RAID protected system drive, you can use your disk image recovery CDs to restore the system.

For image restore procedures, refer to related topics in this Topic Library.

GV STRATUS server partitions

GV STRATUS server types have partitions as follows:

GV STRATUS Express server

This server has four RAID 5 drives and two RAID 1 Solid State Drives. The D: partition is on the Solid State Drives.

Drive letter	Size	Purpose
C	80 GB	System drive
D	approximately 100 GB (92.62 GB with Solid State Drives)	SQL
E	20 GB	Storage for recovery disk image files
F	All remaining space	Proxy storage

GV STRATUS Core server: Dell

This server has four RAID 5 drives and two RAID 1 Solid State Drives. The D: partition is on the Solid State Drives.

Drive letter	Size	Purpose
C	80 GB	System drive
D	approximately 100 GB (92.62 GB with Solid State Drives)	SQL
E	20 GB	Storage for recovery disk image files

GV STRATUS Core server: Fault Tolerant (FT)

The C: and E: partitions are on the first physical drive in the CPU/IO module.

Drive letter	Size	Purpose
C	116 GB	System drive
D	All space on remaining drives.	SQL
E	20 GB	Storage for recovery disk image files

Proxy server, Proxy Storage file system server

This server has two RAID 1 drives.

Drive letter	Size	Purpose
C	75 GB (default size of disk image)	System drive
D	120 GB	SNFS
E	82 GB	Storage for recovery disk image files

Render Engine, Workflow Server

This server has four RAID 5 drives.

Drive letter	Size	Purpose
C	50 GB (default size of disk image)	System drive. Also SNFS on EDIUS XRE Server.
D	All space on remaining drives. Over 1 TB.	Render Engine: SNFS
E	20 GB	Storage for recovery disk image files

Related Topics

GV STRATUS system and server variants on page 220
GV STRATUS server on page 227
GV STRATUS server partitions on page 524

Creating a recovery disk image for storing on E: Dell R610

Do the following at the local server to create a disk image of the C: partition and the D: partition and store the image file on the E: partition:

1. Make sure that media access is stopped and that the system on which you are working is not being used.
2. If you have not already done so, connect keyboard, monitor, and mouse.
3. Do the following:
   a) Insert the Recovery CD.
   b) Restart the machine.
      If there is a problem restarting, hold the standby button down for five seconds to force a hard shutdown. Then press the standby button again to startup.

   The system boots from the Recovery CD.
   The Acronis program loads.
4. At the startup screen, select **True Image Server OEM (Full Version)**.
   The Acronis main window appears.
5. In the Acronis main window, click **Backup**.
   The Create Backup Wizard opens.
6. On the Welcome page, click **Next**.
7. On the Partitions Selection page, do the following:
   a) Select the **(C:)** and the **(D:)** partitions and then click **Next**.
8. On the Backup Archive Location page, do the following:
   a) In the tree view select the **Backup (E:)** partition and enter the name of the image file you are creating.
      Create the file name using the machine hostname and the date. Name the file with the .tib extension.
      For example, if the hostname is MySystem1, in the File name field you enter `E:\MySystem1_20180327.tib`.
   b) Click **Next**.

9. On the Backup Options page, do not change any settings. Click **Next**.
10. On the Archive Comment page, if desired, enter image comments such as the date, time, and software versions contained in the image you are creating. Click **Next**.
11. On the "…ready to proceed…" page, do the following:
    a) Verify that you are creating images from the C: and D: partitions and writing to the E: partition, then click **Proceed**.
12. On the Operation Progress page, observe the progress report.
13. When a message appears indicating a successful backup, click **OK**.
14. Click **Operations | Exit** to exit the Acronis True Image program.

    The machine restarts automatically.
15. Remove the recovery media while the machine is shutting down.

Creating a recovery disk image for storing on E: Dell R620

Do the following at the local server to create a disk image of the C: partition and the D: partition and store the image file on the E: partition:

1. Make sure that media access is stopped and that the system on which you are working is not being used.
2. Connect all motherboard NICs to LAN connections.
3. If you have not already done so, connect keyboard, monitor, and mouse.
4. Do the following:
    a) Insert the Recovery CD.
    b) Restart the machine.

       If there is a problem restarting, hold the standby button down for five seconds to force a hard shutdown. Then press the standby button again to startup.

    The system boots from the Recovery CD.

    The Acronis program loads.
5. On the Acronis Rescue Media page, select **Acronis Backup and Recovery 11.5 (64-bit...)**

    The Acronis Backup and Recovery page opens.
6. On the Acronis Backup and Recovery page, select **Back up now**.

    The Back up now page opens.
7. On the Back up now page, under What to back up, select **Item to back up**.

    The Select item to back up dialog box opens.
8. On the Select item to back up dialog box, do the following:
    a) Under Disk 1 select **C** and **D**. Clear other check boxes.
    b) Click **OK**.

    The Select item to back up dialog box closes.
9. On the Back up now page, under Where to back up, select **Location**.

    The Select location back up dialog box opens.

10. On the Select location back up dialog box, do the following:.
    a) Expand the tree-view **Local folders** node and select **E:**.
    b) Enter a name for your backup.
    c) Click **OK**.

    The Select location back up dialog box closes.
11. On the Back up now page, under How to back up, do the following:
    a) Set Backup type to **Full**.
    b) This is recommended for your first backup. For subsequent backups, you can optionally set this to Incremental or Differential.
    c) Set Validation to **Validate a backup as soon as it is created**.
12. On the Back up now page, click **OK**.

    The backup begins and the Backup Details page opens.
13. On the Backup Details page, select the **Progress** tab to view the progress.
14. Verify when the data is successfully backed up.
15. Close all Acronis pages and the Acronis main window.

    The machine restarts automatically.
16. Remove the recovery media while the machine is shutting down.

The backup consists of a directory and multiple files. Keep all files and directories intact. Do not delete or separate.

Restoring a GV STRATUS server

This section is only for restoring a GV STRATUS server to the same server type as when it shipped new from Grass Valley. Changing a server from one type to the other (for example, from a Express server to a Proxy server or vice versa) is not supported.

Use the procedures below as follows to restore a GV STRATUS server:

- Restore from the system-specific image that shipped with the server. This is the recommended process. Find related topics in this Topic Library.
- Restore from a generic image, then do subsequent tasks to build the server according to its type and intended use in the GV STRATUS system. Only do this if the system-specific image is not available. If you do this, use the appropriate task list below. Find related topics in this Topic Library, unless otherwise directed.

Restoring a GV STRATUS Express server

1. Make hardware connections as follows:
    a) Connect keyboard, monitor, and mouse.
    b) Connect the image LAN cable to the first motherboard port (left most).
    c) Connect 3 LAN cables to the last three motherboard ports.
    d) Connect both AC power cords.
    e) Connect an Acronis bootable USB stick to one of the front USB ports.

2. Restore from the generic image.

   This includes the following:

   a) Restore disk image.
   b) Do Windows setup.

      Enter the Administrator password and the server's computer name.

3. Verify server partitions and configure if necessary.
4. Create proxy partition.
5. Restore network and system configuration.

   This includes the following:

   a) Name adapters.
   b) Reorder adapters.
   c) Set power management settings.
   d) Configure static IP address.

6. Install SQL.
7. Install SiteConfig Discovery Agent.
8. Do any Windows High Priority updates that are not already installed.
9. Install GV STRATUS software.
10. On proxy share security settings make sure the local "Everyone" has read permission.
11. Add the internal system account, which by default is GVAdmin, to the local Administrators group and on proxy share security settings give that account full permissions.

Related Topics

GV STRATUS server partitions on page 524

Restoring a GV STRATUS Core server on a Dell platform

1. Make hardware connections as follows:
   a) Connect keyboard, monitor, and mouse.
   b) Connect the image LAN cable to the first motherboard port (left most).
   c) Connect 3 LAN cables to the last three motherboard ports.
   d) Connect both AC power cords.
   e) Connect an Acronis bootable USB stick to one of the front USB ports.
2. Restore from the generic image.

   This includes the following:

   a) Restore disk image.
   b) Do Windows setup.

      Enter the Administrator password and the server's computer name.

3. Verify server partitions and configure if necessary.

4. Restore network and system configuration.

   This includes the following:

   a) Name adapters.
   b) Reorder adapters.
   c) Set power management settings.
   d) Configure static IP address.

5. Install SQL.
6. Install SiteConfig Discovery Agent.
7. Do any Windows High Priority updates that are not already installed.

Related Topics

GV STRATUS server partitions on page 524

Restoring a GV STRATUS Core Server on a FT Server platform from a generic image

This is the master task that applies to both Type I and Type II FT Server models. As instructed by the steps in this task, use the appropriate Acronis sub-task specified for the Type I or Type II model.

1. Disconnect network cables.
2. Disconnect power cabling from bottom CPU/IO module.
3. In top CPU/IO module, leave drive 0 in slot, remove all other drives.
4. Provide AC power to top CPU/IO module.
5. Provide access to the disk image file to which you are restoring. For example, connect an external drive containing the image.
6. Startup and in BIOS setup disable OS Boot Monitoring.

   Refer to related topics in this Topic Library.

7. Using the Acronis recovery disk image process as appropriate for the FT Server Type I or Type II model, restore the generic disk image to the top CPU/IO module using Acronis.

   The process to boot into Acronis takes several minutes.

   The restore process takes approximately two hours.

   Refer to related topics in this Topic Library.

8. Restart and log in to Windows as Administrator.
9. When prompted, enter Windows operating system product key and activate later.
10. Restart as prompted.
11. Complete items as prompted by the sysprep process, including the following:

    - Time zone
    - Server name
    - Deselect **Automatic Updates**
    - Select **Don't show again at startup**

    The server restarts.

12. If Server Manager opens, select **Don't show again at startup**.
13. In the top CPU/IO module, insert all drives.

14. In the bottom CPU/IO module, insert all drives.
15. Connect power cabling and start up bottom CPU/IO module.
16. Perform dual disk configuration as follows:
    a) In the RDR Utility, create the first Virtual disk.
    b) When prompted to reboot, click **No**.
    c) Manually reboot the system.

    Refer to related topics in this Topic Library.
17. Perform system disk dual configuration as follows:
    a) Right-click on Slot 0 of PCI Module 11 and select **Add Physical Disk To RDR Virtual Disk**.

    Refer to related topics in this Topic Library.
18. Set resync priority as follows:
    a) Set Virtual Disk 0 to high priority In the Logical disk section, highlight **RDR Virtual Disk**, right-click and select **Set Resync Priority**, set to **High** and click **OK**.

       Disk 0 in each chassis blinks rapidly until the initialization is done.

    Refer to related topics in this Topic Library.
19. Repeat steps to create Virtual Disks and map to physical disks.
20. Wait until Disk 0 completes the build process.

    That takes approximately 3 hours.
21. Use Windows utilities and build a Dynamic disk with all other disks, except for drive 0, using the striped mode rather than the span mode.

    Refer to related topics in this Topic Library.
22. Set duplex LAN configuration to team the left NICS in each server and the right NICS in each server.

    Refer to related topics in this Topic Library.
23. Name teams `Control Team` and `FTP Team`.

    Refer to related topics in this Topic Library.
24. Reorder network adapters so the Control Team is first and the FTP Team is second.

    Refer to related topics in this Topic Library.
25. Restart and in BIOS setup enable OS Boot Monitoring.

    Refer to related topics in this Topic Library.
26. Turn off the FT server firewall

    Refer to related topics in this Topic Library.
27. Remove the GVAdmin account from the Deny log on locally list.

    Refer to related topics in this Topic Library.
28. Install SiteConfig Discovery Agent.

    Refer to related topics in this Topic Library.

29. Install SQL.

    Before installing SQL, make sure that you copy the correct `StratusSQLConfigurationFile.ini` file onto the system so that the database is installed on the D:\ partition.

    Refer to related topics in this Topic Library.

30. Activate the Windows operating system.

    Refer to related topics in this Topic Library.

31. Do any Windows High Priority updates that are not already installed.
32. Install GV STRATUS software.
33. If the FT server has a proxy share, on proxy share security settings make sure the local "Everyone" has read permission.
34. If the FT server has a proxy share, add the internal system account, which by default is GVAdmin, to the local Administrators group and on proxy share security settings give that account full permissions.

Related Topics

Setting OS Boot Monitoring in BIOS on page 1724
Acronis 8162: Restoring from the generic recovery disk image Type I on page 1720
Acronis 11.5: Restoring from the generic recovery disk image Type II on page 1721
System disk dual configuration procedure on page 1681
Set resync priority on page 1693
Build dynamic disk on page 1693
Set duplex LAN configuration on page 1694
Name teams on page 1699
Reorder adapters
Turn off FT server firewall on page 1724
Remove GVAdmin account from Deny log on locally list on page 1726
Installing SQL on page 543
Installing the Discovery Agent on a GV STRATUS server on page 544
Activating the Windows operating system on page 544

Restoring a proxy or engine server

This task applies to the following types of GV STRATUS servers:

- Proxy server variant, such as Proxy server, Proxy Storage file system server.
- Engine server variant Render Engine, Workflow Server.

1. Make hardware connections as follows:
   a) Connect keyboard, monitor, and mouse.
   b) Connect the image LAN cable to the first motherboard port (left most).
   c) Connect 3 LAN cables to the last three motherboard ports.
   d) Connect both AC power cords.
   e) Connect an Acronis bootable USB stick to one of the front USB ports.

2. Restore from the generic image.

   This includes the following:

   a) Restore disk image.
   b) Install Fibre Channel card driver.
   c) Do Windows setup.

      Enter the Administrator password and the server's computer name.

3. Verify server partitions and configure if necessary.
4. Restore network and system configuration.

   This includes the following:

   a) Name adapters.
   b) Reorder adapters.
   c) Set power management settings.
   d) Configure static IP address.

5. Install SiteConfig Discovery Agent.
6. Do any Windows High Priority updates that are not already installed.
7. On Proxy server and Proxy Storage file system server, on proxy share security settings make sure the local "Everyone" has read permission.
8. On Proxy server and Proxy Storage file system server, add the internal system account, which by default is GVAdmin, to the local Administrators group and on proxy share security settings give that account full permissions.

Related Topics

GV STRATUS server partitions on page 524

Restoring from a system-specific recovery disk image on E: Dell R610

Use this task to restore a server using an image made from that particular server. If restoring from a generic factory default image, use the appropriate task.

1. Make sure that media access is stopped and that the system on which you are working is not being used.
2. If you have not already done so, connect keyboard, monitor, and mouse.
3. Do the following:

   a) Insert the Recovery CD.
   b) Restart the machine.

      If there is a problem restarting, hold the standby button down for five seconds to force a hard shutdown. Then press the standby button again to startup.

   The system boots from the Recovery CD.

   The Acronis program loads.

4. At the startup screen, select **True Image Server OEM (Full Version)**.

   The Acronis main window appears.

5. In the Acronis main window, click **Recovery**.

   The Restore Data Wizard opens.

6. On the Welcome page, click **Next**.
7. On the Backup Archive Selection page, in the tree view expand the node for the E: partition and select the image file, then click **Next**.
8. On the Restoration Type Selection page, select **Restore disks or partitions** and then click **Next**.
9. On the Partition or Disk to Restore page, select **(C:)** and then click **Next**.
10. On the Restored Partition Location page, select **(C:)** and then click **Next**.
11. On the Restored Partition Type page, leave the selection at **Active** and then click **Next**.
12. On the Restored Partition Size page, leave settings at their defaults. The size reported in the upper pane is the size detected of the actual C: partition. This should be the same as that reported in the Partition size field in the middle of the page. Free space before and Free space after should both be reported at 0 bytes. Click **Next**.
13. On the Next Selection page, depending on the partitions you are restoring, do one of the following:

    - If you are restoring only the C: partition, select **No, I do not** and then click **Next**.

      Skip ahead to the "…ready to proceed…" page in step 20.

    - If you are also restoring the D: partition, select **Yes, I want to restore another partition or hard disk drive** and then click **Next**.

      Continue with the next step in this procedure.

14. On the Partition or Disk to Restore page, select **(D:)** and then click **Next**.
15. On the Restored Partition Location page, select **(D:)** and then click **Next**.

    opens.
16. On the Restored Partition Type page, leave the selection at **Primary** and then click **Next**.
17. On the Restored Partition Size page, leave settings at their defaults. The size reported in the upper pane is the size detected of the actual D: partition. This should be the same as that reported in the Partition size field in the middle of the page. Free space before and Free space after should both be reported at 0 bytes. Click **Next**.
18. On the Next Selection page, select **No, I do not** and then click **Next**.
19. On the Restoration Options page, do not make any selections. Click **Next**.
20. On the "…ready to proceed…" page, verify that you are restoring the correct image to the correct location. Click **Proceed**.
21. On the Operation Progress page, observe the progress report.
22. When a message appears indicating a successful recovery, click **OK**.
23. Click **Operations | Exit** to exit the Acronis True Image program.

    The machine restarts automatically.
24. Remove the recovery media while the machine is shutting down.

Restoring from a system-specific recovery disk image on E: Dell R620

Use this task to restore a server using an image made from that particular server. If restoring from a generic factory default image, do not use this task.

1. Make sure that media access is stopped and that the system on which you are working is not being used.
2. Connect all motherboard NICs to LAN connections.
3. If you have not already done so, connect keyboard, monitor, and mouse.
4. Do the following:
   a) Insert the Recovery CD.
   b) Restart the machine.

      If there is a problem restarting, hold the standby button down for five seconds to force a hard shutdown. Then press the standby button again to startup.

   The system boots from the Recovery CD.

   The Acronis program loads.
5. On the Acronis Rescue Media page, select **Acronis Backup and Recovery 11.5 (64-bit...)**

   The Acronis Backup and Recovery page opens.
6. On the Acronis Backup and Recovery page, select **Recover**.

   The Recover Data page opens.
7. On the Recover Data page, under What to Recover page, select **Select Data**.

   The Data to Recover Selection dialog box opens.
8. On the Data to Recover Selection dialog box, do the following:
   a) Select **Browse**.
   b) In the tree view, expand the **Local Folders** node.
   c) Select the USB drive that contains the NEC-FT disk image.
   d) Click **OK**.

   On the Archive View tab, your backup name is listed.
9. On the Archive View tab, select your backup.
10. Under Backup contents, do the following:
    a) Select **C:** and **D:**.
    b) Click **OK**.

    The Data to Recover Selection dialog box closes.

11. On the Recover data page, under Where to recover, verify the following:

Recover to:	Physical machine
	Clear all
Recover the 'NTFS' partition with MB size to...	Properties: System Reserved ..Size:....MB ..Letter: D
	Clear Disk 1/NTFS (D:)
Recover the 'NTFS' partition with GB size to...	Properties: NTFS ..Size:...GB ..Letter: C
	Clear Disk 1/NTFS (C:)

12. On the Recover Data page, click **OK**.

    The restore process begins.

13. On the My Recovery Details page, select the **Progress** tab to view the progress.

    The image loads in approximately 9 minutes.

14. When the data is successfully restored, click **OK**.
15. Close all Acronis pages and the Acronis main window.

    The machine restarts automatically.

16. Remove the recovery media while the machine is shutting down.

Restoring from the generic recovery disk image on E: Dell R610

There can be multiple versions of the generic recovery disk image on the server's E: partition. Refer to related topics in the server product's release notes to determine which version you should use.

This procedure can be used on a server that needs to be restored to its factory default state. For example, if you neglected to make a first birthday image, you might need to use this procedure. If the image from which you are restoring was made from the specific machine, refer to the appropriate procedure.

NOTE: This procedure restores the server (both C: and D: partitions) to its factory default condition. Passwords and other site-specific configurations are reset to factory defaults.

1. Make sure that media access is stopped and that the system on which you are working is not being used.
2. Connect all motherboard NICs to LAN connections.
3. If the server has a 10 Gig connection, make sure it is connected to the 10 Gig connection on the Ethernet switch.

   If not connected to a switch, 10 Gig network adapter detection and ordering are unpredictable on the restored image.

4. If you have not already done so, connect keyboard, monitor, and mouse.

5. Do the following:
   a) Insert the Recovery CD.
   b) Restart the machine.

      If there is a problem restarting, hold the standby button down for five seconds to force a hard shutdown. Then press the standby button again to startup.

   The system boots from the Recovery CD.

   The Acronis program loads.
6. At the startup screen, select **True Image Server OEM (Full Version)**.

   The Acronis main window appears.
7. In the Acronis main window, click **Recovery**.

   The Restore Data Wizard opens.
8. On the Welcome page, click **Next**.
9. On the Backup Archive Selection page, in the tree view expand the node for the E: partition and select the image file, then click **Next**.
10. On the Restoration Type Selection page, select **Restore disks or partitions** and then click **Next**.
11. On the Partition or Disk to Restore page, select **(C:)** and then click **Next**.
12. On the Restored Partition Location page, select **(C:)** and then click **Next**.
13. On the Restored Partition Type page, leave the selection at **Active** and then click **Next**.
14. On the Restored Partition Size page, leave settings at their defaults. The size reported in the upper pane is the size detected of the actual C: partition. This should be the same as that reported in the Partition size field in the middle of the page. Free space before and Free space after should both be reported at 0 bytes. Click **Next**.
15. On the Next Selection page, select **Yes, I want to restore another partition or hard disk drive** and then click **Next**.
16. On the Partition or Disk to Restore page, select **(D:)** and then click **Next**.
17. On the Restored Partition Location page, select **(D:)** and then click **Next**.

    opens.
18. On the Restored Partition Type page, leave the selection at **Primary** and then click **Next**.
19. On the Restored Partition Size page, leave settings at their defaults. The size reported in the upper pane is the size detected of the actual D: partition. This should be the same as that reported in the Partition size field in the middle of the page. Free space before and Free space after should both be reported at 0 bytes. Click **Next**.
20. On the Next Selection page, select **No, I do not** and then click **Next**.
21. On the Restoration Options page, do not make any selections. Click **Next**.
22. On the "…ready to proceed…" page, verify that you are restoring the correct image to the correct location. Click **Proceed**.
23. On the Operation Progress page, observe the progress report.
24. When a message appears indicating a successful recovery, click **OK**.
25. Click **Operations | Exit** to exit the Acronis True Image program.

    The machine restarts automatically.
26. Remove the recovery media while the machine is shutting down.

27. When prompted, enter the machine name.

    Make sure the name is identical to the name it previously had.

    At first start up after reimage, the system is in Embedded Security Update mode by default.

Restoring from the generic recovery disk image on E: Dell R620

This task restores a server to its factory default state. For example, if you neglected to make a first birthday image, you might need to use this procedure. If the image from which you are restoring was made from the same, specific machine to which it is being restored, do not use this task.

NOTE: This procedure restores the server (C:, D:, and E: partitions) to its factory default condition. Passwords and other site-specific configurations are reset to factory defaults.

1. Make sure that media access is stopped and that the system on which you are working is not being used.
2. Connect all motherboard NICs to LAN connections.
3. If you have not already done so, connect keyboard, monitor, and mouse.
4. Do the following:
   a) Insert the Recovery CD.
   b) Restart the machine.

      If there is a problem restarting, hold the standby button down for five seconds to force a hard shutdown. Then press the standby button again to startup.

   The system boots from the Recovery CD.

   The Acronis program loads.
5. On the Acronis Rescue Media page, select **Acronis Backup and Recovery 11.5 (64-bit...)**

   The Acronis Backup and Recovery page opens.
6. On the Acronis Backup and Recovery page, select **Recover**.

   The Recover Data page opens.
7. On the Recover Data page, under What to Recover page, select **Select Data**.

   The Data to Recover Selection dialog box opens.
8. On the Data to Recover Selection dialog box, do the following:
   a) Select **Browse**.
   b) In the tree view, select the USB drive that contains the generic recovery disk image.

      Even though your backup is on the drive, it is not yet visible.
   c) Click **OK**.

   On the Archive View tab, your backup name is listed.
9. On the Archive View tab, select your backup.
10. Under Backup contents, do the following:
    a) Select **MBR**.
    b) Select **C:**, **D:**, and **E:**.
    c) Click **OK**.

    The Data to Recover Selection dialog box closes.

11. On the Recover data page, under Where to recover, select the correct destination partition for each source partition as follows:
    a) Select **Recover Disk 1 MBR**.
       The MBR Destination dialog box opens.
    b) In the MBR Destination dialog box, select **Disk 1: Dell PERC ...**, as appropriate for the particular Dell platform. The following are valid selections:
       - Disk 1: Dell PERC H710 SCSI
       - Disk 1 : Dell PERC H310 SCSI
    c) Click **OK**.
    d) Select **Recover NTFS (C:)**.
       The Volume Selection dialog box opens.
    e) In the Volume Selection dialog box, select **C**.
    f) Click **OK**.
    g) Select **Recover NTFS (D:)**.
       The Volume Selection dialog box opens.
    h) In the Volume Selection dialog box, select **D**.
    i) Click **OK**.
    j) Select **Recover NTFS (E:)**.
       The Volume Selection dialog box opens.
    k) In the Volume Selection dialog box, select **E**.
    l) Click **OK**.
12. On the Recover Data page, click **OK**.
    The restore process begins.
13. On the My Recovery Details page, select the **Progress** tab to view the progress.
    The image loads in approximately 9 minutes.
14. When the data is successfully restored, click **OK**.
15. Close all Acronis pages and the Acronis main window.
    The machine restarts automatically.
16. Remove the recovery media while the machine is shutting down.
17. When prompted, enter the machine name.
    Make sure the name is identical to the name it previously had.
    After start up, one or more device discovery windows can open. Allow processes to complete without interference.
    At first start up after reimage, the system is in Embedded Security Update mode by default.

Creating the proxy partition on a GV STRATUS Express server

- The Core Services server must be freshly re-imaged and must not have a proxy partition

- The Core Services server must be intended for use as an Express server in the GV STRATUS system

The recommended method is to restore the Express Server using the system specific image that shipped on the server. When you do so, the proxy partition is also restored. However, if for some reason you must create the proxy partition manually, use this procedure.

1. Log into the server as Administrator.
2. On the Windows desktop, next to the **Start** menu, click on the **Server Manager** Icon.
   Server Manager opens.
3. In the Server Manager tree select **Storage | Disk Management**.
4. Right-click on **CD-ROM 0** and select **Change Drive Letter and Paths**.
5. Select the F: drive letter and click the **Change** button.
6. In the **Assign the following drive letter** drop-down list select **G**.
7. Click **OK**.
8. Click **Yes**.
9. Right-click on Disk 0's **Unallocated disk space** and select **New Simple Volume**.
   The New Simple Volume wizard opens.
10. On the wizard's first page, click **Next**.
11. On the Specify Volume Size page, select the maximum size (should be the default) and click **Next**.
12. On the Assign Drive Letter page, select **F** and click **Next**.
13. On the Format Partition page, select **Format this Volume with the following Settings** and make settings as follows:

Option	Setting
File System	NTFS
Allocation Unit Size	Default
Volume Label	Storage
Check	Perform a quick format

NOTE: Do not check "Enable file and folder compression"

14. Click **Next**.
15. Click **Finish**.
    The wizard closes.
16. Verify that the partition has been created.

Restoring network configuration

When you restore a system from its system specific image, network configuration is also restored to the factory default settings. This is the recommended method of restoring network configuration. However, if for some other reason you must configure network settings manually, use the tasks in this section to restore the default network configuration.

Name adapters

1. If not already open, open Network Connections as follows:
   a) Open the Windows **Network and Sharing Center** control panel.
   b) Click **Change Adapter Settings**.
   Network Connections opens.
2. In Network Connections, click **View | Details**.
3. For GV STRATUS servers without an FTP/Streaming connection (Proxy, Proxy Storage file system), verify adapter names.
   The required adapter names are specified in the following table:

Adapter name
Control Connection
Unused Connection 0
Unused Connection 1
Unused Connection 2

4. For GV STRATUS servers with an FTP/Streaming connection but no media (iSCSI) connection, (Express, Core), verify adapter names.
   The required adapter names are specified in the following table:

Adapter names
Control Connection
FTP-Streaming Connection
Unused Connection 1
Unused Connection 2

5. For GV STRATUS servers with an FTP/Streaming connection and with one or two media (iSCSI) connections, (Render Engine), verify adapter names
   The required adapter names are specified in the following table:

Adapter names
Control Connection
FTP-Streaming Connection
Media Connection #1
Media Connection #2

6. Proceed as follows:
   - If all the names on this system are configured correctly to locations, skip the rest of this procedure.
   - If names on this system are not configured correctly, for each adapter name incorrectly configured, complete the remaining steps of this procedure.
7. Select the name in the Name column.
8. Select **File | Rename** to enter rename mode.
9. Type the name required.

Next, reorder adapters.

Reorder adapters

- Adapters must be named correctly
- The control team must be created
- The team and loopback must be named

1. If not already open, open Network Connections as follows:
   a) Open the Windows **Network and Sharing Center** control panel.
   b) Click **Change Adapter Settings**.
   Network Connections opens.
2. Select **Advanced**, then **Advanced Settings...**
3. For GV STRATUS servers without an FTP/Streaming connection (Proxy, Proxy Storage file system), on the **Adapters and Bindings** tab, order adapters as follows:

Control Connection
Unused Connection 0
Unused Connection 1
Unused Connection 2

4. For GV STRATUS servers with an FTP/Streaming connection but no media (iSCSI) connection, (Express, Core), on the **Adapters and Bindings** tab, order adapters as follows:

Control Connection
FTP-Streaming Connection
Unused Connection 1
Unused Connection 2

5. For GV STRATUS servers with an FTP/Streaming connection and with one or two media (iSCSI) connections, (Render Engine), on the **Adapters and Bindings** tab, order adapters as follows:

Control Connection
Media Connection #1
Media Connection #2
FTP-Streaming Connection

6. Click **OK** to close and accept the changes.
7. Close Network Connections.

If continuing with network configuration, next set power management settings.

Set power management settings

1. If not already open, open Network Connections as follows:
   a) Open the Windows **Network and Sharing Center** control panel.
   b) Click **Change Adapter Settings**.
   Network Connections opens.
2. Right-click one of the adapters and select **Properties**.
   The Properties dialog box opens.
3. Click **Configure**.
4. On the **Power Management** tab, uncheck all checkboxes, if they are not already unchecked.
5. Click **OK**.
6. If a "…lose connectivity…" message opens, click **Yes**.
7. Repeat these steps on the remaining network connection in the Network Connections window.

Installing SQL

- SQL must be one of the required system requirements on the server, according to the server's intended use in the GV STRATUS system.
- The GV STRATUS server must be freshly re-imaged and SQL must not yet be installed

The recommended method of restoring SQL is to restore the GV STRATUS server using the system specific image that shipped on the server. When you do so, SQL is also restored to its factory default installation. However, if for some reason you must install SQL manually, use this procedure. SQL is required on GV STRATUS servers with the role of GV STRATUS Database.

If the server should have SQL, install it as follows:

1. Log into the server as Administrator.
2. Run the following batch file.
   `C:\Grass Valley\InstallSQL.bat`
   A console opens.
3. Wait until the console closes. This indicates the install is complete.
   This is a quiet install, so there is no incremental progress indicator.

4. License SQL-Server as follows:
   a) From the Windows desktop, click **Start | All Programs | Microsoft SQL Server | Configuration Tools | SQL Server Installation Center (64 bit)**.

      SQL Server Installation Center opens.
   b) Select **Maintenance | Edition Upgrade**.
   c) Follow the wizard, clicking **OK** and **Next**.
   d) When you arrive at the Product Key page, select **Enter the product key**, type in the product key, and select **I accept the license terms**.
   e) Finish the wizard, clicking **Next** and **Upgrade**.

Installing the Discovery Agent on a GV STRATUS server

If the device that you plan to manage with SiteConfig does not have a SiteConfig Discovery agent installed, use this topic to verify and, if necessary, manually install SiteConfig support software. Doing so allows SiteConfig to discover and manage the device. If the device has any version of the SiteConfig Discovery Agent currently installed, you should use SiteConfig to upgrade the Discovery Agent, rather than installing it manually.

This task applies to any variant of a GV STRATUS server, such as Express, Core, Proxy, Engine, etc.

1. On the device you plan to manage with SiteConfig, open the Windows Services Control Panel and look for the following required item:
   - SiteConfig Discovery Agent
2. Proceed as follows:
   - If you find the required items, no further steps are necessary. SiteConfig support software is installed.
   - If a required item is not present, navigate to your SiteConfig files. If you do not already have these files in convenient location, you can find them on the PC that hosts SiteConfig, in the SiteConfig install location. Then continue with next steps as appropriate.
3. To launch the program that installs the ProductFrame Discovery Agent Service do the following:
   a) Copy the `Discovery Agent Setup` directory to the device.
   b) In the directory, double-click the `DiscoveryAgentServiceSetup.msi` file.

      The setup program launches to install the SiteConfig Discovery Agent.
   c) Follow the setup wizard.
4. When presented with a list of device types, select one of the following as appropriate:
   - StratusCoreServicesServer
5. Complete the setup wizard and restart the device.

   The restart is required after the installation.

Activating the Windows operating system

If a system is restored to its factory default state or otherwise has the Windows operating system re-applied, you might need to activate the operating system. This procedure provides instructions

for doing this while the machine is connected to the Internet. The Activation wizard provides other options, which you can also choose if desired.

To active the Windows operating system, do the following:

1. Make sure the machine is connected to the Internet.
2. From the Windows desktop, in the system tray double-click on the key symbol icon. The Activate window opens.
3. Select **Yes, let's activate Windows over the Internet now** and click **Next**.
4. When prompted, "If you want to register with Microsoft right now.", select **No**.
5. Wait for the connection. If the system times out, you are prompted for entering information in the Internet Protocol Connection dialog. Enter the proxy address and port number as appropriate for your facility's connections.
6. Ensure that "You have successfully activated your copy of Windows" message appears in Activate Windows.
7. Click **OK** to close the Activate Windows.

Renaming a GV STRATUS Core/Express server

This topic is for renaming a GV STRATUS server that has the role of GV STRATUS Core Services. The following GV STRATUS servers have the role of GV STRATUS Core Services:

- GV STRATUS Express server
- GV STRATUS Core server

Please contact Grass Valley Support before attempting to rename a GV STRATUS Core/Express server.

Extensive system configuration is required to achieve a working GV STRATUS system. If you only change the display name, it does not change the Core/Express server host name.

Any name change must include updates to SiteConfig, K2 Config, GV STRATUS Control Panel Services Host, GV STRATUS Database, licensing settings, MDI settings, Proxy settings, Engines settings, network domain change, and interfaces with other applications.

Configuring a Router

You can use Jupiter, Encore, or SMS7000 router in your operation.

You need to configure your router on the Router Configuration panel in the GV STRATUS Control Panel application.

When connecting to a Jupiter router, use the ESswitch interface protocol. If you are connecting a Jupiter router using a serial hub, you need to configure a virtual COM port and install the software before configuring the router.

You can also use Jupiter with the AccuSwitch application that can be configured in the GV STRATUS Control Panel application.

Encore system can be configured to control cross points of a single routing matrix, or expanded to control multiple matrices depending on your system needs.

Configuring Virtual COM port (Jupiter only)

In order to connect to Jupiter router via ethernet, a serial hub needs to be configured.

Before starting to configure the DIGI One SP RS422 Serial to Ethernet Device Server, write down the MAC address located at the bottom of the hardware.

This serial hub will act as a virtual COM port, which enables serial-to-ethernet connectivity as though Jupiter is communicating with GV STRATUS via the local COM port.

DIGI One SP Device Server		**Jupiter Router**	
Pin Name	**Pin Number**	**Pin Number**	**Pin Name**
Rx +	2	3	Tx +
Tx +	3	7	Rx +
Rx -	6	8	Tx -
Tx -	9	2	Rx -

1. A serial crossover cable (also known as null-modem cable) is needed to allow proper communications between Jupiter router and DIGI One SP Device Server. The appropriate pinouts can be referred from the table above.

2. Connect one end of the crossover cable to the device server and the other end to RS422 serial cable to connect to Jupiter.

3. Connect an ethernet cable from the device server to a network point on your LAN.
4. Connect the power supply to the device server.

Related Topics

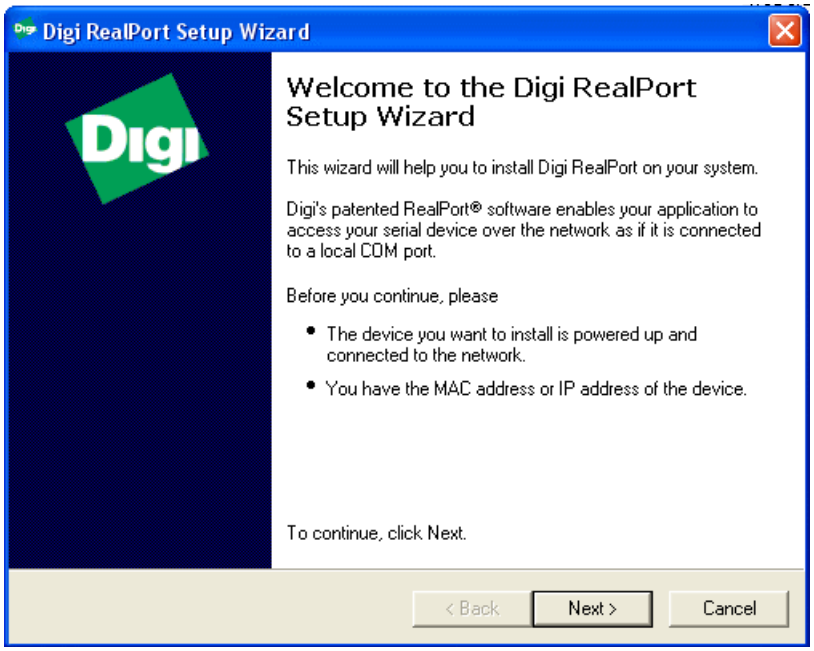
Installing Virtual COM port software (Jupiter only) on page 547

Installing Virtual COM port software (Jupiter only)

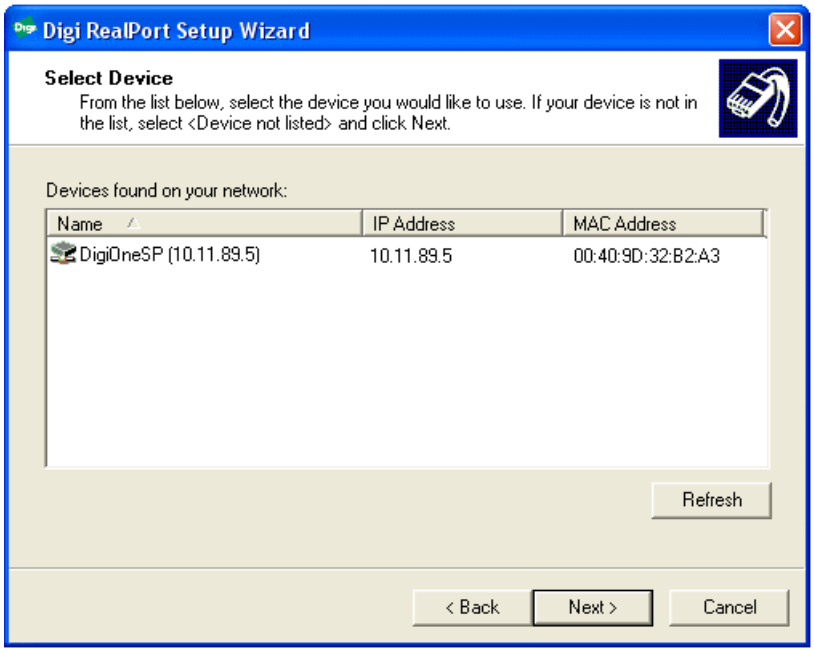
After the virtual COM port has been configured, you need to install the software.

1. Insert the DIGI CD in your CD ROM drive.

2. The setup wizard will automatically be displayed on your screen.
   If not, navigate to the CD ROM drive and double-click **setup.exe**.

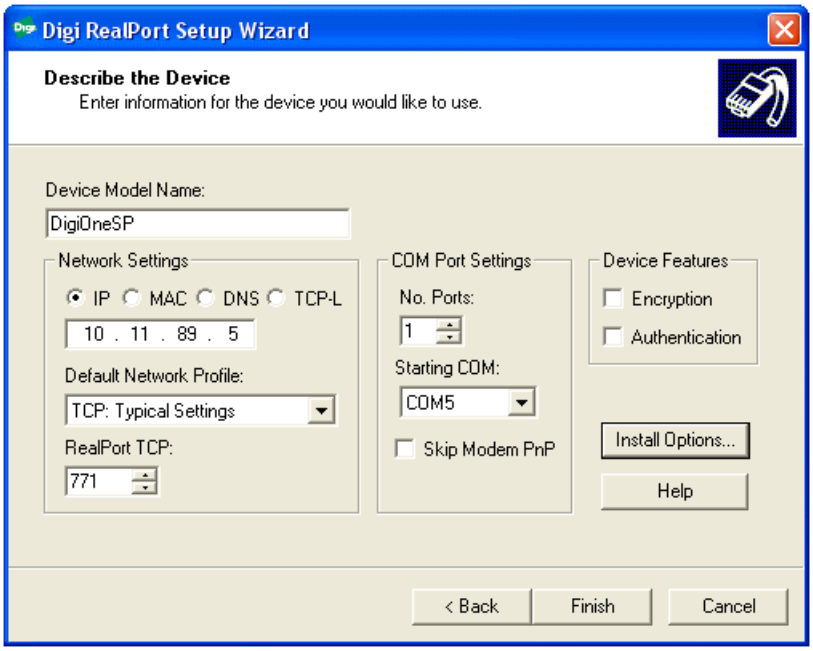


3. Click **Next** and the setup wizard will search your network to locate the DIGI One SP device server.



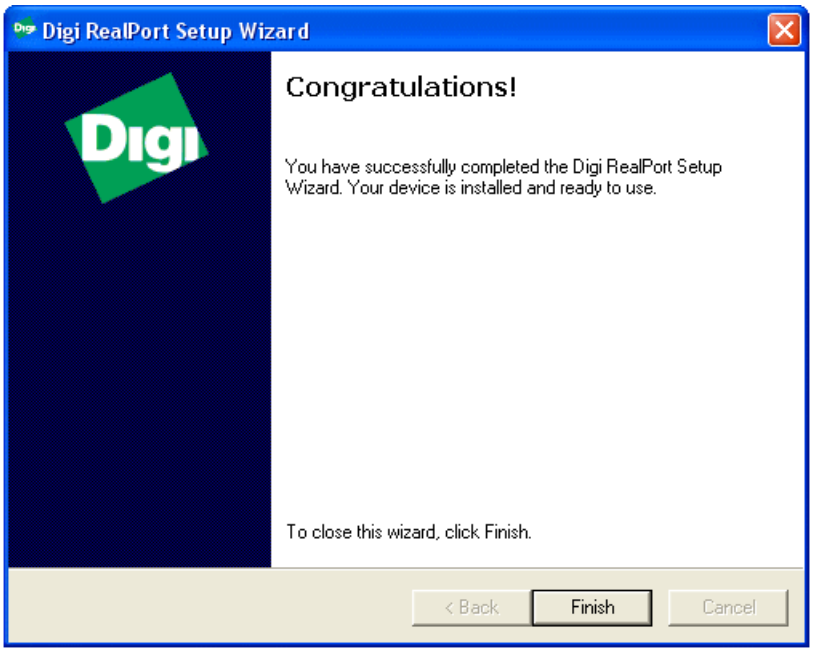
4. Select the device server according to its specific MAC address.

5. Take note of the device IP address and click **Next.**



6. In the Network Settings section, select **IP** and enter the IP address that had been retrieved by the setup wizard.
7. In the COM Port Settings section, set the number of ports to 1 and select the appropriate COM port from the Starting COM drop down list. This will be your virtual COM port.

8. Click **Finish**.



The setup wizard will install the software.

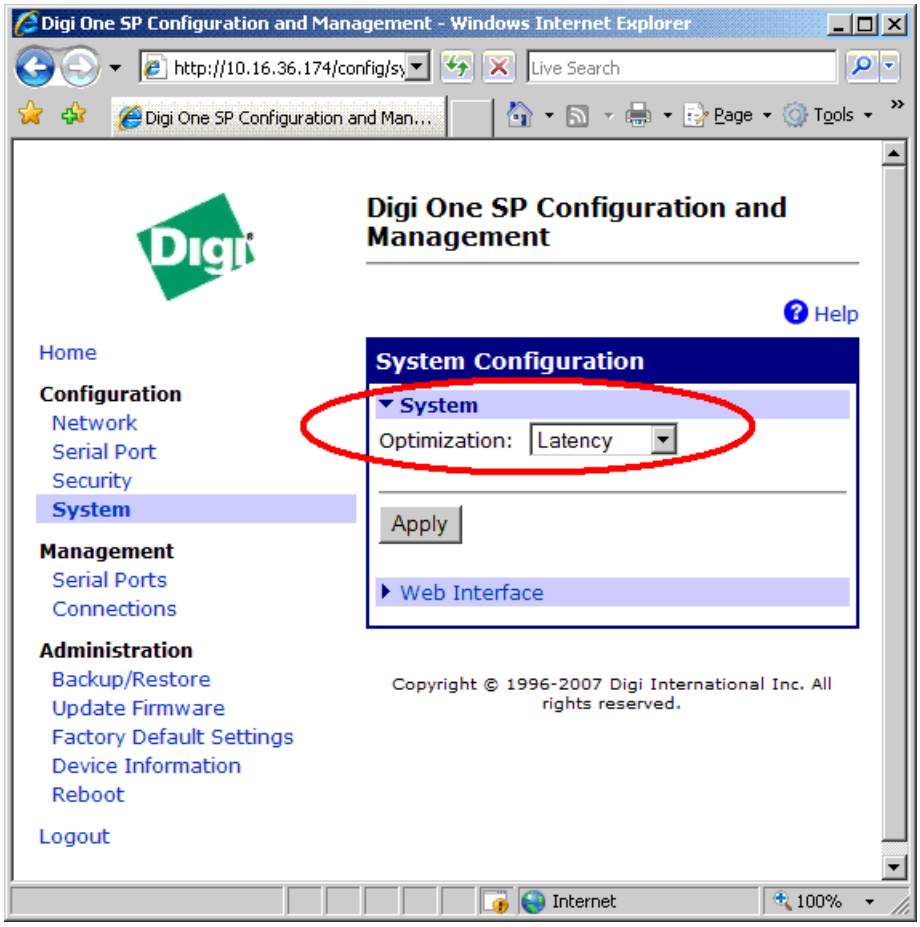
9. Click **Finish** after the installation is done.

   NOTE: Once you have configured the virtual COM port, you need to enter the COM port number in the router configuration panel of the GV STRATUS Control Panel.

10. To avoid unnecessary timeouts on RS422 communication, you need to set the Digi One SP optimization routine to Latency.

    This can be done by launching the configuration page on your web browser. If needed, the default username/password for the Digi One configuration page is root/dbps.

11. Then, go to the System Configuration page and select Latency from the Optimization dropdown list.



Related Topics

Configuring Virtual COM port (Jupiter only) on page 546

Configuring Jupiter-AccuSwitch router control

- The Jupiter Control System CM 4000 with AccuSwitch application must be connected to the Jupiter File Server (Configuration PC) via an IP hub, switch, or media converter. Make sure you have the CM4000 MAC address prior to the configuration.
- The Jupiter Network Suite (JNS) Control Console software must be installed on the Configuration PC. Refer to Jupiter customer documentation for the compatible version of the control software.
- You must have administrator privileges in order to load Jupiter software, launch Jupiter applications, and configure the system.

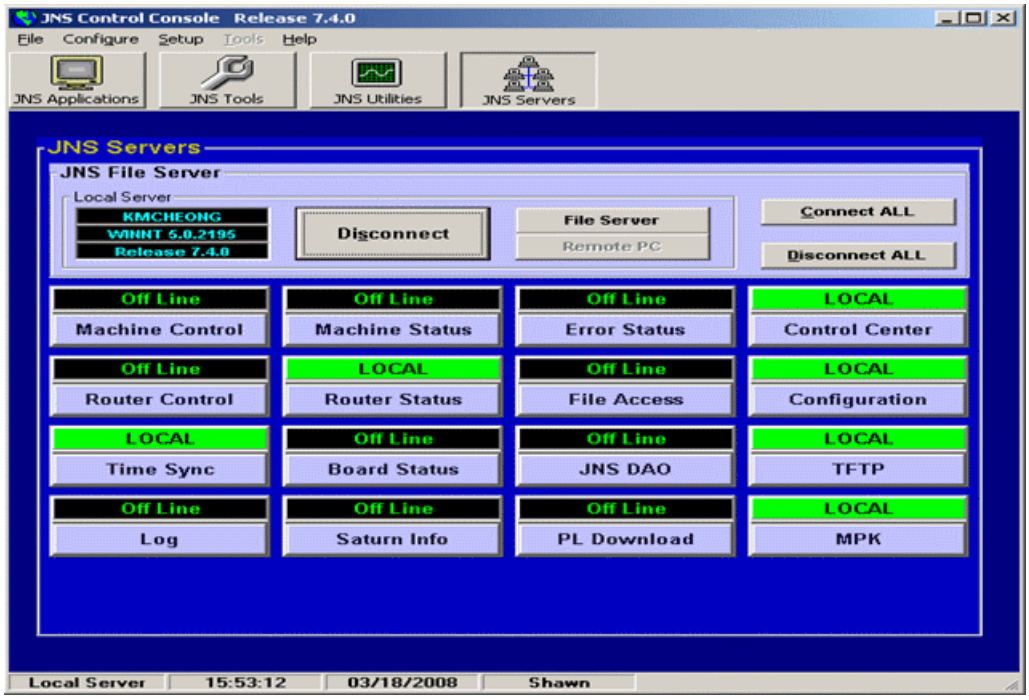
The Jupiter Network Suite (JNS) Control Console software on the Configuration PC provides an interface to the Jupiter Control system CM 4000 through the LAN.

In this configuration, you need to ensure that the IP address of your GV STRATUS Core server is entered in the Network Description list on the Jupiter Configurator Panel.

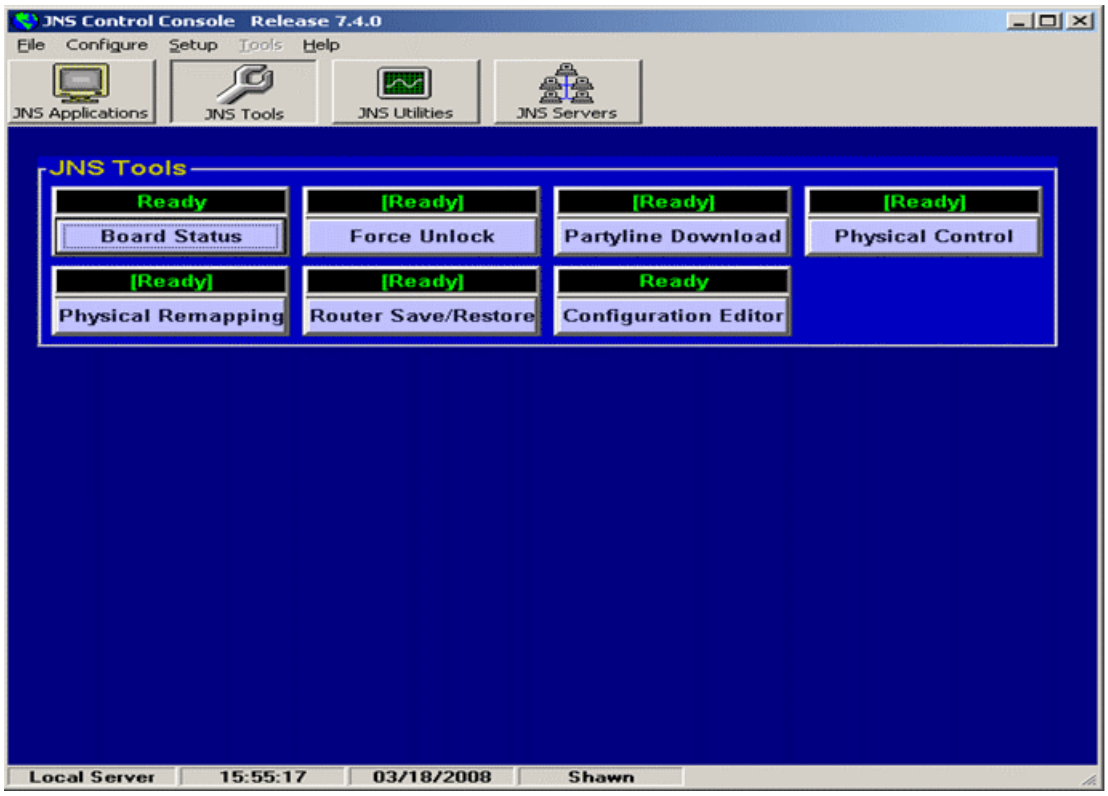
1. Launch the Jupiter Network Suite (JNS) Control Console on the Configuration PC.
2. Click the **JNS Servers** button on the toolbar.

   The **JNS File Server** appears in the JNS Servers panel.
3. Click the **Connect** button.

   With a successful connection, appropriate programs run on the JNS File Server indicated by the **LOCAL** status.



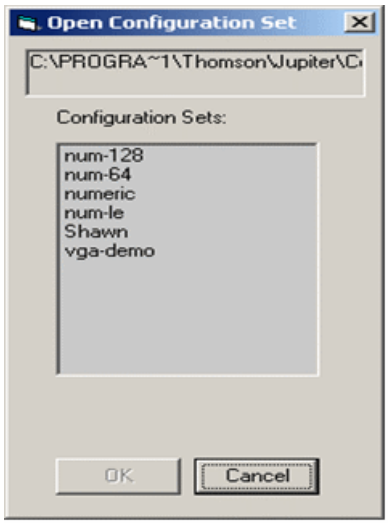
4. Click the **JNS Tools** button on the toolbar and click **Configuration Editor**.



The Jupiter Configurator panel opens.

5. Select **File | Open**.

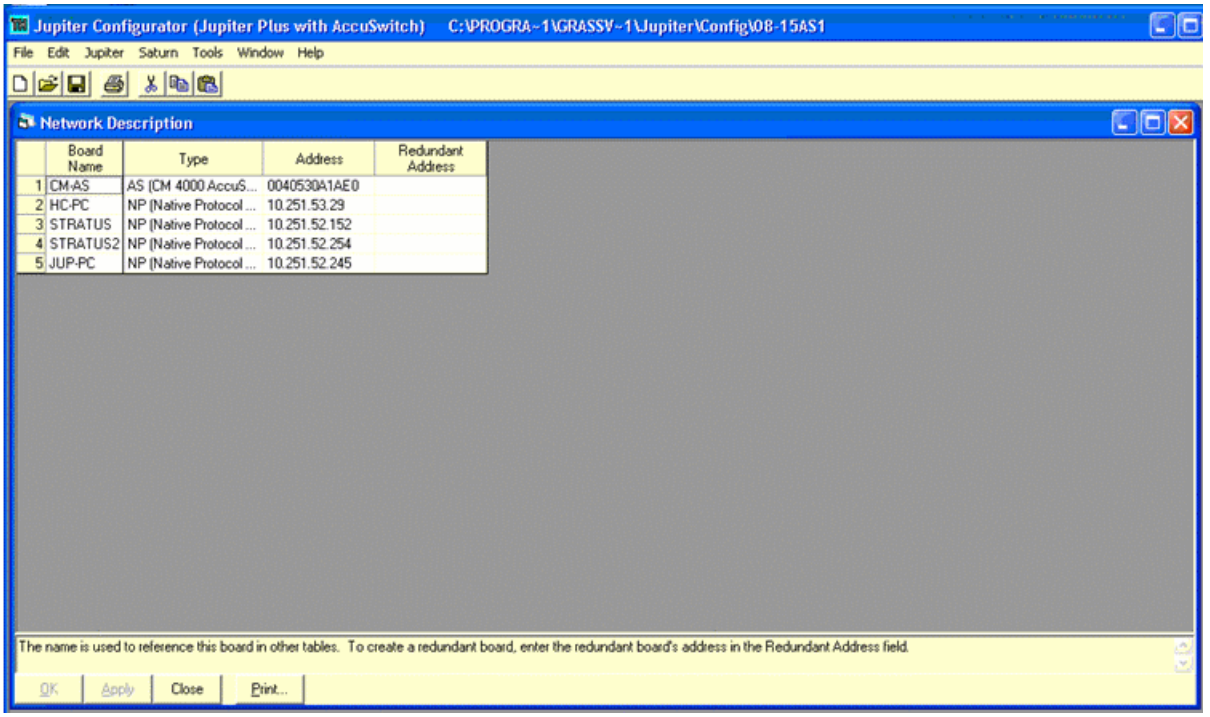
The Open Configuration Set dialog opens.



6. Select your configuration set from the list and click **OK**.

7. Select **Jupiter | Network Description** on the Jupiter Configurator panel.

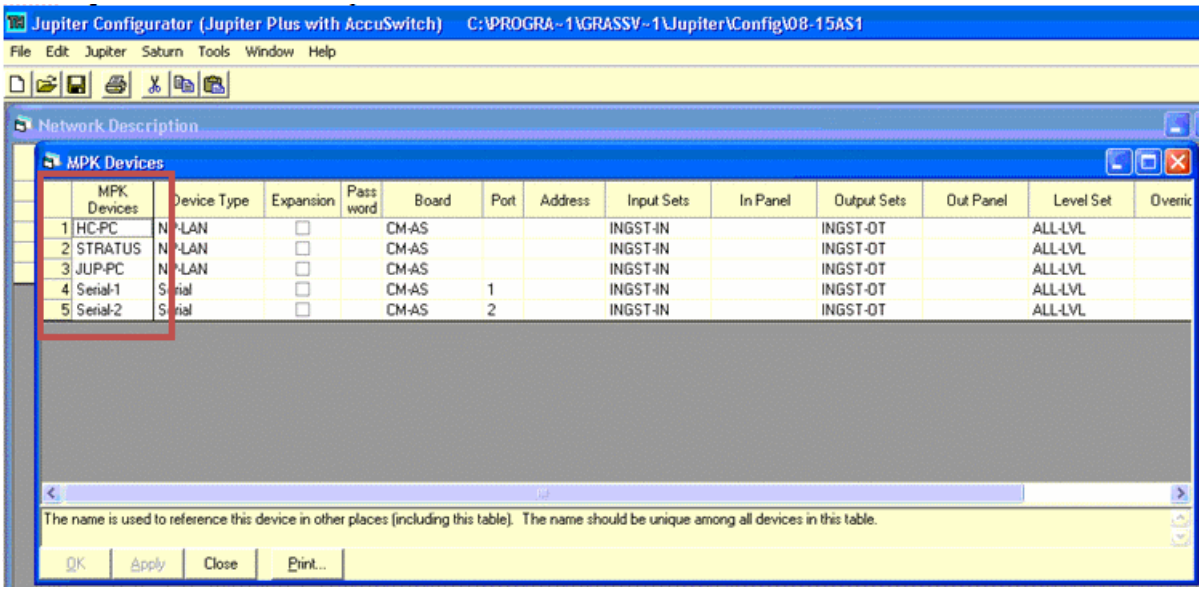
   The Network Description panel opens.



   a) Check that the Jupiter CM4000 MAC address is correct.
   b) Add the GV STRATUS Core server name in the Network Description list.
   c) Set the Type as **NP (Native Protocol)**.
   d) Enter the IP address of the GV STRATUS Core server.

8. Select **Jupiter | MPK Devices** on the Jupiter Configurator panel.

   The MPK Devices panel opens.



   a) Add the GV STRATUS Core server to the list of MPK devices.
   b) Set the Device Type to **NP-LAN**.
   c) Select the board name of your Jupiter Control System CM 4000.
   d) Select the Input Sets, Output Sets, and Level Set for your operation.

9. After the configuration, you need to compile and download your configuration set into the Jupiter Control System CM 4000.

   Refer to the *CM 4000 Control Module Installation and Operating Manual* for more information regarding the compile and download processes.

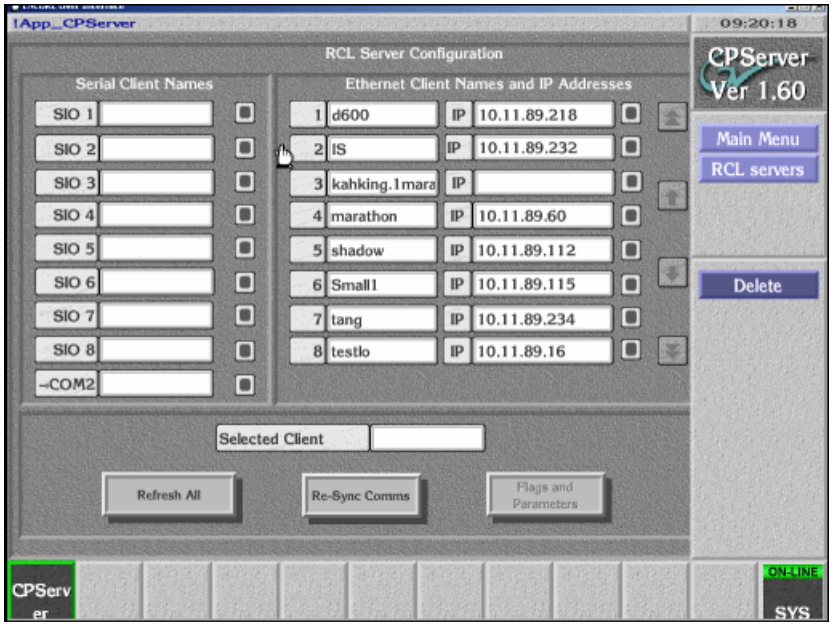
Configuring Encore

Encore system can be configured to control crosspoints of a single routing matrix, or expanded to control multiple matrices depending on your system needs.

You also need to ensure that the IP address of your GV STRATUS Core Services Server is entered in the RCL Server configuration of the Encore router control system.

1. Log on to Encore OUI, select App_CPServer and RCL Servers.

2. On the Ethernet Client Names and IP Addresses section of the RCL Server Configuration window, enter the machine name and IP address of your GV STRATUS Core Services Server.



3. Log out from Encore OUI.
4. In the GV STRATUS Contol Panel application, launch the router configuration panel to configure the Encore router connection.
5. If needed, you can customize the level setting on the **Connection** tab. Select the appropriate level from the drop-down list for video, audio and timecode.

   Select 0 (zero) for the video level if video is the first level in your router control system, 1 if it is the second level and so on.
6. Click **Save** to save changes.

Related Topics

Router Connection settings on page 397
Router Sources settings on page 399
Characters not allowed in router source and destination IDs on page 557

Configuring Router Windows Service (for SMS7000 protocol only)

- This configuration is only for non-STRATUS compatible routers using the SMS7000 protocol.

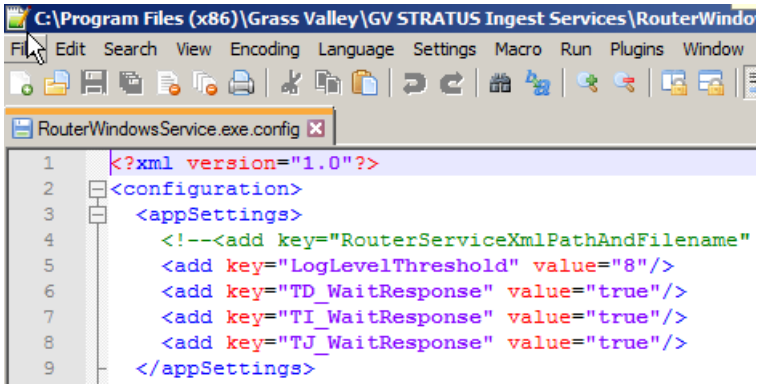
The configuration is needed to prevent router sources switching delay.

1. On the GV STRATUS Core server, go to:

```
C:\Program Files (x86)\Grass Valley\GV STRATUS Ingest
Services\RouterWindowsService.exe
```

2. Open **RouterWindowsService.exe** with an editor to edit the file.

   On the editor, you can view the name of the file as **RouterWindowsService.exe.config** as below:



3. Edit the file by replacing **"true"** with **"false"** in these settings below:

```
<add key="TD_WaitResponse" value="false"/>
<add key="TI_WaitResponse" value="false"/>
<add key="TJ_WaitResponse" value="false"/>
```

4. Click the **Save** button to save your changes.

By default, those settings are always set to **"true"**.

When set to **"false"**, the router service does not wait for response from the router controller. So, there is no delay of switching non-STRATUS compatible routers sources in the GV STRATUS application.

Characters not allowed in router source and destination IDs

Position	Character	Description
Anywhere in name	%	percent
	&	ampersand
	'	apostrophe
At beginning of name		space
At the end of name		space

NOTE: Please refrain from using space and other non-alphanumeric characters in your source and destination IDs, whenever possible.

Set up RMI PC access to high-resolution assets

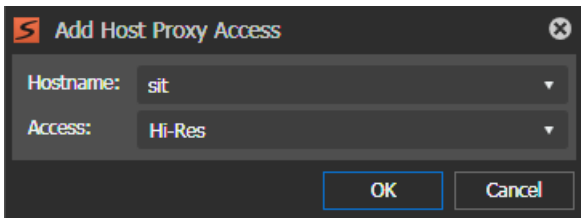
A GV STRATUS client PC on which you use the RMI tool must be one of the following types of GV STRATUS clients:

- Low-resolution (proxy) client PC with SMB access to K2 storage.
- High-resolution client PC on K2 media (iSCSI) network, which requires the GV STRATUS high resolution license.

If you use a low-resolution (proxy) client PC, use Windows Explorer and mount the K2 media storage `V:` drive on the PC.

If you use a high-resolution client PC, use the following steps.

1. In GV STRATUS Control Panel, click **Core | Proxy Config | Proxy Access | Add**.
   The Add Host Proxy Access dialog box opens.



2. For Hostname, select the name of the GV STRATUS client PC that you are setting to high-resolution.
3. For Access, select **Hi-Res**.
4. Click **OK** to save settings and close.

Related Topics

RMI settings on page 396
Proxy Access settings on page 345
About GV STRATUS client PCs on page 416

Working with GVRE Transcoder

Topics in this section provide the necessary information for using the GVRE Transcoder.

About the GVRE Transcoder

GV Render Engine now supports a new function as a generic transcoder for imports and exports. With the introduction of Grass Valley's own transcoder, this improved the import process by writing the rendering result straight into K2 Summit systems compared to transcoding via third party providers. As a result, the new asset is available while it is being imported. While for exports, the related transcoding of export material is improved by reading directly from K2 Summit storage rather than waiting for completion of a previous transfer to a temporary location before transcoding.

For both imports and exports, different transcoding formats are required as follows:

- **Imports** — related transcoding profiles can be taken from GV STRATUS *Formats* configuration
- **Exports** — related transcoding profiles need to be generated by an EDIUS or XRE Transcoder Application

After new transcoding profiles have been imported into the system, they can be used for import and export rules.

The maximum concurrent number of transcode jobs can be configured in the GV STRATUS Control Panel.

SabreTooth Render Engine server license process

Only systems with an Render Engine require this process. The process is on the GV STRATUS server with role of Common Services.

The Render Engine license is installed on the GV STRATUS server with role of Common Services. Typically the GV STRATUS Core server has the role of Common Services. Each license below is a SabreTooth floating license.

STRATUS-CONFORM: This is the current license for the GV STRATUS Render Engine. One STRATUS-CONFORM license is required for each GV STRATUS server running Render Engine software in your GV STRATUS system. Each Render Engine server runs Render Engine software as the Conform Server and Proxy Encoder, so each server requires a license.

STRATUS-GVRE: This is the new license for the GV STRATUS Render Engine. One STRATUS-GVRE license is required for each GV STRATUS server running Render Engine software in your GV STRATUS system as the Conform Server and Proxy Encoder. Only one license is checked out by GV STRATUS Render Engine for conform and proxy functionality, therefore you must either have the **STRATUS-CONFORM** or the **STRATUS-GVRE** license in your GV STRATUS server.

STRATUS-TRANSCODE: This is the new license for the GV STRATUS Render Engine. One STRATUS-TRANSCODE license is required for each GV STRATUS server running Render Engine software in your GV STRATUS system as the Generic Transcoder. This license only enables Transcode jobs, with the maximum number of 10 jobs per server.

The type of license to be installed is determined by the usage of Render Engine in your system by setting the number of maximum concurrent job per functionality for the Render Engine on the Engines tab of GV STRATUS Control Panel.

If you received your system pre-configured from Grass Valley, licenses are already installed, so you can skip these tasks. Otherwise, do the following:

1. Refer to the license sheet that you received with your GV STRATUS license. The license sheet has the Sales Order number that you need.
2. On the GV STRATUS server with role of Common Services, run the SabreTooth License Manager, generate a unique ID, and send the email to Grass Valley requesting your license or licenses.

   Refer to this Topic Library for detailed licensing procedures.
3. When you receive your license file, use SabreTooth License Manager and install it on the server.

Creating Export Transcode Profiles

Exports of transcoded files are based on Transcode Profiles that specify the video codec, resolution, frame rate, field order, timecode, and aspect ratio. Transcode profiles (*.tpd files) must be created with an EDIUS or XRE Transcoder application. Then, those transcode profiles must be added into the GV STRATUS system via the XRE Transcoding Profile Tool.

Each transcode profile is built to correspond to a specific transcode operation via the GVRE Transcoder. Multiple transcode profiles can be created, according to workflow needs and corresponding GV STRATUS rules.

NOTE: Export transcode profile (*.tpd file) for Apple ProRes video compression format is not supported by the EDIUS application, therefore it must be created with the XRE Transcoder application or alternatively procured from Grass Valley.

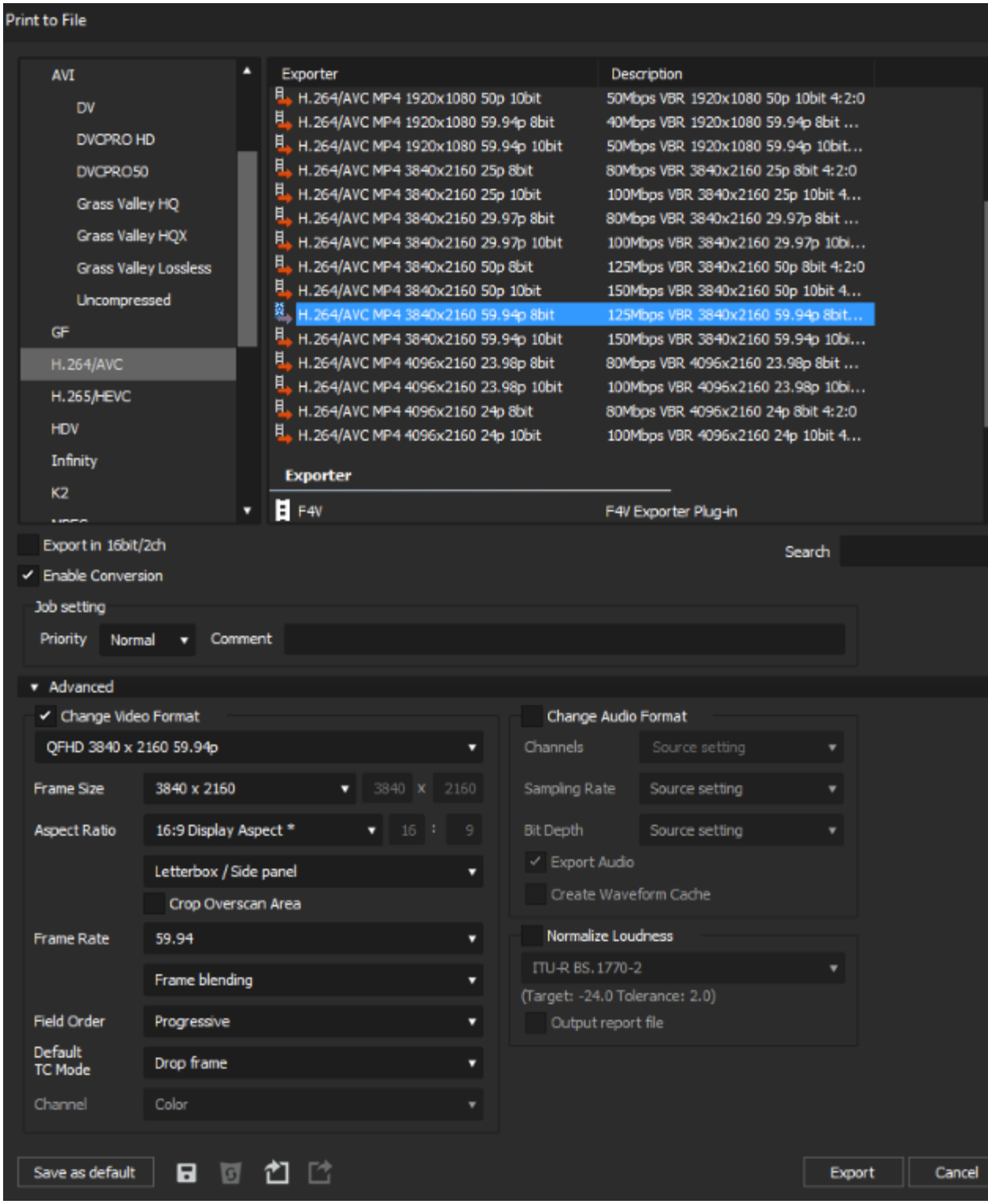
Creating Export Transcode Profiles with EDIUS

Transcode profiles are created by an administrator or advanced user of EDIUS and must be saved to a shared location accessible to users of the XRE Transcoding Profile Tool.

1. In the EDIUS application, open a new project and place a clip on the timeline.

2. Select **File | Export | Print to File**.

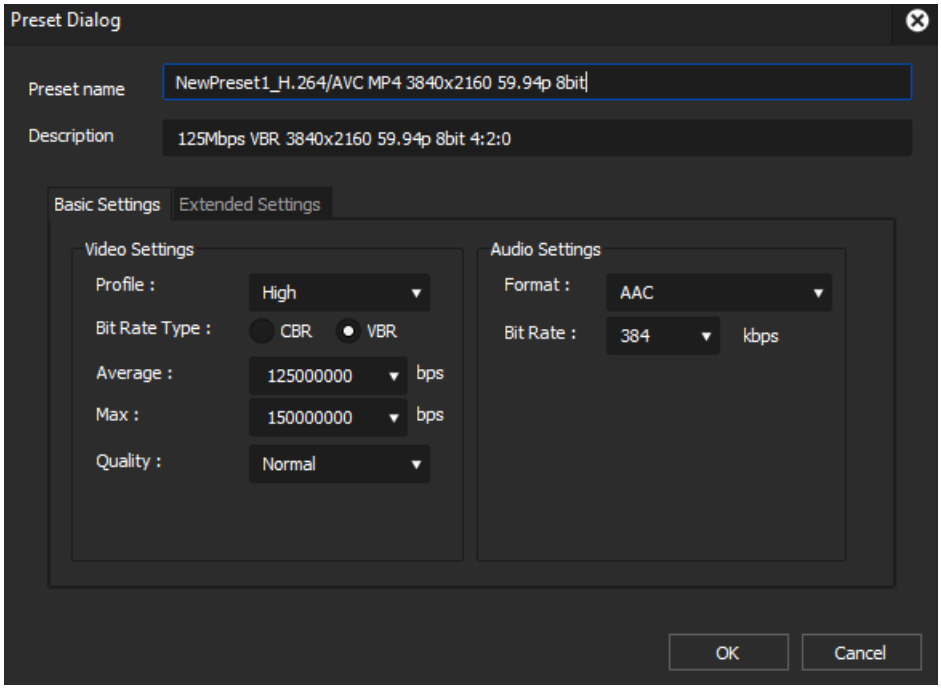
   The Print to File window displays.



3. Select a format on the left column and select the exporter preset on the right column of the window.

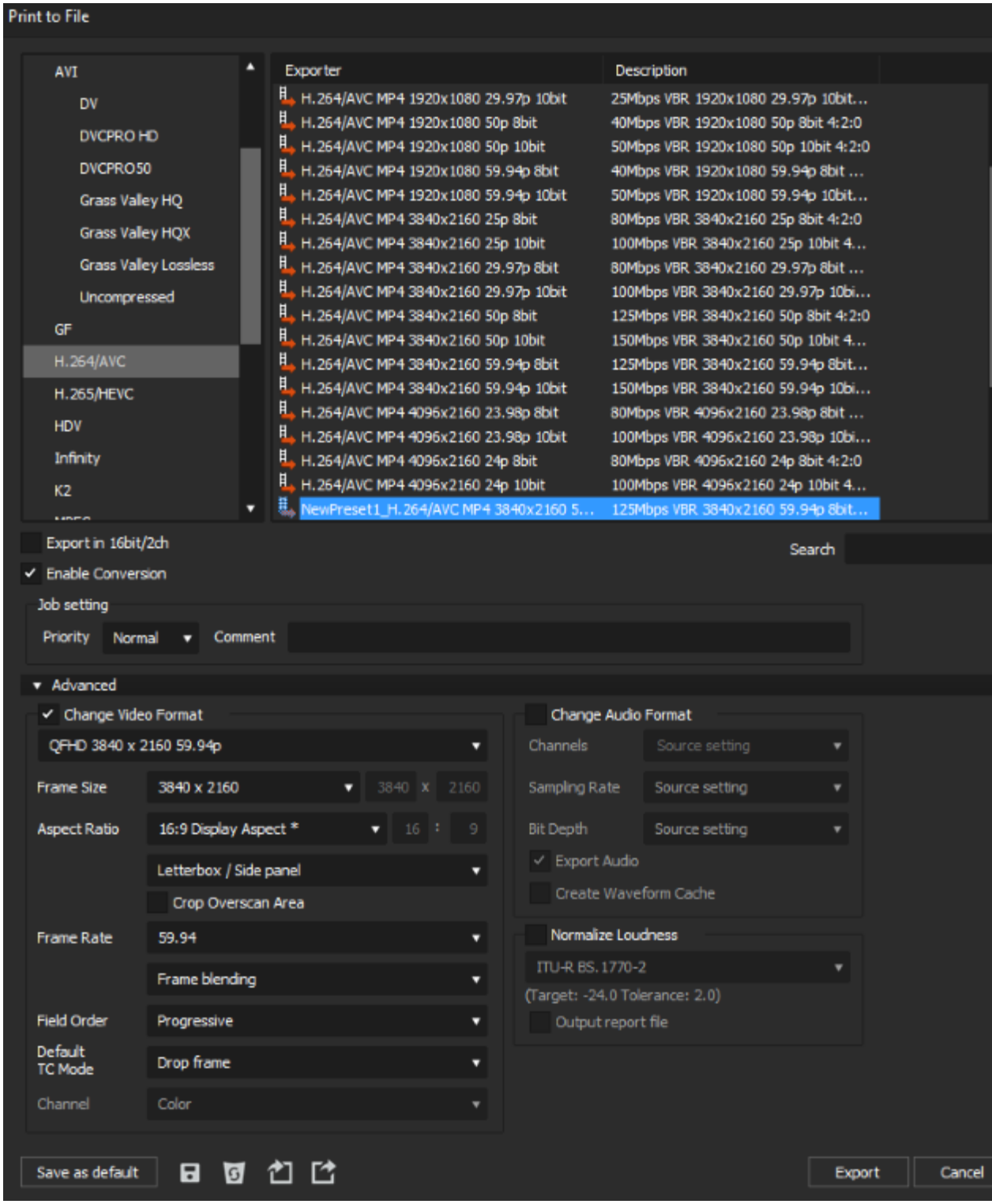
4. Select the **Enable Conversion** check-box.
5. Click the drop-down arrow to expand **Advanced** settings, and set appropriate configuration for the transcode profile.
6. Save the setting by clicking the **Save Preset** button.

   The Preset Dialog appears.



7. Enter the Preset name and click **OK**.

   The newly configured preset appears in the Exporter list.



8. Select the new preset and click the **Export Preset** button.

   The preset or transcode profile is exported as a (*.tpd) file.

   NOTE: The transcode profile (*.tpd file) for Apple ProRes video compression format is not supported by the EDIUS application, therefore it must be created with the XRE Transcoder application or alternatively procured from Grass Valley.

Next, use the XRE Transcoding Profile Tool to add the new transcode profile of GVRE Transcoder into the GV STRATUS system.

Related Topics

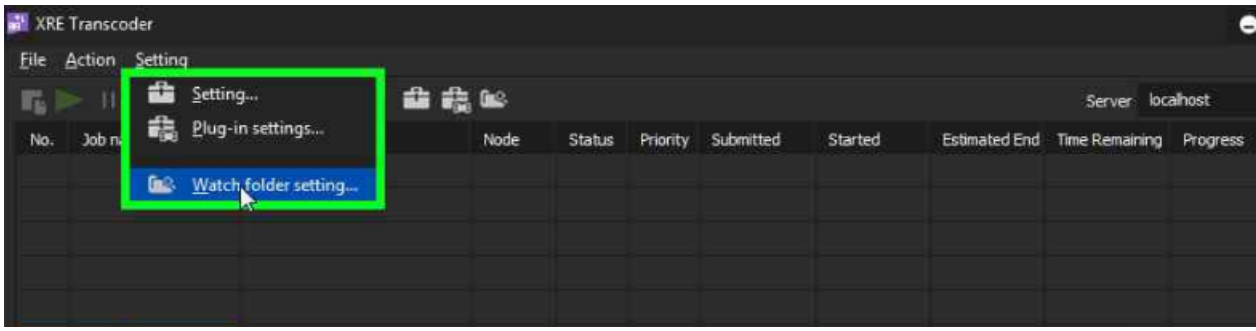
Adding export transcode profiles with the XRE Transcoding Profile Tool on page 569

Creating Export Transcode Profiles with XRE Transcoder

Transcode profiles can also be created in the XRE Transcoder application and must be saved to a shared location accessible to users of the XRE Transcoding Profile Tool.

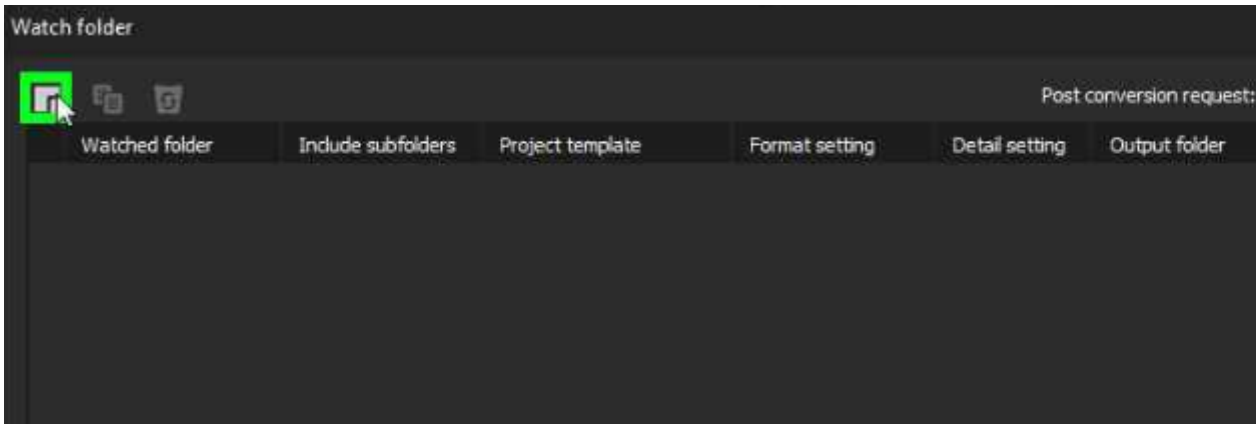
NOTE: Export transcode profile (.tpd file) for Apple ProRes video compression format is not supported by the EDIUS application, therefore it must be created with the XRE Transcoder application.

1. Launch the XRE Transcoder application.



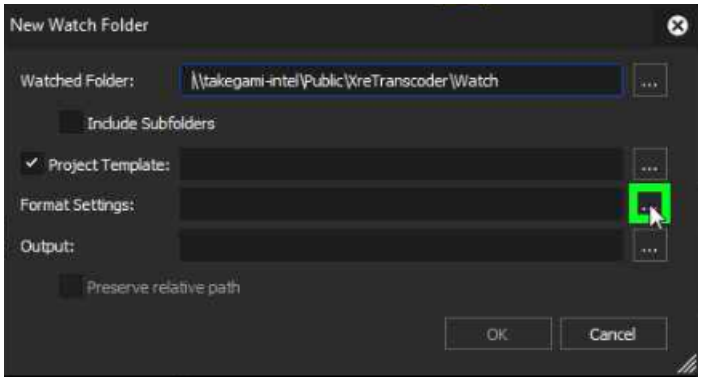
2. Select **Setting | Watch folder setting**.

   The Watch folder window displays.



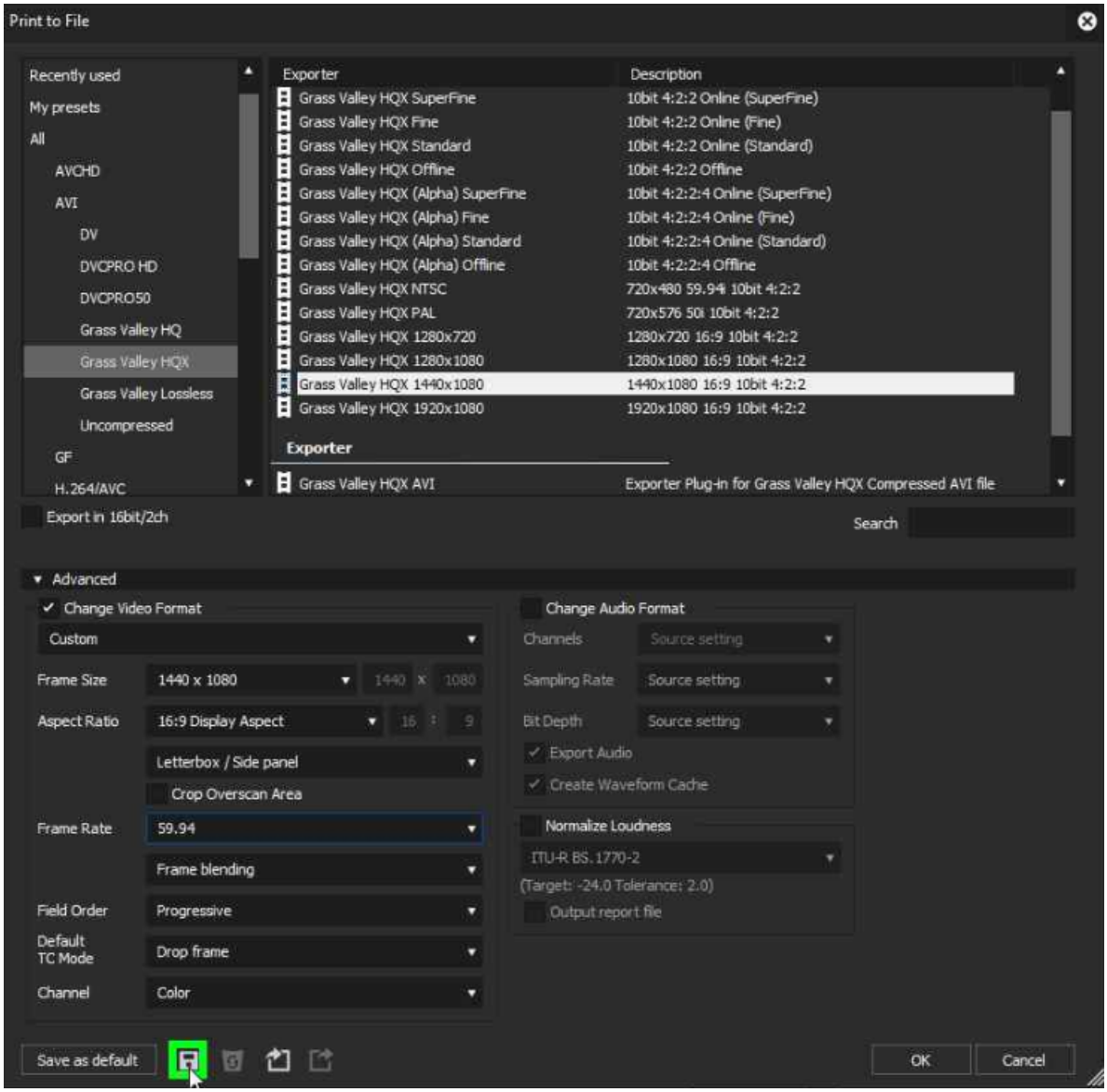
3. Click on the **Add Watch Folder** button.

   The New Watch Folder window appears.



4. At the **Format Settings** option, click the ... button to create the transcode profile.

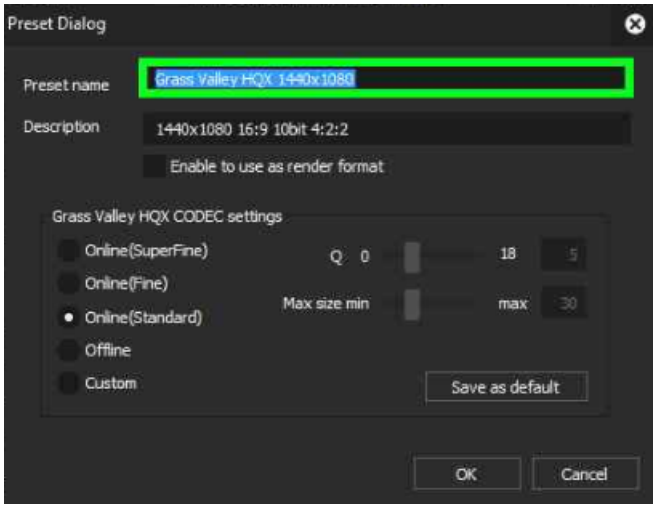
   The Print to File window appears.



5. Select a format on the left column and select the exporter preset on the right column of the window.
6. Click the drop-down arrow to expand the **Advanced** settings.
7. Select the **Change Video Format** check-box, and set appropriate configuration for the transcode profile.

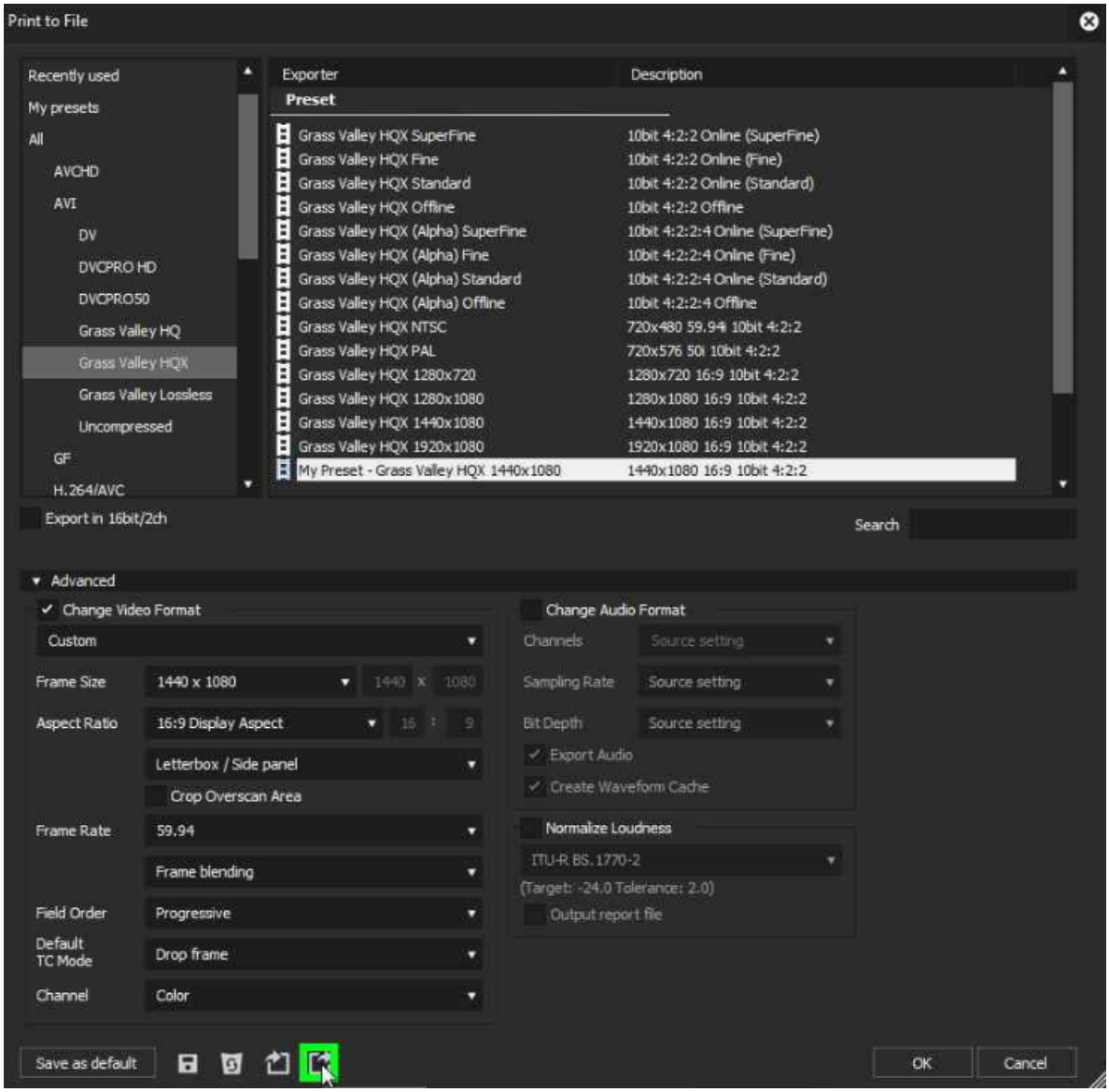
8. Save the setting by clicking the **Save Preset** button.

   The Preset Dialog appears.



9. Enter the Preset name and click **OK**.

   The newly configured preset appears in the Exporter list.



10. Select the new preset and click the **Export Preset** button.
11. Select the export location and click **Save**.

    The **Export succeeded** message appears.

12. Click **OK**.

    The preset or transcode profile is exported as a (*.tpd) file to the selected location.

Next, use the XRE Transcoding Profile Tool to add the new transcode profile of GVRE Transcoder into the GV STRATUS system.

Related Topics

Adding export transcode profiles with the XRE Transcoding Profile Tool on page 569

Adding export transcode profiles with the XRE Transcoding Profile Tool

- The Render Engine software must be installed and configured in the GV STRATUS Core server.
- The STRATUS-TRANSCODE license must be installed in the GV STRATUS Core server.
- A transcode profile (*.tpd file) which has exporter presets must be created with an EDIUS or XRE Transcoder application and must be accessible to the XRE Transcoding Profile Tool.

You must use the XRE Transcoding Profile Tool to add transcode profiles of GVRE Transcoder into the GV STRATUS system.

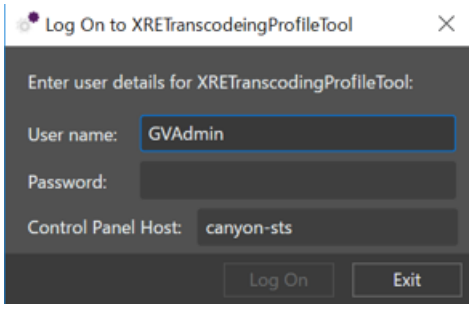
1. Launch the XRE Transcoding Profile Tool from the path below:

   - `C:\Program Files\Grass Valley\XREServer 9\XRETranscodingProfileTool`

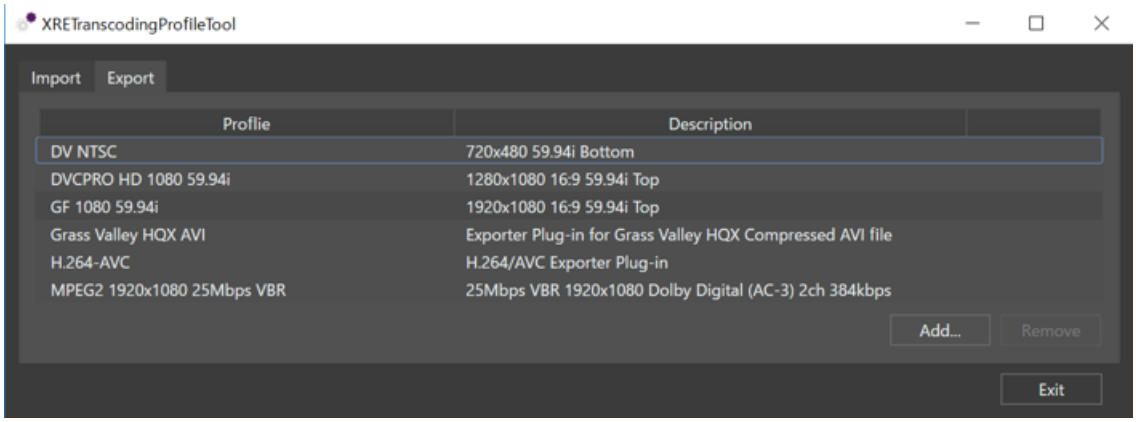
     OR

   - Double-click the **XRE Transcoding Profile Tool** shortcut on your desktop

   The Log On dialog box opens.

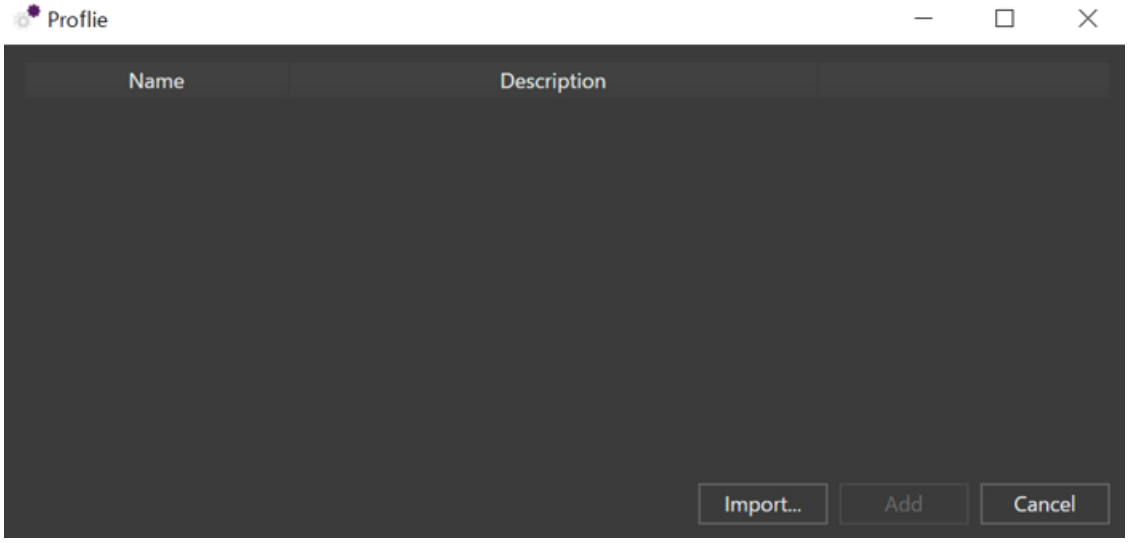


2. Enter your user name and password, then click **Log On**.
3. Click on the **Export** tab to add transcode profiles for export rules.



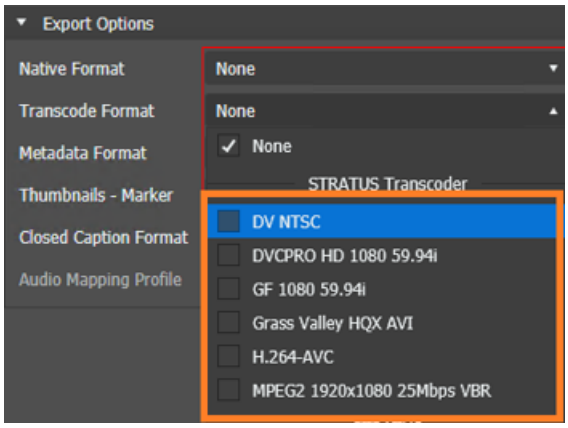
4. Click **Add**.

   The Profile dialog box opens.



5. Click **Import**, then navigate and select exporter presets that had been created earlier with the EDIUS or XRE Transcoder application.
6. Click **Add** to register them as export profiles.

Those selected formats will be available as transcode profiles of STRATUS Transcoder when you configure export rules in the GV STRATUS Control Panel.



Related Topics

Creating Export Transcode Profiles on page 559
Creating Export Transcode Profiles with EDIUS on page 560
Creating Export Transcode Profiles with XRE Transcoder on page 564

Adding import transcode profiles with the XRE Transcoding Profile Tool

- The Render Engine software must be installed and configured in the GV STRATUS Core server.

- The STRATUS-TRANSCODE license must be installed in the GV STRATUS Core server.

You must use the XRE Transcoding Profile Tool to add transcode profiles of GVRE Transcoder into the GV STRATUS system.

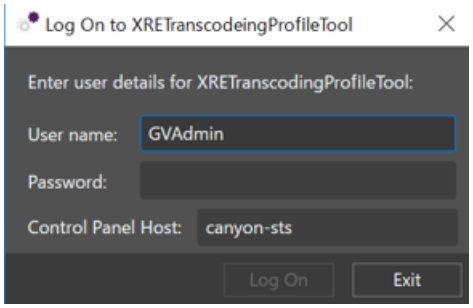
1. Launch the XRE Transcoding Profile Tool from the path below:

   - `C:\Program Files\Grass Valley\XREServer 9\XRETranscodingProfileTool`

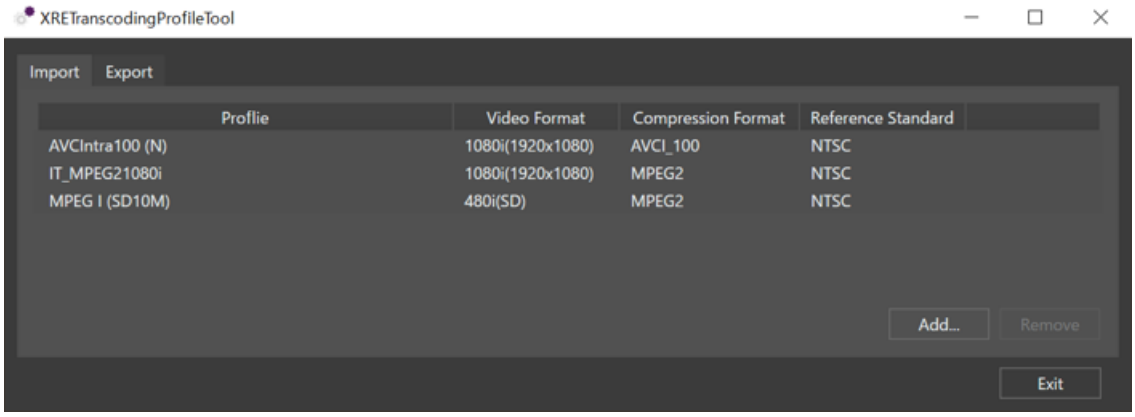
     OR

   - Double-click the **XRE Transcoding Profile Tool** shortcut on your desktop

   The Log On dialog box opens.

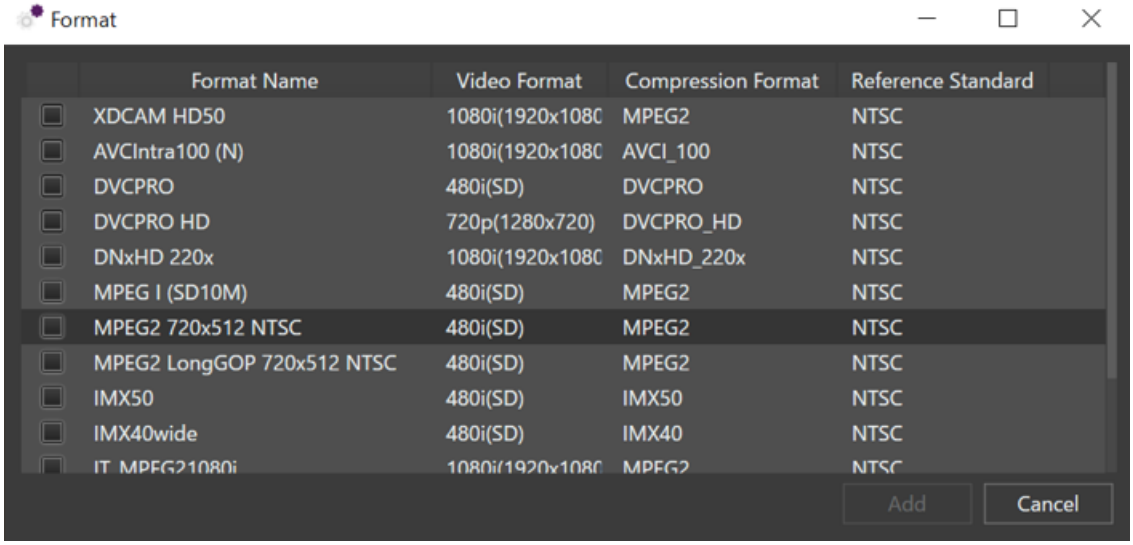


2. Enter your user name and password, then click **Log On**.
3. Click on the **Import** tab to add transcode profiles for import rules.



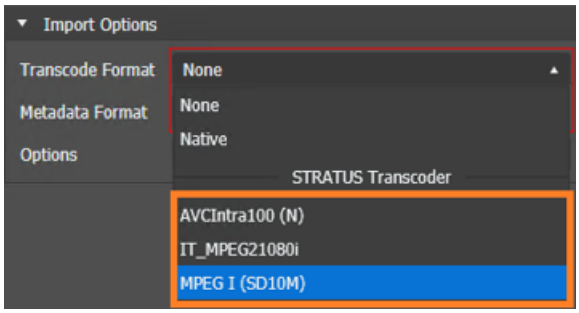
4. Click **Add**.

   The Format dialog box displays all registered formats in the GV STRATUS Control Panel.



5. Select format(s) for your import transcode profiles, and click **Add**.

Those selected formats will be available as transcode profiles of STRATUS Encoder when you configure import rules in the GV STRATUS Control Panel.



GVRE Transcoder supported formats

When you use import or export rules in the GV STRATUS application, you can set assets to be transcoded via the GVRE Transcoder. Transcoding profiles must be imported into the system before they can be used by import and export rules.

Refer to topics in this section for GVRE Transcoder supported formats.

GVRE Transcoder supported import formats

The following formats are supported by GVRE Transcoder for GV STRATUS import rules:

Container format	Video Compression format	Audio Compression format	File Extension	Note
3GPP	H.264/AVC	AAC	*.3gp,*.3g2,*.amc	-

	MPEG4			
AVCHD	H.264/AVC	AC-3	*.m2ts,*.mts	-
		LPCM		
AVI	DV	LPCM	*.avi	-
	DVCPRO			
	DVCPRO 50			
	DVCPR0 HD			
	Grass Valley HQ			
	Grass Valley HQX			
	Grass Valley Lossless			
	Uncompressed RGB			
	Uncompressed RGBA			
	Uncompressed YUY2			
	Uncompressed UYVY			
	Uncompressed v210			
DIF stream	DV	LPCM	*.dif,*.dv	-
	DVCPRO			
	DVCPRO 50			
	DVCPRO HD			
Flash Video	H.264/AVC	AAC	*.f4v	-
		LPCM		
MPEG Program Stream	MPEG1	MPEG 1 Audio Layer-2	*.mpg,*.mpeg,*.m2p,*.mp2,*vob,*.vro	-
	MPEG2	AC-3		
		LPCM		
MPEG Transport Stream	MPEG2	MPEG 1 Audio Layer-2	*.m2t, *.ts	-
		AC-3		
	H.264/AVC	AAC		
		LPCM		

MPEG Video Stream	MPEG1		*.mpv,*.m2v	-
	MPEG2			
MP4	H.264/AVC	AAC	*.mp4,*.m4v	-
	H.265/HEVC	LPCM		
	MPEG2			
	MPEG4			
MXF	AVC-Intra	LPCM	*.mxf	-
	AVC-Ultra			
	DNxHD			
	DV			
	DVCPRO			
	DVCPRO 50			
	DVCPRO HD			
	Grass Valley HQ			
	Grass Valley HQX			
	H.264/AVC			
	JPEG2000			
	MPEG2			
	MPEG2 IMX			
	Apple ProRes			
QuickTime Movie	Apple ProRes	AAC	*.mov	-
	DNxHD	LPCM		
	DNxHR			
	AVC-Intra			
	AVC-Ultra			
	DV			
	DVCPRO			
	DVCPRO 50			
	DVCPRO HD			
	Grass Valley HQ			

	Grass Valley HQX			
	H.264/AVC			
	H.265/HEVC			
	MJPEG			
	MPEG2			
	MPEG2 IMX			
	MPEG4			
RED	RED	RED	*.R3D	-
Windows Media	Windows Media Video	Windows Media Audio	*.wmv,*.asf	You need to enable the Windows "Desktop Experience" feature on your GVRE server so that GVRE can use components of Windows Media.

GVRE Transcoder supported export formats

The following formats are supported by GVRE Transcoder for GV STRATUS export rules:

Container format	Video Compression format	Audio Compression format	File Extension	Note
AVCHD	H.264/AVC	Dolby Digital (AC-3)	*.m2ts	-
		LPCM		
AVI	DV	LPCM	*.avi	-
	DVCPRO 50			
	DVCPR0 HD			
	Grass Valley HQ			
	Grass Valley HQX			
	Grass Valley Lossless			
	Uncompressed RGB			
	Uncompressed RGBA			
	Uncompressed YUY2			

	Uncompressed UYVY			
	Uncompressed v210			
Flash Video	H.264/AVC	AAC	*.f4v	-
HDV	MPEG-2 Transport Stream	MPEG 1 Audio Layer-2	*.m2t	-
K2 (GXF)	AVC-Intra 50	LPCM	*.GXF	-
	AVC-Intra 100			
	AVC-LongG			
	D10			
	DNxHD			
	DV			
	DVCPRO 25			
	DVCPRO 50			
	DVCPRO HD			
	JPEG2000			
	MPEG-2			
MPEG-2 Program Stream	MPEG-2	MPEG 1 Audio Layer-2	*.mpg,*m2p	-
		LPCM		
		Dolby Digital (AC-3)		
MP4	H.264/AVC	AAC	*.mp4	-
MXF	AVC-Intra 50	LPCM	*.mxf	-
	AVC-Intra 100			
	AVC-Intra 200			
	AVC-LongG			
	D10			
	DNxHD			
	DV			
	DVCPRO 25			
	DVCPRO 50			

	DVCPRO HD			
	Grass Valley HQ			
	Grass Valley HQX			
	JPEG2000			
	MPEG-2			
	Apple ProRes			Export transcode profile (.tpd file) for Apple ProRes video compression format is not supported by the EDIUS application, therefore it must be created with the XRE Transcoder application or alternatively procured from Grass Valley.
QuickTime Movie	Apple ProRes	LPCM	*.mov	Export transcode profile (.tpd file) for Apple ProRes video compression format is not supported by the EDIUS application, therefore it must be created with the XRE Transcoder application or alternatively procured from Grass Valley.
	Grass Valley HQ			
	Grass Valley HQX			
Windows Media	Windows Media Video	Windows Media Audio	*.wmv	You need to enable the Windows "Desktop Experience" feature on your GVRE server so that GVRE can use components of Windows Media.

Configuring Rules

The topics in this section provide instructions for configuring GV STRATUS system rules.

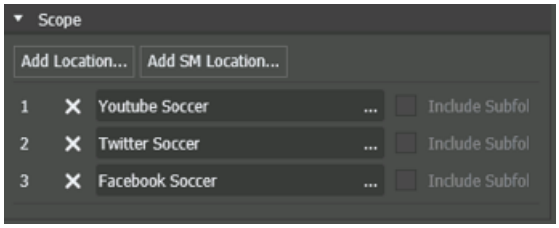
Adding a delete rule

The GV STRATUS Rules Engine can watch a location and delete assets that match your criteria.

1. Log in to the GV STRATUS Control Panel application with administrator privileges.

2. In the GV STRATUS Control Panel application, click **General | Rules**.
3. Click **Add**.

   Rule Editor settings open.
4. In the **Rule Type** drop-down list select **Delete**.
5. In the **Name** field type in a name for the rule you are configuring.
6. In the **Description** field type in a description for the rule you are configuring.
7. In **Scope** settings, specify the location or locations in which the rule operates.



   a) Click **Add Location** or **Add SM Location**.

      The Location Selection dialog box opens.

      If you clicked **Add SM Location**, the Location Selection dialog box displays all social media locations that had been configured.

   b) Navigate to and select the desired location.

      You can select multiple locations in the **Location Selection** dialog box.

      For Transfer, Export, Custom, Archive, and Transfer to Avid rules, you can also select logical asset locations under **Groups | Lost and Found**.

      If desired, you can edit scope location path manually in the text box.

      This is the location that contains the files on which the rule operates. Every time the rule runs, it looks in this location to determine if there are any assets that match the rule conditions and then operates on the assets that match.

   c) Click **OK**.

      The location is added to the **Scope** list.

   d) For a location in the list, if you want the rule to operate on sub-folders as well, select **Include Subfolders**.

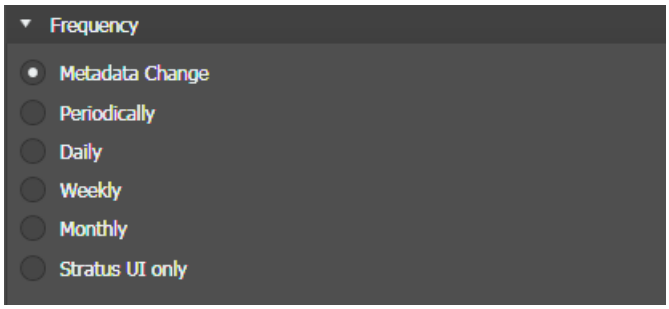
      When this is selected, if there are multiple directories under the selected location, the rule operates in each of the sub-directories.

   e) Repeat these steps to add additional locations as desired.

   f) To change a location in the list, click the **Browse** button ···

   g) To remove a location from the list, click **X**.

8. In **Frequency** settings, specify how often the Rules Engine triggers the rule.

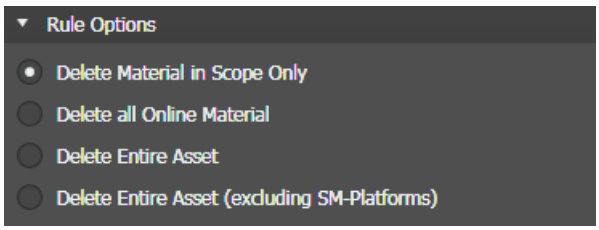


   a) Select one of the following options:

   - **Metadata Change**: The rule is constantly monitoring files in the “Scope” folder (and file types depend on the rule condition).
   - **Periodically**: Sets the number of minutes.
   - **Daily**: Sets the number of days.
   - **Weekly**: Sets the number of weeks.
   - **Monthly**: Sets the day of each month.
   - **STRATUS UI only**: The rule is only applicable when triggered by users via the context menu in Asset List of the STRATUS UI.

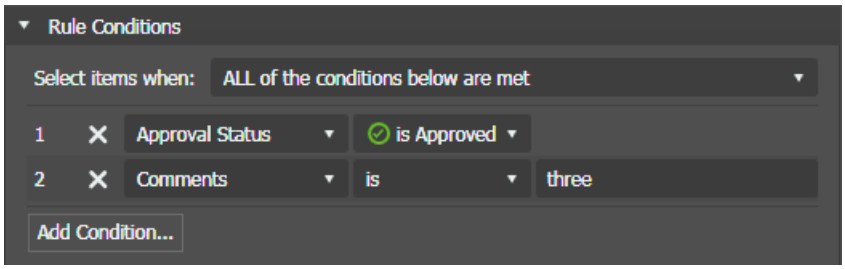
   For Daily, Weekly, and Monthly options, a **Start Time** setting opens. Set the day and time the rule is triggered for the first time.

9. In **Rule Options** settings, specify how the asset is deleted. Select one of the following options:



   - **Delete Material in Scope Only**: Deletes the online material which is present under the selected scope only.
   - **Delete all Online Material**: Deletes online material only.
   - **Delete Entire Asset**: Deletes online material, archived material, published material on social media platforms, and proxy.
   - **Delete Entire Asset (excluding SM-Platforms)**: Deletes online material, archived material, and proxy; except published material on social media platforms.

10. In **Rule Conditions** settings, specify the conditions the Rules Engine looks for to qualify an asset.



11. In the **Select items when** drop down list, select one of the following:

    - **ALL of the conditions below are met**: Assets that match all conditions.
    - **ANY of the conditions below are met**: Assets that match any condition.
    - **Custom**: A Custom Expression field opens in which you can enter a custom expression.

    Conditions and custom expressions are similar to those in GV STRATUS Advanced Search. Simple boolean operators AND, OR, and NOT are supported. Enter these operators in all capital letters.

12. Configure conditions as follows:

    - For each condition (1, 2, 3, 4, etc) click the **Add Condition** button and select from lists to define the condition.
    - Click the **X** button to remove a condition from the list.

    The **is Empty** setting and the period (.) mark are also supported when creating conditions. In case you want to use a 'relative time' (for example the asset 'Modified Date' is before 2 minutes ago) as a rule condition, you should not use rule triggers based on 'Metadata Changes' but use 'periodically' rule triggers only and enter a cycle time (for example 3, 4 or 5 minutes). This is because when a 'relative time' matches the condition, but no metadata change happens at the same time, the rule will not trigger in your operation.

    If a newly created custom metadata field is not available in the **Add Condition** dialog, restart the GV STRATUS Control Panel application.

13. Click **Save**.

Next, enable the rule.

Related Topics

About advanced query syntax, advanced searches and custom expressions on page 423

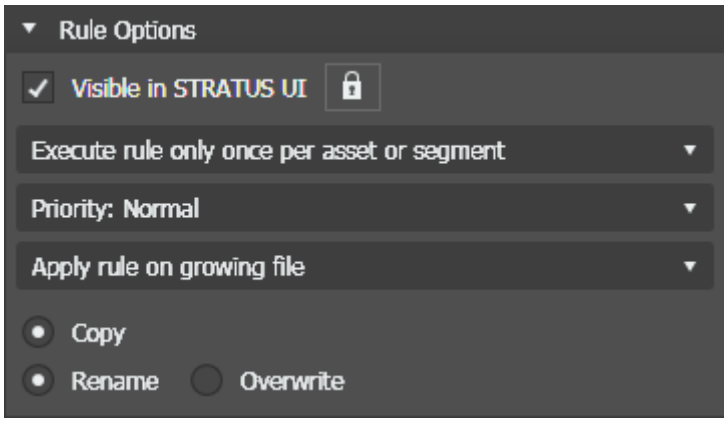
Adding an export rule

The GV STRATUS Rules Engine can watch a source location that is in the GV STRATUS system and export assets that match your criteria to a location that is external to the GV STRATUS system. An export rule can export clips, subclips, and playlists. For playlists, a conform job is automatically triggered to render the complex asset as a simple clip. The Rules Engine exports the assets to the destination that you configure. For an export rule, only K2 storage locations are available as the source scope. Other locations, such as FTP, are not available.

1. Log in to the GV STRATUS Control Panel application with administrator privileges.
2. In the GV STRATUS Control Panel application, click **General | Rules**.

3. Click **Add**.
   Rule Editor settings open.
4. In the **Rule Type** drop-down list select **Export**.
5. In the **Name** field type in a name for the rule you are configuring.
6. In the **Description** field type in a description for the rule you are configuring.

7. In **Rule Options** settings, specify the rule behavior.

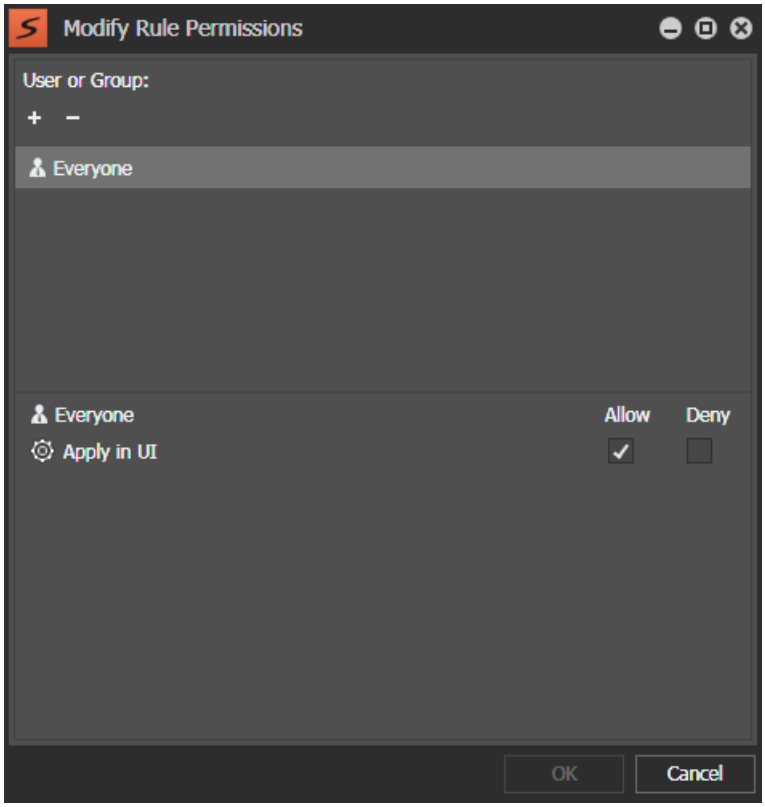


a) Select the **Visible in STRATUS UI** check-box if you want to trigger the rule via context menu in the Asset List panel.

By default, all users can see all rules that had been set to **Visible in STRATUS UI**.

To configure the rule to be only visible to specific user or user groups, click the button.

The Modify Rule Permissions dialog box appears.



To assign permissions, click **+** and enter any user or group in the **Add Users or Groups** dialog box. If necessary, click **Advanced** to open Windows operating system dialog box to find and validate users or groups.

- **+** : Opens the **Add Users or Groups** dialog box to assign users or groups with permissions.
- **-** : Removes a user or group from the list.

After adding specific user or group, set permission for **Apply in UI** setting by selecting **Allow** or **Deny** as appropriate.

b) Select whether the rule copies the asset.

c) Select whether the rule renames or overwrites the asset.

- **Rename**: The rule appends a suffix to the new asset file name. The existing asset is retained.
- **Overwrite**: The new asset overwrites the existing asset. The existing asset is deleted.

d) Select when the rule is applied each asset.

- **Execute rule only once per asset**: The rule is applied once per asset. The Rules Engine uses data stored in the asset's **ExecutedByRules** metadata field to determine if the rule has been applied to the asset. If it has been applied, the Rules Engine does not apply it again, even if the rule criteria still match for the asset.
- **Execute every time rule conditions apply**: The rule can be applied multiple times per asset, if the asset matches rule conditions multiple times.

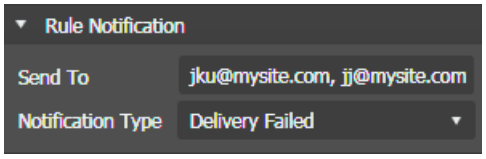
e) Select the priority that the Rules Engine processes the rule, with the transfers and transcodes the rule controls, when there are multiple rules in a queue waiting to be processed.

- **Priority: High**: Put this rule in a queue with other high priority rules and process through the high priority rule queue before any normal priority or low priority rules.
- **Priority: Normal**: Put this rule in a queue with other normal priority rules and process through the normal priority rule queue after any high priority but before any low priority rules.
- **Priority: Low**: Put this rule in a queue with other low priority rules and process through the low priority rule queue after any high priority or medium priority rules.

f) Select the condition when the rule is applied to each asset.

- **Apply rule on growing file**: The rule is applied to all files, including those that are still recording.
- **Apply rule on completed files**: The rule is only applied to files that have finished recording.

8. In **Rule Notification** settings, specify the notification behavior, if desired.



a) Enter email addresses to which emails are sent.

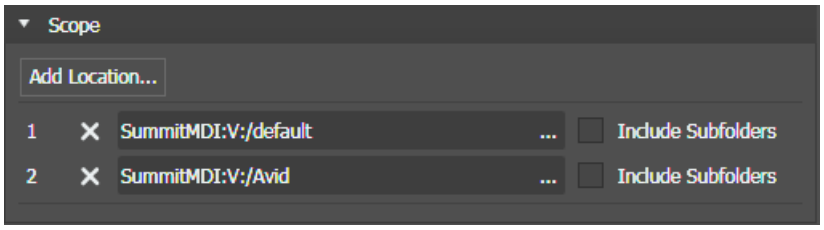
Separate multiple email addresses with a comma.

b) Select one or more notification types:

- **Delivery Failed**: Emails are sent if the rule operation fails.
- **Delivery Completed**: Emails are sent if the rule operation succeeds.

In order to send emails, the email server must be configured in Workflow Engine settings.

9. In **Scope** settings, specify the location or locations in which the rule operates.



a) Click **Add location**.

The **Location Selection** dialog box opens.

b) Navigate to and select the desired location.

You can select multiple locations in the **Location Selection** dialog box.

For Transfer, Export, Custom, Archive, and Transfer to Avid rules, you can also select logical asset locations under **Groups | Lost and Found**.

If desired, you can edit scope location path manually in the text box.

This is the location that contains the files on which the rule operates. Every time the rule runs, it looks in this location to determine if there are any assets that match the rule conditions and then operates on the assets that match.

c) Click **OK**.

The location is added to the **Scope** list.

d) For a location in the list, if you want the rule to operate on sub-folders as well, select **Include Subfolders**.

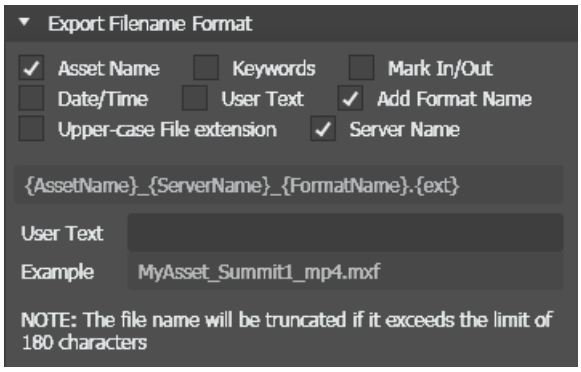
When this is selected, if there are multiple directories under the selected location, the rule operates in each of the sub-directories.

e) Repeat these steps to add additional locations as desired.

f) To change a location in the list, click the **Browse** button ⋯

g) To remove a location from the list, click **X**.

10. In **Export Filename Format** settings, set the convention for the name of the exported file.



a) Select each filename option that you want to be a part of the exported file name.

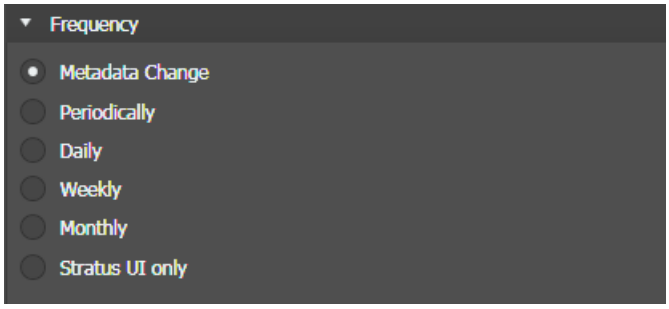
The order in which you select filename options determines the order in which they appear in the file name.

b) Make sure **Add Format Name** is selected if you intend to configure **Export Options** settings for multiple transcode formats.

Multiple transcode formats result in multiple files, so the format must be part of the name to avoid file overwrite. One transcode format results in one file only, so the format is not required as part of the file name.

Asset Name is set by default, as the exported file or files must have a name.

11. In **Frequency** settings, specify how often the Rules Engine triggers the rule.



a) Select one of the following options:

- **Metadata Change**: The rule is constantly monitoring files in the "Scope" folder (and file types depend on the rule condition).
- **Periodically**: Sets the number of minutes.
- **Daily**: Sets the number of days.
- **Weekly**: Sets the number of weeks.
- **Monthly**: Sets the day of each month.
- **STRATUS UI only**: The rule is only applicable when triggered by users via the context menu in Asset List of the STRATUS UI.

For Daily, Weekly, and Monthly options, a **Start Time** setting opens. Set the day and time the rule is triggered for the first time.

12. In **Export Options** settings, configure the format of the exported files.

You can select either a **Native Format** or a **Transcode Format**, but not both.

a) For **Native Format**, select the interchange standard in which to export.

When a **Native Format** is selected, **Transcode Format** is automatically set to None and disabled.

b) For **Transcode Format**, configure as follows:

- Select **None**: The exported file is the same format as the source on the K2 storage system.
- Select one or more transcode formats as follows:
  - Select a single format for the transcoder.
  - To use multiple formats from a single transcoder, select the formats for that transcoder.

  You cannot select multiple transcoders.

To select multiple formats, first make sure that in **Export Filename Format** settings, **Add Format Name** is selected. If **Add Format Name** is not selected, only one transcode format is allowed.

When a **Transcode Format** is selected, **Native Format** is automatically set to None and disabled.

The **Transcode Format** list is populated by the transcode profiles that you create and place in the transcode profile directory.

Supported transcoders include Harmonic ProMedia™ Carbon (formerly Carbon Coder™), Telestream Vantage™, Elemental® , Harmonic WFS, and GVRE Transcoder.

You can also select **STRATUS Native Proxy Format** in the **Transcode Format** list so existing proxy assets can be exported without the need for transcoding.

If no high resolution asset is available, you can still export the proxy asset and XML metadata file from the location in **Groups | Lost and Found**.

c) For **Metadata Format**, select as follows to additionally export an XML metadata file:

- **None**: No additional XML metadata file is exported.
- **Final Cut Pro**: Metadata is exported to a Final Cut Pro project XML file. Set all other Export Options to None to export metadata only.
- **GV STRATUS Simple**: Metadata is exported to a GV STRATUS schema XML file.

These metadata format selections are XSL transforms of the STRATUS XML metadata. If you need a customized transform for your workflow, contact Grass Valley Support.

Set all other Export Options to None to export metadata only.

If you select a metadata format, the **Metadata-Destination Path** field is enabled.

d) For **Metadata-Destination Path**, configure as follows:

- If you are exporting the metadata file to the same destination as the asset file, leave this field blank. The file goes to the path configured in **Destination** settings.
- If you are exporting the metadata file to a different destination than the asset file, enter the metadata file's destination path. For an FTP path, use a `ftp://server/path` convention. For a UNC path, use a `\\server\share\path` convention.

e) If you entered a **Metadata-Destination Path**, configure **User Credentials** for that destination.

f) For **Thumbnails - Marker**, select as follows:

- **None**: The export does not contain thumbnails.
- **Marker Thumbnail Quality - High**: High: The export contains a full-resolution JPG thumbnail with no compression (100%).
- **Marker Thumbnail Quality - Medium**: The export contains a full-resolution JPG thumbnail compressed 85%.
- **Marker Thumbnail Quality - Low**: Low: The export contains a half-resolution JPG thumbnail compressed 70%.
- **Reference Thumbnail Quality - High**: High: The export contains a key-frame marker with full-resolution JPG thumbnail of no compression (100%).
- **Reference Thumbnail Quality - Medium**: The export contains a key-frame marker with full-resolution JPG thumbnail compressed 85%.
- **Reference Thumbnail Quality - Low**: Low: The export contains a key-frame marker with half-resolution JPG thumbnail compressed 70%.

An export thumbnail is defined by a `tn` marker added to the source asset. Multiple thumbnails are exported when the source asset has multiple `tn` markers. Additionally the default or user defined thumbnail can be exported. Exported thumbnail files are automatically named according to asset names with the timecode extension **_hh-mm-ss-ff** so that each JPG file can be differentiated. The first exported thumbnail JPG file has the same name as the asset.

g) For **Closed Caption Format**, select as follows:

- **None**: No additional Close Caption file is exported.
- **K2-SCC**: Workflow Engine extracts CEA-608 information stored in Ancillary data (CEA-708) from the asset on the K2 system and exports to a file in SCC format.
- **K2-SRT**: Workflow Engine extracts CEA-608 information stored in Ancillary data (CEA-708) from the asset on the K2 system and exports to a file in SRT format.
- **K2-TTML**: Workflow Engine extracts CEA-608 information stored in Ancillary data (CEA-708) from the asset on the K2 system and exports to a file in TTML format.

Only K2 system metadata extraction is recommended. It has much better performance than transcoder metadata extraction.

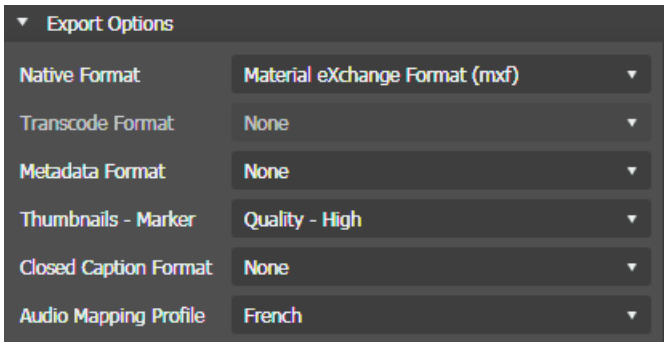
If you select a Closed Caption format, the **CC-Destination Path** field is enabled.

h) For **CC-Destination Path**, configure as follows:

- If you are exporting the Closed Caption file to the same destination as the asset file, leave this field blank. The file goes to the path configured in **Destination** settings.
- If you are exporting the Closed Caption file to a different destination than the asset file, enter the Closed Caption file's destination path. For an FTP path, use a `ftp://server/path` convention. For a UNC path, use a `\\server\share\path` convention.

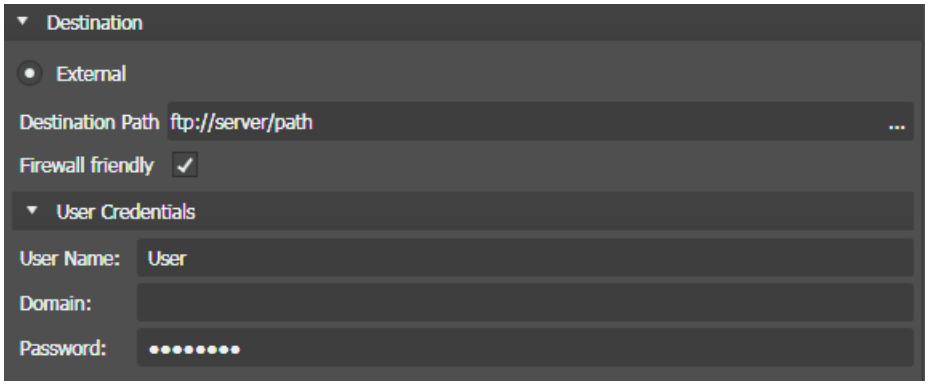
i) If you entered a **CC-Destination Path**, configure **User Credentials** for that destination.

j) For **Audio Mapping Profile**, configure as follows:



- The Native Format setting must be set to **Material eXchange Format (mxf)**. If set to any other format, the Audio Mapping Profile drop-down list is not selectable.
- Audio Mapping Profiles must have been configured in the Audio Tag Management setting of GV STRATUS Control Panel prior to configuring rules.
- If you want to transfer content with a subset of the existing audio tracks to Avid, you can configure an existing Audio Mapping Profile to the locations configuration.

13. In **Destination** settings, define the destination location on which the rule operates.



For Export rules, the destination must be a location that is external to the GV STRATUS system and not managed by the GV STRATUS system. An external location is not visible in the GV STRATUS application Navigator panel.

You can set any destinations for exports as follows:

- **FTP path**: `ftp://server/path`
- **UNC path**: `\\server\share\path`
- **FASP path**: `fasp://<Aspera server>/<directory name>`

If the destination is a network share accessible from the machine hosting the GV STRATUS Control Panel application, you can click the **Browse** button ··· to configure **Destination Path**.

The **Firewall friendly** checkbox is only visible if the selected **Native Format** is GXF or MXF, and FTP path is entered as the destination path. If the **Firewall friendly** checkbox is selected, asset transfer will be performed by the Data Mover engine. If not selected, asset transfer will be performed by K2 Summit.

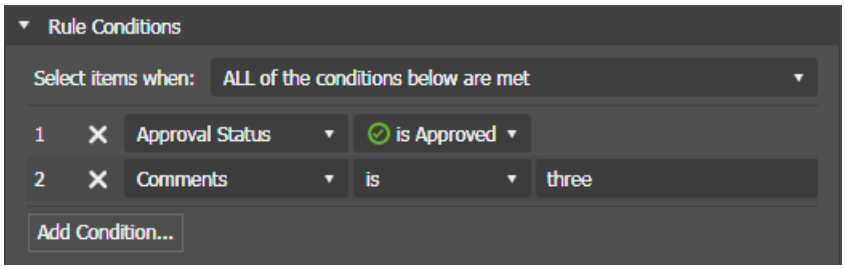
14. Configure **User Credentials** as required.

    If a UNC path destination, requirements for user credentials are as follows:

    - If both the K2 system and the export location are on the same domain, you can use domain credentials.
    - If the K2 system and the export location are on different domains and the domains have a trust relationship, you can use domain credentials.
    - If the K2 system and the export location both have a local user with the same name and password, you can use the local user credentials.

    Other UNC path user credentials are not supported.

15. In **Rule Conditions** settings, specify the conditions the Rules Engine looks for to qualify an asset.



16. In the **Select items when** drop down list, select one of the following:

    - **ALL of the conditions below are met**: Assets that match all conditions.
    - **ANY of the conditions below are met**: Assets that match any condition.
    - **Custom**: A Custom Expression field opens in which you can enter a custom expression.

    Conditions and custom expressions are similar to those in GV STRATUS Advanced Search. Simple boolean operators AND, OR, and NOT are supported. Enter these operators in all capital letters.

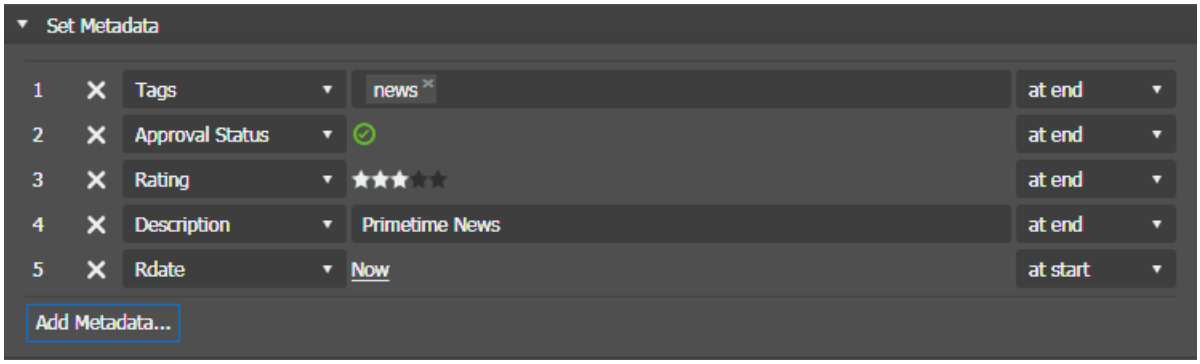
17. Configure conditions as follows:

    - For each condition (1, 2, 3, 4, etc) click the **Add Condition** button and select from lists to define the condition.
    - Click the **X** button to remove a condition from the list.

    The **is Empty** setting and the period (.) mark are also supported when creating conditions. In case you want to use a ‘relative time’ (for example the asset ‘Modified Date’ is before 2 minutes ago) as a rule condition, you should not use rule triggers based on ‘Metadata Changes’ but use ‘periodically’ rule triggers only and enter a cycle time (for example 3, 4 or 5 minutes). This is because when a ‘relative time' matches the condition, but no metadata change happens at the same time, the rule will not trigger in your operation.

    If a newly created custom metadata field is not available in the **Add Condition** dialog, restart the GV STRATUS Control Panel application.

18. In **Set Metadata** settings, define the metadata that Rules Engine will set during the execution of a rule for an asset.



19. Configure metadata as follows:

- For each metadata, click the **Add Metadata** button and select from the drop-down list to select the metadata.
- Define the metadata value which will be added into the data field of the asset when the rule is applied to.
- Select whether to enter the metadata value at the start or the end of the rule workflow.
- Click the **X** button to remove a metadata from the list.

If a newly created custom metadata field is not available in the drop-down list, restart the GV STRATUS Control Panel application.

You can create new custom metadata by selecting **Core | Metadata | Custom Metadata | Add** in the GV STRATUS Control Panel.

20. Click **Save**.

In the exported content, custom metadata values entered here replace any current values. So if you previously entered values for these same custom metadata fields elsewhere in the GV STRATUS system, those values are overwritten in the exported content by the values you enter here.

Next, enable the rule.

Related Topics

Adding a Carbon Coder transcode profile on page 643
Adding a Vantage transcode profile on page 647
Adding an Elemental transcode profile on page 648
Adding a thumbnail marker on page 643
About advanced query syntax, advanced searches and custom expressions on page 423
Adding a Carbon Coder transcode profile on page 643

Adding an import rule

The GV STRATUS Rules Engine can watch a source location that is external to the GV STRATUS system and when files arrive, import the files that match your criteria to a location that is in the GV STRATUS system. An import rule can transcode, as well as import metadata, as part of the import. The imported asset has a metadata field that specifies the source location from which it was imported.

Any SMB location can be used for importing media. If you want to use FTP, the same location must be exposed using the SMB protocol. For example, you can install an FTP server pointing to the location which is already accessible via SMB.

After the import operation, the Rules Engine changes the name of the original source file, adding a suffix that indicates success or failure. The Rules Engine periodically deletes files more than seven days old, as a housekeeping operation.

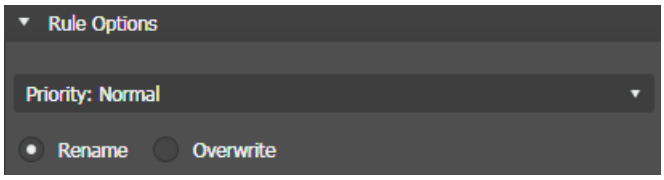
GV STRATUS implements file name length limits for import rules as below to honor the limitations of standard Windows File Systems (248 characters) and the K2 Summit Video server (~110 characters).

1. Import rules will ignore files that have been delivered with a file path including file name length above *210 characters*.
2. Files that have been imported with the pure file name length longer than 110 characters will be imported into the system but will be truncated. The file name/asset name length will be truncated to approximately 110 characters. The original source-filename will be saved in the assets metadata *description* field.

1. Log in to the GV STRATUS Control Panel application with administrator privileges.
2. In the GV STRATUS Control Panel application, click **General | Rules**.
3. Click **Add**.

   Rule Editor settings open.
4. In the **Rule Type** drop-down list select **Import**.
5. In the **Name** field type in a name for the rule you are configuring.
6. In the **Description** field type in a description for the rule you are configuring.

7. In **Rule Options** settings, specify the rule behavior.



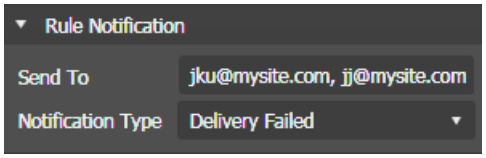
   a) Select the priority that the Rules Engine processes the rule, with the transfers and transcodes the rule controls, when there are multiple rules in a queue waiting to be processed.

      - **Priority: High**: Put this rule in a queue with other high priority rules and process through the high priority rule queue before any normal priority or low priority rules.
      - **Priority: Normal**: Put this rule in a queue with other normal priority rules and process through the normal priority rule queue after any high priority but before any low priority rules.
      - **Priority: Low**: Put this rule in a queue with other low priority rules and process through the low priority rule queue after any high priority or medium priority rules.

   b) If an asset of the same name already exists at the destination location, configure the rule behavior:

      - **Rename**: A suffix is appended to the imported asset name. The existing asset is retained.
      - **Overwrite**: The imported asset overwrites the existing asset. The existing asset is deleted. If the GV STRATUS system does not allow the existing asset to be deleted, the import fails. For example, if the asset has a subclip, the GV STRATUS system does not allow the existing asset to be deleted.

8. In **Rule Notification** settings, specify the notification behavior, if desired.



   a) Enter email addresses to which emails are sent.

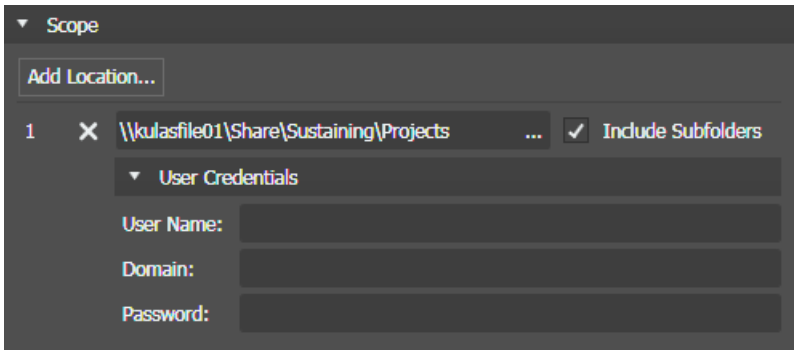
      Separate multiple email addresses with a comma.

   b) Select one or more notification types:

      - **Delivery Failed**: Emails are sent if the rule operation fails.
      - **Delivery Completed**: Emails are sent if the rule operation succeeds.

   In order to send emails, the email server must be configured in Workflow Engine settings.

9. In **Scope** settings, specify the source location or locations the rule watches.



   a) Click **Add location**.

      The **Location Selection** dialog box opens.

   b) Navigate to and select the desired SMB location.

      This is the location that contains the files on which the rule operates. Every time the rule runs, it looks in this location to determine if there are any new files that match the rule conditions and then operates on the files that match.

   c) Click **OK**

      The location is added to the **Scope** list.

   d) For a location in the list, if you want the rule to operate on sub-folders as well, select **Include Subfolders**.

      When this is selected, if there are multiple directories under the selected location, the rule operates in each of the sub-directories.

   e) Repeat these steps to add additional locations as desired.

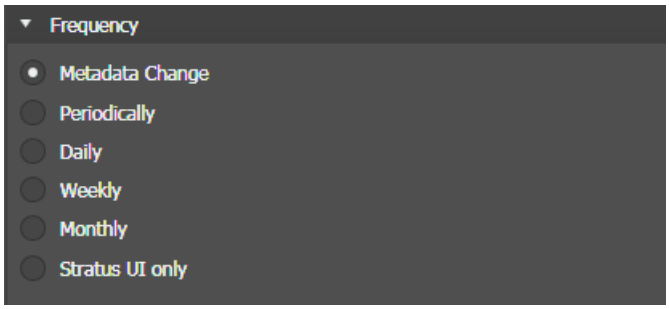
   f) To change a location in the list, click the **Browse** button ···

   g) To remove a location from the list, click **X**.

   Consider system load when configuring multiple import locations. An example guideline for a small GV STRATUS system, such as an Express system, is that you do not exceed ten import locations.

10. Configure **User Credentials** as required for the source locations.

11. In **Frequency** settings, specify how often the Rules Engine triggers the rule.

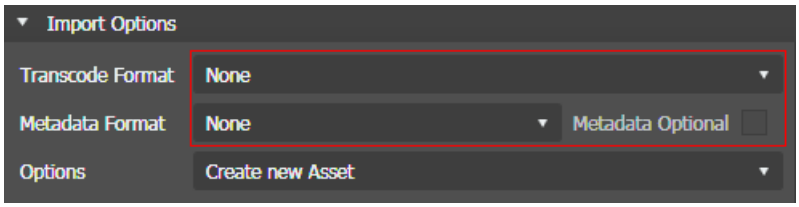


a) Select one of the following options:

- **Metadata Change**: The rule is constantly monitoring files in the “Scope” folder (and file types depend on the rule condition).
- **Periodically**: Sets the number of minutes.
- **Daily**: Sets the number of days.
- **Weekly**: Sets the number of weeks.
- **Monthly**: Sets the day of each month.
- **STRATUS UI only**: The rule is only applicable when triggered by users via the context menu in Asset List of the STRATUS UI.

For Daily, Weekly, and Monthly options, a **Start Time** setting opens. Set the day and time the rule is triggered for the first time.

12. In **Import Options** settings, configure the format of the imported assets.



a) For **Transcode Format**, select as follows:

- **None**: Metadata only is imported. Media essence is not imported. If selected, a Metadata Format must be selected.
- **Native**: The files to be imported are in a format supported by the K2 and GV STRATUS system, such as GXF, MXF, MOV, MPG (PS), etc.
- **<format>**: As available for your transcode format, the file is transcoded to the selected format.

Supported transcoders include Harmonic ProMedia™ Carbon (formerly Carbon Coder™), Telestream Vantage™, Elemental® , Harmonic WFS, Avid MEWS, and GVRE Transcoder.

The list is populated by the transcode profiles that you create and place in the transcode profile directory. For import rules, the profile must be a format supported by the K2 and GV STRATUS system and the profile name must have the prefix `Import_`, such as `Import_HD_MXF-D10_NTSC_50.PCP`.

b) For **Metadata Format**, select as follows:

- **None**: No metadata is imported.
- **GV STRATUS Simple Import**: Metadata is imported from a GV STRATUS schema XML metadata file named the same as the media file. If custom metadata is included in the metadata file, those custom metadata fields must be configured in the GV STRATUS system. If the fields are not configured, the custom metadata is not imported.

If a metadata format is selected, the **Metadata Optional** setting is enabled.

c) If enabled, select **Metadata Optional** to specify the following behavior:

- If the media file and metadata file are present, the import operation begins immediately and imports the metadata.
- If the media file is present and the metadata file is not present, the import operation waits 30 seconds.
  - If the metadata file arrives within 30 seconds, the import operation begins and imports the metadata.
  - If the metadata file does not arrive within 30 seconds, the import operation begins and no metadata is imported.
- If the media file is not present and the metadata file is present, the Rules Engine waits 24 hours.
  - If the media file arrives within 24 hours, the import operation begins and imports the media and the metadata.
  - If the media file does not arrive within 24 hours, the Rules Engine renames the metadata file and ignores it for future import rule operations.

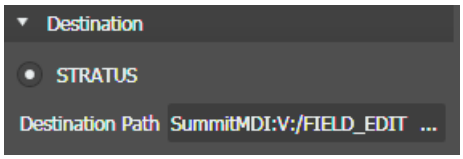
If **Metadata Optional** is not selected, the import operation fails if both media and metadata files are not present.

d) For **Options**, select as follows:

- **Create New Asset**: A GV STRATUS asset is created for the imported material. If metadata only is imported, a metadata-only asset is created.
- **Update Asset Metadata**: The imported metadata updates the metadata and essence of an existing asset.

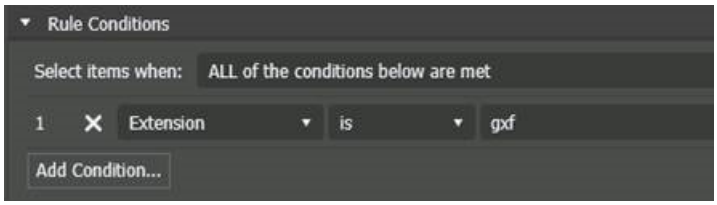
For more information about importing metadata, refer to related topics in this Topic Library.

13. In **Destination** settings, specify the destination of the assets on which the rule operates.



The destination must be a location in the GV STRATUS system. This is a location that is in the GV STRATUS application Navigator panel under the Locations node.

14. In **Rule Conditions** settings, specify the conditions the Rules Engine *File System Watcher* looks for to qualify the essence material to be imported into GV STRATUS as a new asset.



Considerations regarding **Rule Conditions** are as follows:

- **Supported native essence types**: GXF, MXF and MOV.
- **Other video/audio formats**: Transcoding is required for other video/audio formats to be imported into GV STRATUS. If needed, the GVRE Transcoder or a third party transcoder (such as Harmonic, Telestream, Elemental) could be added to convert the source file first into a supported high-resolution format.
- **Update Asset Metadata**: To update metadata for an existing GV STRATUS asset, a GV STRATUS compliant XML format must be provided. Then, the **Rule Condition** must be set to search for files with "XML" extension to trigger the import rule.

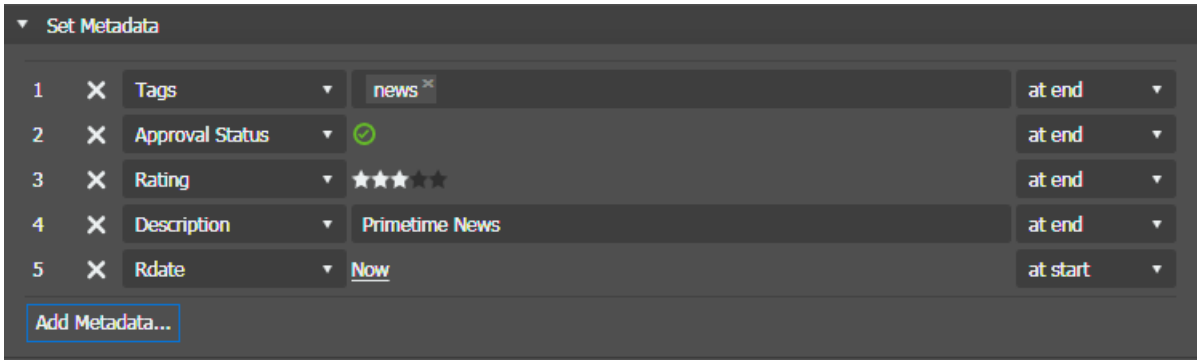
For example, segments and segmentations can be updated via the GV STRATUS schema XML metadata file. Segments are identified by name, type, in, and out; while segmentations are identified by name and type in the XML metadata file. If there is a change specified in the metadata file, it will be updated via the import rule.

15. In the **Select items when** drop down list, select one of the following:

    - **ALL of the conditions below are met**: Assets that match all conditions.
    - **ANY of the conditions below are met**: Assets that match any condition.
    - **Custom**: A Custom Expression field opens in which you can enter a custom expression.

    Conditions and custom expressions are similar to those in GV STRATUS Advanced Search. Simple boolean operators AND, OR, and NOT are supported. Enter these operators in all capital letters.

16. In **Set Metadata** settings, define the metadata that Rules Engine will set during the execution of a rule for an asset.



17. Configure metadata as follows:

    - For each metadata, click the **Add Metadata** button and select from the drop-down list to select the metadata.
    - Define the metadata value which will be added into the data field of the asset when the rule is applied to.
    - Select to apply the metadata value only at the end of the rule workflow. For import rules, the Set Metadata setting only supports the metadata value at the end of the workflow since no asset exists in GV STRATUS yet at the beginning of import.
    - Click the **X** button to remove a metadata from the list.

    If a newly created custom metadata field is not available in the drop-down list, restart the GV STRATUS Control Panel application.

    You can create new custom metadata by selecting **Core | Metadata | Custom Metadata | Add** in the GV STRATUS Control Panel.

18. Click **Save**.

Next, enable the rule.

Related Topics

Adding a Carbon Coder transcode profile on page 643
Adding a Vantage transcode profile on page 647
Adding an Elemental transcode profile on page 648
Importing metadata to create or update assets on page 653

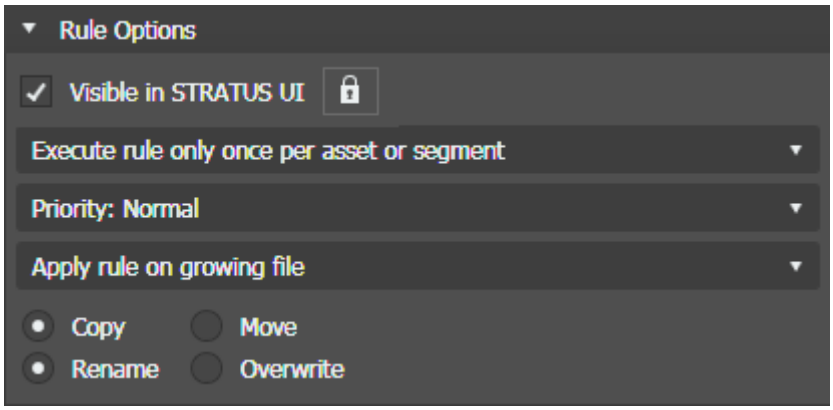
Adding a transfer rule

The GV STRATUS Rules Engine can watch a source location that is in the GV STRATUS system and transfer assets that match your criteria to a destination location that is also in the GV STRATUS system. The Rules Engine transfers the assets to the destination that you configure. For playlists, a conform job is automatically triggered to render the complex asset as a simple clip at the destination.

1. Log in to the GV STRATUS Control Panel application with administrator privileges.
2. In the GV STRATUS Control Panel application, click **General | Rules**.
3. Click **Add**.

   Rule Editor settings open.
4. In the **Rule Type** drop-down list select **Transfer**.
5. In the **Name** field type in a name for the rule you are configuring.
6. In the **Description** field type in a description for the rule you are configuring.

7. In **Rule Options** settings, specify the rule behavior.

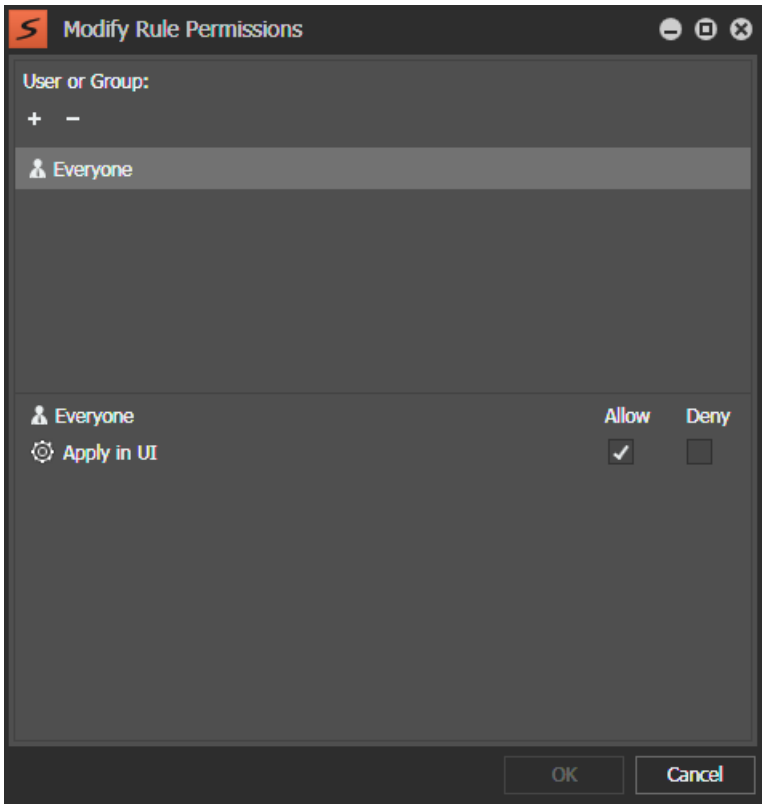


a) Select the **Visible in STRATUS UI** check-box if you want to trigger the rule via context menu in the Asset List panel.

By default, all users can see all rules that had been set to **Visible in STRATUS UI**.

To configure the rule to be only visible to specific user or user groups, click the button.

The Modify Rule Permissions dialog box appears.



To assign permissions, click **+** and enter any user or group in the **Add Users or Groups** dialog box. If necessary, click **Advanced** to open Windows operating system dialog box to find and validate users or groups.

- **+** : Opens the **Add Users or Groups** dialog box to assign users or groups with permissions.

- **-** : Removes a user or group from the list.

After adding specific user or group, set permission for **Apply in UI** setting by selecting **Allow** or **Deny** as appropriate.

b) Select whether the rule copies or moves the asset.

If you select **Move**, after the rule transfers the asset, it removes the source asset from the GV STRATUS system.

c) Select whether the rule renames or overwrites the asset.

- **Rename**: The rule appends a suffix to the new asset file name. The existing asset is retained.
- **Overwrite**: The new asset overwrites the existing asset. The existing asset is deleted.

d) Select when the rule is applied each asset.

- **Execute rule only once per asset**: The rule is applied once per asset. The Rules Engine uses data stored in the asset's **ExecutedByRules** metadata field to determine if the rule has been applied to the asset. If it has been applied, the Rules Engine does not apply it again, even if the rule criteria still match for the asset.
- **Execute every time rule conditions apply**: The rule can be applied multiple times per asset, if the asset matches rule conditions multiple times.

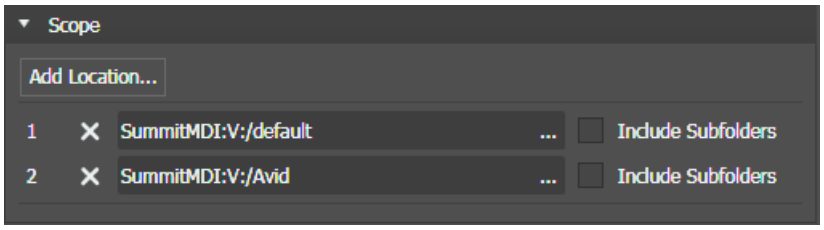
e) Select the priority that the Rules Engine processes the rule, with the transfers and transcodes the rule controls, when there are multiple rules in a queue waiting to be processed.

- **Priority: High**: Put this rule in a queue with other high priority rules and process through the high priority rule queue before any normal priority or low priority rules.
- **Priority: Normal**: Put this rule in a queue with other normal priority rules and process through the normal priority rule queue after any high priority but before any low priority rules.
- **Priority: Low**: Put this rule in a queue with other low priority rules and process through the low priority rule queue after any high priority or medium priority rules.

f) Select the condition when the rule is applied to each asset.

- **Apply rule on growing file**: The rule is applied to all files, including those that are still recording.
- **Apply rule on completed files**: The rule is only applied to files that have finished recording.

8. In **Scope** settings, specify the location or locations in which the rule operates.



a) Click **Add location**.

The **Location Selection** dialog box opens.

b) Navigate to and select the desired location.

You can select multiple locations in the **Location Selection** dialog box.

For Transfer, Export, Custom, Archive, and Transfer to Avid rules, you can also select logical asset locations under **Groups | Lost and Found**.

If desired, you can edit scope location path manually in the text box.

This is the location that contains the files on which the rule operates. Every time the rule runs, it looks in this location to determine if there are any assets that match the rule conditions and then operates on the assets that match.

c) Click **OK**.

The location is added to the **Scope** list.

d) For a location in the list, if you want the rule to operate on sub-folders as well, select **Include Subfolders**.

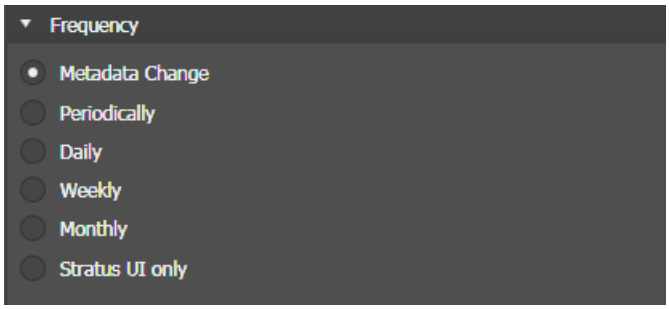
When this is selected, if there are multiple directories under the selected location, the rule operates in each of the sub-directories.

e) Repeat these steps to add additional locations as desired.

f) To change a location in the list, click the **Browse** button ···

g) To remove a location from the list, click **X**.

9. In **Frequency** settings, specify how often the Rules Engine triggers the rule.



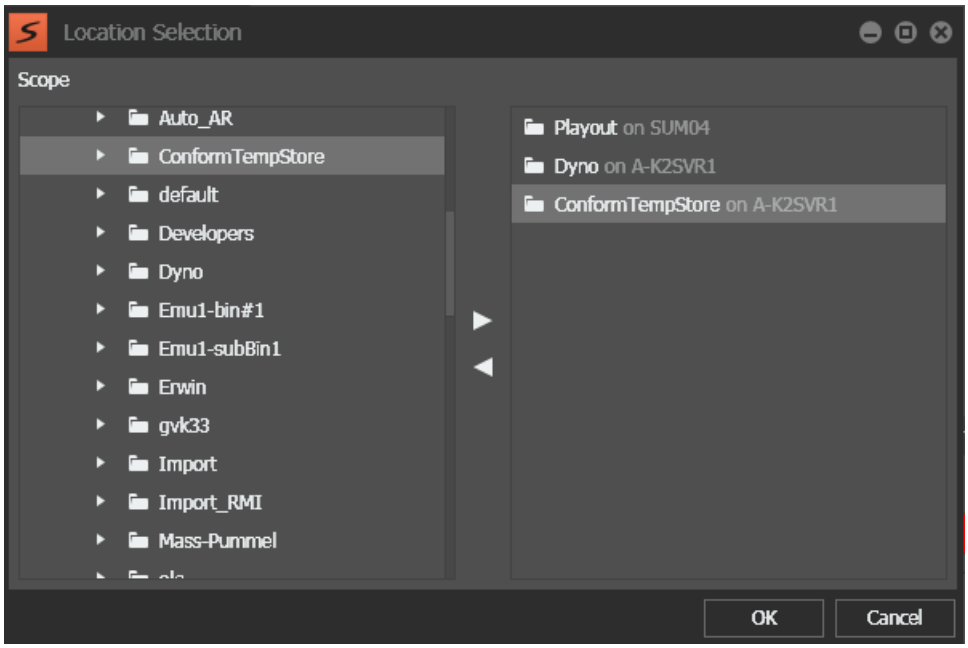
a) Select one of the following options:

- **Metadata Change**: The rule is constantly monitoring files in the “Scope” folder (and file types depend on the rule condition).
- **Periodically**: Sets the number of minutes.
- **Daily**: Sets the number of days.
- **Weekly**: Sets the number of weeks.
- **Monthly**: Sets the day of each month.
- **STRATUS UI only**: The rule is only applicable when triggered by users via the context menu in Asset List of the STRATUS UI.

For Daily, Weekly, and Monthly options, a **Start Time** setting opens. Set the day and time the rule is triggered for the first time.

10. In **Destination** settings, click **Add location** to specify the destination of the assets on which the rule operates.

    The **Location Selection** dialog box opens.



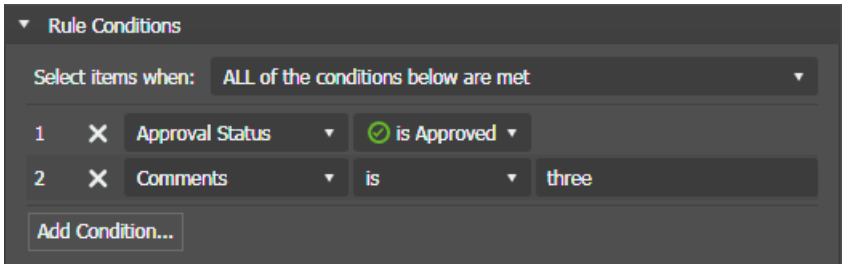
    The destination must be a location in the GV STRATUS system. This is a location that is in the GV STRATUS application Navigator panel under the Locations node.

    You can select multiple locations in the **Location Selection** dialog box, if desired. When multiple locations are selected, you are not allowed to select **Move** in the Rule Options section. However **Copy, Rename, and Overwite** options are available when you want to transfer to multiple destinations. You can only move single assets via the transfer rule.

11. For Destination Path, click the **Browse** button ⋯.

    The Select Destination Path dialog box opens.

12. Navigate to the desired location and click **OK**.
13. In **Rule Conditions** settings, specify the conditions the Rules Engine looks for to qualify an asset.



14. In the **Select items when** drop down list, select one of the following:

    - **ALL of the conditions below are met**: Assets that match all conditions.
    - **ANY of the conditions below are met**: Assets that match any condition.
    - **Custom**: A Custom Expression field opens in which you can enter a custom expression.

    Conditions and custom expressions are similar to those in GV STRATUS Advanced Search. Simple boolean operators AND, OR, and NOT are supported. Enter these operators in all capital letters.

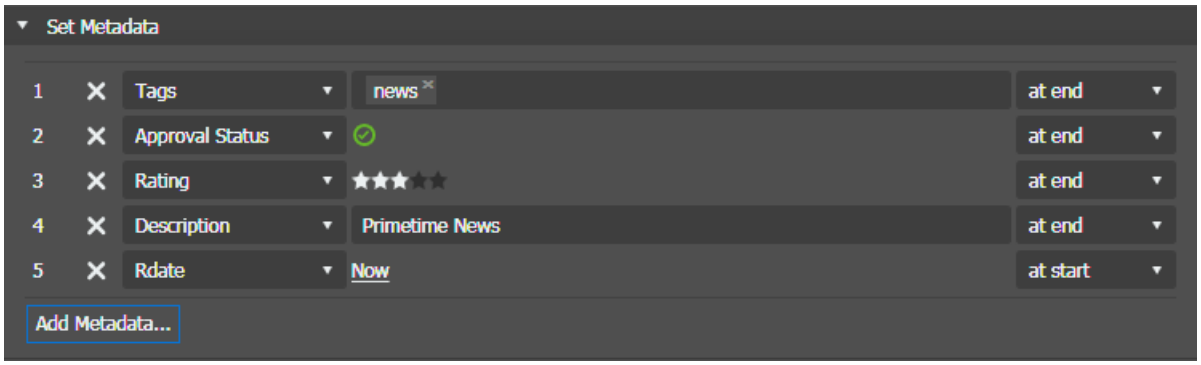
15. Configure conditions as follows:

    - For each condition (1, 2, 3, 4, etc) click the **Add Condition** button and select from lists to define the condition.
    - Click the **X** button to remove a condition from the list.

    The **is Empty** setting and the period (.) mark are also supported when creating conditions. In case you want to use a 'relative time' (for example the asset 'Modified Date' is before 2 minutes ago) as a rule condition, you should not use rule triggers based on 'Metadata Changes' but use 'periodically' rule triggers only and enter a cycle time (for example 3, 4 or 5 minutes). This is because when a 'relative time' matches the condition, but no metadata change happens at the same time, the rule will not trigger in your operation.

    If a newly created custom metadata field is not available in the **Add Condition** dialog, restart the GV STRATUS Control Panel application.

16. In **Set Metadata** settings, define the metadata that Rules Engine will set during the execution of a rule for an asset.



17. Configure metadata as follows:

    - For each metadata, click the **Add Metadata** button and select from the drop-down list to select the metadata.
    - Define the metadata value which will be added into the data field of the asset when the rule is applied to.
    - Select whether to enter the metadata value at the start or the end of the rule workflow.
    - Click the **X** button to remove a metadata from the list.

    If a newly created custom metadata field is not available in the drop-down list, restart the GV STRATUS Control Panel application.

    You can create new custom metadata by selecting **Core | Metadata | Custom Metadata | Add** in the GV STRATUS Control Panel.

18. Click **Save**.

Next, enable the rule.

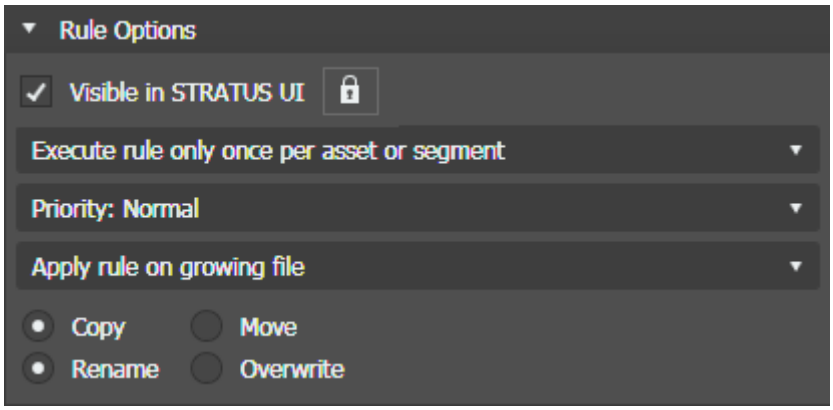
Adding an archive rule

The GV STRATUS Rules Engine can watch a location that is in the GV STRATUS system and transfer assets that match your criteria to an archive location. An archive rule can export clips, subclips, and playlists. For playlists, a conform job is automatically triggered to render the complex asset as a simple clip. The Rules Engine transfers the assets to the destination that you configure.

1. Log in to the GV STRATUS Control Panel application with administrator privileges.
2. In the GV STRATUS Control Panel application, click **General | Rules**.
3. Click **Add**.

   Rule Editor settings open.
4. In the **Rule Type** drop-down list select **Archive**.
5. In the **Name** field type in a name for the rule you are configuring.
6. In the **Description** field type in a description for the rule you are configuring.

7. In **Rule Options** settings, specify the rule behavior.

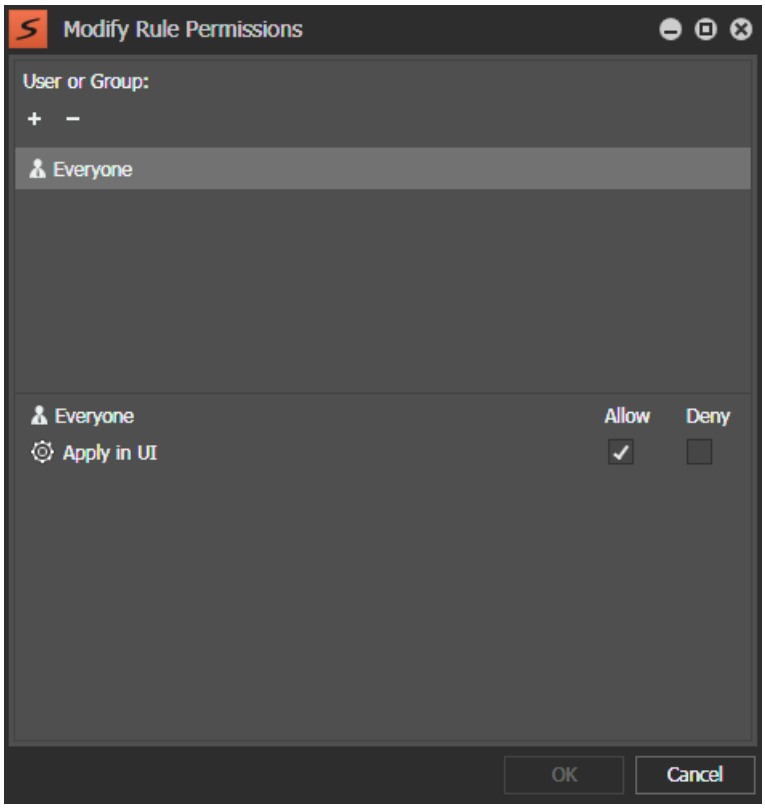


a) Select the **Visible in STRATUS UI** check-box if you want to trigger the rule via context menu in the Asset List panel.

By default, all users can see all rules that had been set to **Visible in STRATUS UI**.

To configure the rule to be only visible to specific user or user groups, click the button.

The Modify Rule Permissions dialog box appears.



To assign permissions, click **+** and enter any user or group in the **Add Users or Groups** dialog box. If necessary, click **Advanced** to open Windows operating system dialog box to find and validate users or groups.

- **+** : Opens the **Add Users or Groups** dialog box to assign users or groups with permissions.

- **-** : Removes a user or group from the list.

After adding specific user or group, set permission for **Apply in UI** setting by selecting **Allow** or **Deny** as appropriate.

b) Select whether the rule copies or moves the asset.

If you select **Move**, after the rule transfers the asset, it removes the source asset from the GV STRATUS system.

c) Select whether the rule renames or overwrites the asset.

- **Rename**: The rule appends a suffix to the new asset file name. The existing asset is retained.
- **Overwrite**: The new asset overwrites the existing asset. The existing asset is deleted.

d) Select when the rule is applied each asset.

- **Execute rule only once per asset**: The rule is applied once per asset. The Rules Engine uses data stored in the asset's **ExecutedByRules** metadata field to determine if the rule has been applied to the asset. If it has been applied, the Rules Engine does not apply it again, even if the rule criteria still match for the asset.
- **Execute every time rule conditions apply**: The rule can be applied multiple times per asset, if the asset matches rule conditions multiple times.

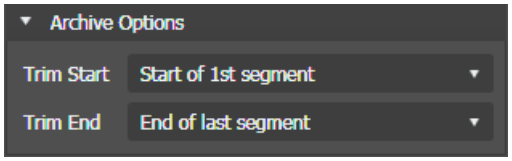
e) Select the priority that the Rules Engine processes the rule, with the transfers and transcodes the rule controls, when there are multiple rules in a queue waiting to be processed.

- **Priority: High**: Put this rule in a queue with other high priority rules and process through the high priority rule queue before any normal priority or low priority rules.
- **Priority: Normal**: Put this rule in a queue with other normal priority rules and process through the normal priority rule queue after any high priority but before any low priority rules.
- **Priority: Low**: Put this rule in a queue with other low priority rules and process through the low priority rule queue after any high priority or medium priority rules.

f) Select the condition when the rule is applied to each asset.

- **Apply rule on growing file**: The rule is applied to all files, including those that are still recording.
- **Apply rule on completed files**: The rule is only applied to files that have finished recording.

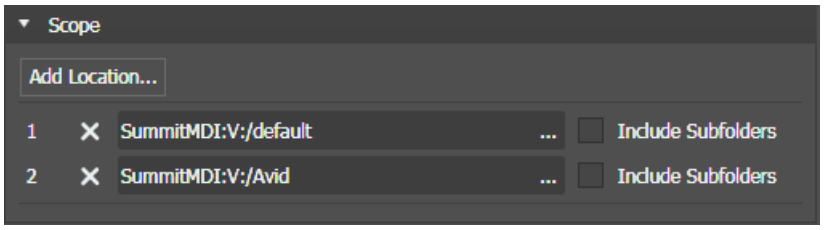
8. In **Archive Options** settings, specify the rule behavior if you only want to archive partial of the asset.



- **Trim Start**: Select the start of the segment to be archived.
- **Trim End**: Select the end of the segment to be archived.

NOTE: When this rule is applied to assets, assumed segments are existing, then the duration of the STRATUS asset is automatically adjusted.

9. In **Scope** settings, specify the location or locations in which the rule operates.



For archive rules, only valid K2 system locations are available.

a) Click **Add location**.

The **Location Selection** dialog box opens.

b) Navigate to and select the desired location.

You can select multiple locations in the **Location Selection** dialog box.

For Transfer, Export, Custom, Archive, and Transfer to Avid rules, you can also select logical asset locations under **Groups | Lost and Found**.

If desired, you can edit scope location path manually in the text box.

This is the location that contains the files on which the rule operates. Every time the rule runs, it looks in this location to determine if there are any assets that match the rule conditions and then operates on the assets that match.

c) Click **OK**.

The location is added to the **Scope** list.

d) For a location in the list, if you want the rule to operate on sub-folders as well, select **Include Subfolders**.

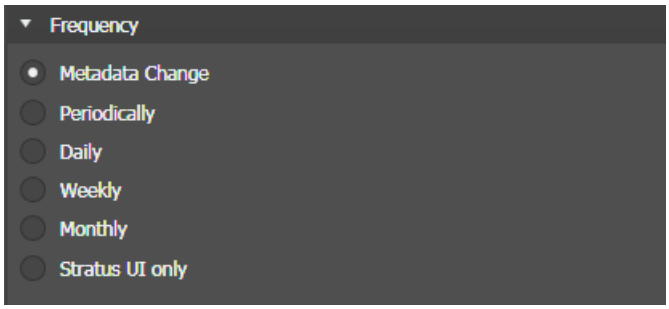
When this is selected, if there are multiple directories under the selected location, the rule operates in each of the sub-directories.

e) Repeat these steps to add additional locations as desired.

f) To change a location in the list, click the **Browse** button ⋯

g) To remove a location from the list, click **X**.

10. In **Frequency** settings, specify how often the Rules Engine triggers the rule.

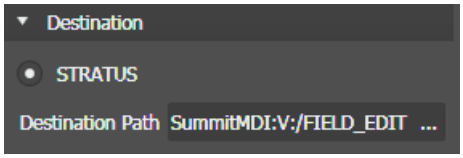


a) Select one of the following options:

- **Metadata Change**: The rule is constantly monitoring files in the "Scope" folder (and file types depend on the rule condition).
- **Periodically**: Sets the number of minutes.
- **Daily**: Sets the number of days.
- **Weekly**: Sets the number of weeks.
- **Monthly**: Sets the day of each month.
- **STRATUS UI only**: The rule is only applicable when triggered by users via the context menu in Asset List of the STRATUS UI.

For Daily, Weekly, and Monthly options, a **Start Time** setting opens. Set the day and time the rule is triggered for the first time.

11. In **Destination** settings, specify the destination of the assets on which the rule operates.



The destination must be a location in the GV STRATUS system. This is a location that is in the GV STRATUS application Navigator panel under the Locations node.

12. For Destination Path, click the **Browse** button ···.

The Select Destination Path dialog box opens.

13. Navigate to the desired location and click **OK**.
14. In **Rule Conditions** settings, specify the conditions the Rules Engine looks for to qualify an asset.

15. In the **Select items when** drop down list, select one of the following:

    - **ALL of the conditions below are met**: Assets that match all conditions.
    - **ANY of the conditions below are met**: Assets that match any condition.
    - **Custom**: A Custom Expression field opens in which you can enter a custom expression.

    Conditions and custom expressions are similar to those in GV STRATUS Advanced Search. Simple boolean operators AND, OR, and NOT are supported. Enter these operators in all capital letters.

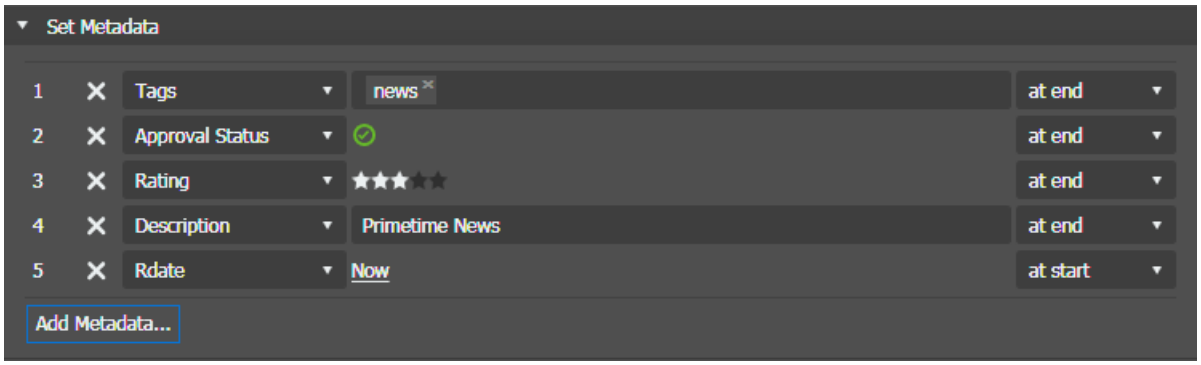
16. Configure conditions as follows:

    - For each condition (1, 2, 3, 4, etc) click the **Add Condition** button and select from lists to define the condition.
    - Click the **X** button to remove a condition from the list.

    The **is Empty** setting and the period (.) mark are also supported when creating conditions. In case you want to use a 'relative time' (for example the asset 'Modified Date' is before 2 minutes ago) as a rule condition, you should not use rule triggers based on 'Metadata Changes' but use 'periodically' rule triggers only and enter a cycle time (for example 3, 4 or 5 minutes). This is because when a 'relative time' matches the condition, but no metadata change happens at the same time, the rule will not trigger in your operation.

    If a newly created custom metadata field is not available in the **Add Condition** dialog, restart the GV STRATUS Control Panel application.

17. In **Set Metadata** settings, define the metadata that Rules Engine will set during the execution of a rule for an asset.



18. Configure metadata as follows:

    - For each metadata, click the **Add Metadata** button and select from the drop-down list to select the metadata.
    - Define the metadata value which will be added into the data field of the asset when the rule is applied to.
    - Select whether to enter the metadata value at the start or the end of the rule workflow.
    - Click the **X** button to remove a metadata from the list.

    If a newly created custom metadata field is not available in the drop-down list, restart the GV STRATUS Control Panel application.

    You can create new custom metadata by selecting **Core | Metadata | Custom Metadata | Add** in the GV STRATUS Control Panel.

19. Click **Save**.

Next, enable the rule.

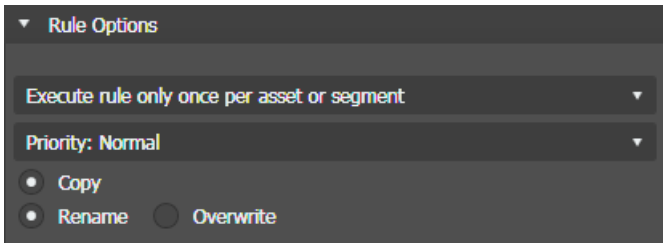
Adding a restore rule

The GV STRATUS Rules Engine can watch a location that is in an archive system and transfer assets that match your criteria to a location that is in the GV STRATUS system. The Rules Engine transfers the assets to the destination that you configure.

1. Log in to the GV STRATUS Control Panel application with administrator privileges.
2. In the GV STRATUS Control Panel application, click **General | Rules**.
3. Click **Add**.

   Rule Editor settings open.
4. In the **Rule Type** drop-down list select **Restore**.
5. In the **Name** field type in a name for the rule you are configuring.
6. In the **Description** field type in a description for the rule you are configuring.

7. In **Rule Options** settings, specify the rule behavior.



For restore rules, you can copy only. The move option is not available.

a) Select when the rule is applied each asset.

- **Execute rule only once per asset**: The rule is applied once per asset. The Rules Engine uses data stored in the asset's **ExecutedByRules** metadata field to determine if the rule has been applied to the asset. If it has been applied, the Rules Engine does not apply it again, even if the rule criteria still match for the asset.
- **Execute every time rule conditions apply**: The rule can be applied multiple times per asset, if the asset matches rule conditions multiple times.

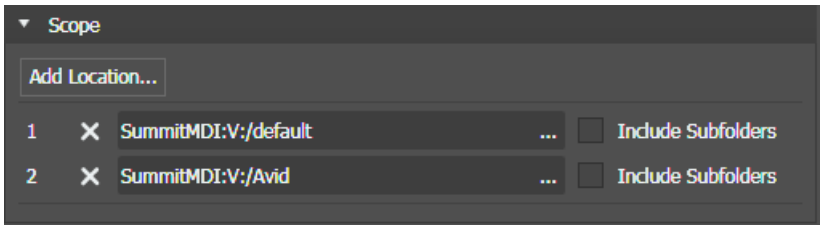
b) Select the priority that the Rules Engine processes the rule, with the transfers and transcodes the rule controls, when there are multiple rules in a queue waiting to be processed.

- **Priority: High**: Put this rule in a queue with other high priority rules and process through the high priority rule queue before any normal priority or low priority rules.
- **Priority: Normal**: Put this rule in a queue with other normal priority rules and process through the normal priority rule queue after any high priority but before any low priority rules.
- **Priority: Low**: Put this rule in a queue with other low priority rules and process through the low priority rule queue after any high priority or medium priority rules.

c) Select whether the rule renames or overwrites the asset.

- **Rename**: The rule appends a suffix to the new asset file name. The existing asset is retained.
- **Overwrite**: The new asset overwrites the existing asset. The existing asset is deleted.

8. In **Scope** settings, specify the location or locations in which the rule operates.



For restore rules, only valid archive locations are available.

a) Click **Add location**.

The **Location Selection** dialog box opens.

b) Navigate to and select the desired location.

You can select multiple locations in the **Location Selection** dialog box.

For Transfer, Export, Custom, Archive, and Transfer to Avid rules, you can also select logical asset locations under **Groups | Lost and Found**.

If desired, you can edit scope location path manually in the text box.

This is the location that contains the files on which the rule operates. Every time the rule runs, it looks in this location to determine if there are any assets that match the rule conditions and then operates on the assets that match.

c) Click **OK**.

The location is added to the **Scope** list.

d) For a location in the list, if you want the rule to operate on sub-folders as well, select **Include Subfolders**.

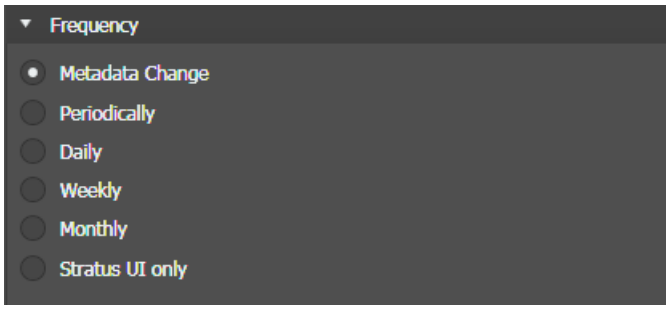
When this is selected, if there are multiple directories under the selected location, the rule operates in each of the sub-directories.

e) Repeat these steps to add additional locations as desired.

f) To change a location in the list, click the **Browse** button ⋯

g) To remove a location from the list, click **X**.

9. In **Frequency** settings, specify how often the Rules Engine triggers the rule.

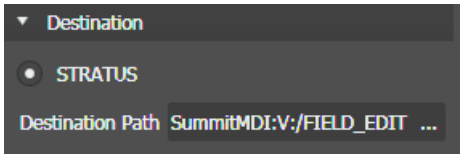


   a) Select one of the following options:

   - **Metadata Change**: The rule is constantly monitoring files in the "Scope" folder (and file types depend on the rule condition).
   - **Periodically**: Sets the number of minutes.
   - **Daily**: Sets the number of days.
   - **Weekly**: Sets the number of weeks.
   - **Monthly**: Sets the day of each month.
   - **STRATUS UI only**: The rule is only applicable when triggered by users via the context menu in Asset List of the STRATUS UI.

   For Daily, Weekly, and Monthly options, a **Start Time** setting opens. Set the day and time the rule is triggered for the first time.

10. In **Destination** settings, specify the destination of the assets on which the rule operates.



   For restore rules, the destination must be a K2 system location. Assets cannot be restored to other GV STRATUS system locations.

11. For Destination Path, click the **Browse** button ···.

    The Select Destination Path dialog box opens.

12. Navigate to the desired location and click **OK**.
13. In **Rule Conditions** settings, specify the conditions the Rules Engine looks for to qualify an asset.

14. In the **Select items when** drop down list, select one of the following:

    - **ALL of the conditions below are met**: Assets that match all conditions.
    - **ANY of the conditions below are met**: Assets that match any condition.
    - **Custom**: A Custom Expression field opens in which you can enter a custom expression.

    Conditions and custom expressions are similar to those in GV STRATUS Advanced Search. Simple boolean operators AND, OR, and NOT are supported. Enter these operators in all capital letters.

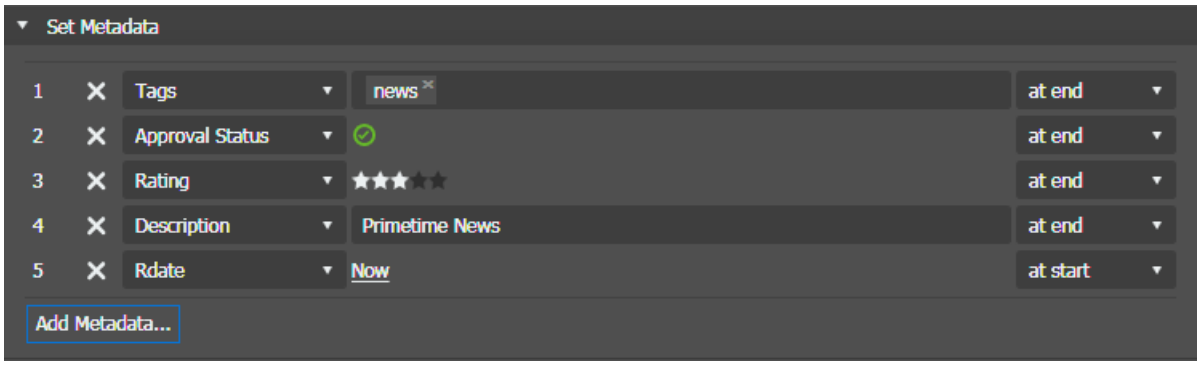
15. Configure conditions as follows:

    - For each condition (1, 2, 3, 4, etc) click the **Add Condition** button and select from lists to define the condition.
    - Click the **X** button to remove a condition from the list.

    The **is Empty** setting and the period (.) mark are also supported when creating conditions. In case you want to use a 'relative time' (for example the asset 'Modified Date' is before 2 minutes ago) as a rule condition, you should not use rule triggers based on 'Metadata Changes' but use 'periodically' rule triggers only and enter a cycle time (for example 3, 4 or 5 minutes). This is because when a 'relative time' matches the condition, but no metadata change happens at the same time, the rule will not trigger in your operation.

    If a newly created custom metadata field is not available in the **Add Condition** dialog, restart the GV STRATUS Control Panel application.

16. In **Set Metadata** settings, define the metadata that Rules Engine will set during the execution of a rule for an asset.



17. Configure metadata as follows:

    - For each metadata, click the **Add Metadata** button and select from the drop-down list to select the metadata.
    - Define the metadata value which will be added into the data field of the asset when the rule is applied to.
    - Select whether to enter the metadata value at the start or the end of the rule workflow.
    - Click the **X** button to remove a metadata from the list.

    If a newly created custom metadata field is not available in the drop-down list, restart the GV STRATUS Control Panel application.

    You can create new custom metadata by selecting **Core | Metadata | Custom Metadata | Add** in the GV STRATUS Control Panel.

18. Click **Save**.

Next, enable the rule.

Custom rules

A selection of **Custom** is available on the **Rule Type** drop-down list. A custom rule requires consultation with Grass Valley and development of a custom workflow. The custom workflow must be in place before you can configure a custom rule. Contact Grass Valley Support for more information.

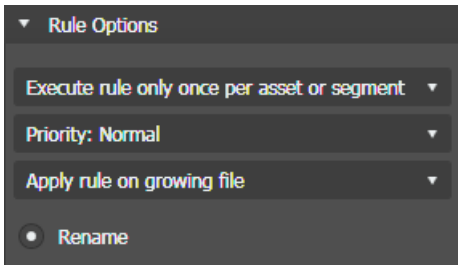
Adding a transfer to Avid rule

The GV STRATUS Rules Engine can watch a source location that is in the GV STRATUS system and transfer assets that match your criteria to a preconfigured destination location in the Avid system. For playlists, a conform job is automatically triggered to render the complex asset as a simple clip at the destination.

1. Log in to the GV STRATUS Control Panel application with administrator privileges.
2. In the GV STRATUS Control Panel application, click **General | Rules**.
3. Click **Add**.

   Rule Editor settings open.
4. In the **Rule Type** drop-down list select **Transfer to Avid**.
5. In the **Name** field type in a name for the rule you are configuring.
6. In the **Description** field type in a description for the rule you are configuring.

7. In **Rule Options** settings, specify the rule behavior.



a) Select when the rule is applied each asset.

- **Execute rule only once per asset or segment**: The rule is applied once per asset or segment. The Rules Engine uses data stored in the asset's **ExecutedByRules** metadata field to determine if the rule has been applied to the asset. If it has been applied, the Rules Engine does not apply it again, even if the rule criteria still match for the asset.
- **Execute every time rule conditions apply**: The rule can be applied multiple times per asset, if the asset matches rule conditions multiple times.

b) Select the priority that the Rules Engine processes the rule, with the transfers and transcodes the rule controls, when there are multiple rules in a queue waiting to be processed.

- **Priority: High**: Put this rule in a queue with other high priority rules and process through the high priority rule queue before any normal priority or low priority rules.
- **Priority: Normal**: Put this rule in a queue with other normal priority rules and process through the normal priority rule queue after any high priority but before any low priority rules.
- **Priority: Low**: Put this rule in a queue with other low priority rules and process through the low priority rule queue after any high priority or medium priority rules.

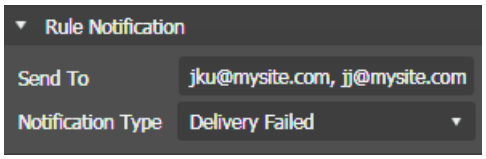
c) Select the condition when the rule is applied to each asset.

- **Apply rule on growing file**: The rule is applied to all files, including those that are still recording.
- **Apply rule on completed files**: The rule is only applied to files that have finished recording.

d) If an asset of the same name already exists at the destination location, configure the rule behavior:

- **Rename**: A suffix is appended to the imported asset name. The existing asset is retained.

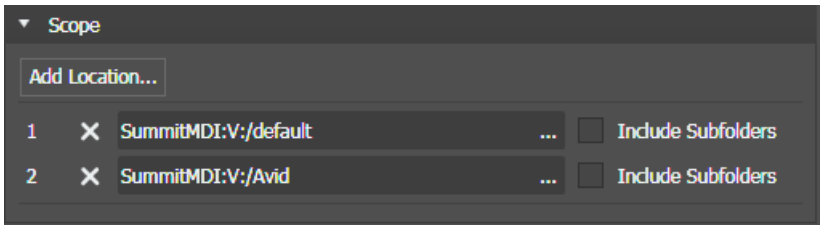
8. In **Rule Notification** settings, specify the notification behavior, if desired.



   a) Enter email addresses to which emails are sent.
      Separate multiple email addresses with a comma.
   b) Select one or more notification types:
      - **Delivery Failed**: Emails are sent if the rule operation fails.
      - **Delivery Completed**: Emails are sent if the rule operation succeeds.

   In order to send emails, the email server must be configured in Workflow Engine settings.

9. In **Scope** settings, specify the location or locations in which the rule operates.



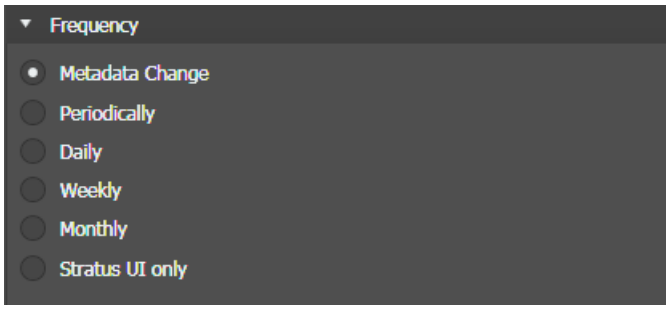
   a) Click **Add location**.
      The **Location Selection** dialog box opens.
   b) Navigate to and select the desired location.

      You can select multiple locations in the **Location Selection** dialog box.

      For Transfer, Export, Custom, Archive, and Transfer to Avid rules, you can also select logical asset locations under **Groups | Lost and Found**.

      If desired, you can edit scope location path manually in the text box.
      This is the location that contains the files on which the rule operates. Every time the rule runs, it looks in this location to determine if there are any assets that match the rule conditions and then operates on the assets that match.
   c) Click **OK**.
      The location is added to the **Scope** list.
   d) For a location in the list, if you want the rule to operate on sub-folders as well, select **Include Subfolders**.
      When this is selected, if there are multiple directories under the selected location, the rule operates in each of the sub-directories.
   e) Repeat these steps to add additional locations as desired.
   f) To change a location in the list, click the **Browse** button ···
   g) To remove a location from the list, click **X**.

10. In **Frequency** settings, specify how often the Rules Engine triggers the rule.



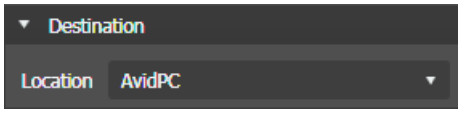
a) Select one of the following options:

- **Metadata Change**: The rule is constantly monitoring files in the "Scope" folder (and file types depend on the rule condition).
- **Periodically**: Sets the number of minutes.
- **Daily**: Sets the number of days.
- **Weekly**: Sets the number of weeks.
- **Monthly**: Sets the day of each month.
- **STRATUS UI only**: The rule is only applicable when triggered by users via the context menu in Asset List of the STRATUS UI.

For Daily, Weekly, and Monthly options, a **Start Time** setting opens. Set the day and time the rule is triggered for the first time.

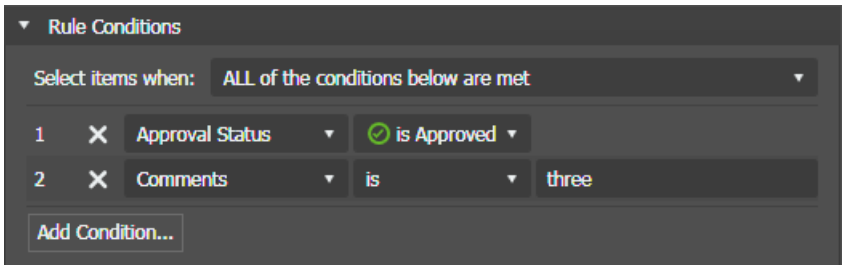
11. For Destination Path, click the **Browse** button ···.
The Select Destination Path dialog box opens.

12. In **Destination** setting, select the location of the assets to be transferred.



The location must be an Avid system that had been configured in **General | Locations Config | Locations Configuration**. If not configured, the location is not available in the **Location** drop-down list.

13. In **Rule Conditions** settings, specify the conditions the Rules Engine looks for to qualify an asset.



14. In the **Select items when** drop down list, select one of the following:

    - **ALL of the conditions below are met**: Assets that match all conditions.
    - **ANY of the conditions below are met**: Assets that match any condition.
    - **Custom**: A Custom Expression field opens in which you can enter a custom expression.

    Conditions and custom expressions are similar to those in GV STRATUS Advanced Search. Simple boolean operators AND, OR, and NOT are supported. Enter these operators in all capital letters.

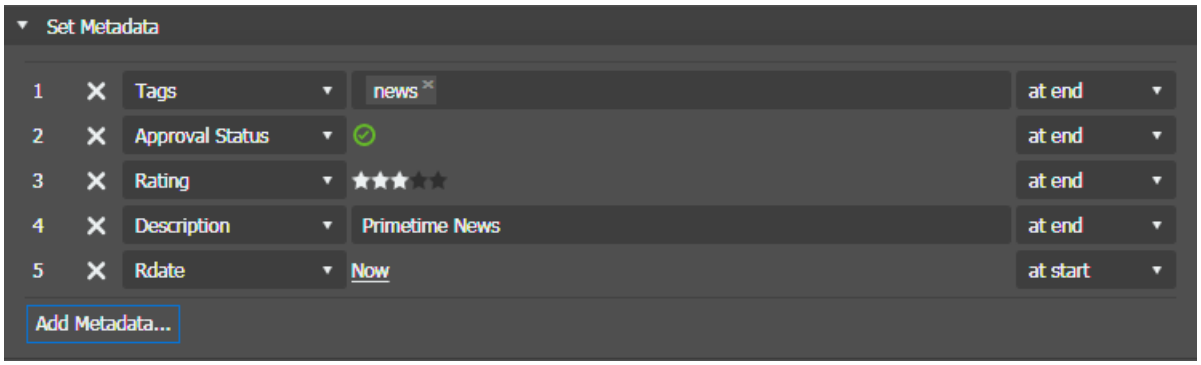
15. Configure conditions as follows:

    - For each condition (1, 2, 3, 4, etc) click the **Add Condition** button and select from lists to define the condition.
    - Click the **X** button to remove a condition from the list.

    The **is Empty** setting and the period (.) mark are also supported when creating conditions. In case you want to use a 'relative time' (for example the asset 'Modified Date' is before 2 minutes ago) as a rule condition, you should not use rule triggers based on 'Metadata Changes' but use 'periodically' rule triggers only and enter a cycle time (for example 3, 4 or 5 minutes). This is because when a 'relative time' matches the condition, but no metadata change happens at the same time, the rule will not trigger in your operation.

    If a newly created custom metadata field is not available in the **Add Condition** dialog, restart the GV STRATUS Control Panel application.

16. In **Set Metadata** settings, define the metadata that Rules Engine will set during the execution of a rule for an asset.



17. Configure metadata as follows:

    - For each metadata, click the **Add Metadata** button and select from the drop-down list to select the metadata.
    - Define the metadata value which will be added into the data field of the asset when the rule is applied to.
    - Select whether to enter the metadata value at the start or the end of the rule workflow.
    - Click the **X** button to remove a metadata from the list.

    If a newly created custom metadata field is not available in the drop-down list, restart the GV STRATUS Control Panel application.

    You can create new custom metadata by selecting **Core | Metadata | Custom Metadata | Add** in the GV STRATUS Control Panel.

18. Click **Save**.

Next, enable the rule.

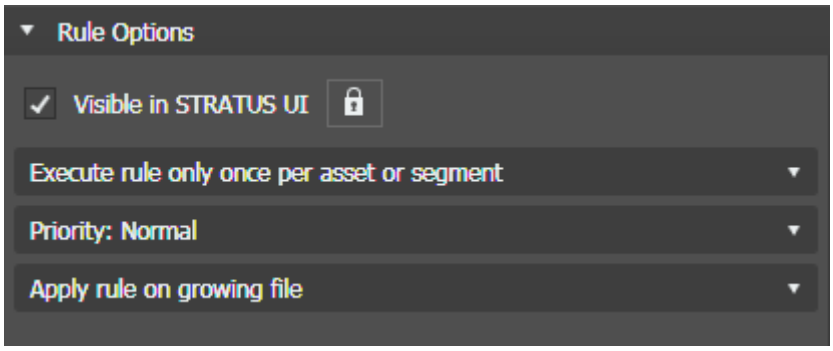
Adding a publish external media network rule

The GV STRATUS Rules Engine can watch a source location in the GV STRATUS system and publish assets to one or multiple external media accounts. The Rules Engine exports and publishes the assets to the external media destination that you configured. In addition to the video/audio essence, you can also configure whether to include metadata, thumbnail, or Close Caption information when the asset gets published.

1. Log in to the GV STRATUS Control Panel application with administrator privileges.
2. In the GV STRATUS Control Panel application, click **General | Rules**.
3. Click **Add**.

   Rule Editor settings open.
4. In the **Rule Type** drop-down list select **Publish External Media Network**.
5. In the **Name** field type in a name for the rule you are configuring.
6. In the **Description** field type in a description for the rule you are configuring.

7. In **Rule Options** settings, specify the rule behavior.

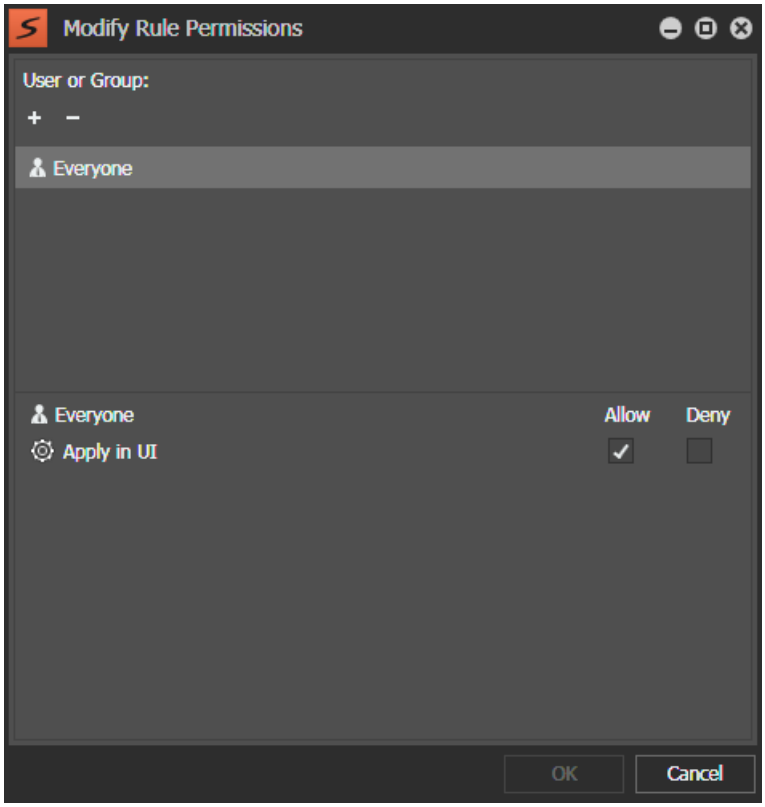


a) Select the **Visible in STRATUS UI** check-box if you want to trigger the rule via context menu in the Asset List panel.

By default, all users can see all rules that had been set to **Visible in STRATUS UI**.

To configure the rule to be only visible to specific user or user groups, click the button.

The Modify Rule Permissions dialog box appears.



To assign permissions, click **+** and enter any user or group in the **Add Users or Groups** dialog box. If necessary, click **Advanced** to open Windows operating system dialog box to find and validate users or groups.

- **+** : Opens the **Add Users or Groups** dialog box to assign users or groups with permissions.
- **-** : Removes a user or group from the list.

After adding specific user or group, set permission for **Apply in UI** setting by selecting **Allow** or **Deny** as appropriate.

b) Select when the rule is applied each asset.

- **Execute rule only once per asset or segment**: The rule is applied once per asset. The Rules Engine uses data stored in the asset's **ExecutedByRules** metadata field to determine if the rule has been applied to the asset. If it has been applied, the Rules Engine does not apply it again, even if the rule criteria still match for the asset.
- **Execute every time rule conditions apply**: The rule can be applied multiple times per asset, if the asset matches rule conditions multiple times.

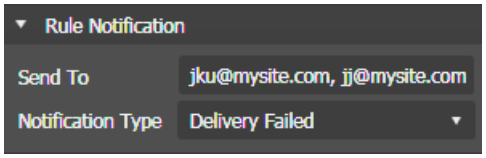
c) Select the priority that the Rules Engine processes the rule, with the transfers and transcodes the rule controls, when there are multiple rules in a queue waiting to be processed.

- **Priority: High**: Put this rule in a queue with other high priority rules and process through the high priority rule queue before any normal priority or low priority rules.
- **Priority: Normal**: Put this rule in a queue with other normal priority rules and process through the normal priority rule queue after any high priority but before any low priority rules.
- **Priority: Low**: Put this rule in a queue with other low priority rules and process through the low priority rule queue after any high priority or medium priority rules.

d) Select the condition when the rule is applied to each asset.

- **Apply rule on growing file**: The rule is applied to all files, including those that are still recording.
- **Apply rule on completed files**: The rule is only applied to files that have finished recording.

8. In **Rule Notification** settings, specify the notification behavior, if desired.



a) Enter email addresses to which emails are sent.

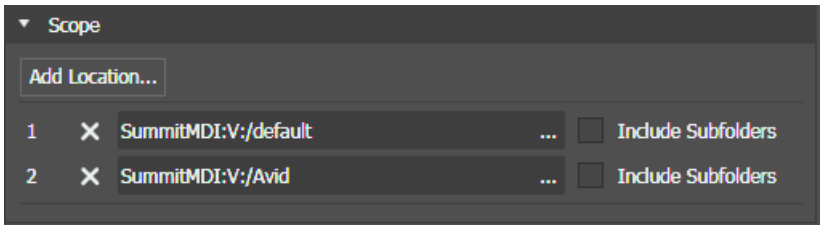
Separate multiple email addresses with a comma.

b) Select one or more notification types:

- **Delivery Failed**: Emails are sent if the rule operation fails.
- **Delivery Completed**: Emails are sent if the rule operation succeeds.

In order to send emails, the email server must be configured in Workflow Engine settings.

9. In **Scope** settings, specify the location or locations in which the rule operates.



a) Click **Add location**.

The **Location Selection** dialog box opens.

b) Navigate to and select the desired location.

You can select multiple locations in the **Location Selection** dialog box.

For Transfer, Export, Custom, Archive, and Transfer to Avid rules, you can also select logical asset locations under **Groups | Lost and Found**.

If desired, you can edit scope location path manually in the text box.

This is the location that contains the files on which the rule operates. Every time the rule runs, it looks in this location to determine if there are any assets that match the rule conditions and then operates on the assets that match.

c) Click **OK**.

The location is added to the **Scope** list.

d) For a location in the list, if you want the rule to operate on sub-folders as well, select **Include Subfolders**.

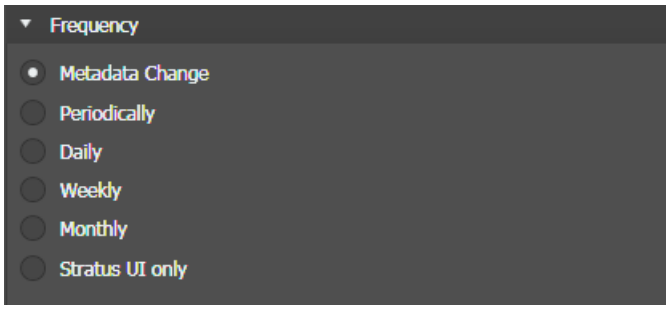
When this is selected, if there are multiple directories under the selected location, the rule operates in each of the sub-directories.

e) Repeat these steps to add additional locations as desired.

f) To change a location in the list, click the **Browse** button ⋯

g) To remove a location from the list, click **X**.

10. In **Frequency** settings, specify how often the Rules Engine triggers the rule.

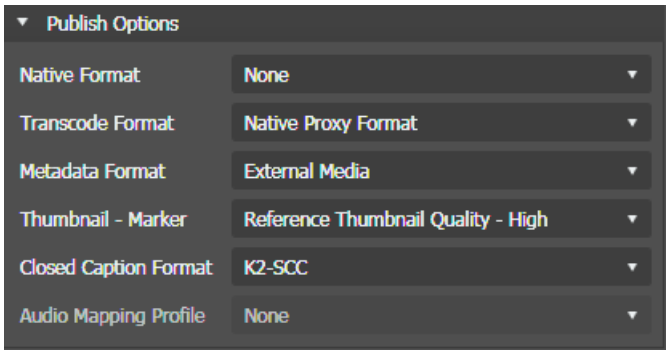


a) Select one of the following options:

- **Metadata Change**: The rule is constantly monitoring files in the “Scope” folder (and file types depend on the rule condition).
- **Periodically**: Sets the number of minutes.
- **Daily**: Sets the number of days.
- **Weekly**: Sets the number of weeks.
- **Monthly**: Sets the day of each month.
- **STRATUS UI only**: The rule is only applicable when triggered by users via the context menu in Asset List of the STRATUS UI.

For Daily, Weekly, and Monthly options, a **Start Time** setting opens. Set the day and time the rule is triggered for the first time.

11. In **Publish Options** settings, configure format of the published files.



You can select either a **Native Format** or a **Transcode Format**, but not both.

a) For **Native Format**, select the interchange standard in which to publish.

When a **Native Format** is selected, **Transcode Format** is automatically set to None and disabled.

b) For **Transcode Format**, configure as follows:

- Select **None**: The published file is the same format as the source on the K2 storage system.
- Select **Native Proxy Format**: The published file is the same format as the proxy on GV STRATUS system.
- Select one or more transcode formats as follows:
  - Select a single format for the transcoder.
  - To use multiple formats from a single transcoder, select the formats for that transcoder.

  You cannot select multiple transcoders.

When a **Transcode Format** is selected, **Native Format** is automatically set to None and disabled.

The **Transcode Format** list is populated by the transcode profiles that you create and place in the transcode profile directory.

c) For **Metadata Format**, select as follows to additionally export the metadata file:

- **None**: No metadata file is exported.
- **External Media**: The single metadata profile combines the metadata to be exported for all External Media Platforms.

d) For **Thumbnails - Marker**, select as follows:

- **None**: The export does not contain thumbnails.
- **Marker Thumbnail Quality - High**: High: The export contains a full-resolution JPG thumbnail with no compression (100%).
- **Marker Thumbnail Quality - Medium**: The export contains a full-resolution JPG thumbnail compressed 85%.
- **Marker Thumbnail Quality - Low**: Low: The export contains a half-resolution JPG thumbnail compressed 70%.
- **Reference Thumbnail Quality - High**: High: The export contains a key-frame marker with full-resolution JPG thumbnail of no compression (100%).
- **Reference Thumbnail Quality - Medium**: The export contains a key-frame marker with full-resolution JPG thumbnail compressed 85%.

- **Reference Thumbnail Quality - Low**: Low: The export contains a key-frame marker with half-resolution JPG thumbnail compressed 70%.

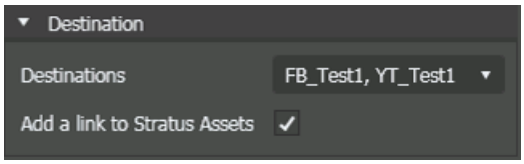
NOTE: Some platforms such as Twitter, do not allow the publish of thumbnails as an additional option. While Facebook allows only one thumbnail to be published.

e) For **Closed Caption Format**, select as follows:

- **None**: No additional Close Caption file is exported.
- **K2-SCC**: Workflow Engine extracts CEA-608 information stored in Ancillary data (CEA-708) from the asset on the K2 system and exports to a file in SCC format.
- **K2-SRT**: Workflow Engine extracts CEA-608 information stored in Ancillary data (CEA-708) from the asset on the K2 system and exports to a file in SRT format.
- **K2-TTML**: Workflow Engine extracts CEA-608 information stored in Ancillary data (CEA-708) from the asset on the K2 system and exports to a file in TTML format.

NOTE: Some platforms such as Twitter, do not allow the publish of Closed Caption information as an additional option. While Facebook supports the SRT Closed Caption files only.

12. In **Destination** settings, select the destination location on which the rule operates.



The destination must be a location that is already configured on the External Media tab within Locations Configuration in GV STRATUS Control Panel.

You can select multiple destinations for external media platforms as follows:

- **Facebook**
- **Twitter**
- **YouTube**
- **Verizon**

13. Select the **Add a link to Stratus Assets** check-box to include the External Media URL of the published asset in GV STRATUS as below:

14. In **Rule Conditions** settings, specify any conditions the Rules Engine looks for to qualify an asset.

    Below is an example of conditions in the **Rule Conditions** section:

15. In the **Select items when** drop down list, select one of the following:

    - **ALL of the conditions below are met**: Assets that match all conditions.
    - **ANY of the conditions below are met**: Assets that match any condition.
    - **Custom**: A Custom Expression field opens in which you can enter a custom expression.

    Conditions and custom expressions are similar to those in GV STRATUS Advanced Search. Simple boolean operators AND, OR, and NOT are supported. Enter these operators in all capital letters.

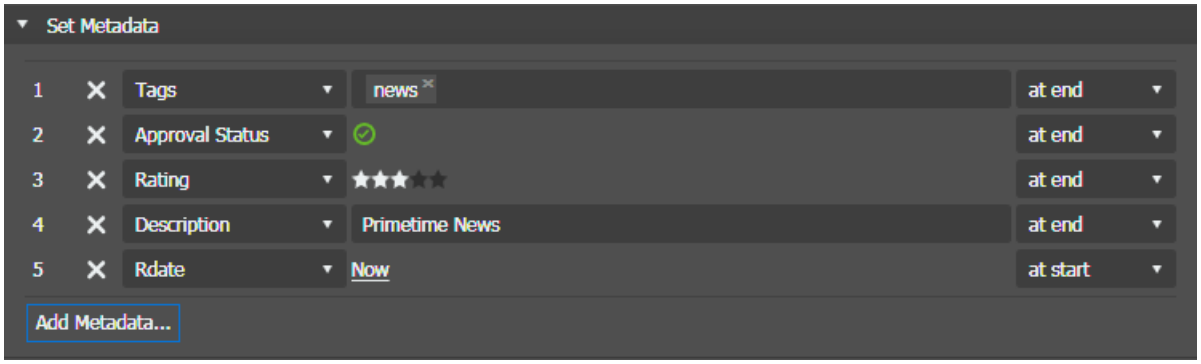
16. Configure conditions as follows:

    - For each condition (1, 2, 3, 4, etc) click the **Add Condition** button and select from lists to define the condition.
    - Click the **X** button to remove a condition from the list.

    The **is Empty** setting and the period (.) mark are also supported when creating conditions. In case you want to use a 'relative time' (for example the asset 'Modified Date' is before 2 minutes ago) as a rule condition, you should not use rule triggers based on 'Metadata Changes' but use 'periodically' rule triggers only and enter a cycle time (for example 3, 4 or 5 minutes). This is because when a 'relative time' matches the condition, but no metadata change happens at the same time, the rule will not trigger in your operation.

    If a newly created custom metadata field is not available in the **Add Condition** dialog, restart the GV STRATUS Control Panel application.

17. In **Set Metadata** settings, define the metadata that Rules Engine will set during the execution of a rule for an asset.



18. Configure metadata as follows:

    - For each metadata, click the **Add Metadata** button and select from the drop-down list to select the metadata.
    - Define the metadata value which will be added into the data field of the asset when the rule is applied to.
    - Select whether to enter the metadata value at the start or the end of the rule workflow.
    - Click the **X** button to remove a metadata from the list.

    If a newly created custom metadata field is not available in the drop-down list, restart the GV STRATUS Control Panel application.

    You can create new custom metadata by selecting **Core | Metadata | Custom Metadata | Add** in the GV STRATUS Control Panel.

19. Click **Save**.

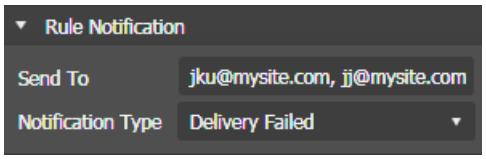
Next, enable the rule.

Adding a media network counts rule

The GV STRATUS Rules Engine can watch an external media location and gather statistical information from assets that had been published to the External Media Account. Multiple external media accounts and configured locations are supported for the media network counts rule. After applying the rule, information such as the number of View-, Like- and Share-counts are stored as asset metadata in the GV STRATUS system.

1. Log in to the GV STRATUS Control Panel application with administrator privileges.
2. In the GV STRATUS Control Panel application, click **General | Rules**.
3. Click **Add**.

   Rule Editor settings open.
4. In the **Rule Type** drop-down list select **Media Network Counts**.
5. In the **Name** field type in a name for the rule you are configuring.
6. In the **Description** field type in a description for the rule you are configuring, if desired.
7. In **Rule Notification** settings, specify the notification behavior, if desired.



   a) Enter email addresses to which emails are sent.

      Separate multiple email addresses with a comma.

   b) Select one or more notification types:

      - **Delivery Failed**: Emails are sent if the rule operation fails.
      - **Delivery Completed**: Emails are sent if the rule operation succeeds.

   In order to send emails, the email server must be configured in Workflow Engine settings.

8. In **Scope** settings, specify the location or locations in which the rule operates.

   a) Click **Add location**.

      The **Location Selection** dialog box opens.

   b) Navigate to and select the desired external media location.

      You can select multiple locations in the **Location Selection** dialog box.

      This is the external media location that contains the assets on which the rule operates. Every time the rule runs, it looks in this location to determine if there are any assets that match the rule conditions and then operates on the assets that match.

   c) Click **OK**.

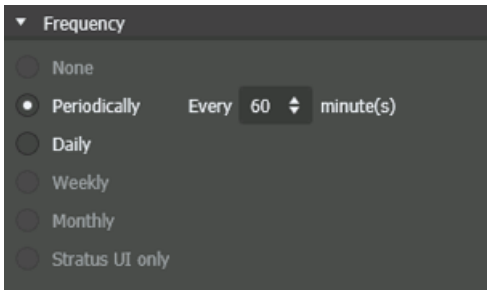
      The location is added to the **Scope** list.

   d) Repeat these steps to add additional locations as desired.

   e) To change a location in the list, click the **Browse** button ⋯

   f) To remove a location from the list, click **X**.

9. In **Frequency** settings, specify how often the Rules Engine triggers the rule.



   a) Select one of the following options:

      - **Periodically**: Sets the period with the minimum setting of 60 minutes. It must be set between 60 to 120 minutes to not overload the Rules Engine.
      - **Daily**: Sets the number of days.

      For the Daily option, a **Start Time** setting opens. Set the day and time the rule is triggered for the first time.

10. Click **Save**.

Next, enable the rule.

Example rules: Export segments, assets

You can create a rule that exports one of the following:

- Approved standard segments that are part of a live segmentation

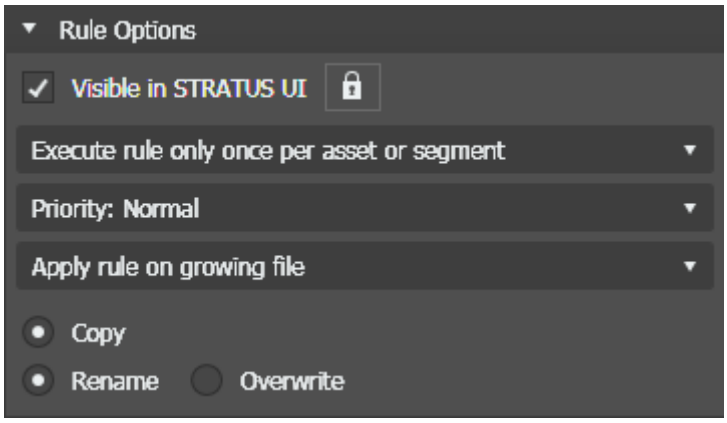
- Approved assets

To export both segments and assets, you must configure one rule for segments and another rule for assets. These rules are examples of typical rules used in the Digital Media Platform workflow. These rules are customized for the specific workflow at the customer site.

1. Log in to the GV STRATUS Control Panel application with administrator privileges.
2. In the GV STRATUS Control Panel application, click **General | Rules**.
3. Click **Add**.

   Rule Editor settings open.
4. In the **Rule Type** drop-down list select **Export**.
5. In the **Name** field type in a name for the rule you are configuring.
6. In the **Description** field type in a description for the rule you are configuring.

7. In **Rule Options** settings, specify the rule behavior.

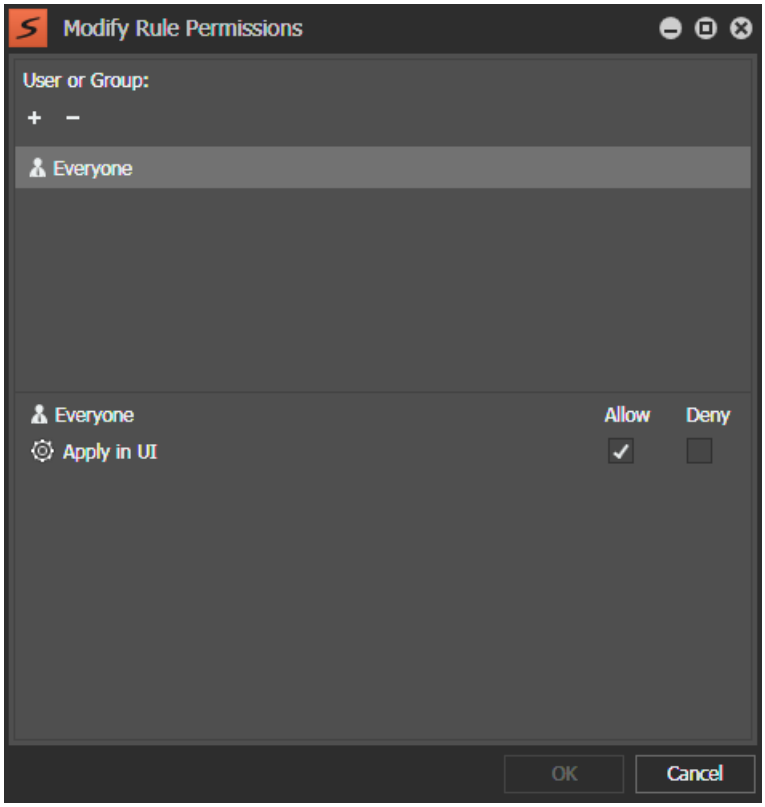


a) Select the **Visible in STRATUS UI** check-box if you want to trigger the rule via context menu in the Asset List panel.

By default, all users can see all rules that had been set to **Visible in STRATUS UI**.

To configure the rule to be only visible to specific user or user groups, click the button.

The Modify Rule Permissions dialog box appears.



To assign permissions, click **+** and enter any user or group in the **Add Users or Groups** dialog box. If necessary, click **Advanced** to open Windows operating system dialog box to find and validate users or groups.

- **+** : Opens the **Add Users or Groups** dialog box to assign users or groups with permissions.
- **-** : Removes a user or group from the list.

After adding specific user or group, set permission for **Apply in UI** setting by selecting **Allow** or **Deny** as appropriate.

b) Select whether the rule copies the asset.

c) Select whether the rule renames or overwrites the asset.

- **Rename**: The rule appends a suffix to the new asset file name. The existing asset is retained.
- **Overwrite**: The new asset overwrites the existing asset. The existing asset is deleted.

d) Select when the rule is applied each asset.

- **Execute rule only once per asset**: The rule is applied once per asset. The Rules Engine uses data stored in the asset's **ExecutedByRules** metadata field to determine if the rule has been applied to the asset. If it has been applied, the Rules Engine does not apply it again, even if the rule criteria still match for the asset.
- **Execute every time rule conditions apply**: The rule can be applied multiple times per asset, if the asset matches rule conditions multiple times.

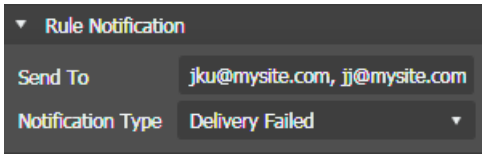
e) Select the priority that the Rules Engine processes the rule, with the transfers and transcodes the rule controls, when there are multiple rules in a queue waiting to be processed.

- **Priority: High**: Put this rule in a queue with other high priority rules and process through the high priority rule queue before any normal priority or low priority rules.
- **Priority: Normal**: Put this rule in a queue with other normal priority rules and process through the normal priority rule queue after any high priority but before any low priority rules.
- **Priority: Low**: Put this rule in a queue with other low priority rules and process through the low priority rule queue after any high priority or medium priority rules.

f) Select the condition when the rule is applied to each asset.

- **Apply rule on growing file**: The rule is applied to all files, including those that are still recording.
- **Apply rule on completed files**: The rule is only applied to files that have finished recording.

8. In **Rule Notification** settings, specify the notification behavior, if desired.



a) Enter email addresses to which emails are sent.

Separate multiple email addresses with a comma.

b) Select one or more notification types:

- **Delivery Failed**: Emails are sent if the rule operation fails.
- **Delivery Completed**: Emails are sent if the rule operation succeeds.

In order to send emails, the email server must be configured in Workflow Engine settings.

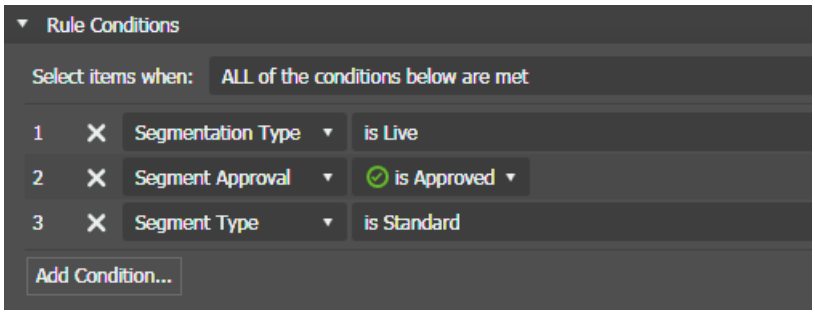
9. In **Scope** settings, specify the location or locations in which the rule operates.
   a) Click **Add location**.
      The **Location Selection** dialog box opens.
   b) Navigate to and select the desired location.
      This is the location that contains the files on which the rule operates. Every time the rule runs, it looks in this location to determine if there are any assets that match the rule conditions and then operates on the assets that match.
   c) Click **OK**.
      The location is added to the **Scope** list.
   d) Do not select **Include Subfolders**.
10. In **Export Filename Format** settings, set the convention for the name of the exported file.
    Select **Asset Name** only.
11. In **Frequency** settings, specify how often the Rules Engine triggers the rule, as follows:
    - **Metadata Change**: The rule is constantly monitoring assets in the "Scope" location.
12. In **Export Options** settings, configure the format of the exported files.
    a) For **Transcode Format**, configure as follows:
       - Configure a specific transcode format (MP4 AVC), as it exists in a currently configured Elemental transcode profile.

       When a **Transcode Format** is selected, **Native Format** is automatically set to None and disabled.
    b) For **Metadata Format**, select as follows to additionally export an XML metadata file:
       - Select **GV STRATUS Simple**.

       If you select a metadata format, the **Metadata-Destination Path** field is enabled.
    c) For **Metadata-Destination Path**, configure as follows:
       - You are exporting the metadata file to the same destination as the asset file, so leave this field blank. The file goes to the path configured in **Destination** settings.
    d) For **Thumbnails - Marker**, select as follows:
       - **None**: The export does not contain thumbnails.
    e) For **Closed Caption Format**, select as follows:
       - **K2-SCC**: Workflow Engine extracts CEA-608 information stored in Ancillary data (CEA-708) from the asset on the K2 system and exports to a file in SCC format.

       If you select a Closed Caption format, the **CC-Destination Path** field is enabled.
    f) For **CC-Destination Path**, configure as follows:
       - You are exporting the Closed Caption file to the same destination as the asset file, so leave this field blank. The file goes to the path configured in **Destination** settings.
13. In **Destination** settings, enter `\\server\folder`.

14. In **Rule Conditions** settings, specify the conditions the Rules Engine looks for to qualify an asset.



15. In the **Select items when** drop down list, select **ALL of the conditions below are met**.
16. For each condition (1, 2, 3) click the **Add Condition** button and select from lists to define the condition.

- For a rule that exports segments, configure conditions as follows:

1	Segmentation Type	is Live
2	Segment Approval	is Approved
3	Segment Type	is Standard

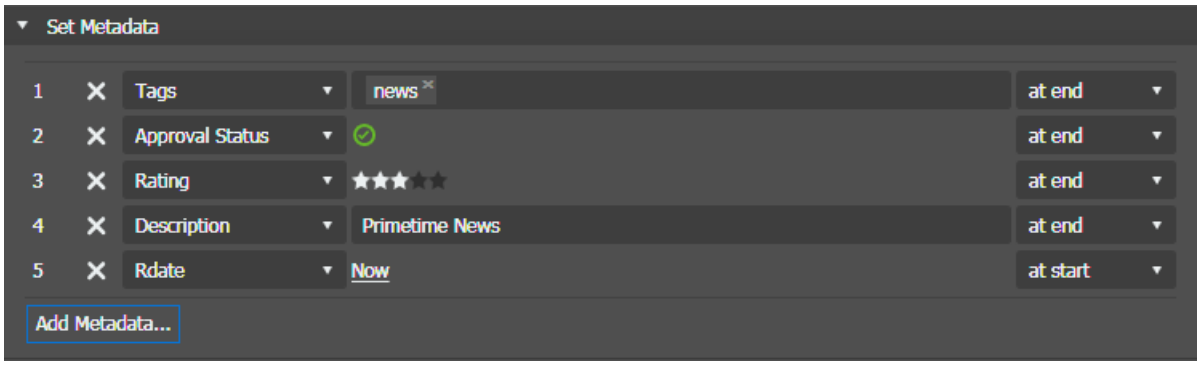
In the list of conditions, segment custom metadata is listed in its own section, separate from asset custom metadata.

- For a rule that exports assets, configure conditions as follows:

1	Asset Approval	is Approved
2	PrimaryAngle	is True

You can set the rule to transfer all angles of an asset if you set the **PrimaryAngle** condition to **is True**.

17. In **Set Metadata** settings, define the metadata that Rules Engine will set during the execution of a rule for an asset.



18. Configure metadata as follows:

    - For each metadata, click the **Add Metadata** button and select from the drop-down list to select the metadata.
    - Define the metadata value which will be added into the data field of the asset when the rule is applied to.
    - Select whether to enter the metadata value at the start or the end of the rule workflow.
    - Click the **X** button to remove a metadata from the list.

    If a newly created custom metadata field is not available in the drop-down list, restart the GV STRATUS Control Panel application.

    You can create new custom metadata by selecting **Core | Metadata | Custom Metadata | Add** in the GV STRATUS Control Panel.

19. Click **Save**.

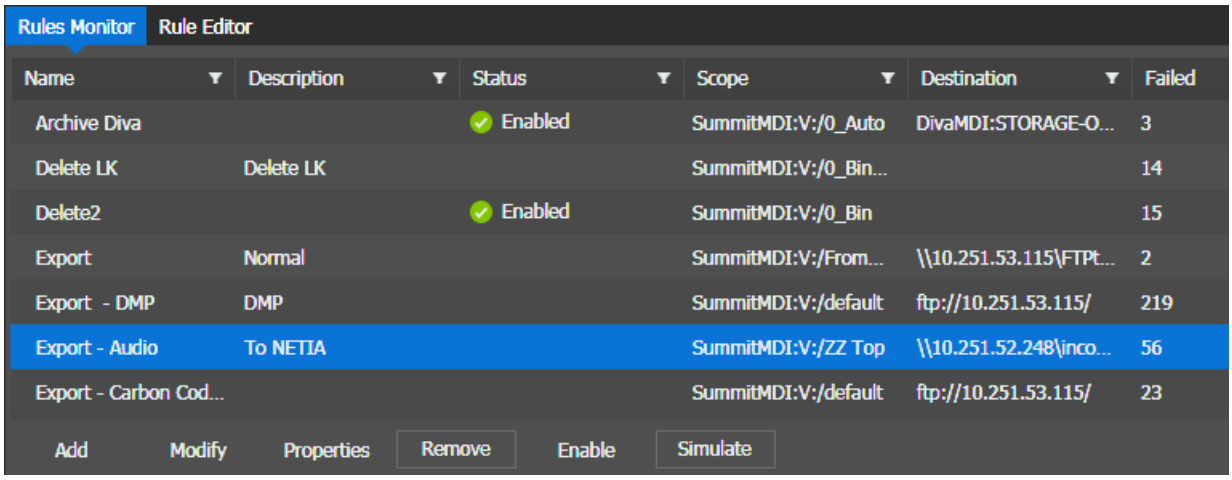
Next, enable the rule.

Enabling and disabling rules

You can make a rule become active or inactive while retaining its configuration.

1. Log in to the GV STRATUS Control Panel application with administrator privileges.
2. In the GV STRATUS Control Panel application, click **General | Rules**.
3. Select **Rules Monitor**.

   The Rules Monitor list is displayed.

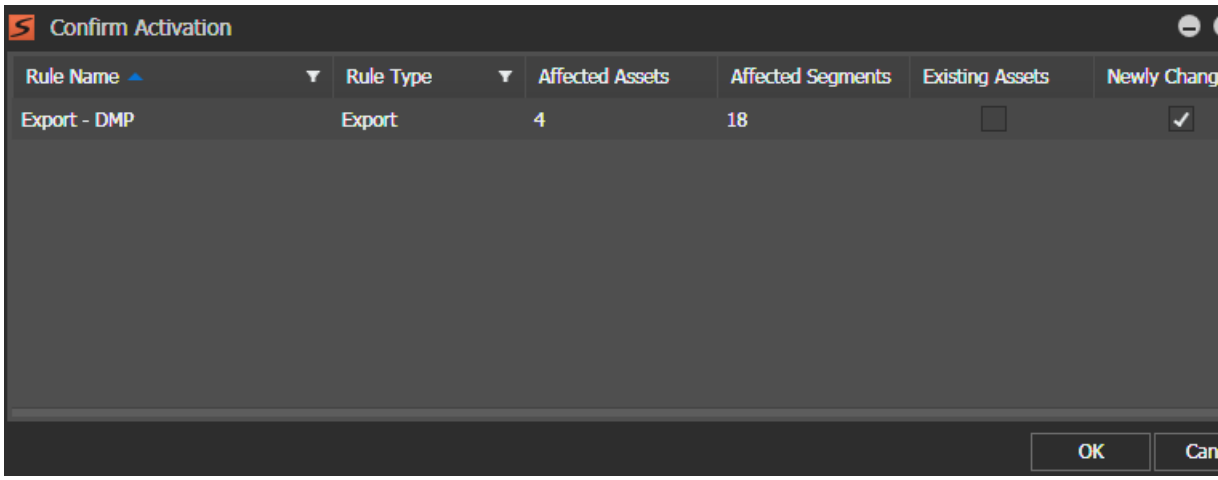


4. To disable a rule, select a rule with a Status that reports Enabled and click **Disable**.

   The button toggles between Enable and Disable, depending on the status of the selected rule.

5. To enable a rule, do the following:
   a) Select a rule with a Status that does not report Enabled and click **Enable**.

      The **Confirm Activation** dialog box opens and reports the number of current segments and assets to which the rule applies.



   b) Select options as follows:

   - **All existing Assets**: The rule immediately evaluates existing assets and takes action accordingly.

     NOTE: Take care when using this option. Assets for which the rule action successfully completed previously can have the rule action applied again, resulting in a large amount of unnecessary rule activity.
   - **Newly changed Assets only**: The rules is enabled but it does not take action on existing assets. Rather, it waits until an asset changes and then evaluates the asset to take action.
   - **Cancel**: The rule is not enabled.

Consider the Rules Engine setting Startup Mode and the Confirm Activation option when you enable a rule, as the behavior is similar. With the Rules Engine setting you specify the behavior of all currently enabled rules when the Rules Engine starts up. With the Confirm Activation option, you specify the behavior of an individual rule when you manually enable the rule.

Related Topics

Rules engine settings on page 334

About Control Panel, SiteConfig, and K2Config settings on page 433

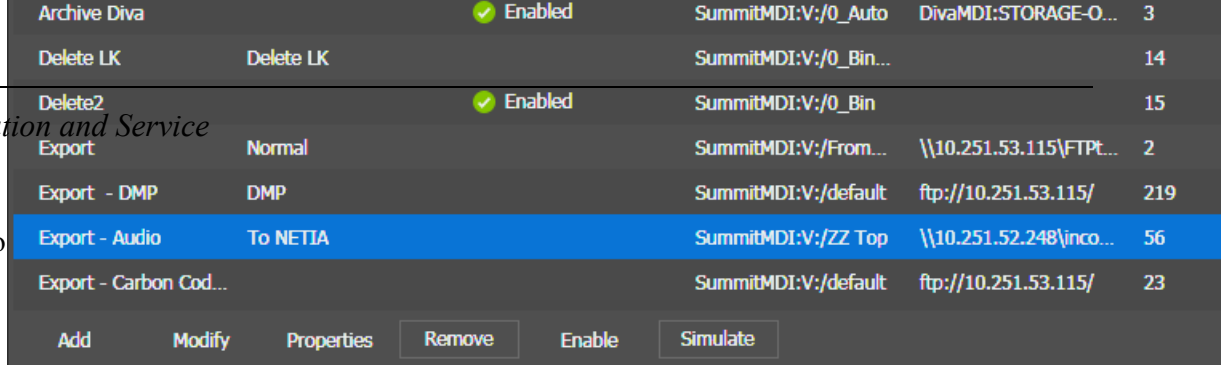
Simulating rules

Before enabling a rule, you can run a rule as a simulation to determine the assets affected by the rule. This avoids the long processing time and resource load that can result when enabling a rule that affects more assets than you expect.

NOTE: Rule simulation does not apply to Import Rules.

1. Log in to the GV STRATUS Control Panel application with administrator privileges.
2. In the GV STRATUS Control Panel application, click **General | Rules**.

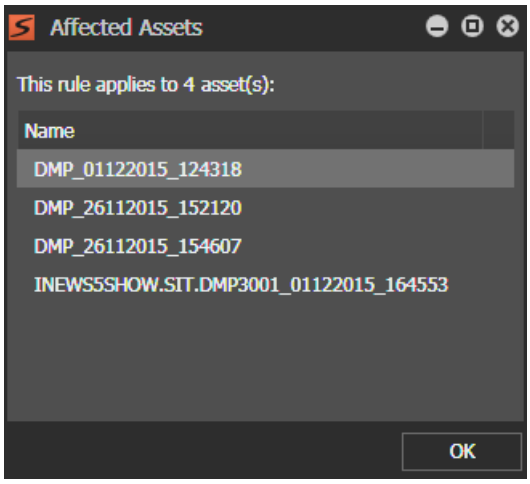
3. Do



   -
   - Open a rule in the **Rule Editor** by clicking **Add** or **Modify** as appropriate.

4. Click **Simulate**.

   The **Affected Assets** dialog box opens and reports the number of current assets to which the rule applies. It also lists the affected assets.

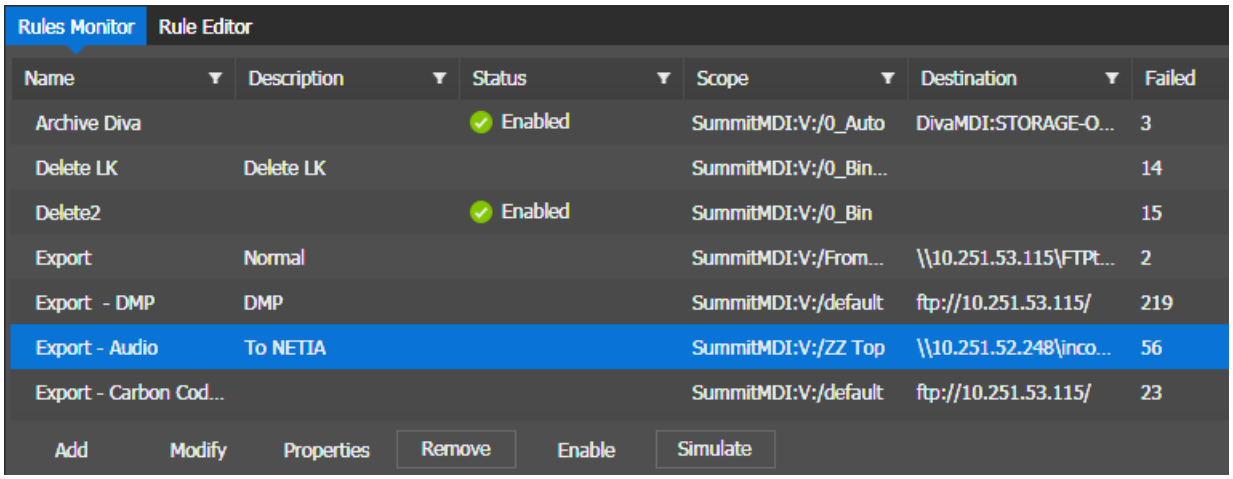


5. On the **Affected Assets** dialog box, click **OK** to close.

Monitoring rules

You can view reports of rule operations to check the results of your enabled rules.

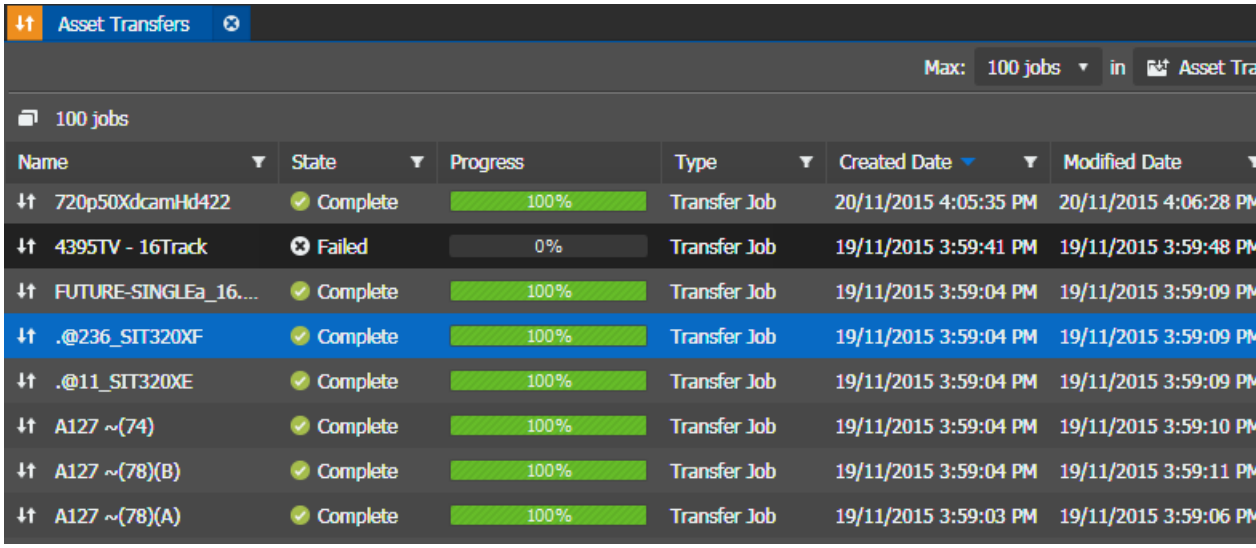
1. In the GV STRATUS Control Panel application, in Rules Monitor Settings, click **Refresh** and then view the report in the Failed column.



You can also right-click and select **Reset Counters** from the context menu to reset values in the Failed and Succeeded columns back to zero. The reset is allowed for single and multiple rules at the same time on enabled and disabled rules.

2. To monitor GV STRATUS system jobs triggered by you and by others, in the GV STRATUS application Navigator panel, do one of the following according to the types of jobs you are monitoring:

   - Double-click **Monitors | Jobs** and sort on the **Type** column.
   - Double-click **Monitors | Jobs | Asset Transfers**
   - Double-click **Monitors | Jobs | Conform**
   - Double-click **Monitors | Jobs | Rules Workflows**
   - Double-click **Monitors | Jobs | Transcodes**



   The Jobs List displays GV STRATUS operations that can be monitored. Operations that are currently in progress or have failed are also displayed.

   While transferring, if the destination quota is reached, the transfer job will fail gracefully in the Jobs Monitor and the partial asset will be deleted from the destination.

3. To change the priority of an upcoming job in the queue of jobs waiting to be processed, right-click an upcoming job, select **Change Priority**, and then select one of the following:

Options	Description
High	The job will be processed with high priority.
Normal	The job will be processed with normal priority.
Low	The job will be processed with low priority.

   You must be assigned the Queue Management role in GV STRATUS Control Panel in order to change job priority. If not assigned, menu selections are disabled.

4. To stop the GV STRATUS system from running an upcoming job, right-click an upcoming job and select **Cancel**.

5. To navigate to the asset of a specific job, do one of the following:
   - Right-click on the job and select **View Related | Asset**.

     The asset displays in the Asset List. Double-click the asset to view it in the Inspector.
   - Double-click the job in Jobs Monitor.

     The job and asset properties display on separate tabs in the Inspector. Click on the **Asset** tab, and double-click the asset to view it in the Inspector.
6. To view all related jobs to export and transfer-to-playout rules, do the following:
   a) Select **Monitors | Jobs** and double-click on **Rules Workflows**.
   b) Double-click on an export or transfer job in the **Rules Workflows** monitor.

      The properties, asset, and related jobs display on separate tabs in the Inspector.
   c) Click on the **Jobs** tab to view all related jobs to the selected rule workflow.
7. To remove a completed job from the list, right-click a completed job and select **Delete**.
8. Click the **Refresh** button if the Jobs List is not updated.

Copying rules

You can copy rules in the Rules Monitor to save time when you need to configure several rules in your operation.

1. In the GV STRATUS Control Panel application, go to **General | Rules | Rules Monitor**.
2. Select a rule or multiple rules that you want to copy in the Rules Monitor.
3. Right-click on the rule(s) and select **Duplicate Rule(s)**.

   The duplicated rule appears in the Rules Monitor with the same rule name and appended with this default suffix: **_Copy(1)**

   If the same rule is duplicated multiple times, the value of the default suffix increments every time.

Exporting rules

You can export rules to another GV STRATUS system to avoid recreation of rules from scratch. Therefore, you can save time when configuring the other GV STRATUS system.

1. In the GV STRATUS Control Panel application, go to **General | Rules | Rules Monitor**.
2. Select a rule or multiple rules that you want to export in the Rules Monitor.
3. Right-click on that rule(s) and select **Export to XML | Save selected Rule**.

   You can also select **Save all Rules** if you want to export all your configured rules.
4. Browse to select the export location and click **Save**.

   The rule is exported as an XML file to the selected location.

Importing rules

You can import rules from another GV STRATUS system to avoid recreating rules repeatedly.

1. In the GV STRATUS Control Panel application, go to **General | Rules | Rules Monitor**.
2. Right-click on the Rules Monitor panel and select **Import from XML | Append existing Rule(s)**.

   You can also select **Skip existing Rule(s)** if you don't want to import the same as existing rules.
3. Browse to select the XML file at the import location and click **Open**.

   The rule is imported into your GV STRATUS Control Panel and appears in the Rules Monitor panel.

Applying rules via the GV STRATUS UI

- The **Visible in STRATUS UI** check-box must be selected under **Rule Options** section in **General | Rules | Rule Editor** of GV STRATUS Control Panel. If permissions settings had been configured, only specific users and groups are allowed to apply the rules via GV STRATUS UI.
- Optionally, select **STRATUS UI only** option under **Frequency** section when configuring the rule in **Rule Editor** tab to only trigger the rule from the UI.
- The rule must be enabled in GV STRATUS Control Panel.

You can trigger rules to be applied on assets via context menu in the Asset List. This is applicable to Export, Transfer, Archive, Custom, and Publish Social Media rules.

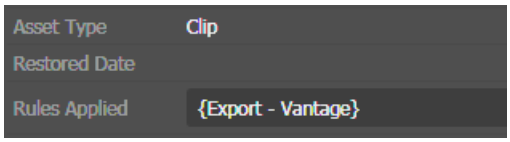
1. In GV STRATUS application, select an asset to be applied with the rule in Asset List.
2. Right-click on the asset and select **Apply Rule | {Rule Name}**.

The rule is automatically triggered and applied on the asset.

***NOTE: Triggering a rule via Asset List will ignore whatever Rule Conditions that have been set up for the rule in* GV STRATUS Control Panel.**

You can see the progress of applied rule in Jobs Monitor. In the Type column, the job displays as **Rules Workflow Job**.

After the job is completed, you can see the rule name in the **Rules Applied** field on the Properties tab of the asset in Inspector.



Related Topics

Adding an archive rule on page 605
Adding an export rule on page 580
Adding a transfer rule on page 598
Enabling and disabling rules on page 636

Identifying assets affected by rules

In the GV STRATUS application you can determine if the Rules Engine has applied a rule to an asset. You do this by searching on the name of the rule. Therefore, create rule names that contain a unique term on which you can search.

In the GV STRATUS application, do an Advanced Search with conditions such as the following:

Rules Applied | contains | <unique term>

For example, if all your export rule names contain the unique term "export", then your search condition is as follows:

Rules Applied | contains | export

The search returns a list of all the assets affected by rules with the unique term in their name.

Adding a thumbnail marker

When configuring an export rule, if you choose to export thumbnails, you must define the thumbnail for an exported asset. An export thumbnail is defined by a `tn` marker added to the source asset. Multiple thumbnails are exported when the source asset has multiple `tn` markers.

1. Load the asset into a GV STRATUS component that adds markers, such as Inspector, Source Viewer, or Channel Panel.
2. In the asset, identify the image to use as an export thumbnail.
3. Add a marker at the image location and name it as `tn`.

The thumbnail at the marker is exported by the export rule.

You can see the export rule is automatically triggered in the **Rules Applied** field on the Properties tab of the Inspector.

You can also see the thumbnail transfer progress in Jobs Monitor.

Related Topics

Adding an export rule on page 580

Adding a Carbon Coder transcode profile

GV STRATUS rules support transcode profiles you create using third party applications. This topic provide steps for the Harmonic ProMedia™ Carbon (formerly Carbon Coder™) application. Refer to the manufacturer's product latest documentation for the list of supported formats.

1. Create the transcode profile as required by your workflow, with requirements as follows:
   - Only one output format per transcode profile is supported by GV STRATUS rules.
   - For import rules, the profile must be a format supported by the K2 and GV STRATUS system and the profile name must have the prefix `Import_`, such as `Import_HD_MXF-D10_NTSC_50.PCP`.
2. Identify the transcode profile file.

   For the ProMedia application, it is the project file, with a *pcp* file extension.
3. Identify the GV STRATUS server that hosts the GV STRATUS Xcode Control Engine. Typically this is the GV STRATUS Core server.

4. Copy the transcode profile to the following directory on the Xcode Control Engine host:

   `C:\Program Files\Grass Valley\STRATUS Transcode Engine\Profiles\RhozetCC`

5. Wait approximately one minute for the GV STRATUS system to detect the transcode profile.

Transcode profiles are available as Transcode Formats when configuring GV STRATUS rules.

Related Topics

Xcode Control engine settings on page 329

Adding a Harmonic WFS transcode profile

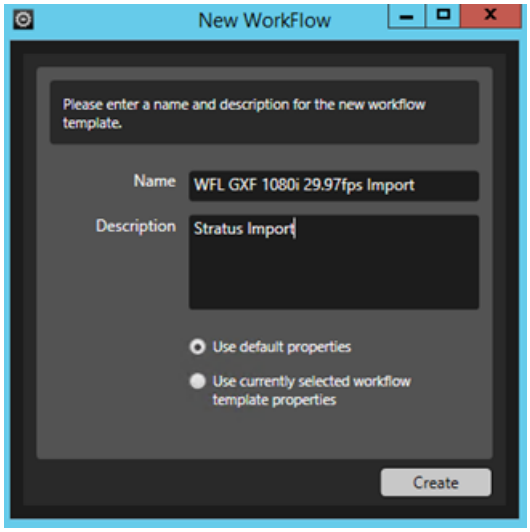
GV STRATUS supports transcode workflow with third party applications. This topic provides steps for the Harmonic WFS application. Refer to the manufacturer's product latest documentation for more info.

1. From the Windows Start Menu, click **Programs | Rhozet | WFS**.

   The WFS Manager (Rhozet Workflow Manager) opens.

2. Select **Tools | Workflow Editor.**
3. Click the **+** button next to **Workflow Templates**.

   The New Workflow dialog opens.



4. Create your new workflow, by entering the following:

   1. Enter a Name for the workflow.
   2. Enter the Description as follows:

      - If you want to use it as a **STRATUS Export** transcode profile, enter **Stratus** in the description field.
      - If you want to use it as a **STRATUS Import** transcode profile, enter **Stratus Import** in the description field.

5. Click the **Create** button.

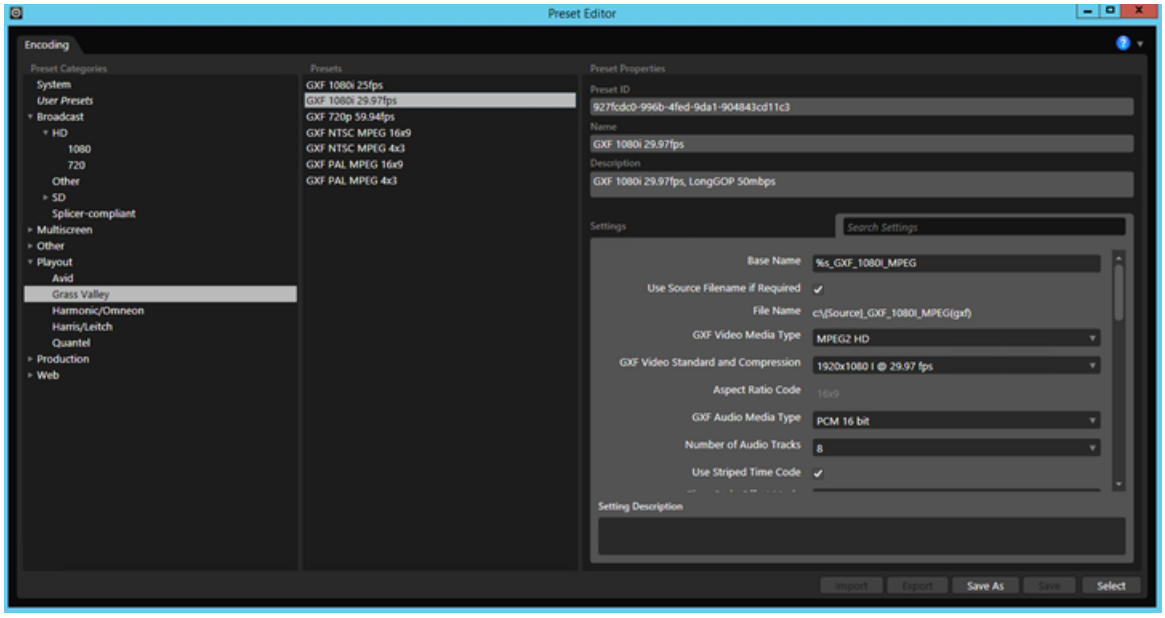
   The Workflow Editor shows the properties of the new Workflow.

6. Right-click on the **Transcode Targets** property and select **Add Target**.

   A new target node displays.

7. To configure the Preset, click the **Browse** button.

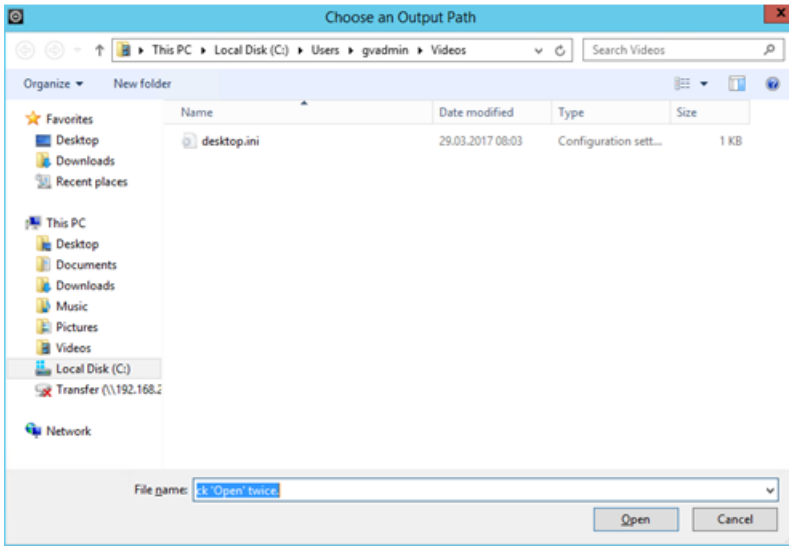
   The Preset Editor displays.



8. Select a preset from the list, or create your own “User Preset”.
9. Click the **Select** button to use the Preset and close the dialog.

10. To configure the Output Path of the new target, click the **Browse** button.

    The Output Path dialog opens.



11. Select any path and click **Open**.

    It is required to be able to save the Workflow Template, but it will be overwritten by the GV STRATUS Transcode Engine when the workflow is executed from GV STRATUS application.

    Both Preset and Output Path are now configured for the new target.

12. Click the **Apply** button to apply the new changes to Harmonic transcode workflow.

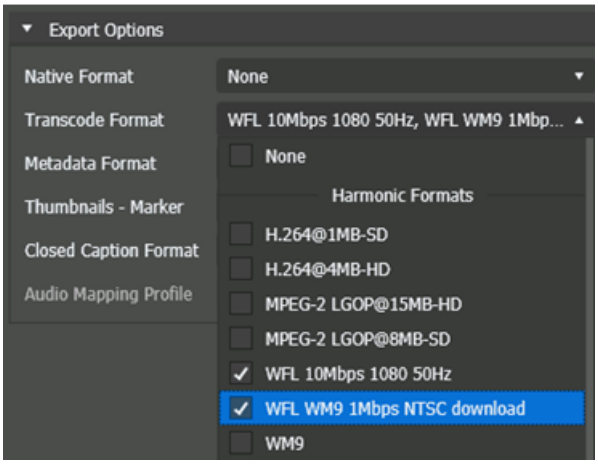
13. Repeat steps 3-12 above to configure more transcode profiles, if needed.

    You can use the new workflow after 2 minutes, for the GV STRATUS Transcode Engine to query the list of workflows from Harmonic WFS.

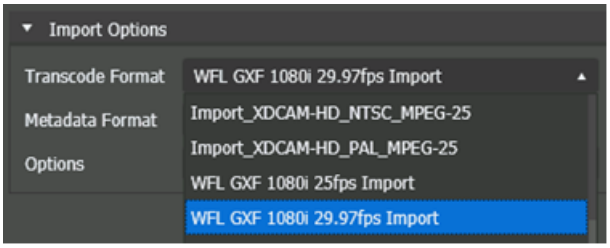
14. Lastly, restart the GV STRATUS Control Panel application to get the newly configured transcode profiles.

The Harmonic WFS transcode profiles are available as Transcode Formats when configuring GV STRATUS rules.

Example of the Harmonic WFS transcode format for the export rule:



Example of the Harmonic WFS transcode format for the import rule:



Adding a Vantage transcode profile

GV STRATUS rules support transcode profiles you create using third party applications. This topic provide steps for the Telestream Vantage™ application. Refer to the manufacturer's product latest documentation for the list of supported formats.

On the GV STRATUS server that hosts the GV STRATUS Xcode Control Engine (typically this is the GV STRATUS Core server), you can find Vantage workflow files at `C:\Program Files\Grass Valley\STRATUS Transcode Engine\Profiles\Vantage`. The files at this location are templates. They are not active Vantage workflows and GV STRATUS rules do not detect these files as transcode profiles. To use one of these template files, you must import it into Vantage Workflow Designer in the "STRATUS" category and activate it as a Vantage workflow. After it is activated in the

"STRATUS" category, GV STRATUS rules automatically discover the Vantage workflow as a transcode profile. It is not necessary to copy files to the Xcode Control Engine host.

1. Using the Vantage Workflow Designer, create the transcode profile as required by your workflow, with requirements as follows:
   a) Create a "STRATUS" category.
   b) Import or create Vantage workflows in the "STRATUS" category.

      If desired, you can copy template Vantage workflows from the Xcode Control Engine host at `C:\Program Files\Grass Valley\STRATUS Transcode Engine\Profiles\Vantage` to an accessible location and import them into Vantage Workflow Designer.

      - For an export rule, the profile description must start with the word `Stratus`.
      - For an import rule, the profile must be a format supported by the K2 and GV STRATUS system and the profile description must start with the words `Stratus Import`.

   c) Configure the **Receive** action.

      This must be the first action in the workflow.

   d) In the Receive action, for **Media Files**, set the **Expected Nickname** to **Original**.
   e) Configure the **Flip** action.

      This must be the second action in the wokflow.

   f) In the Flip action, set **Input media file nickname** to **Original**.
   g) In the Flip action, set **Output Location** to the **OutputPath** variable.
   h) When you are done editing the Vantage workflow, click the **Release** button and then the **Activate** button.

      The Vantage workflow is now activated in the "STRATUS" category.

   Only one output format per transcode profile is supported by GV STRATUS rules.
2. Wait approximately one minute for the GV STRATUS system to detect the transcode profile.

Transcode profiles are available as Transcode Formats when configuring GV STRATUS rules.

Related Topics

Xcode Control engine settings on page 329

Adding an Elemental transcode profile

GV STRATUS rules support transcode profiles you create using third party applications. This topic provides steps for the Elemental® Server web application. Refer to the manufacturer's product latest documentation for the list of supported formats.

1. In GV STRATUS Control Panel Xcode Control engine settings, configure working directory, Elemental server and transcode settings.

2. Using the Elemental Server web application, do the following:
   a) Configure the working directory as a mount point in Elemental.
      This is the working directory that you configured in Xcode Control engine settings.
   b) Configure profiles for use by GV STRATUS rules as follows:
      - Only one output format per transcode profile is supported by GV STRATUS rules.
      - For an export rule, the profile description must start with the word `Stratus`.
      - For an import rule, the profile must be a format supported by the K2 and GV STRATUS system and the profile description must start with the words `Stratus Import`.

   Refer to Elemental product documentation as necessary.
3. Wait approximately two minutes for the GV STRATUS system to detect the Elemental configuration as a transcode profile.

Transcode profiles are available as Transcode Formats when configuring GV STRATUS rules.

Related Topics

Xcode Control engine settings on page 329

Adding export transcode profiles with the XRE Transcoding Profile Tool

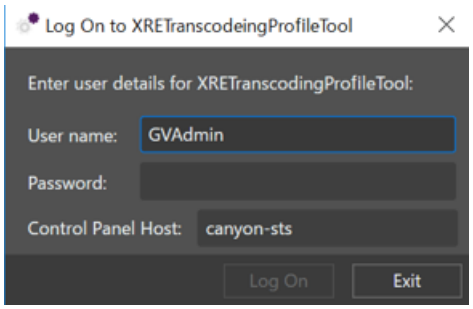
- The Render Engine software must be installed and configured in the GV STRATUS Core server.
- The STRATUS-TRANSCODE license must be installed in the GV STRATUS Core server.
- A transcode profile (*.tpd file) which has exporter presets must be created with an EDIUS or XRE Transcoder application and must be accessible to the XRE Transcoding Profile Tool.

You must use the XRE Transcoding Profile Tool to add transcode profiles of GVRE Transcoder into the GV STRATUS system.

1. Launch the XRE Transcoding Profile Tool from the path below:
   - *`C:\Program Files\Grass Valley\XREServer 9\XRETranscodingProfileTool`*

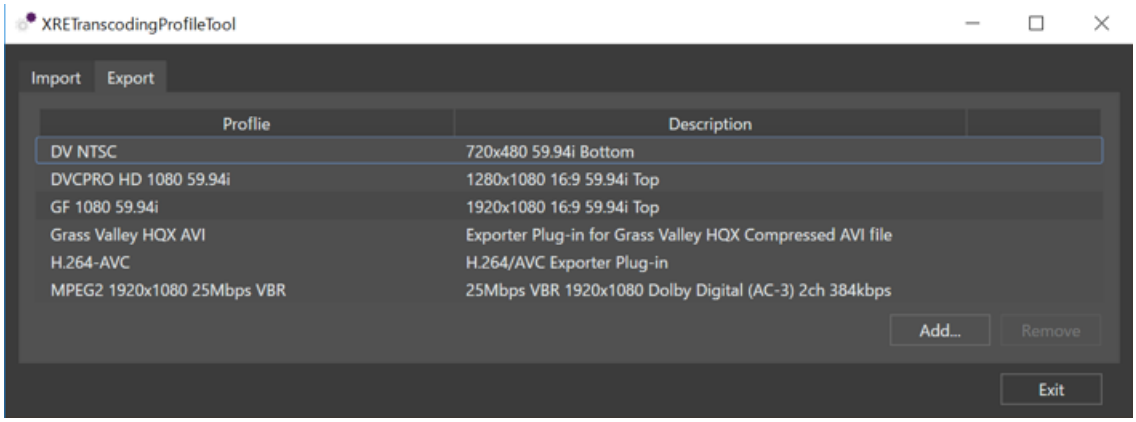
     OR
   - Double-click the **XRE Transcoding Profile Tool** shortcut on your desktop

   The Log On dialog box opens.



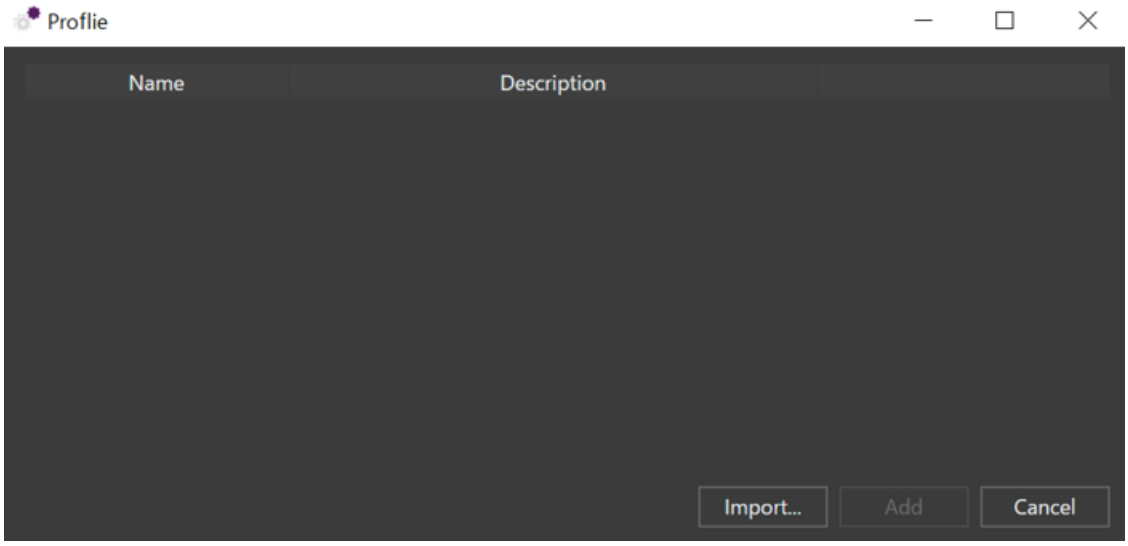
2. Enter your user name and password, then click **Log On**.

3. Click on the **Export** tab to add transcode profiles for export rules.



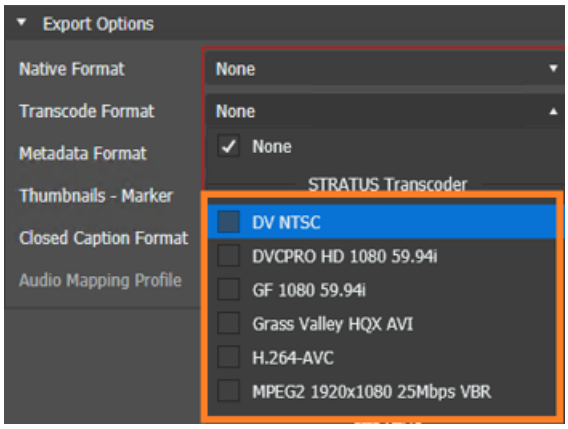
4. Click **Add**.

   The Profile dialog box opens.



5. Click **Import**, then navigate and select exporter presets that had been created earlier with the EDIUS or XRE Transcoder application.
6. Click **Add** to register them as export profiles.

Those selected formats will be available as transcode profiles of STRATUS Transcoder when you configure export rules in the GV STRATUS Control Panel.



Related Topics

Creating Export Transcode Profiles on page 559
Creating Export Transcode Profiles with EDIUS on page 560
Creating Export Transcode Profiles with XRE Transcoder on page 564

Adding import transcode profiles with the XRE Transcoding Profile Tool

- The Render Engine software must be installed and configured in the GV STRATUS Core server.
- The STRATUS-TRANSCODE license must be installed in the GV STRATUS Core server.

You must use the XRE Transcoding Profile Tool to add transcode profiles of GVRE Transcoder into the GV STRATUS system.

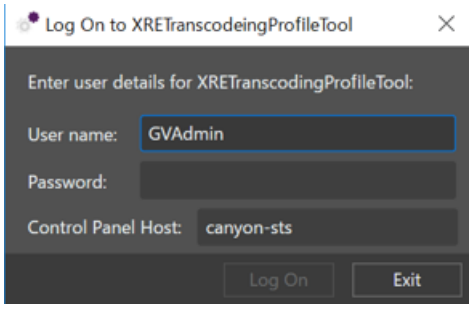
1. Launch the XRE Transcoding Profile Tool from the path below:

   - `C:\Program Files\Grass Valley\XREServer 9\XRETranscodingProfileTool`

     OR

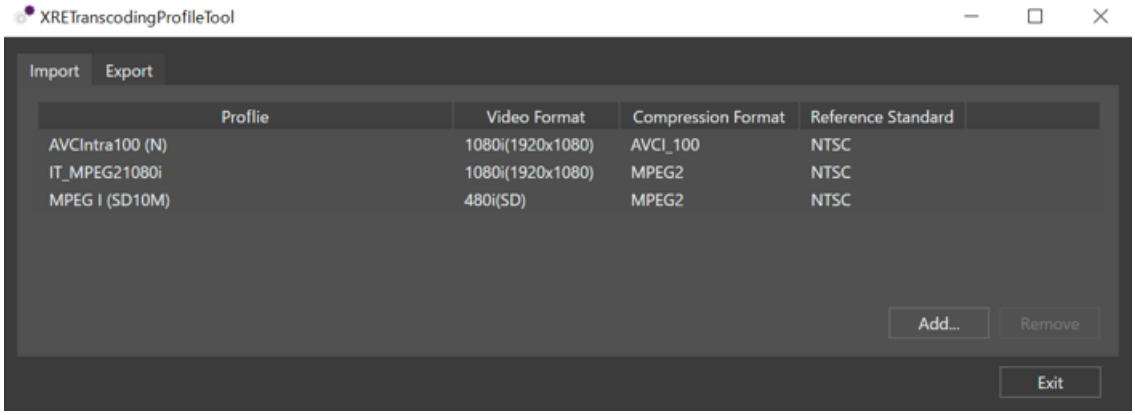
   - Double-click the **XRE Transcoding Profile Tool** shortcut on your desktop

   The Log On dialog box opens.



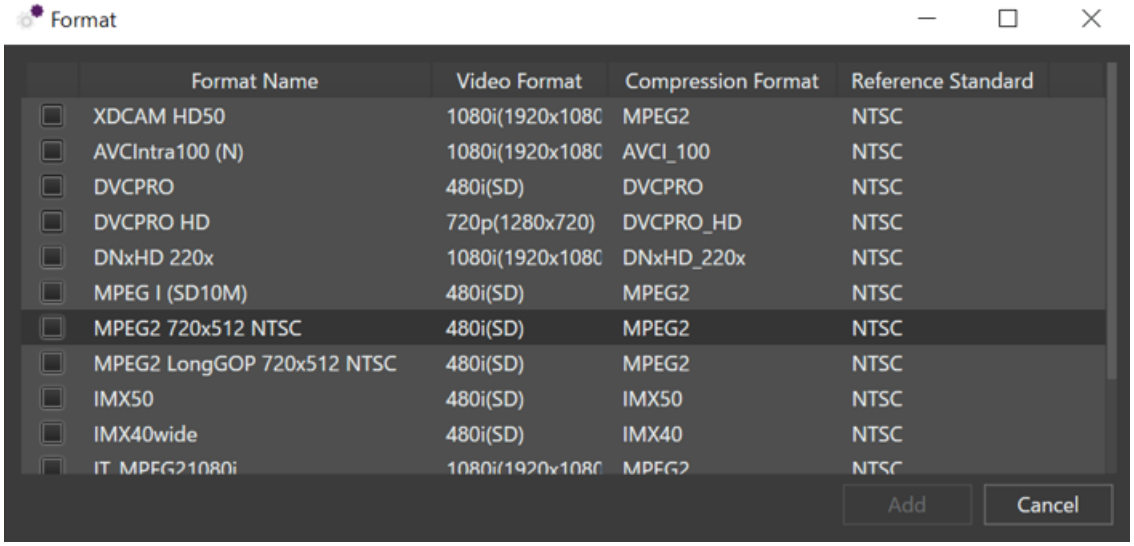
2. Enter your user name and password, then click **Log On**.

3. Click on the **Import** tab to add transcode profiles for import rules.



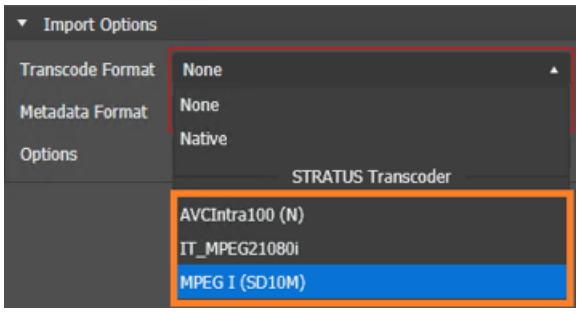
4. Click **Add**.

   The Format dialog box displays all registered formats in the GV STRATUS Control Panel.



5. Select format(s) for your import transcode profiles, and click **Add**.

Those selected formats will be available as transcode profiles of STRATUS Encoder when you configure import rules in the GV STRATUS Control Panel.



Configuring Aspera

GV STRATUS rules support file transfer using third party applications. This topic provides steps for Aspera.

1. On the Aspera server, add the following to the config file at *C:\Program Files (x86)\Aspera\Enterprise Server\etc\aspera.conf*.

```
<server>
<http_port>9091</http_port>
<enable_http>true</enable_http>
<ssh_port>22</ssh_port>
</server>
<central_server>
<port>40001</port>
<address>127.0.0.1</address>
<schema_validation>disable</schema_validation>
</central_server>
```

2. Save the config file.

Disabling previous YouTube configuration

You must disable the previous YouTube configuration because it is not supported any longer in this release.

1. In the GV STRATUS Control Panel, go to **General | Rules | Rules Monitor**.
2. Select all activated rules with a previously configured YouTube destination, and click **Disable**.
3. Click **Remove** to delete all those rules.
4. In the GV STRATUS application, go to Jobs Monitor and delete all rules and transfer jobs.
5. In the GV STRATUS Core server, go to Resource Maintenance UI and select the SubResource Provider.
6. Delete the resource.

Create a new "Publish Social Media" rule in order to continue publishing content to the YouTube channel. For more info, refer to *Configure Social Media Engine* on page 805 and *Adding a publish external media network rule* on page 621.

Importing metadata to create or update assets

You can use GV STRATUS Import rules metadata features to exchange assets with external systems. You can import metadata for an asset that already exists in the GV STRATUS system. This updates the asset's metadata without changing the media essence. You can also update both asset's metadata and media essence, if desired.

Conversely, you can import metadata for an asset that does not yet exist in the GV STRATUS system. This creates a metadata-only GV STRATUS asset, ready for future updates with media essence.

A typical workflow for an existing GV STRATUS asset is as follows:

- Export a GV STRATUS asset's closed caption metadata as an XML file to a translation vendor.
- The translation vendor adds translated versions to the closed caption metadata.

- Import the closed caption metadata XML file into the GV STRATUS system, using GV STRATUS Rule Import Options as follows:
  - Transcode Format: None
  - Metadata Format: GV STRATUS Simple Import
  - Options: Update Asset Metadata
- The GV STRATUS asset now includes the translated closed caption metadata.

The metadata XML file must contain the asset's unique ID.

A typical workflow for creating a new GV STRATUS asset is as follows:

- Provide a copy of a clip to a translation vendor.
- The translation vendor creates closed caption information in an XML file that complies with GV STRATUS metadata.
- Import the closed caption metadata XML file into the GV STRATUS system, using GV STRATUS Rule Import Options as follows:
  - Transcode Format: None
  - Metadata Format: GV STRATUS Simple Import
  - Options: Create New Asset
- The GV STRATUS system creates a metadata-only asset.
- Import the clip with the media essence into the GV STRATUS system.
- The media essence becomes a part of the GV STRATUS asset.

Configuring the XML metadata file name extension

GV STRATUS rules support file transfer into external management systems. For compatibility with the external system, you can set a specific file name extension in the XML metadata export profile for smooth transfers in your operation.

1. On the machine where the Transcode Control Engine is installed, locate the folder containing the metadata export profiles in the path below:

   C:\Program Files\Grass Valley\STRATUS Transcode Engine\Profiles\AssetMetadataExport

2. Select the XSLT metadata export profile, create a copy, and rename the file.

   For example, copy "GV STRATUS Simple.xslt" and rename the new file as "GV STRATUS MRSS.xslt".

3. Open the new file with a text editor of your choice, e.g. Notepad.exe.
4. Add the line below with the desired file extension anywhere (but not inside an XML tag):

   ```
   <!-- FileExtension="mrss" -->
   ```

   It is recommended to add it directly above the line with the first template match: *<xsl:template match="/">*

5. Click **Save** and close the file.

For the XSLT metadata export profile, it is just an XML comment line. However, it will activate the Transcode Control Engine to create the correct file name extension as specified.

Inserting file names of exported files in the XML metadata file

Previously there is no way to access file names of essences that were transferred via export rules, especially when exporting multiple essence files with a transcoding step in between. Now users are able to insert file names and other details in the XML metadata file that will be exported via export rules. Those file names can be extracted later via automated processing.

1. On the machine where the Transcode Control Engine is installed, locate the folder containing the metadata export profiles in the path below:

   C:\Program Files\Grass Valley\STRATUS Transcode Engine\Profiles\AssetMetadataExport

2. Select the XSLT metadata export profile, create a copy, and rename the file.

   For example, copy "GV STRATUS Simple.xslt" and rename the new file as "GV STRATUS Extended.xslt".

3. Open the new file with a text editor of your choice, e.g. Notepad.exe.
4. Add a new XML node that contains all essence file names, thumbnails, CloseCaption file, metadata file, and their file paths as in the example below:

```
          -Native file: assetname_Keywords_Mark In_Date_UserText.gxf

          -transcoded file(s): assetname_Keywords_Mark
In_Date_UserText_FormatName.mp4;  assetname_Keywords_Mark
In_Date_UserText_FormatName.wmv; ...

          -TN's: assetname_Keywords_Mark
In_Date_UserText_10:03:05:00.jpg; ....

         -CloseCaption file: ftp://server/path; assetname_Keywords_Mark
 In_Date_UserText_FormatName.mp4

          -Metadata file: ftp://server7path;  assetname_Keywords_Mark
In_Date_UserText_FormatName.xml
```

5. Click **Save** and close the file.

Transcode rule access

To support third party transcode applications in GV STRATUS rules, servers, network shares, and application must have access to one another over the media network.

A working directory must be created manually as a network share and configured in GV STRATUS Control Panel. The Xcode Control engine temporarily places files in the working directory while exporting an asset. The directory must have enough capacity for your largest concurrent exports and must be hosted by a system with sufficient system resources to process your workload. Grass Valley recommends that the directory be on the K2 storage system, either K2 SAN or if no K2 SAN is present, a standalone K2 Summit system. The working directory must be accessible as follows:

- From the K2 system

- From the transcode application host
- From the GV STRATUS server(s) running the Workflow Engine and the Xcode Control engine.
- The internal system account, which by default is GVAdmin, must have access to the directory.
- If using Elemental® , the directory share must be configured in the Elemental Server web application as a mount point. Refer to Elemental® for more information.

The transcode application host must have access as follows:

- FTP access to K2 storage.
- If source files are located on a network share, the transcode application host must have access to the share.
- The network share directory to which the transcode application writes its output.
- Full access to the shared working directory.

The Xcode Control engine must have access as follows:

- The network share directory to which the transcode application writes its output.
- Full access to the shared working directory.
- For Harmonic ProMedia™ Carbon (formerly Carbon Coder™):
  - Network access to the Carbon Server port 1120.
- For Telestream Vantage™:
  - Network access to the Vantage Server port 8676.
  - Full access to the `Store` share on the Vantage server.

Publishing content to Social Media platforms

GV STRATUS version 6.0 introduces the Social Media Management, which allows you to directly publish content and metadata (providing it is supported by the social media platform) to popular social media networks (such as Facebook, Twitter, and YouTube) and track those assets so you can see their popularity on the social platforms, then also delete and manage the content via GV STRATUS for simple housekeeping.

With GV STRATUS version 6.5, the External Media Engine is introduced to support publishing via Social Media CMS-Systems. Instead of managing each social media platform individually, GV STRATUS users may assign third party CMS-Systems to manage and publish contents to their various Social Media accounts. The External Media Engine supports all the same functionalities of the Social Media Engine such as directly publish content and metadata to social media platforms, track popularity of published assets, and easy workflow to delete media and metadata if needed.

Video content and (optionally) stills, closed captions and metadata can be immediately published from the system to Facebook, Twitter or YouTube. Users in News or Live Production will be able to distribute their content to their viewers and subscribers without the need for complex downstream systems. GV STRATUS will control the creation, transcoding and publishing of the media, exporting and uploading the asset metadata in parallel.

The GV STRATUS Social Media Management will also collect statistics and usage info for these assets, allowing users to immediately see how their content is being consumed and rated on individual social platforms.

The GV STRATUS Social Media Management also tracks the assets on the social networks so that, when the time comes for housekeeping of the assets in the GV STRATUS system, you can also delete the media and metadata from each social media platform. This means a much simpler and cleaner workflow for media managers and digital teams when they use GV STRATUS.

For more information, refer to the *GV STRATUS Social Media Management page*.

Related Topics

Social Media Engine Server set up process on page 802
Social Media engine settings on page 337
External Media locations configuration settings on page 375
Configure and authenticate Facebook location on page 809
Configure and authenticate Twitter location on page 812
Configure and authenticate YouTube location on page 815

Supported formats for Facebook

This specification applies to the publish of assets from GV STRATUS system to Facebook.

Formats supported are as follows:

Type	Supported formats
Video	3g2, 3gp, 3gpp, asf, avi, dat, divx, dv, f4v, flv, gif, m2ts, m4v, mkv, mod, mov, mp4, mpe, mpeg, mpeg4, mpg, mts, nsv, ogm, ogv, qt, tod, ts, vob, and wmv
Close Caption	SubRip (.srt)
Thumbnail	PNG, and JPG (1 thumbnail along with the Video/Audio content)

NOTE: A standard Facebook account has the file size limitation of 1 GB, or 20 minutes clip duration.

Supported formats for Twitter

This specification applies to the publish of assets from GV STRATUS system to Twitter.

Format supported is as follows:

Supported format		Notes
Video	mp4	A standard Twitter account has the file size limitation of 500 MB, or 10 minutes clip duration.

NOTE: Twitter does not support any Close Caption formats and thumbnails as additional information to Video/Audio content.

Supported formats for YouTube

This specification applies to the publish of assets from GV STRATUS system to YouTube.

Formats supported are as follows:

Supported formats		Notes
Video	1080p HD	—
	MPEG-2	Saved with a .MPG extension
	MPEG-4	—
Audio	Dolby AC-3	For MPEG-2, with audio bitrate: 128 kbps or more
	MPEG Layer II	For MPEG-2, with audio bitrate: 128 kbps or more
	AAC	For MPEG-4, with audio bitrate: 128 kbps or more
Close Caption	SubRip (.srt)	Only basic versions of these files are supported. No style information (markup) is recognized. The file must be in plain UTF-8.
	TTML: Timed-Text Markup Language (.ttml)	In partial implementation. SMPTE-TT extensions supported for *CEA-608* features. iTunes Timed Text (iTT) file format is supported; iTT is a subset of *TTML, Version 1.0*. Styling and positioning are supported.
	Scenarist Closed Caption (.scc)	These files have an exact representation of *CEA-608 data*, which is the preferred format whenever captions are based on CEA-608 features.
Thumbnail	JPG	1 thumbnail along with the Video/Audio content. YouTube creates three individual thumbnails per upload based on their algorithm, and only one can be selected as the clip thumbnail.

NOTE: A standard YouTube account has the file size limitation of 2 GB and the clip duration depends on the used video codec.

Social/External Media matrix

GV STRATUS supports the option to export either No metadata with the Video/Audio essence, or allows selecting the default profile **External Media** from the Metadata Format drop-down list when configuring the **Publish External Media network** rule.

GV STRATUS supports these features for Social/External Media platform as follows:

Supported Features	YouTube	Twitter	Facebook	Verizon
Video/Audio Essence				
Publish Hi-Res (SD, HD)	**MXF, GXF, MOV**	Not supported.	**MOV**	**MXF, GXF**

Supported Features	YouTube	Twitter	Facebook	Verizon
Publish GV Stratus Lo-Res (MPEG4)	Supported.	Supported.	Supported.	Supported.
Publish other Lo-Res essence formats	Supported.	Not supported.	Supported.	Supported.
Associated Metadata				
Publish metadata - Asset Name	Supported.	Supported.	Supported.	Supported.
Publish metadata - Asset Description	Supported.	Supported.	Supported.	Supported.
Publish metadata - Asset Tags	Not supported.	Supported.	Not supported.	Supported.
Publish metadata - Privacy status	Supported. • For **Public** status only	Not supported.	Not supported.	Not supported.
Publish - 'Closed Caption (CC) Language' information	Supported. • For **en** only	Not supported.	Supported. • For **en_US** only	Not supported.
Publish - 'Content Category' information	Supported.	Not supported.	Supported. • For **OTHER** only	Supported.
Associated reference image				
Publish associated Thumbnail	Supported.	Not supported.	Supported.	Supported.
Associated Closed Caption				
Publish associated Closed Caption	**SRT ; TTML**	Not supported.	**SRT**	**SCC**
Gathering of statistics				
Gather Counts -> View	Supported.	Not supported.	Not supported.	Not supported.
Gather Counts -> Like	Supported.	Supported.	Supported.	Not supported.

Supported Features	YouTube	Twitter	Facebook	Verizon
Gather Counts -> Share	Not supported.	Supported.	Supported.	Not supported.
Manage media on platform				
Check cyclic whether media still exist	Supported.	Supported.	Supported.	Supported.
Delete media on platform	Supported.	Supported.	Supported.	Supported.

By default, the above listed GV STRATUS Asset metadata are published to the social/external media platform. Some of them are configurable to GV STRATUS Custom Metadata field(s) such as the Asset -Name, -Description, or -Tags.

If you want to modify the configuration, it is recommended to edit the provided .xslt file and save it under a different name here:

C:\Program Files\Grass Valley\STRATUS Transcode Engine\Profiles\AssetMetadataExport\SocialMedia

For the **Content Category** metadata field: By default, custom metadata fields must be created manually by an administrator. In this case, the Social Media Engine once installed creates this *Custom Metadata field* automatically.

If there was nothing entered for an asset, default values are published depending on the individual platform.

Setting up GV STRATUS in ENPS

The GV STRATUS application needs to be installed on ENPS client machines in order to use the GV STRATUS ActiveX within ENPS.

To set up GV STRATUS as ActiveX device in ENPS, you need to modify your ENPS configuration.

1. On the ENPS server, find the *enps.ini* file and add the following to the **[ENPS]** section:

   ```
   QTMediaExtensions=.mov,.mp4
   ```

2. On an ENPS client, log in as the administrator and start up ENPS.

3. From the ENPS folder, select **System Maintenance | MOS Configuration | New** and create a new MOS entry with these parameters:

ID	The MOS ID; this value is case sensitive and must match the MOS ID configured in the XMOS Server Options.The recommended format is <family>.<machine>.<location>.<enterprise>.mos. Standard practice is to use station call letters for location and station group abbreviation for enterprise.
Description	GV STRATUS
IP	The IP address or host name of the machine hosting the SDB Server and the XMOS Server.
ActiveX	GV.STRATUS.1
Default Settings	Leave blank. These settings are configured during installation.
Program	The group ID that had been configured in **System Maintenance	Groups**.
MOS Version	2.6 or 2.8.2
Local DragDrop	Off
Auto Create	On
Story Send	On

4. From the ENPS folder, select **System Maintenance | Global Configuration Options**, add a new property named `AddMOSObjDuration` and set its value to **1**.

   NOTE: `AddMOSObjDuration` is the optional setting that allows the duration of clips to be automatically included in the rundown timing. If you prefer to manually enter the duration of your story and clips, do not activate this setting.

5. Add **mp4** to the `MOSBrowseMediaExtensions` property, as can be seen below:

   ```
   MOSBrowseMediaExtensions=bmp,jpg,jpeg,mp4,3gp,wmv,wav,sdp,ts
   ```

6. Restart the ENPS client application.

Setting up Avid workstations with GV STRATUS

The MEWS system must be installed and operational.

Work through the topics in this section to set up the workflow between GV STRATUS and Avid Media Composer®.

MEWS Server set up process

Only systems with a MEWS Server require this process. Use SiteConfig for software install of GV STRATUS components. On the GV STRATUS Core server, use SabreTooth and install the MEWS license.

1. *SiteConfig MEWS Server network set up* on page 662. Only systems with a MEWS Server require this process.

2. *SiteConfig MEWS Server software install* on page 663. Only systems with a MEWS Server require this process.
3. *SabreTooth MEWS license process* on page 665. Only systems with a MEWS Server require this process.

SiteConfig MEWS Server network set up

Only systems with a MEWS Server require this process.

Adding a MEWS Server to the SiteConfig system description

- MEWS Servers are racked, cabled, and powered on.
- The system description must contain a group.

This topic applies to a MEWS Server.

1. In the **Network Configuration | Devices** tree view, right-click a group and select **Add Device**.
2. Configure settings for the device you are adding as follows:
   - Family: GV STRATUS
   - Device Type: GV STRATUS Server
   - Model: GV STRATUS MEWS Server
   - Name – This is the device name, as displayed in the SiteConfig device tree view and device list view. This name can be different than the host name (network name). You can accept the default name or enter a name of your choice. Devices in the tree view are sorted alphabetically.
   - Amount — Select the number of MEWS Servers, according to your system design.
   - Platform — Select **x64**.
   - Control network– Select the control network.
   - Starting Address – Select from the list of available addresses on the selected control network. If adding multiple devices, this is the starting address, with addresses assigned sequentially to each device added.
3. Click **OK** to save settings and close.

   SiteConfig adds the MEWS Server to the system description as a placeholder device.
4. Verify that unmanaged control network interface is configured correctly and modify if necessary.

Next, add the server to the control network.

Adding a GV STRATUS server to the control network with SiteConfig

Use SiteConfig to configure network settings on a separate GV STRATUS server.

Before doing this task, make sure the GV STRATUS server is added as a placeholder device to the SiteConfig system description.

The following steps are the standard tasks for adding a device to the control network using SiteConfig. Use these steps for the GV STRATUS server you are adding.

1. Discover the device using SiteConfig device discovery.
2. Assign the discovered device to the placeholder device in the SiteConfig system description.
3. Modify the control network interface to ensure communication on the control network.

4. Modify the host name and/or device name as desired.
5. Ping the device to verify network communication.
6. Verify credentials to ensure SiteConfig can install software on the device.
7. Generate and/or add to host tables as appropriate for your network.

Related Topics

Adding a device to a network with SiteConfig on page 490
Adding a device to a network with SiteConfig on page 490

SiteConfig MEWS Server software install

Only systems with a MEWS Server require this process.

- If your GV STRATUS system has one or more MEWS Servers, install software on those servers.

Setting deployment options

- A software package must be assigned to the deployment group and applicable deployment tasks must be displayed in the Tasks area.

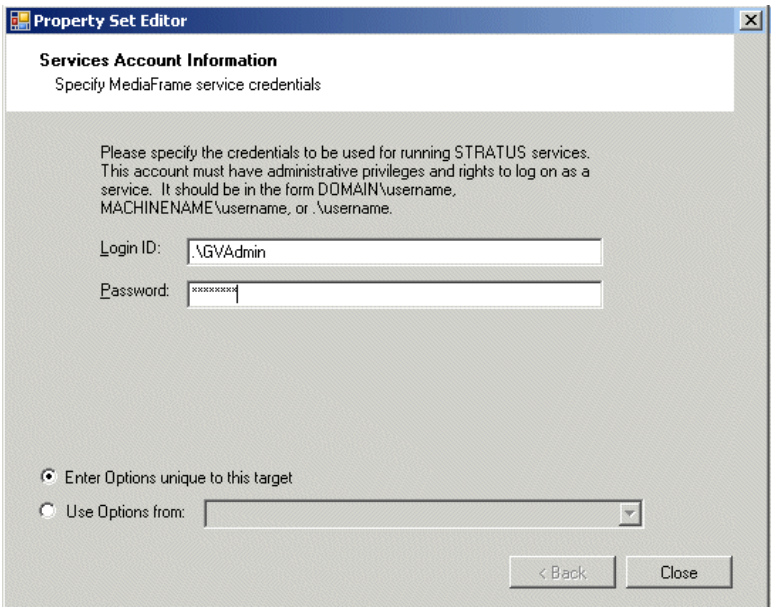
1. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.
2. In the Tasks list view, view tasks and determine if you must set deployment options.

   Tasks that need to have deployment options set display in the Details column a message stating "Deployment options required."

   If you select a task that needs to have its deployment options set, the Start Deployment button is disabled and the message is displayed next to the button.
3. Do one of the following to set deployment options:
   - Double-click the task.
   - Select the task and click the **Options** button.

   A wizard opens.

4. Work through wizards and set deployment options for GV STRATUS software as follows:

Software	Deployment options
GrassValley_STRATUS_CommonServices GrassValley_STRATUS_ControlPanelService GrassValley_STRATUS_CoreServices GrassValley_STRATUS_CRArchive_MDI GrassValley_STRATUS_Databases GrassValley_STRATUS_DataMover GrassValley_STRATUS_DIVA_MDI GrassValley_STRATUS_ExternalMedia GrassValley_STRATUS_FlashNet_MDI GrassValley_STRATUS_GFTP_MDI GrassValley_STRATUS_HttpProxyServer GrassValley_STRATUS_IngestServices GrassValley_STRATUS_Masstech_MDI GrassValley_STRATUS_MediaFlow GrassValley_STRATUS_MEWS GrassValley_STRATUS_Proxy_MDI GrassValley_STRATUS_ProxyStreamingService GrassValley_STRATUS_RenderEngine GrassValley_STRATUS_Rules GrassValley_STRATUS_ScheduledTransferEngine GrassValley_STRATUS_SocialMedia GrassValley_STRATUS_Summit_MDI GrassValley_STRATUS_TrafficGateway GrassValley_STRATUS_Transcode GrassValley_STRATUS_WebApps GrassValley_STRATUS_WebClient GrassValley_DeviceKeyService GrassValley_LogManager GrassValley_LogViewer	 Use the local system account if your system is on a workgroup or if it's on a domain but uses the local system account in SQL. Use a domain\admin account if the account was previously mapped in SQL to the MediaFrame, MediaFlow, RulesEngine and WFPersistence databases. Entering account credentials allows you to use the **Use options from** feature for all other devices of the same type. Once you enter the account credentials this way on the first device, it becomes the template from which options for other devices are copied.

5. If you have multiple devices of the same type, you can enter deployment options for one of them using the wizard. Then, when you bring up the same wizard on every device, you can choose the **Use options from** radio button and select the first device for which you set options.

   SiteConfig copies the options you set for the first device and fills in the blanks on the wizard.

Installing software on a MEWS Server

Only systems with one or more MEWS Servers require this process. Use SiteConfig to install software on the MEWS Servers.

- The server on which you are installing software is in the SiteConfig system description and communicating on the control network.
- The server on which you are installing software has its credentials set in SiteConfig to allow access.
- The GV STRATUS MEWS Engine must not be installed together with any other engine to avoid conflict for the usage of port 8081.

1. Verify the SiteConfig roles currently assigned to the server. If the roles are not correct for your system design, add or remove roles accordingly. Roles are as follows:
   - GV STRATUS MEWS Engine
   - GV Log Manager
2. Add the server to a deployment group, such as the GV STRATUS deployment group.
3. Add the following files to the deployment group:
   - *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
     - *GrassValley_STRATUS_MEWS_x.x.x.cab*
     - *GrassValley_LogManager_x.x.x.cab*

   Refer to release notes for version numbers.
4. Do the SiteConfig **Check Software** operation on the server.
5. Verify that deployment tasks are set to **Install** for the files listed above.

   If a WFRegMon install task appears, install it as well. It is required to support Grass Valley software installers. There is no uninstall task.
6. Deploy software to the server.
7. Restart as prompted.
8. After deployment is complete, start the MEWS Service.

Next, license the MEWS Server.

SabreTooth MEWS license process

Only the GV STRATUS server with role of Common Services requires this process.

The following MEWS license is installed on the GV STRATUS server with role of Common Services. Typically the GV STRATUS Core server has the role of Common Services.

These licenses are required for each MEWS Service software component in your GV STRATUS system. They are SabreTooth floating licenses, not restricted to a single computer.

- STRATUS-XCODECONTROLMEWSEXT
- STRATUS-XCODECONTROLMEWS

The STRATUS-XCODECONTROLMEWSEXT license supports native format transfers between Avid and GV STRATUS, without transcoding capability. With this license, native format is the only supported transcode format for imports via the rules engine.

The STRATUS-XCODECONTROLMEWS license is optional for added functionality: it supports all MEWS transcode formats in import rules.

NOTE: Multiple MEWS licenses of the same type are not supported in a* GV STRATUS *system.

1. Refer to the license sheet that you received with your GV STRATUS license. The license sheet has the Sales Order number that you need.
2. On the GV STRATUS server with role of Common Services, run the SabreTooth License Manager, generate a unique ID, and send the email to Grass Valley requesting your license or licenses.

   Refer to this Topic Library for detailed licensing procedures.
3. When you receive your license file, use SabreTooth License Manager and install it on the server.

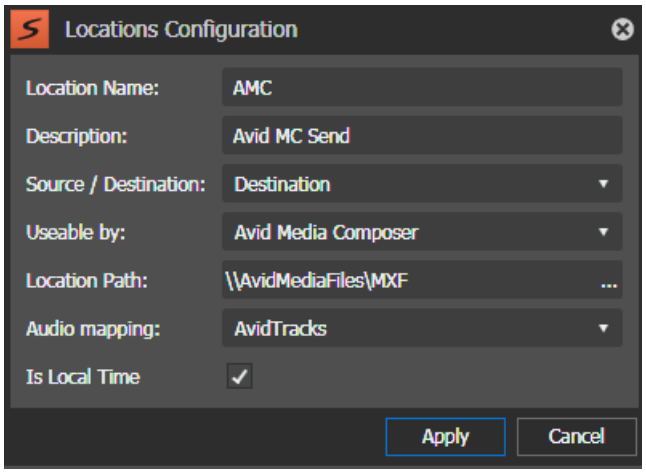
Configure Avid Media Composer send destinations

Only systems that send assets to Avid Media Composer® workstations require this process.

- A separate server machine was configured and the MEWS software deployed by SiteConfig.
- A "STRATUS-XCODECONTROLMEWSEXT" or "STRATUS-XCODECONTROLMEWS" license is available.

For each Avid Media Composer® workstation, configure a location as follows:

1. In GV STRATUS Control Panel, navigate to **General | Locations Config | Locations Configuration | Add**.

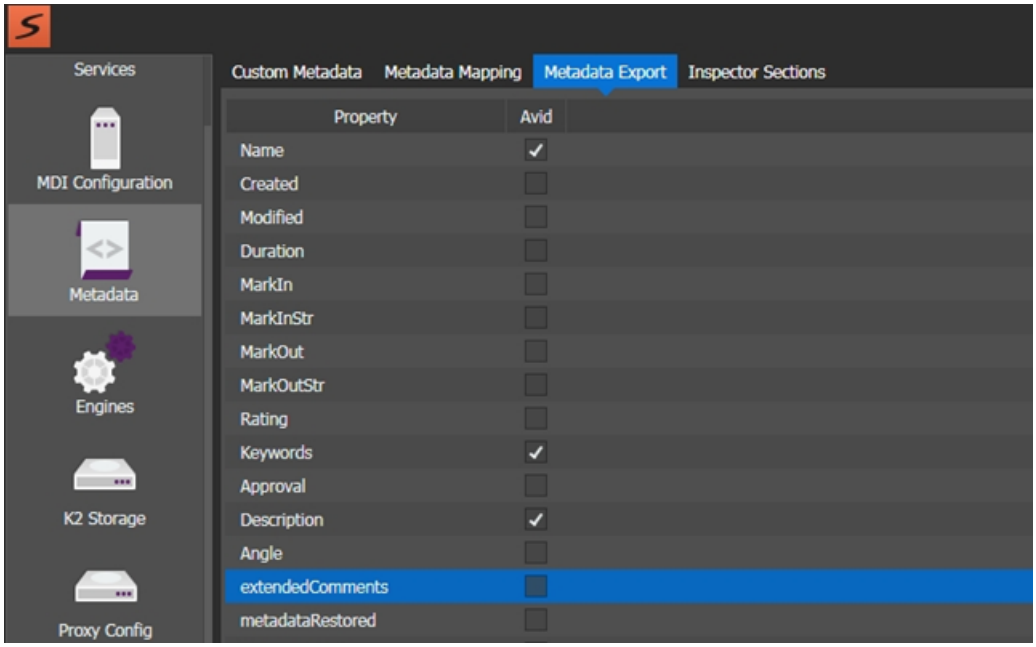


2. Configure as follows:

Setting or button	Description
Location Name	The name of the location, as it appears in the application. This can be any name, as appropriate for your workflow. This identifies the Avid Media Composer® workstation when sending assets to Avid in the GV STRATUS application.
Description	Your description of the location.
Source / Destination	Set to **Destination**.
Usable by	Set to **Avid Media Composer**.
Location Path	The UNC path to the `Avid MediaFiles\MXF` folder on the Avid Media Composer® workstation. You can browse to the folder location to select the correct destination in your network.
Audio mapping	This setting is only applicable when Avid Media Composer, Avid ISIS, or Avid Interplay system is selected. Specifies the audio track mapping of assets to be exported into Avid system. Audio track profiles can be created via the Audio Tag Management setting in the GV STRATUS Control Panel. Those audio profiles are then selectable in the **Audio Mapping** drop-down list when configuring export into the Avid system.
Is Local Time	Specifies the date and time of metadata fields for Avid in local time, instead of UTC. This setting is only applicable when Avid Media Composer, Avid ISIS, or Avid Interplay system is selected.

3. Click **Apply**.
4. To configure which GV STRATUS metadata fields are transferred, go to **Metadata | Metadata Export** in GV STRATUS Control Panel.

5. Select metadata fields under the **Avid** column that should be passed when assets are sent from GV STRATUS.



Related Topics

Using the GV STRATUS application with Avid on page 1227

Configure Avid ISIS send destinations

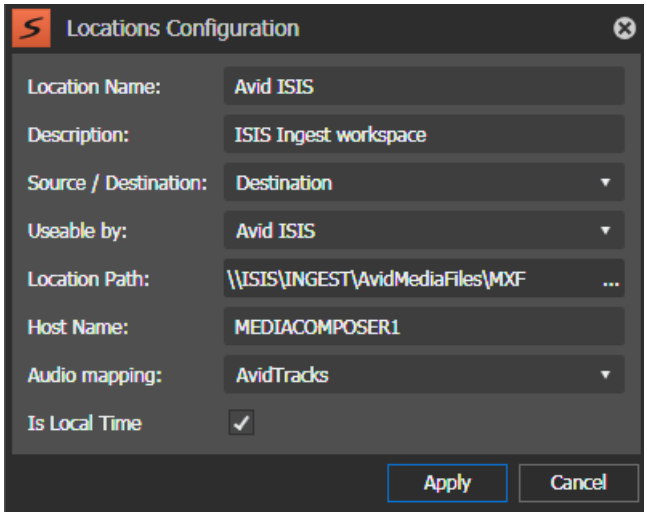
Only systems that send assets to Avid ISIS storage require this process.

- A separate server machine was configured and the MEWS software deployed by SiteConfig.
- A "STRATUS-XCODECONTROLMEWSEXT" or "STRATUS-XCODECONTROLMEWS" license is available.

- The Avid ISIS storage system must be installed and operational.

Configure a location as follows:

1. In GV STRATUS Control Panel, navigate to **General | Locations Config | Locations Configuration | Add**.

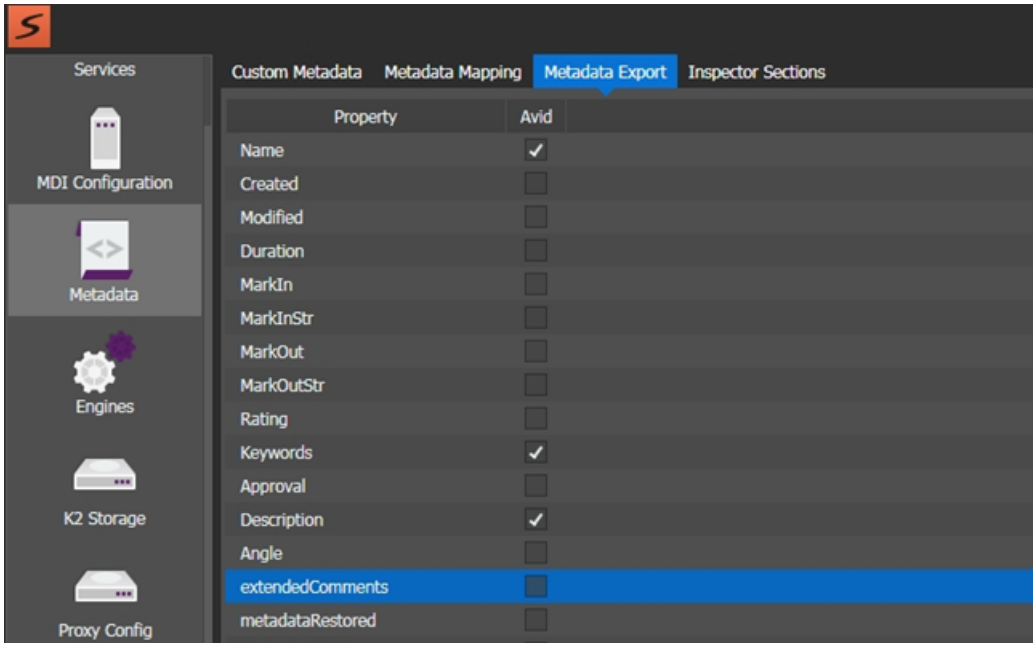


2. Configure as follows:

Setting or button	Description
Location Name	The name of the location, as it appears in the application. This can be any name, as appropriate for your workflow. This identifies the Avid ISIS storage when sending assets to Avid in the GV STRATUS application.
Description	Your description of the location.
Source / Destination	Set to **Destination**.
Usable by	Set to **Avid ISIS**.
Location Path	The UNC path to the `Avid MediaFiles\MXF` folder within the required workspace on the Avid ISIS storage. You can browse to the folder location to select the correct destination in your network.
Host Name	The host name of the Media Composer workstation that is going to use the content (drag and drop into Avid bin) from GV STRATUS.
Audio mapping	This setting is only applicable when Avid Media Composer, Avid ISIS, or Avid Interplay system is selected. Specifies the audio track mapping of assets to be exported into Avid system. Audio track profiles can be created via the Audio Tag Management setting in the GV STRATUS Control Panel. Those audio profiles are then selectable in the **Audio Mapping** drop-down list when configuring export into the Avid system.
Is Local Time	Specifies the date and time of metadata fields for Avid in local time, instead of UTC. This setting is only applicable when Avid Media Composer, Avid ISIS, or Avid Interplay system is selected.

3. Click **Apply**.
4. To configure which GV STRATUS metadata fields are transferred, go to **Metadata | Metadata Export** in GV STRATUS Control Panel.

5. Select metadata fields under the **Avid** column that should be passed when assets are sent from GV STRATUS.



Configure Avid Interplay send destinations

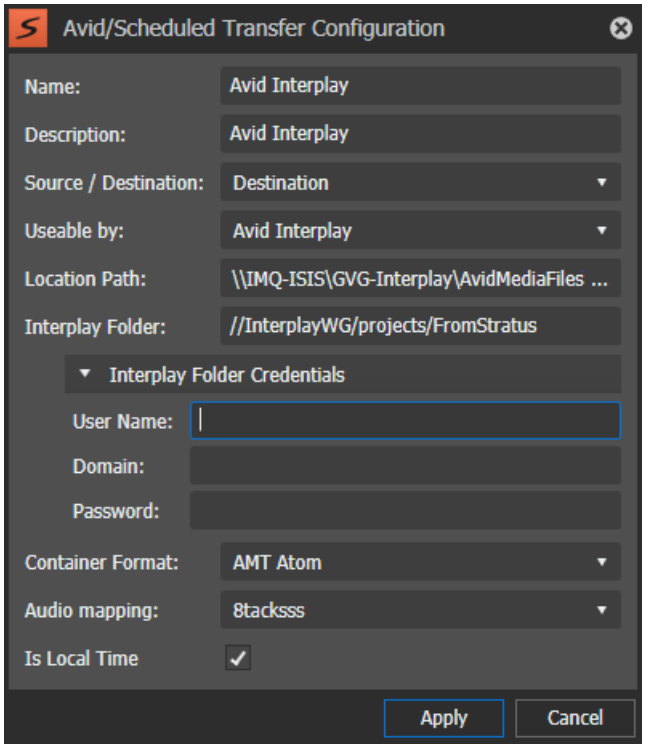
Only systems that send assets to Avid Interplay require this process.

- A separate server machine was configured and the MEWS software deployed by SiteConfig.
- A "STRATUS-XCODECONTROLMEWSEXT" or "STRATUS-XCODECONTROLMEWS" license is available.

- The Avid ISIS storage system must be installed and operational.

Configure a location as follows:

1. In GV STRATUS Control Panel, navigate to **General | Locations Config | Locations Configuration | Add**.

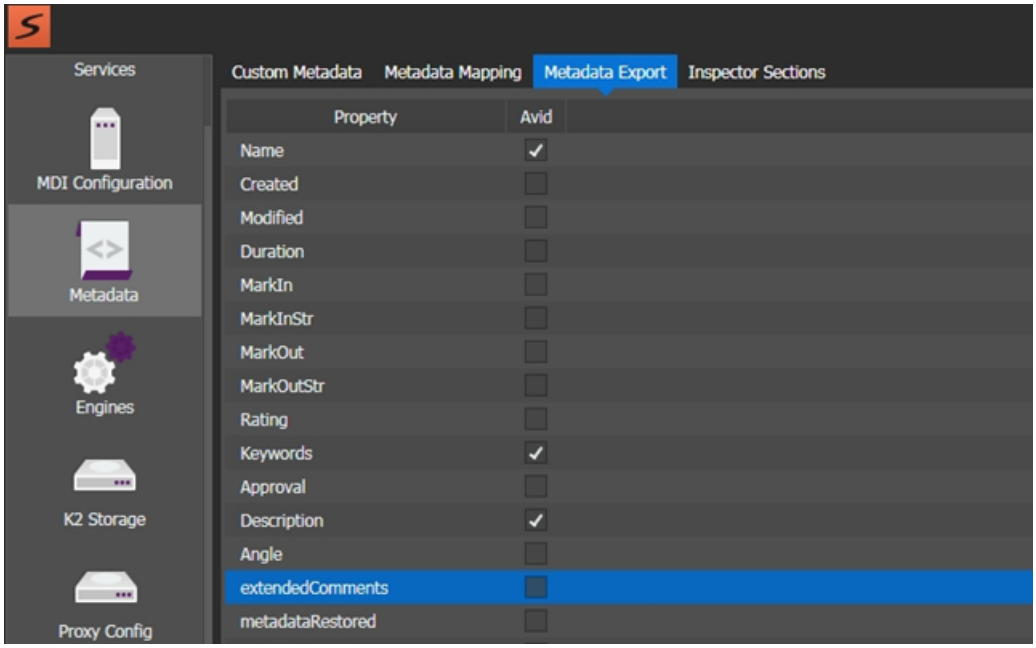


2. Configure as follows:

Setting or button	Description
Location Name	The name of the location, as it appears in the application. This can be any name, as appropriate for your workflow. This identifies the Avid Interplay system when sending assets to Avid in the GV STRATUS application.
Description	Your description of the location.
Source / Destination	Set to **Destination**.
Usable by	Set to **Avid Interplay**.
Location Path	The UNC path to the `Avid MediaFiles\MXF` folder within the required workspace on the Avid ISIS storage. You can browse to the folder location to select the correct destination in your network.
Interplay Folder	The Interplay folder where the asset and corresponding metadata will be checked-in to Interplay. Use the following format: `//InterplayWorgroup/folderlevel1/folderlevel` For example: `//InterplayWG/projects/FromStratus`
Interplay Folder Credentials	The user name, domain name, and password to access the Interplay folder.
Container Format	MEWS offers two container types when sending assets from GV STRATUS to Avid Interplay. Select one from the folowing: • **MEWS Atoms** - do not support growing files. • **AMT Atoms** - support sending (opening and editing) growing files from K2 to Avid. Select this option if you intend to send K2 files to Avid Interplay while they're still recording. ***NOTE: For assets transfers via AMT Atoms, markers must be named with valid Avid Interplay "user name" for markers to be successfully transferred into the Avid system.*** ***Important: AMT Atoms do not support any 1080p formats at the moment. Select MEWS Atoms if you need to send 1080p assets to Avid Interplay.***
Audio mapping	This setting is only applicable when Avid Media Composer, Avid ISIS, or Avid Interplay system is selected. Specifies the audio track mapping of assets to be exported into Avid system. Audio track profiles can be created via the Audio Tag Management setting in the GV STRATUS Control Panel. Those audio profiles are then selectable in the **Audio Mapping** drop-down list when configuring export into the Avid system.

Setting or button	Description
Is Local Time	Specifies the date and time of metadata fields for Avid in local time, instead of UTC. This setting is only applicable when Avid Media Composer, Avid ISIS, or Avid Interplay system is selected.

3. Click **Apply**.
4. To configure which GV STRATUS metadata fields are transferred to Interplay, go to **Metadata | Metadata Export** in GV STRATUS Control Panel.
5. Select metadata fields under the **Avid** column that should be passed to Interplay when assets are sent from GV STRATUS.



Adding the Transfer to Avid rule for automatic transfers into Avid ISIS / Interplay systems

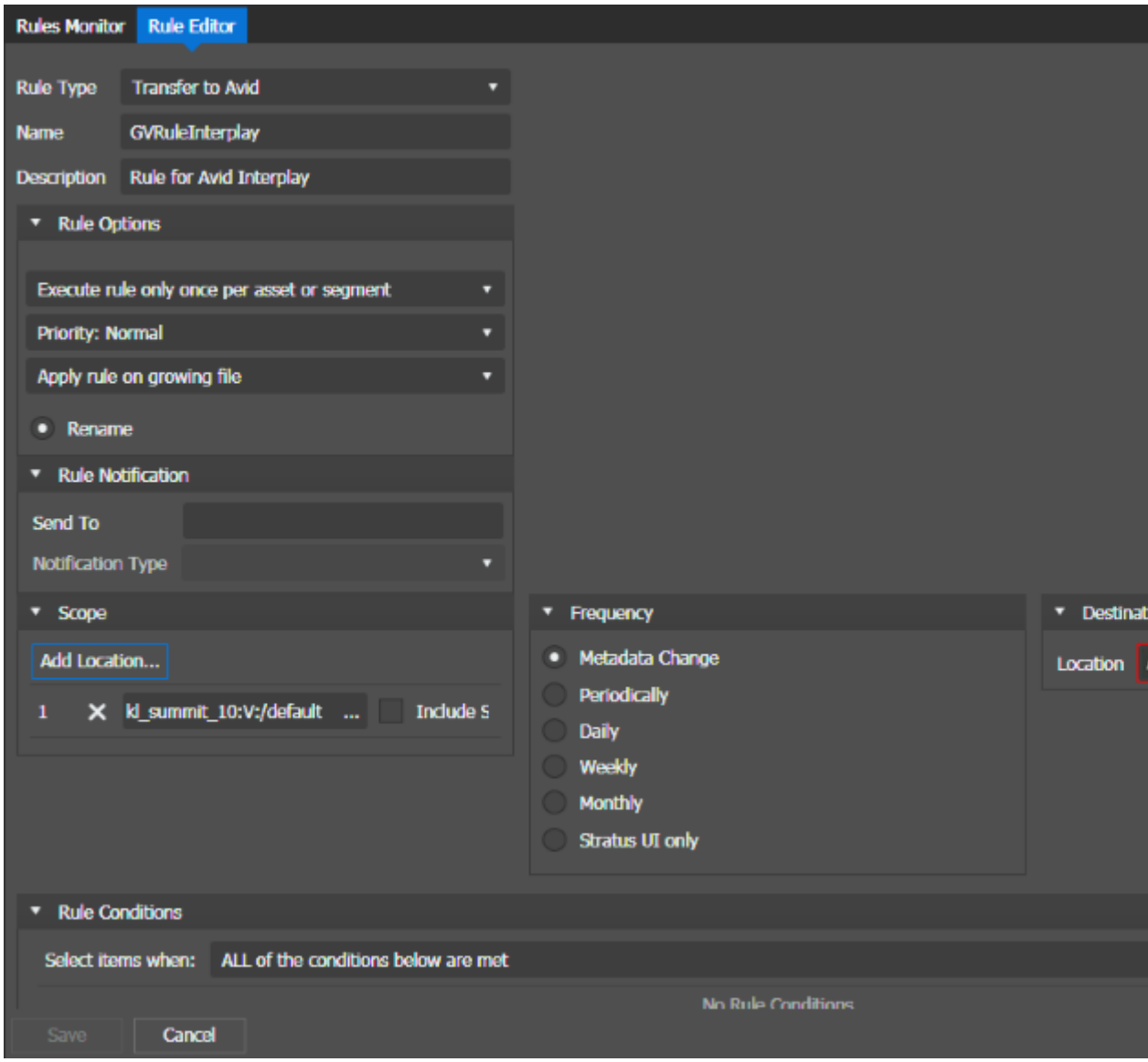
GV STRATUS allows the automatic process of sending content from GV STRATUS / K2 systems to Avid Interplay / ISIS via a workflow rule.

- The MEWS system must be installed and operational.
- The MEWS system must be configured in GV STRATUS Control Panel Engines settings.

- The Avid ISIS storage system must be installed and operational.

Configure the rule as follows:

1. In GV STRATUS Control Panel, navigate to **General | Rules | Rule Editor | Add**.



2. Configure the rule as follows:

Setting or button	Description
Rule Type	Select **Transfer to Avid**.
Name	Enter a rule name as it will appear in the Rules Monitor page.
Scope | Add Location	Select the GV STRATUS bin to which the rule will apply, exporting assets from GV STRATUS to ISIS/Interplay.
Frequency	Select when the rule is triggered.
Destination	Select the previously configured Avid Interplay destination. In the example above, it would be called "AvidInterplay".
Rule Conditions | Add Condition	Choose the preferred criteria which will trigger the export. For example, if a custom metadata field has been created in GV STRATUS called "Send to Avid", which when selected, will trigger the material transfer. In the example above, only when assets are set to a rating of 5 stars, the transfer rule is triggered.
Set Metadata | Add Metadata	Define the metadata value which will be added into the data field of the asset when the rule is applied to. For each metadata, click the **Add Metadata** button and select from the drop-down list to select the metadata.

3. Click **Save**.
4. Next, enable the rule.

Assets from GV STRATUS are transferred automatically according to the scope set up for the rule, to the pre-determined ISIS workspace and checked-in to the relevant Interplay folder.

Asset transfer jobs can be monitored in the Avid Transfer Monitor as well as on the GV STRATUS Asset Transfers Monitor.

Adding an Avid import rule

- The MEWS system must be installed and operational.

The GV STRATUS Rules Engine can watch a source location on one or more Avid Media Composer® workstations and when files arrive, import the Avid files to a location that is in the GV STRATUS system. The imported asset has a metadata field that specifies the source location from which it was imported.

Use a SMB location for importing.

After the import operation, the Rules Engine changes the name of the original source file, adding a suffix that indicates success or failure. The Rules Engine periodically deletes files more than seven days old, as a housekeeping operation.

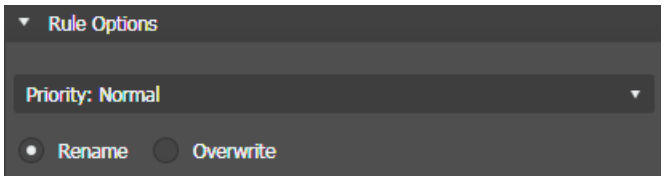
Create one import rule for each of your Avid Media Composer® workstations.

1. Log in to the GV STRATUS Control Panel application with administrator privileges.
2. In the GV STRATUS Control Panel application, click **General | Rules**.

3. Click **Add**.

   Rule Editor settings open.

4. In the **Rule Type** drop-down list select **Import**.
5. In the **Name** field type in a name for the rule you are configuring. Create a name that identifies the Avid Media Composer® workstation to which this rule applies.
6. In the **Description** field type in a description for the rule you are configuring.
7. In **Rule Options** settings, specify the rule behavior.



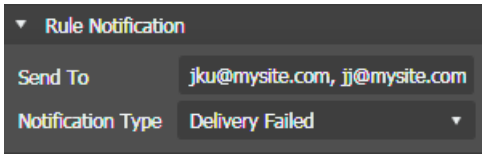
   a) Select the priority that the Rules Engine processes the rule, with the transfers and transcodes the rule controls, when there are multiple rules in a queue waiting to be processed.

      - **Priority: High**: Put this rule in a queue with other high priority rules and process through the high priority rule queue before any normal priority or low priority rules.
      - **Priority: Normal**: Put this rule in a queue with other normal priority rules and process through the normal priority rule queue after any high priority but before any low priority rules.
      - **Priority: Low**: Put this rule in a queue with other low priority rules and process through the low priority rule queue after any high priority or medium priority rules.

   b) If an asset of the same name already exists at the destination location, configure the rule behavior as follows:

      - **Rename**: A suffix is appended to the imported asset name. The existing asset is retained.

8. In **Rule Notification** settings, specify the notification behavior, if desired.



   a) Enter email addresses to which emails are sent.

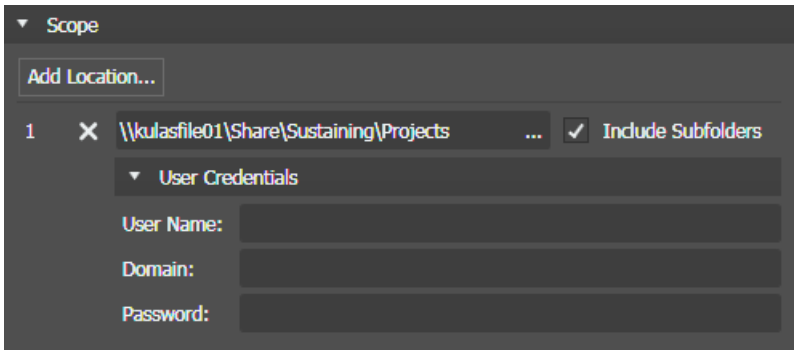
      Separate multiple email addresses with a comma.

   b) Select one or more notification types:

      - **Delivery Failed**: Emails are sent if the rule operation fails.
      - **Delivery Completed**: Emails are sent if the rule operation succeeds.

   In order to send emails, the email server must be configured in Workflow Engine settings.

9. In **Scope** settings, specify the source location or locations the rule watches.



   a) Click **Add location**.

      The **Location Selection** dialog box opens.

   b) Enter the UNC path as follows:

      <Avid Media Composer PC name or IP>\Avid MediaFiles\Export

      If using a name, it must be resolvable to an IP address via a host file.

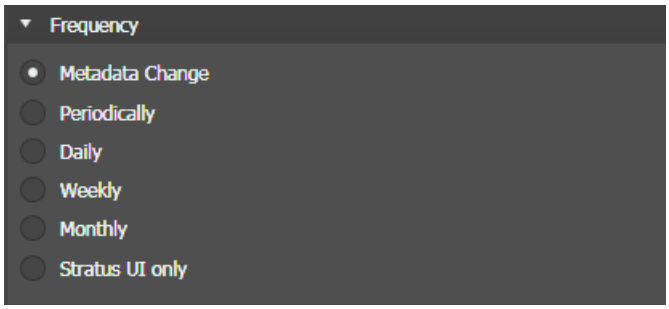
      This is the location that contains the files on which the rule operates. Every time the rule runs, it looks in this location to determine if there are any new files that match the rule conditions and then operates on the files that match.

   c) Click **OK**.

      The location is added to the **Scope** list.

   d) For a location in the list, do not select **Include Subfolders**.

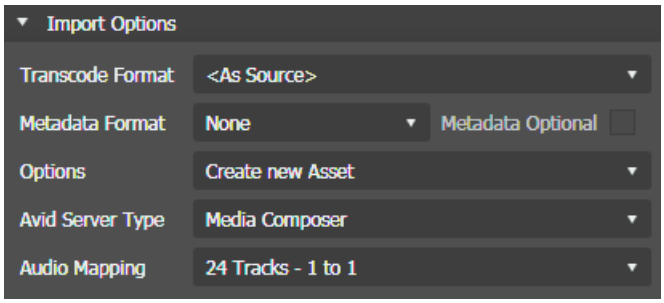
10. Configure **User Credentials** as required for the source locations.
11. In **Frequency** settings, specify how often the Rules Engine triggers the rule.



   a) Select the following option:

      - **Metadata Change**: The rule is constantly monitoring assets in the "Scope" location.

12. In **Import Options** settings, configure the format of the imported assets.



a) For **Transcode Format**, select **<As Source>**.

If you have the STRATUS-XCODECONTROLMEWS license, you can select any transcode format listed under MEWS Formats in the drop-down list.

b) For **Metadata Format**, select as follows:

- **None**: No metadata is imported.

c) For **Options**, select as follows:

- **Create new Asset**: A GV STRATUS asset is created for the imported material. If metadata only is imported, a metadata-only asset is created. This is not applicable for Avid imports.
- **Update Asset Metadata**: The imported metadata updates the metadata and essence of an existing asset. This is not applicable for Avid imports.

d) For **Avid Server Type**, select as follows:

- **Media Composer**: If the import is from Avid Media Composer workstations.
- **Isis**: If the import is from Avid ISIS storage system.

e) For **Audio Mapping** of the imported asset, select as follows:

- **8 Tracks - Mix Back**: The combination of 8 audio tracks configured to be imported with the asset. This profile is just an example and must be configured per system on the file level under "`C:\Program Files\Grass Valley\STRATUS Transcode Engine\Profiles\MEWS`", usually on Core Server, with the NotePad.
- **24 Tracks - 1 to 1**: The automatic 1 to 1 mapping from the 24 audio tracks of the asset.

  NOTE: Silent tracks are generated in case there are less audio tracks available.
- **None**: All audio tracks will be imported with the asset. This is the default setting for assets with no more than 24 audio tracks.

13. In **Destination** settings, specify a location in the GV STRATUS system.

The destination must be a location in the GV STRATUS system. This is a location that is in the GV STRATUS application Navigator panel under the Locations node.

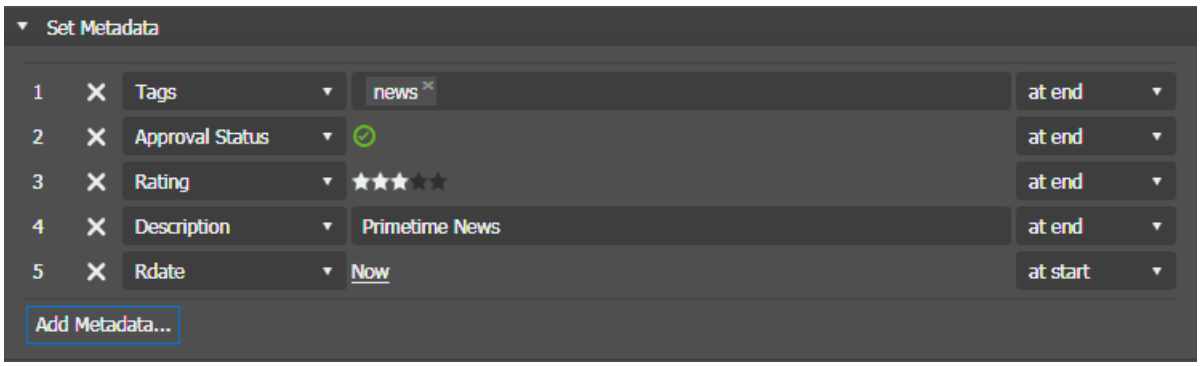
14. In **Rule Conditions** settings, specify the conditions the Rules Engine looks for to qualify an asset.
15. In the **Select items when** drop down list, select **ALL of the conditions below are met**.

16. Configure conditions as follows:

1	Extension	is AAF

a) Click the **Add Condition** button and select from lists to define the condition.
b) Type `AAF` in the value field.

17. In **Set Metadata** settings, define the metadata that Rules Engine will set during the execution of a rule for an asset.



18. Configure metadata as follows:

- For each metadata, click the **Add Metadata** button and select from the drop-down list to select the metadata.
- Define the metadata value which will be added into the data field of the asset when the rule is applied to.
- Select whether to enter the metadata value at the start or the end of the rule workflow.
- Click the **X** button to remove a metadata from the list.

If a newly created custom metadata field is not available in the drop-down list, restart the GV STRATUS Control Panel application.

You can create new custom metadata by selecting **Core | Metadata | Custom Metadata | Add** in the GV STRATUS Control Panel.

19. Click **Save**.

Next, enable the rule.

Related Topics

Using the GV STRATUS application with Avid on page 1227

Configure folders on the Avid workstation

1. On each Avid workstation, create the following folder at the root of the `C:` drive:
   - `Avid MediaFiles`
2. Share the `Avid MediaFiles` folder to Everyone with full access.

3. Create the following subfolders in the *Avid MediaFiles* folder:
   - *MXF*
   - *Export*

Create Avid Send To option for GV STRATUS

1. In Avid Media Composer, select any sequence and click **File | Send To | Make New**.
   The **Send To: Make New** dialog box opens.
2. Set **Destination** to *C:\Avid MediaFiles\Export*
3. Select **Export Setting 1**
4. From the **Export Setting 1** drop-down list, select **Untitled**.
5. Click **Options**.
   The **Export Settings** dialog box opens.
6. From the **Export As** drop-down list, select **AAF**.
7. Select **Video / Data Details**.
   a) Verify that **Export Method** is set to **Link to (Don't Export) Media**.
   b) Select **Render Video Effects**.
   c) Select **Transcode Video To** and from the drop-down list select the desired K2 compatible export format and codec.
   d) Leave other settings at default values.
8. Select **Audio Details**.
   a) Verify that **Export Method** is set to **Link to (Don't Export) Media**.
   b) Select **Include Rendered Audio Effects**.
   c) Select **Render all Audio Effects**.
   d) Leave other settings at default values.
9. Click **Save As**, enter an appropriate name, such as `GV STRATUS` and click **OK**.
10. On the **Send To: Make New** dialog box, click **Save As Template**.
    The **Save As** dialog box opens.
11. Name the file `GV STRATUS` and click **Save**.

The **GV STRATUS** option now appears in the **Send To** menu.

Avid/MEWS considerations

- GV STRATUS supports operation with multiple MEWS engines running on separate servers. Each MEWS engine supports up to 3 concurrent transcode jobs at a time.

- To ensure the MEWS Service machine(s) are correctly configured and the required license exists, you should check whether the resources provided per MEWS Service are registered in the GV STRATUS Control Panel via **Core | Resource Management | Resource Monitor**. The status of the MEWS license and MEWS Server machine should be **Online** on the Resource Monitor. Below are corresponding display of both MEWS licenses in SabreTooth and the Resource Monitor:

SabreTooth MEWS Licenses	SubResource Provider in Resource Monitor
STRATUS-XCODECONTROLMEWSEXT	MEWS
STRATUS-XCODECONTROLMEWS	MEWS-ELITE

- When editing HD material you must use an HD project. When editing SD material you must use an SD project.
- The GV STRATUS rule that imports an Avid sequence must use a transcode format that matches the Avid Media Composer Project window Format settings. If transcoding, an HD project must use an HD transcode format and an SD project must use an SD transcode format. If not transcoding, select **As Source**.
- The latest MEWS version supports AVC-Intra 100 1080p 50Hz format. Since Avid Media Composer is not supporting the format yet, the GV STRATUS Transcode Engine provides a transcode profile for MEWS to convert asset format from AVC-Intra 100 1080p 50Hz to **DNxHD 1080p (115/120/145 Mb/s)** for use in Avid systems.

  NOTE: AVC-Intra 100 1080p 60 Hz is not supported by MEWS.
- The Avid sequence can be of mixed codecs but they must be the same definition/standard.
- Assets transferred from GV STRATUS to Avid via MEWS retain GV STRATUS markers and keywords.
  - In Avid Media Composer, a GV STRATUS marker displays a red indicator and a GV STRATUS keyword displays a yellow indicator.
  - When transferred as AMT-Atom container, GV STRATUS Marker and Keyword names will be replaced by a valid Avid user name so that they can be imported into Avid. The original names will be added to the Avid *Comment field* together with the GV STRATUS description metadata, semicolon separated. The user name is extracted from the Location configuration in GV STRATUS Control Panel in the *Interplay Folder*.
  - Markers are only transferred if they exist in GV STRATUS before the transfer was initiated.
  - When transferring a still recording asset, markers will not display in the Avid system. Markers will only display if the clip is loaded into the Avid Media Composer after recording is stopped and the transfer is complete.
  - If the asset is already in the Avid Media Composer project bin, a refresh is required. In the context menu, select **Interplay | Update from Interplay** to refresh.
- Asset metadata are automatically transferred into Avid if configured in the **Metadata Export** tab of GV STRATUS Control Panel. Metadata fields can be selected under the Avid column, and automatically transferred when assets are sent from GV STRATUS.

- For a standalone Avid Media Composer workstation, configure Media Composer as follows:
  - In Media Creation settings, on every tab set **Video Drive** and **Audio Drive** to the *C:* drive.
  - In Export Settings, set **Export As** to **AAF** and for both **Video/Data Details** and **Audio Details**, do the following:
    - Set **Export Method** to **Consolidate Media**.
    - Set all Media Destinations to **Media Drive** and select **Use Media Creation Settings**.

- For a system with AVID ISIS, do the following:
  - Install Avid ISIS Client Manager on the following
    - The machine where the XCode Control Engine is running
    - The machine where MEWS is running
    - Every Avid Media Composer workstation
  - Configure Avid ISIS Client Manager as follows:
    - Map a drive, such as drive *Z:*, to the ISIS share.
    - Configure the user to the internal system account, which by default is GVAdmin
  - For an AVID ISIS Media Composer workstation, configure Media Composer as follows:
    - In Media Creation settings, on every tab set **Video Drive** and **Audio Drive** to the drive letter, such as drive *Z:*, mapped to ISIS.
    - In Export Settings, set **Export As** to **AAF** and for both **Video/Data Details** and **Audio Details**, do the following:
      - Set **Export As** to **AAF**.
      - Set **Export Method** to **Link to (Don't Export) Media**.
      - Set all Media Destinations to **Media Drive**.
  - Configure GV STRATUS as follows:
    - The GV STRATUS Xcode Control Engine Service and the MEWS Service must be installed to use the internal system account, which by default is GVAdmin.
    - In GV STRATUS Control Panel Locations Configuration settings, **Location Path** must point to the *\MXF* subfolder on Avid ISIS and **Host Name** must point to the hostname of the Avid Media Composer workstation.
    - Create an Import Rule Watchfolder, which is a share that can be accessed by the Rules Engine and the Avid Media Composer workstations.
    - Create an Import Rule as follows:
      - Source: The Import Rule Watchfolder
      - Destination: K2 folder
      - Transcode Format: a MEWS format that matches the Avid project.
      - Avid Server Type: Isis
      - Avid Media Host: The Isis server name
      - Set Rule Conditions to trigger on .aaf file extension

Refer to Avid Media Composer product documentation for more information.

Related Topics

SabreTooth MEWS license process on page 665
Resource Management settings on page 352

Configure iNews for Monitor On

The iNews system must be installed and operational.

1. In the SYSTEM.MOS-MAP configuration, verify or configure according to the following example:

```
TABLE-START DeviceTable
CAMIO        moscg        A B C D
stratusuk    vidmos
TABLE-END
```

2. In the SYSTEM.MAP configuration, verify that the MOS reference for video is on the first line according to the following example:

```
rundowns.bulletins.test      rundowns.bulletins.test                  -

            monitor              1505
  mossvr           uk004                -          mct-cg
  mos              vidmos             UPDATE         -
  mos               moscg              -          storytext
```

   If the MOS reference for video is on the second line, the status is not reported.

3. In the story form and the rundown queue form, add the following fields:

Options	Description
Current field: Label	MOS TITLE
Current field: Label size	mos-title
Current field: Type	10
Current field: Edit size	15
Attributes: Read-Only	Selected
Attributes: Affects Ready	Selected
Attributes: Write Group	!<none>
Type: Editbox	Selected

Options	Description
Current field: Label	MOS DUR
Current field: Label size	mos-duration
Current field: Type	7
Current field: Edit size	7
Attributes: Read-Only	Cleared
Attributes: Affects Ready	Selected
Attributes: Write Group	!<none>
Type: Duration Control	Selected

Options	Description
Current field: Label	MOS
Current field: Label size	mos-active
Current field: Type	5
Current field: Edit size	16
Attributes: Read-Only	Selected
Attributes: Affects Ready	Cleared
Attributes: Write Group	!<none>
Type: Editbox	Selected

Options	Description
Current field: Label	Event Status
Current field: Label size	event-status
Current field: Type	10

Options	Description
Current field: Edit size	9
Attributes: Read-Only	Cleared
Attributes: Affects Ready	Cleared
Attributes: Write Group	!<none>
Type: Editbox	Selected

4. Copy the MOS objects into the rundown.

Status is displayed.

Configuring custom metadata for House Number List

For the integration between traffic system and the House Number List, you need to add below custom fields manually in the Metadata settings of GV STRATUS Control Panel application.

If GV STRATUS security is enforced, your credentials must give you read and write permissions for all 5 custom metadata fields below:

Field name	Type
House Number	Text - 256 Characters
Program	Boolean
Content Name	Text - 256 Characters
Content Description	Text - 256 Characters
Content Type	Text - 256 Characters

Related Topics

Custom Metadata settings on page 318

Database planning and maintenance strategies

The topics in this section help you establish a plan in the event a GV STRATUS system fails.

Core Services server failure considerations

The GV STRATUS Core server must have a database maintenance plan in place. The maintenance plan backs up the SQL database on a regular basis and stores it in a safe location. In the case of server failure the database can then be restored to minimize data loss.

If the SQL Server Agent service is ever stopped, so is your maintenance plan. Make sure that the service is set to start automatically.

A Fault Tolerant (FT) server is available from Grass Valley to further protect the integrity of the system.

Logging in to Microsoft SQL Server Management Studio

If directed by a documented procedure or by Grass Valley Support, you can view and make SQL database settings in Microsoft SQL Server Management Studio.

1. Make sure you are logged in to the database host system with Administrator privileges.
2. Open the Windows operating system Services control panel and verify that the SQL Server Agent service startup type is set to automatic and that it is started.
3. From the Windows desktop click **Start | All Programs | Microsoft SQL Server** and select **Microsoft SQL Server Management Studio**.

   Microsoft SQL Server Management Studio opens.
4. Log on and connect to your SQL Server as follows:
   - **Server type:** Database Engine
   - **Server name:** (local)
   - **Authentication:** Windows Authentication
5. Identify the databases that are a part of the GV STRATUS system, which include the following:
   - ISDB
   - MediaFlow
   - MediaFrame
   - RulesEngine
   - WfPersistence

Setting the SQL server memory limit

The SQL server depends on memory to cache information from databases on disk for fast access. If more data exists on disk than can be held in memory, the SQL server performance will degrade.

To avoid low memory issues on the GV STRATUS Core server or the standalone Database server, the memory that should be assigned to SQL server depends on the memory size of the physical device.

Grass Valley recommends the setting of SQL server memory limit according to the table below:

Physical Memory	SQL server memory limit	Approximate number of assets supported
12 GB	5120 MB	200,000 – 350,000
16 GB	8192 MB	320,000 – 560,000
32 GB	18,432 MB	720,000 – 1,260,000
48 GB	32,768 MB	1,280,000 – 2,240,000
64 GB	47,104 MB	1,900,000 – 3,360,000

Set the SQL server memory limit as follows:

1. From the Windows desktop click **Start | All Programs | Microsoft SQL Server** and select **Microsoft SQL Server Management Studio**.

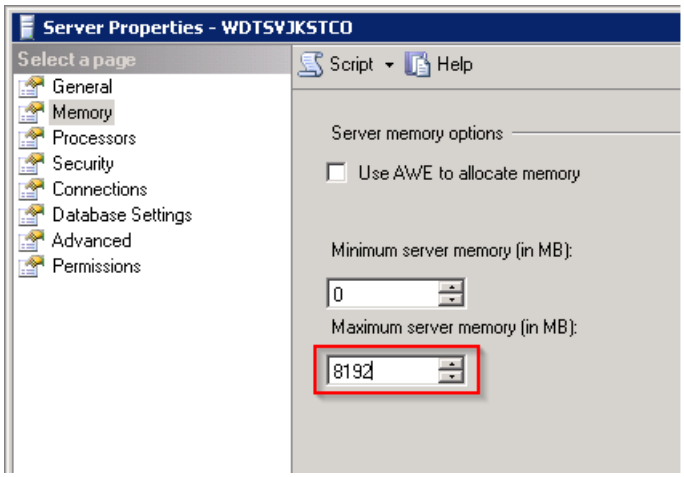
   Microsoft SQL Server Management Studio opens.

2. Log on as an Administrator.
3. Right-click on the SQL server name and select **Properties** from the context menu.

   The **Server Properties** dialog opens.

4. Click **Memory**.

   The Memory page opens.



5. In the **Maximum server memory** setting, enter your SQL server memory limit in MB.
6. Click **OK**.

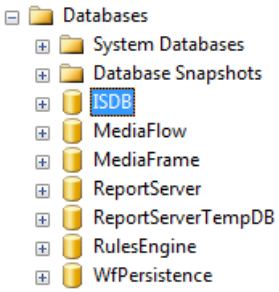
A restart of the server is not necessary, but recommended.

Setting Custom Metadata in the Ingest Database

- Procure the **06_Create_spUpdateFieldTypeAndCustomProperty-sql.zip** file before configuring this setting.
- This setting is required after a new installation of the Ingest database, and not required on an upgrade of the Ingest database.
- This setting is required for systems with the role of GV STRATUS Database Server.
- The GV STRATUS system must have been installed before performing these configuration steps.

1. Launch the Microsoft SQL Server Management Studio.
2. Log on as an Administrator.

3. In the tree-view, click **Databases | ISDB**.



   If **ISDB** does not exist under the **Databases** node, reinstall GV STRATUS with the **GV STRATUS Database Server** SiteConfig role.

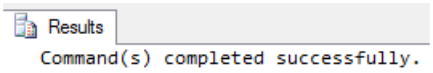
4. On the Main Menu, select **File | Open | File** and browse to select the **06_Create_spUpdateFieldTypeAndCustomProperty-sql.zip** file that you obtained earlier.

   A new query window opens on your right pane.

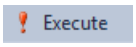
5. On the query window, do one of the following:

   - Click the **Parse** button.
   - Press **Ctrl + F5** keys.

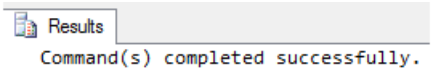
   The message below displays.



6. Then, do one of the following:

   - Click the **Execute** button. 
   - Press the **F5** key.

   The message below displays.



7. Close the Microsoft SQL Server Management Studio.
8. On the GV STRATUS Core server, go to **Services** and restart the **GV Stratus Ingest DB** service.

Disabling the Auto Close feature in Ingest Database

This is only required for an upgrade of the Ingest database.

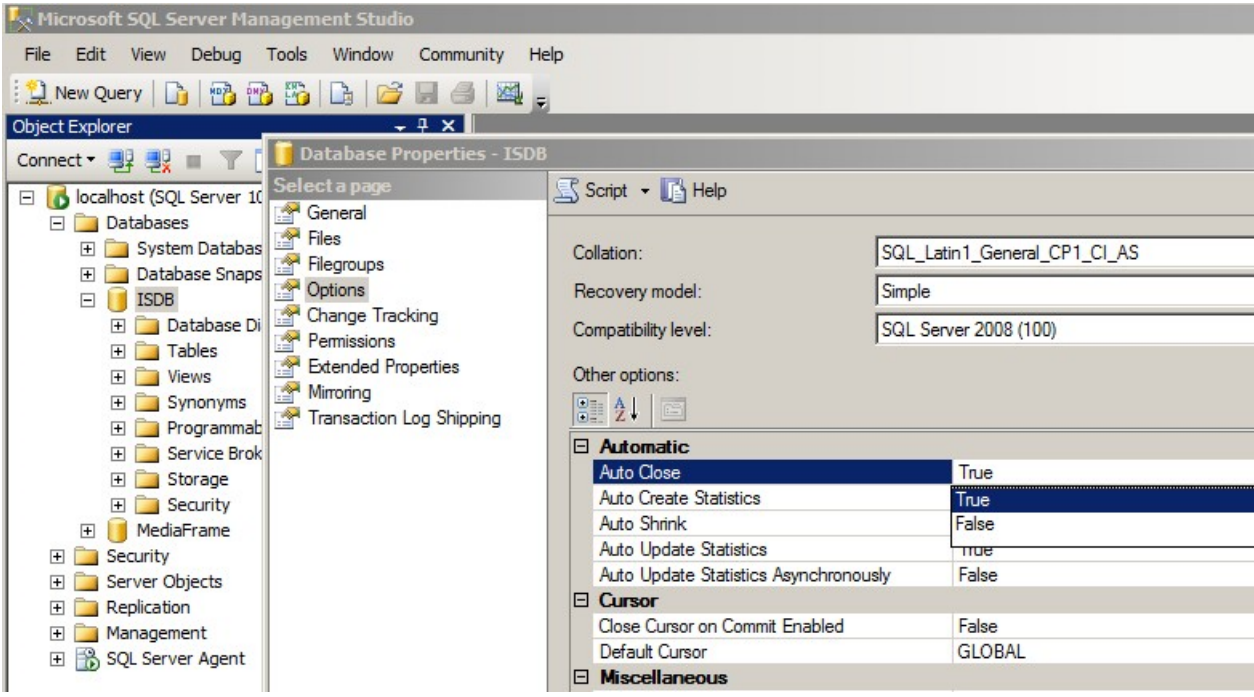
It is not required on a newly installed Ingest database since it will be set automatically during installation.

The Auto Close feature must be disabled to prevent the Ingest database from going offline automatically.

1. Open and log in to Microsoft SQL Server Management Studio.
2. Go to **Databases** and select **ISDB**.

3. Right-click on **ISDB** and select **Properties**.

   The **Database Properties - ISDB** window opens.



4. Select the **Options** page.
5. In the **Automatic** section, select **Auto Close** and set the value to **False**.
6. Click **OK**.

   The Auto Close feature for Ingest Database is disabled.

Creating the GV STRATUS maintenance plan

Maintenance plans automate database tasks necessary to ensure database integrity and recovery in case of data loss.

If you moved the GV STRATUS database to a new/different server machine, you have to create the GV STRATUS maintenance plan on the particular machine separately.

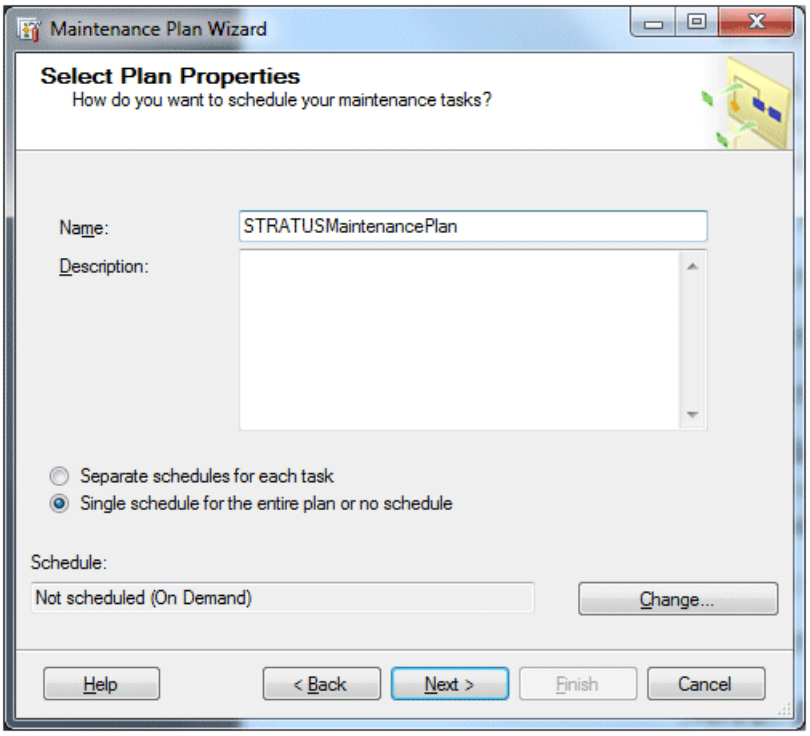
Grass Valley recommends that the database backup location be network storage, preferably one that is backed up or has some kind of RAID protection. If the database is backed up to a network share, the account under which SQL Server (MSSQLSERVER) and SQL Server Agent (MSSQLSERVER) run must have permission to write to the network share. If these services are running a virtual Network Service or NT Service\MSSQLSERVER account, then the network share must have permission for the computer account (e.g., `yourDomain\StratusCoreServer$`).

To create or manage maintenance plans, you must log in as a member of the sysadmin fixed server role.

1. Open and log in to Microsoft SQL Server Management Studio.
2. In the tree-view, open the **Management | Maintenance Plans** nodes.
3. Right-click the **Maintenance Plans** node a select **Maintenance Plan Wizard**.

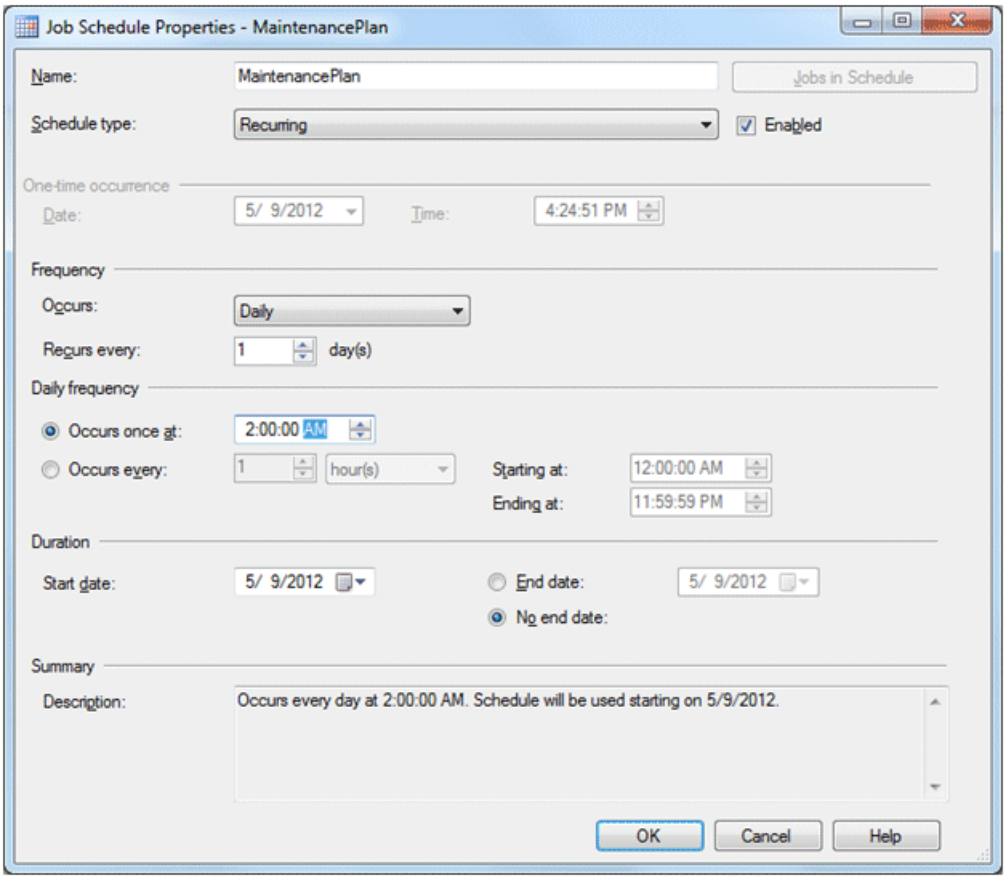
   The Maintenance Plan Wizard opens.

4. On the Maintenance Plan Wizard, click **Next**.
   The Select Plan Properties page opens.



5. On the Select Plan Properties page do the following:
   a) In the Name field, type `StratusMaintenancePlan`.
   b) Select **Single schedule for the entire plan or no schedule**

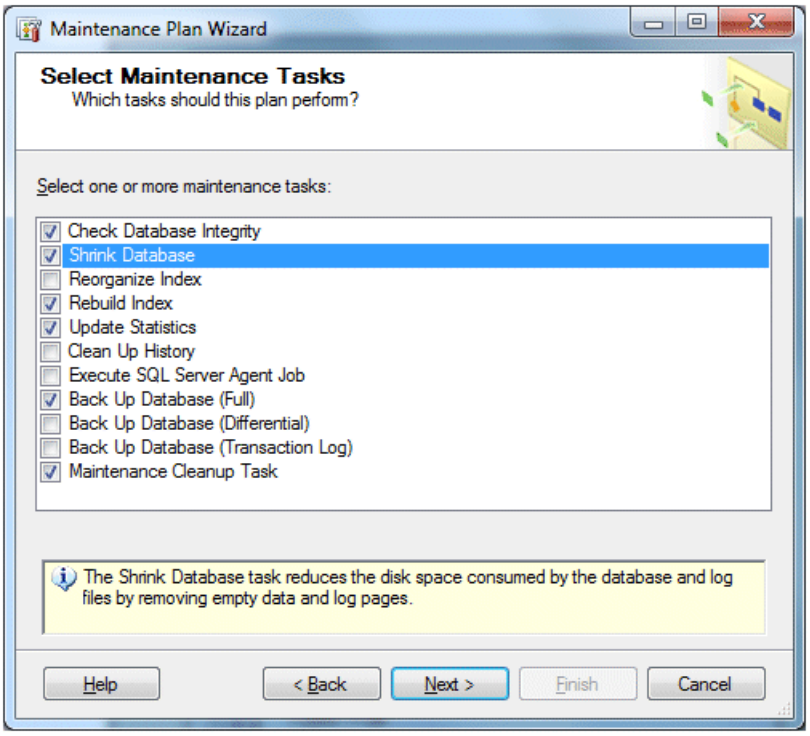
6. Click **Change**.
   The Job Schedule Properties dialog box opens.



7. In the **Frequency** section do the following:
   a) In the **Occurs** drop-down list select **Daily**.
   b) Set **Recurs every:** to **1** day.
8. In the **Daily frequency** section do the following:
   a) Select **Occurs once at:**
   b) Accept the default time of **12:00:00 AM** or change it to a time more suitable to your site.
9. In the **Duration** section, verify the following:
   a) **Start Date** is today's date.
   b) **No end date** is selected.

10. Click **OK** and **Next**.

    The Select Maintenance Tasks page opens.



11. Select the following:

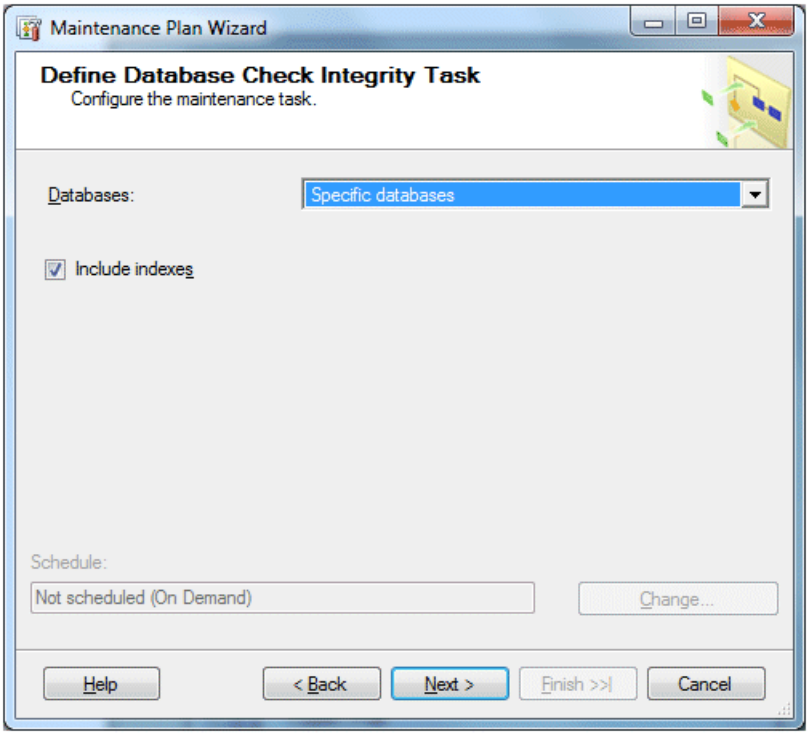
    - Check Database integrity
    - Shrink Database
    - Rebuild Index
    - Update Statistics
    - Back Up Database (Full)
    - Maintenance Cleanup Task

12. Click **Next**.

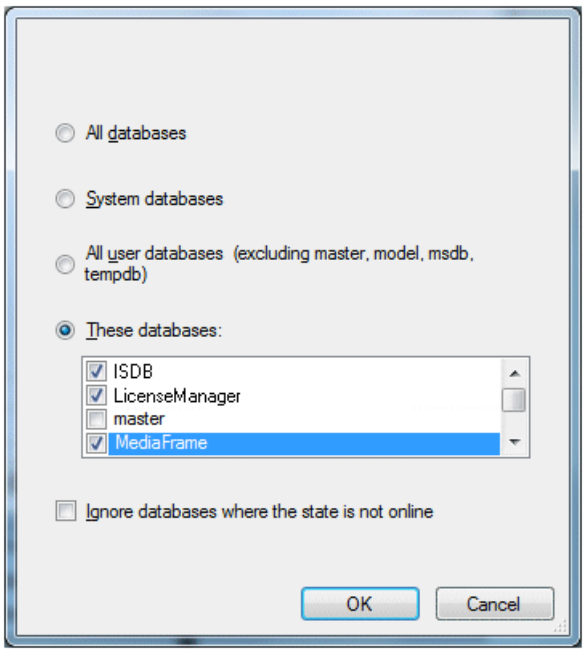
    The Select Maintenance Task Order page opens.

13. On the Select Maintenance Task Order page, leave settings at the default configuration. Click **Next**.

    The Define Database Check Integrity Task page opens.



14. On the Define Database Check Integrity Task page, do the following:
    a) Click the **Databases** drop-down list.
       A dialog box opens.

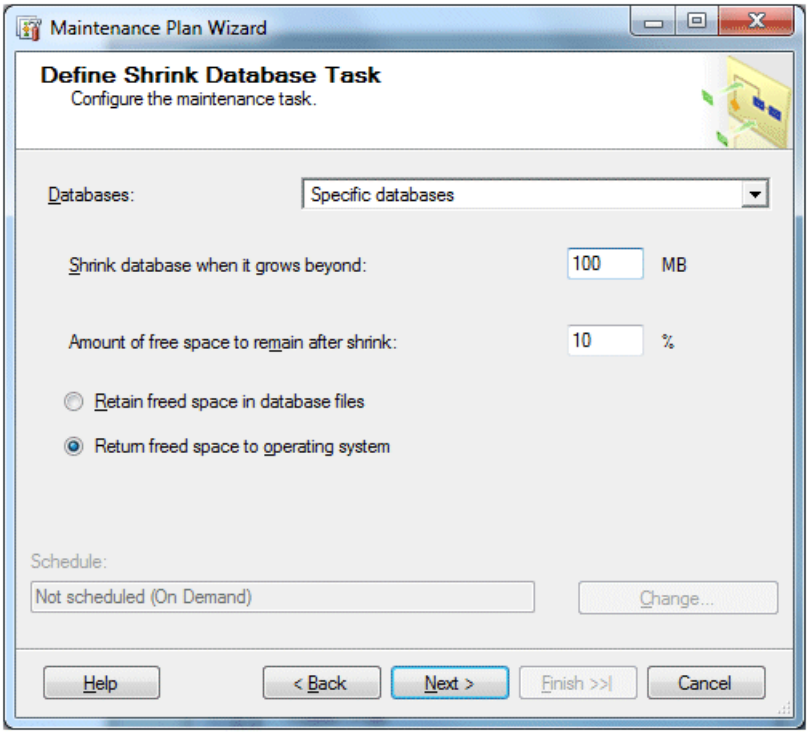


    b) Select **These databases** and select the following from the list:

       - ISDB
       - MediaFlow
       - MediaFrame
       - RulesEngine
       - WfPersistence

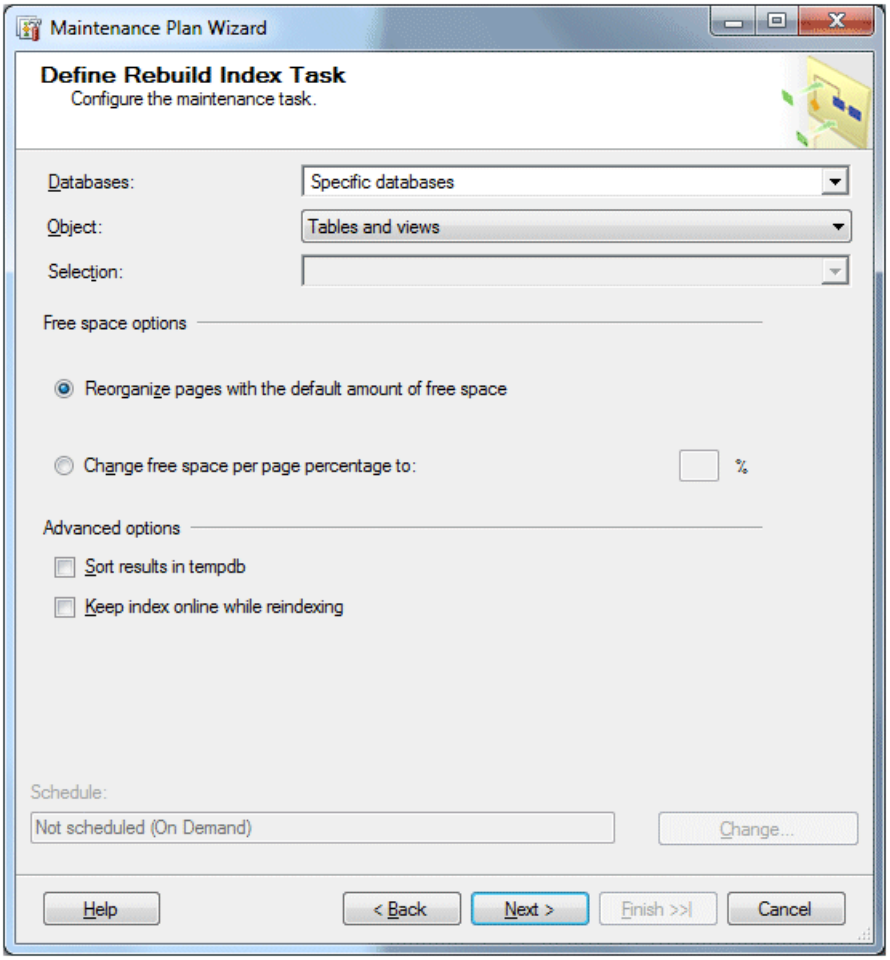
    c) Click **OK** to save settings and close the dialog box.
    d) On the Define Database Check Integrity Task page, select **Include indexes**.
    e) Click **Next**.

    The Define Shrink Database Task page opens.


Maintenance Plan Wizard
Define Shrink Database Task
Configure the maintenance task.
Databases:
Specific databases
Shrink database when it grows beyond:
100
MB
Amount of free space to remain after shrink:
10
%
Retain freed space in database files
Return freed space to operating system
Schedule:
Not scheduled (On Demand)
Change...
Help
< Back
Next >
Finish >>|
Cancel

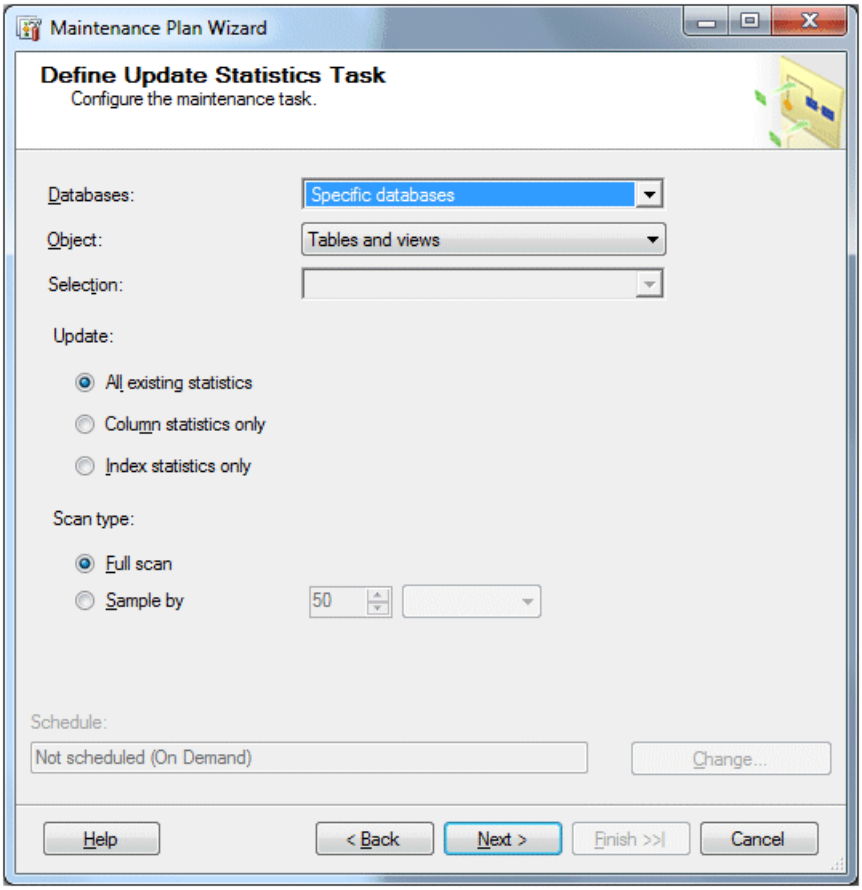
15. On the Define Shrink Database Task page, do the following:
    a) Click the **Databases** drop-down list, and select the following:
        - ISDB
        - MediaFlow
        - MediaFrame
        - RulesEngine
        - WfPersistence
    b) Click **OK**.
    c) Set **Shrink database when it grows beyond:** to **100** MB.
    Leave other settings at the default configuration.
    d) Click **Next**.

The Define Rebuild Index Task page opens.



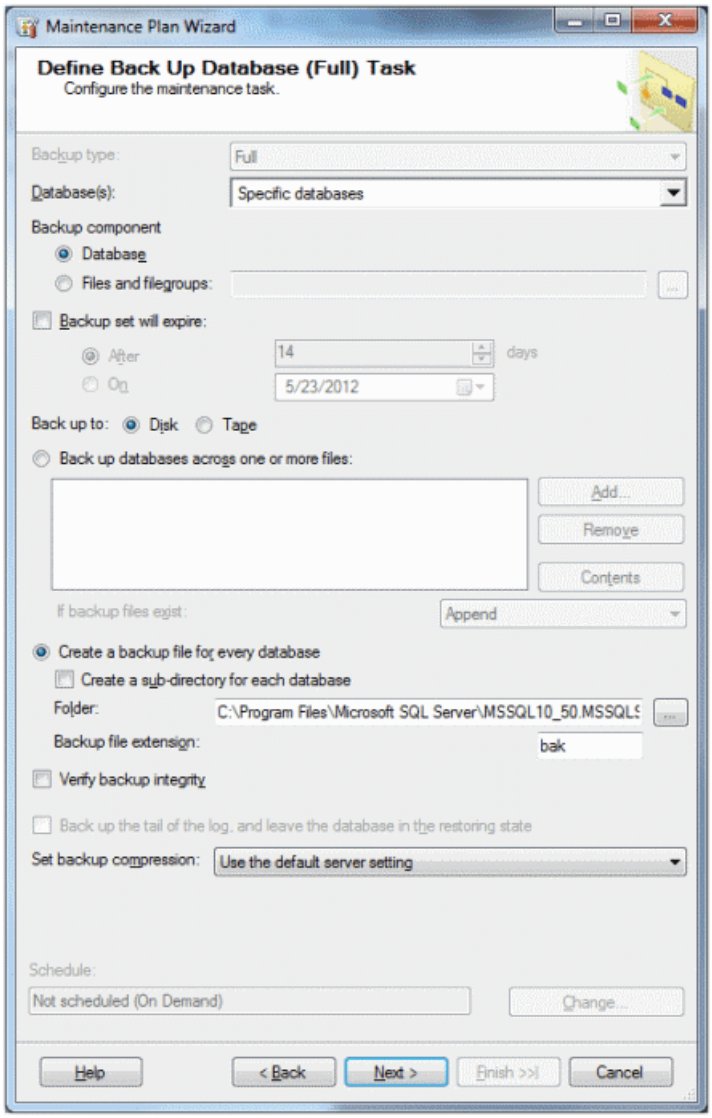
16. On the Define Rebuild Index Task page, do the following:
    a) Click the **Databases** drop-down list, and select the following:
        - ISDB
        - MediaFlow
        - MediaFrame
        - RulesEngine
        - WfPersistence
    b) Click **OK**.
       Leave other settings at the default configuration.
    c) Click **Next**.

The Define Update Statistics Task page opens.



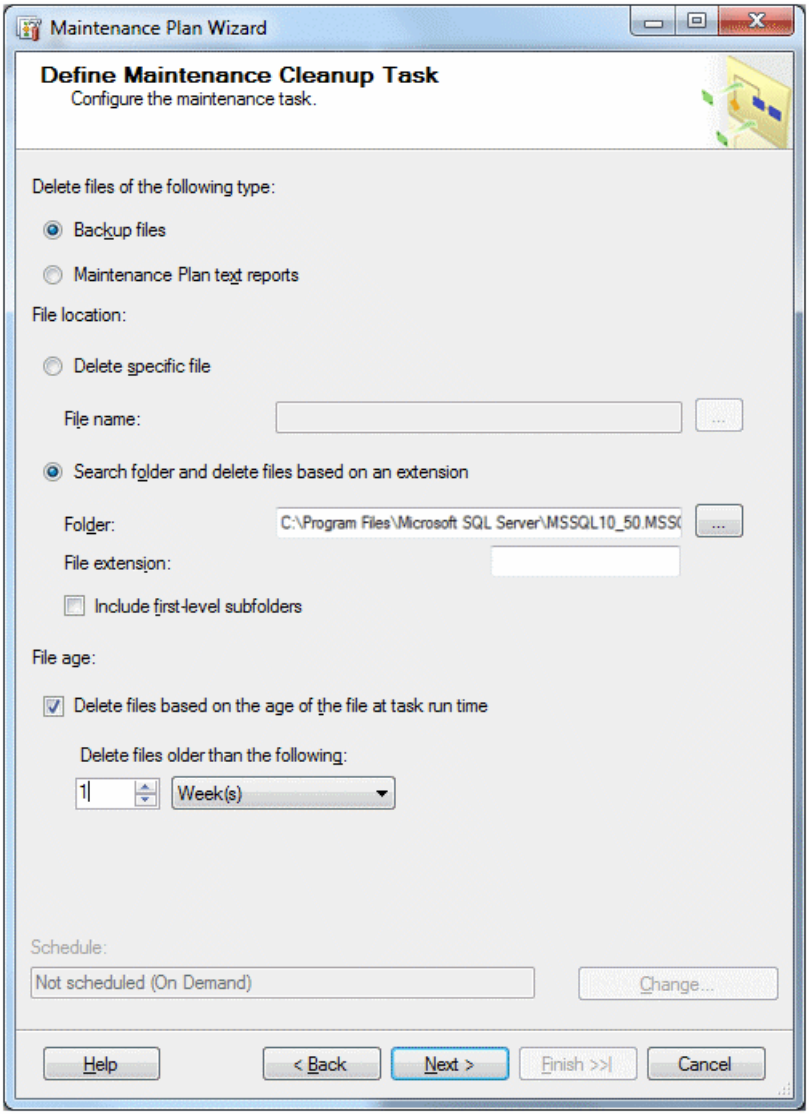
17. On the Define Update Statistics Task page, do the following:
    a) Click the **Databases** drop-down list, and select the following:
        - ISDB
        - MediaFlow
        - MediaFrame
        - RulesEngine
        - WfPersistence
    b) Click **OK**.
       Leave other settings at the default configuration.
    c) Click **Next**.

The Define Back Up Database (Full) Task page opens.



18. On the Define Back Up Database (Full) Task page, do the following:
    a) Click the **Databases** drop-down list, and select the following:
        - ISDB
        - MediaFlow
        - MediaFrame
        - RulesEngine
        - WfPersistence
    b) Click **OK**.
    c) Select **Create a backup file for every database**.
    d) In the **Folder** field, enter the path to your site's database backup location.
       Copy the folder path so you can paste it on the next page.
    e) In the **Backup file extension** field, enter **bak** as the file extension.
       Leave other settings at the default configuration.
    f) Click **Next**.

    The Define Maintenance Cleanup Task page opens.



19. On the Define Maintenance Cleanup Task page, do the following:
    a) In the **File location** section, select **Search folder and delete files based on an extension**.
    b) In the **Folder** field, paste the path of your site's database backup location that you copied earlier.
    c) In the **File extension** field, leave it blank.

       : Do not enter `.bak` as it prevents files from getting automatically deleted and quickly fills up the core's C: drive without warning.

    d) In the **File age** section, select **Delete files based on the age of the file at task run time**.
    e) Set **Delete files older than the following:** to **1** week.

       Leave other settings at the default configuration.

    f) Click **Next**.

    The Select Report Options page opens.

20. On the Select Report Options page, leave settings at the default configuration. Click **Next**.
    The Complete the Wizard page opens.
21. On the Complete the Wizard page, click **Finish**.
    The Maintenance Plan Wizard Progress page opens and reports progress.
22. When the page reports success for all actions, click **Close**.

The GV STRATUS maintenance plan is created.

Before continuing with other database maintenance plan operations, close and re-open Microsoft SQL Server Management Studio.

Next, verify the database maintenance plan status.

Verifying the database maintenance plan status

1. Open and log in to Microsoft SQL Server Management Studio.
2. In the tree-view, open the **Management | Maintenance Plans** nodes.
3. Right-click on a plan and select **View History**.
   The Log File Viewer window opens.
4. View the status report.

If an error occurs, it is likely that the SQL Server Agent is not started. Start the service and start over.

Testing the backup

Before doing this task, verify that logging is turned off for IIS.

Database performance can be downgraded while this test is in progress, but the database remains operational during the test.

1. Open and log in to Microsoft SQL Server Management Studio.
2. In the tree-view, open the **Management | Maintenance Plans** nodes.
3. Right-click on a plan and select **Execute**.
   the Execute Maintenance Plan dialog box opens and reports progress.
4. To check for errors, view the history.

Modifying the maintenance plan backup location

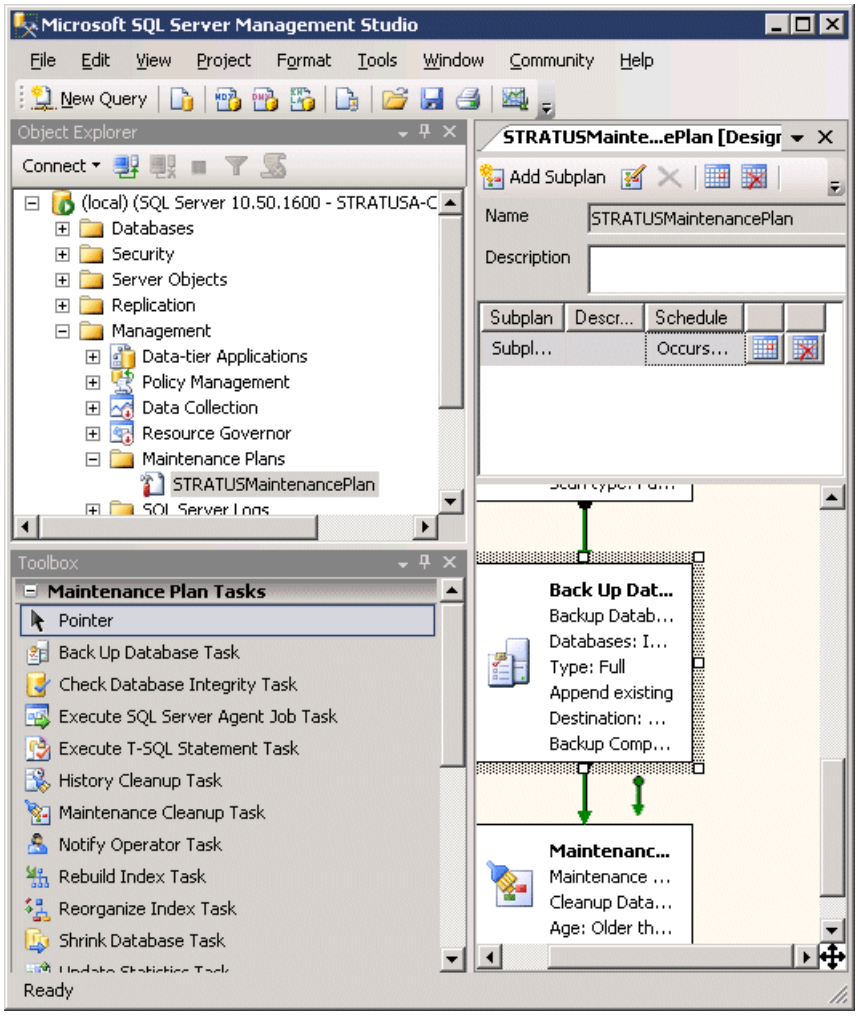
Maintenance plans automate database tasks necessary to ensure database integrity and recovery in case of data loss.

Grass Valley recommends that the database backup location be network storage, preferably one that is backed up or has some kind of RAID protection. If the database is backed up to a network share, the account under which SQL Server (MSSQLSERVER) and SQL Server Agent (MSSQLSERVER) run must have permission to write to the network share. If these services are running a virtual Network Service or NT Service\MSSQLSERVER account, then the network share must have permission for the computer account (e.g., *yourDomain\StratusCoreServer$*).

To create or manage maintenance plans, you must log in as a member of the sysadmin fixed server role.

1. Open and log in to Microsoft SQL Server Management Studio.
2. In the tree-view, open the **Management | Maintenance Plans** nodes.
3. Right-click the plan, and click **Modify**.

   A Plan Design panel opens.



4. Double-click **Backup Database Task**.

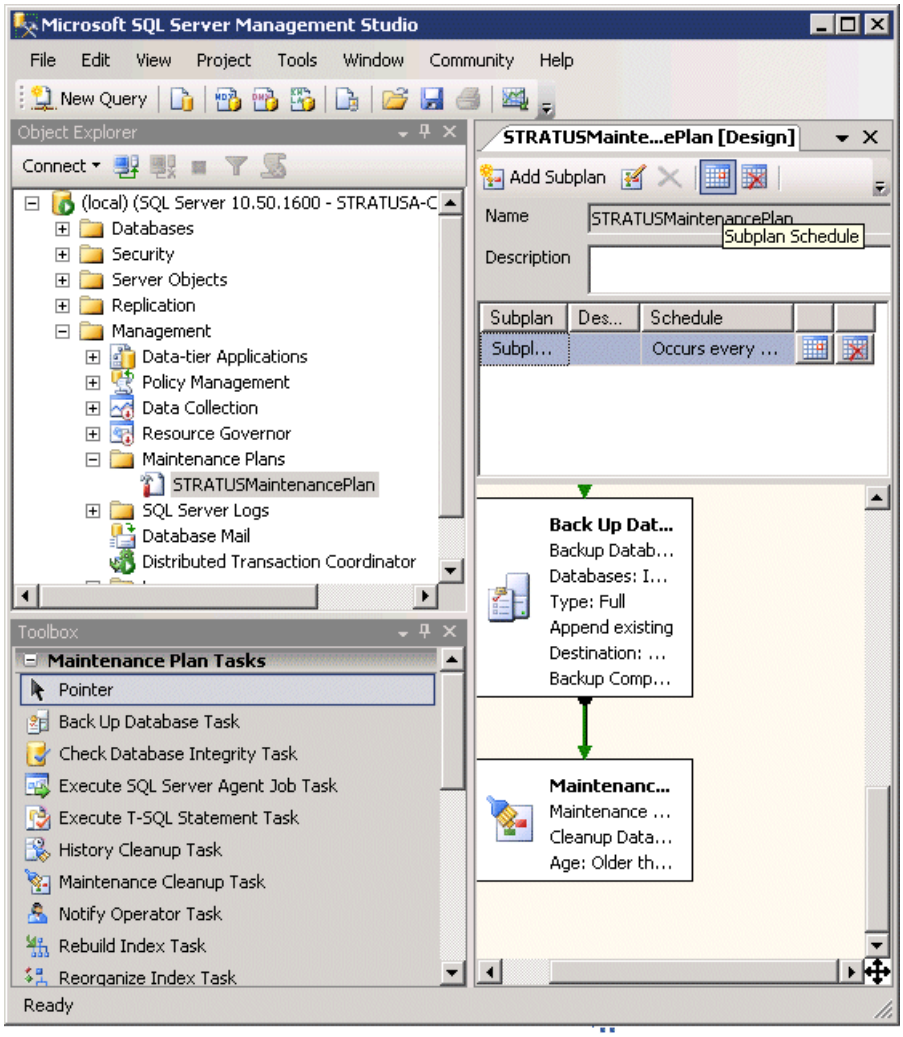
   The Backup Database Task dialog box opens.
5. In the Backup Database Task dialog box, in the **Folder** field, modify the backup directory path.
6. Click **OK** on the Backup Database Task dialog box.
7. Close Server Management Studio and answer **Yes** when prompted to save changes.

Modifying the maintenance plan schedule

The backup should occur at a time that does not conflict with peak usage of the system. Use the following procedure to modify the schedule:

1. Open and log in to Microsoft SQL Server Management Studio.
2. In the tree-view, open the **Management | Maintenance Plans** nodes.
3. Right-click the plan, and click **Modify**.

   A Plan Design panel opens.



4. In the Plan Design panel list, select the subplan.
5. With the subplan selected, click the **Subplan Schedule** button in the toolbar.

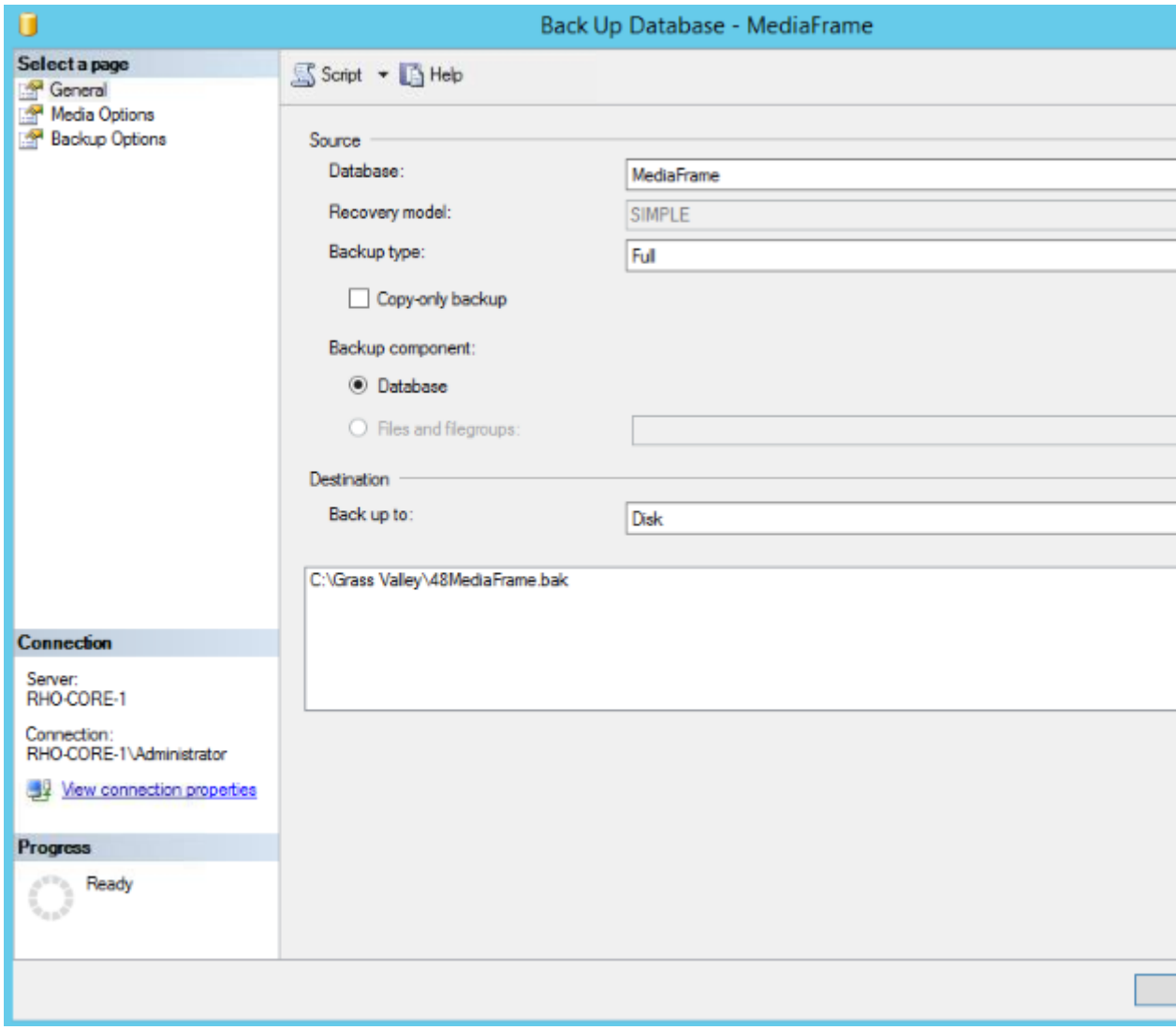
   The Job Schedule Properties dialog box opens
6. In the Job Schedule Properties dialog box, enter the new schedule details.
7. Click **OK** on the Job Schedule Properties dialog box.
8. Close Server Management Studio and answer **Yes** when prompted to save changes.

Backing up a database

Grass Valley recommends that you back up all the databases of the GV STRATUS system before upgrading to the latest version of the software or before moving your databases from the GV STRATUS Core server to a standalone Database Server. With a database backup, you can avoid any lost of feed schedules and the need to key in everything again in case of a system crash. The backup could also be placed on another machine or an external drive for extra precaution.

1. Open and log in to Microsoft SQL Server Management Studio.
2. In the tree-view expand the **Databases** node and identify the databases of the GV STRATUS system to backup, which are the following:
   - ISDB
   - MediaFlow
   - MediaFrame
   - RulesEngine
   - WfPersistence

3. Right-click on a database and select **Tasks | Back Up**.



4. On the General page, select a database to be backed up from the **Database** drop-down list.
5. Select **Full** on the **Backup type** drop-down list.
6. In the Destination section, click **Add** and select the backup destination.
7. On the Media Options page, select **Back up to the existing media set** and **Overwrite all existing backup sets**.
8. On the Backup Options page, enter the name of the backup database.
9. Click **OK**.
10. Repeat for other databases of the GV STRATUS system that you are backing up.

Restoring a database

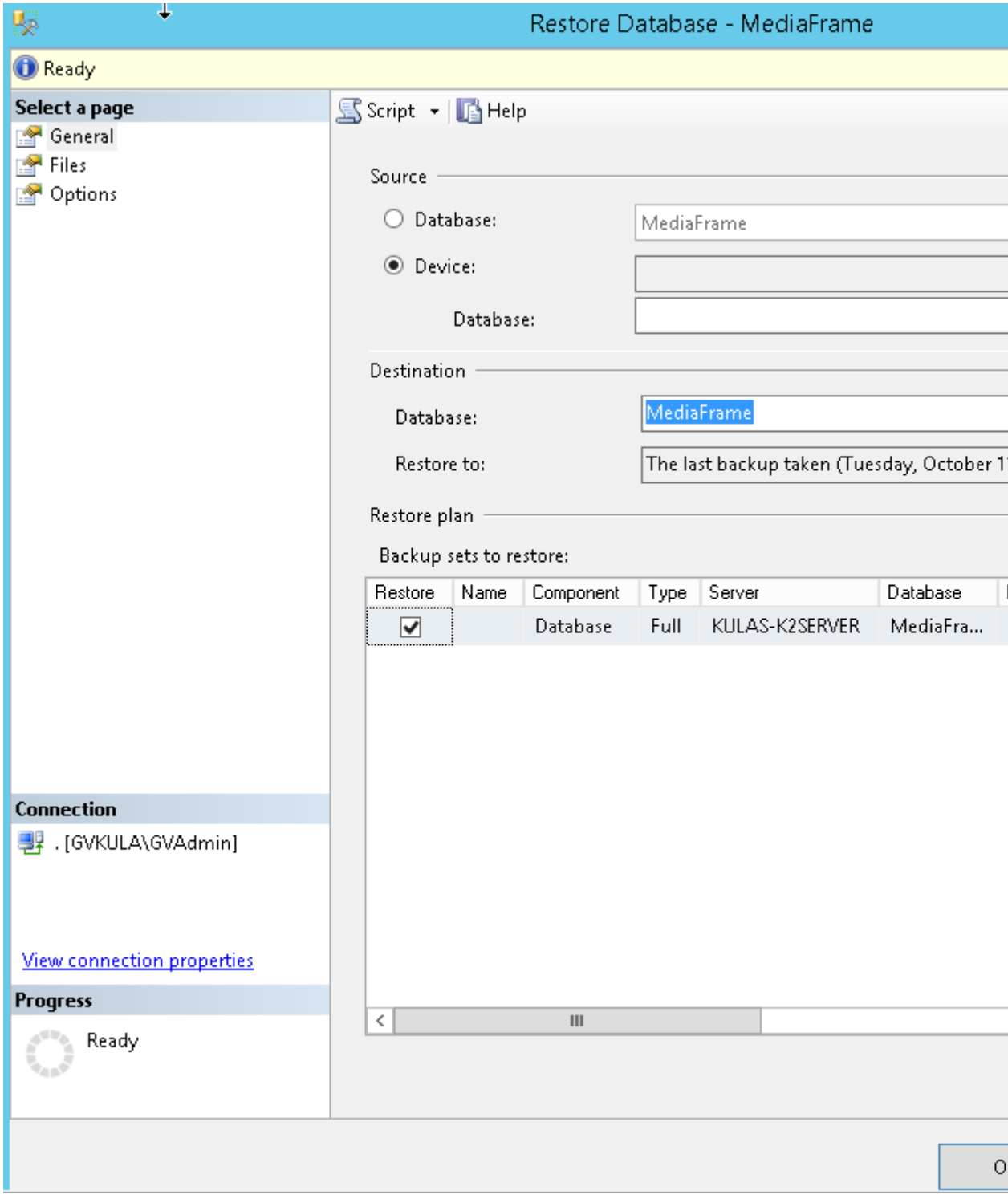
- The back up process of all GV STRATUS databases have been completed and backup locations already identified.

- Ensure that previously existing databases with the same name have been deleted from the restore destination.
- For the restore at a new standalone Database server, delete the previously installed GV STRATUS databases because they were automatically created during the initial installation via SiteConfig.

1. On the GV STRATUS Core server do the following:
   a) In Internet Information Services (IIS) Manager, stop the IIS Web server.
   b) In the Windows operating system Control Panel, stop all of the GV services.
2. Open and log in to Microsoft SQL Server Management Studio.
3. In the tree-view expand the **Databases** node and identify the databases of the GV STRATUS system to restore, which are the following:
   - ISDB
   - MediaFlow
   - MediaFrame
   - RulesEngine
   - WfPersistence

4. Right-click on a database, and select **Tasks | Restore | Database**.

   The Restore Database window opens.



5. In the **Source** section, select **Device** and click **...**.

6. Click **Add**, navigate to the database backup location, select the backup file, click **OK** and **OK**.

   If there are multiple backup files, check the date of the file and make sure you are selecting the correct file.

7. In the **Destination** section, select the database.
8. In the **Restore plan** section, select the checkbox under the **Restore** column to select the backup database to be restored.
9. In the **Options** page, do the following steps:
   - In the Restore options section, check the box to **Overwrite the existing database**.
   - In the Server connections section, check the box to **Close existing connections to destination database**, if possible.
10. Click **OK**.
11. Restart the GV STRATUS Core server.

    The GV STRATUS database is now restored.

12. If you are switching database servers, start the IIS Web server in Internet Information Services (IIS) Manager.
13. On the GV STRATUS Control Panel, click **Core | STRATUS Core Services | Primary Site** and select the Database Server Machine from the **STRATUS Database Server** drop-down list.

    Changing the **STRATUS Database Server** setting on the GV STRATUS Control Panel starts the switch over process to the newly added standalone Database Server.

14. If there were changes to assets/metadata on the system since the database backup, select **Core | Search Index Config** in the GV STRATUS Control Panel and click **Reset Index**.

Related Topics

STRATUS Core Services settings on page 296

Updating the maintenance plan after renaming the server

Before updating the maintenance plan, verify that you have has SQL Server Integration Services (SSIS) installed. SSIS is part of the typical SQL Server installation.

If you rename the GV STRATUS server, you must update the maintenance plan. Renaming the server does not alter the maintenance plan.

The maintenance plan update can be divided into three main sections:

Stage 1: Exporting the maintenance plan to a file

Stage 2: Updating the file with the new server name

Stage 3: Importing the modified plan

1. Open SQL Server Management Studio (SSMS) on the server.
2. Open a connection to the local Database Engine and to the local Integration Services. (Use the Connect drop down button in SSMS.)
3. Locate the STRATUSMaintenancePlan under **Integration Services | Stored Packages | MSDB | Maintenance Plans**.
4. Right-click on the maintenance plan to bring up the context menu, and select **Export Package**.

5. Select **File System** in the Package Location drop-down list.
6. Enter or browse to a desired location in the Package Path text box.
7. Click **OK** and verify that the file was created by navigating to the specified location.
8. Open the file in a text editor, such as Notepad.
9. Replace all occurrences of the old server name with the new server name, and save the file.
10. In SSMS, right-click on **Integration Services Stored Packages| MSDB|Maintenance Plans**.
11. From the context menu, select **Import Package**.
12. Specify the same path as you did in step 6.
13. If the modified maintenance plan has the same name as the original, a warning is displayed indicating that the Maintenance Plan will be overwritten. Click **OK**.

    NOTE: Do not import the package file (e.g. STRATUSMaintenancePlan.dtsx) into another maintenance plan.

Clearing the GV STRATUS database

If your GV STRATUS Database has data problems, you can clear all data and start over with a blank database.

NOTE: This procedure deletes all metadata, markers, keywords, associations, and other data created by the GV STRATUS application. Do not use this procedure if you have data that you want to retain in your GV STRATUS Database.

1. Uninstall the GV STRATUS core services.
2. Delete the GV STRATUS Database as follows:
   a) Open and log in to Microsoft SQL Server Management Studio.
   b) In the tree-view expand the **Databases** node and identify the databases of the GV STRATUS system.
   c) Right-click on **MediaFrame** and select **Delete**.
   d) Select **Close existing connections** and then click **OK**.
3. Re-install the GV STRATUS core services.

The GV STRATUS core services install a blank GV STRATUS Database, then re-populate the GV STRATUS Database with the assets it finds on your K2/Summit/SAN systems.

Related Topics

Logging in to Microsoft SQL Server Management Studio on page 687

Changing passwords

Use the topics in this section to avoid errors when changing passwords.

Changing administrator passwords

Grass Valley systems recognize security levels based on Windows users and groups, and pre-configured GVAdmin / GV STRATUS Internal System Account.

For ongoing security you should only change these accounts credentials or create unique accounts with similar administrative privileges.

Use the topics in this section to avoid errors when changing administrator passwords.

Changing Windows Administrator passwords

The Windows Administrator account is typically used for initial setup, configuration, and software deployment on a Grass Valley system.

If the Windows Administrator password changes or you use different account for setup, configuration, and software deployment, you must change credentials that SiteConfig uses for the target devices.

Use topics in this section to avoid errors when changing passwords.

1. *Changing passwords on Windows 7 and Windows Servers* on page 715. Follow steps in this topic to change Windows Administrator Password on all GV STRATUS Servers and K2 Machines.
2. *Changing SiteConfig credentials* on page 711. On each device, verify that Windows administrator user account credentials are the same as those that SiteConfig uses to access the device. If you need to create a new account or use another account with administrator privileges, then you must update SiteConfig with the same credentials.
3. *Fully qualified domain configuration* on page 913. If the system is fully integrated into a domain, you can use a domain account that has local administrator rights. Then you must update SiteConfig with the same domain account credentials.

Changing SiteConfig credentials

In SiteConfig, the remote target credentials need to be updated for any device using the Windows Administrator credentials to deploy software. This can be done by either changing the global credentials for device types or changing each device to override the global credentials to match the corresponding Windows Administrator credentials.

1. Change the global credentials for the following Device Types: GV STRATUS Server, GV STRATUS Client, Control Point PC, K2 Server, K2 Summit Client – SAN, and K2 Summit Client – Standalone to match the corresponding Windows Administrator credentials.
2. Proceed as follows:
   - If you previously applied credentials to the device that were different than the global credentials and now you want to apply the global device type credentials, select **Use Global Credentials**.
   - If you want to apply credentials to the device that are different than the device-type credentials, select **Override Global Credentials**.

   The Set Device Logon Credentials dialog box opens.
3. Enter the user name and password for the device and click **OK**.
4. To test the credentials, right-click on the device and choose **Remote Desktop** to start a session to the device.
5. On each device, verify the Windows administrator user account credentials are the same as those that SiteConfig uses to access the device.

Changing GV STRATUS Internal System account passwords

GVAdmin is the default account that is used for the GV STRATUS Internal System Account and to connect to other Grass Valley products. The GV STRATUS system uses this account to access assets, database, file share and some other internal functions.

If the GV STRATUS internal system account password changes or you use a different administrator account, you must change credentials used for all GV STRATUS Servers and K2 Machines.

NOTE: The GVAdmin password does not support the '@' sign as part of the password.

Use topics in this section to avoid errors when changing passwords.

1. *Changing passwords on Windows 7 and Windows Servers* on page 715. Change GVAdmin password on all GV STRATUS Servers and K2 Machines. To change the password, you need to follow the recommended guidelines for changing Windows account password. Follow steps in this topic to change GV STRATUS Internal System account password on all GV STRATUS Servers and K2 Machines.
2. *Configure SQL Security logins* on page 919. If your system is running SQL services under the local GVAdmin account, follow steps in this topic to update the GVAdmin credentials using SQL Server Configuration Manager for the SQL Server (MSSQLServer) and SQL Server Agent (MSSQLServer).
3. Update GVAdmin password in the following configuration if using the GVAdmin account in GV STRATUS Control Panel:
   - Stratus Core Services | Primary Site | Internal system Account
   - Stratus Core Services | Remote Site
   - MDI Configuration | Grass Valley Media Server MDI
   - MDI Configuration | GFTP MDI
   - K2 Storage | Remote K2 Storage
   - Location Config | Locations Configuration
   - Ingest | Channel Setup
   - RMI | Import to K2 Settings
   - TX Scheduler | Channel Setup

   NOTE: For Remote Push transfers the account that is used gets validated locally. So if you are using the workgroup GVAdmin account for remote push transfers, both systems need to have the same password for this account.

4. Update these components via SiteConfig to use the new credentials and reinstall these software:

   GrassValley_STRATUS_CoreServices

   GrassValley_STRATUS_DataMover

   GrassValley_STRATUS_DIVA_MDI

   GrassValley_STRATUS_FlashNet_MDI

   GrassValley_STRATUS_Masstech_MDI

   GrassValley_STRATUS_GFTP_MDI

   GrassValley_STRATUS_HttpProxyServer

   GrassValley_STRATUS_MediaFlow

   GrassValley_STRATUS_MEWS

   GrassValley_STRATUS_Proxy_Encoder

   GrassValley_STRATUS_RenderEngine

   GrassValley_STRATUS_Rules

   GrassValley_STRATUS_ScheduledTransferEngine

   GrassValley_STRATUS_Summit_MDI

   GrassValley_STRATUS_TrafficGateway

   GrassValley_STRATUS_Transcode

   GrassValley_Log_Manager

   GrassValley_Log_Viewer

5. If you don't reinstall for the other packages, you need to modify the following on the GV STRATUS servers:

   a. Configure GV STRATUS windows services to log on with the new credentials. From the following list, identify the services running on the server, and configure each of those services to logon with the appropriate credentials.

      - GV STRATUS ASK
      - GV STRATUS Conform Engine
      - GV STRATUS Data Mover Engine
      - GV STRATUS MDI DIVA.
      - GV STRATUS MDI Encoder.
      - GV STRATUS MDI Flashnet.
      - GV STRATUS MDI Masstech.
      - GV STRATUS MDI GFTP
      - GV STRATUS MDI Proxy
      - GV STRATUS MDI Summit
      - GV STRATUS MediaFlow Workflow Engine
      - GV STRATUS Resolver
      - GV STRATUS Rules Wizard
      - GV STRATUS Traffic Gateway
      - GV STRATUS Xcode Control
      - Grass Valley XRE Controller
      - GV Log Manager

   b. Update the StratusAppPool with the correct credentials, as follows:

      a. Open the Windows operating system Server Manager.
      b. In the tree-view navigate to Roles | Web Server (IIS) | Internet Information Services (IIS) Manager | Connections | <server_name> | Application Pools.
      c. For the StratusAppPool, update to use the correct credentials.
      d. For the HttpProxyAppPool, update to use the correct credentials.

   c. On every EDIUS and Render Engine server, use the XRE AdminConsole | Plug-in to update the credentials for every K2 server in the Importer/Exporter | K2 (SAN) | Server list.

   d. On the K2 Media Servers and K2 standalones that are hosting the Stratus Summit Service, update the credentials in the configuration file at: *C:\Program Files (x86)\Grass Valley\STRATUS Summit Service\Atlas.Service.Summit.ServiceHost.exe.config*

      For example:

```
<appSettings>
            <add key="Hostname" value="localhost"/>
            <add key="Username" value="GVAdmin"/>
            <add key="Password" value="your_password"/>
            <add key="Domain"   value=" "/>
          </appSettings>
```

   Restart the GV STRATUS Summit Services to put the change into effect. This setting will need to be updated everytime you reinstall the software.

Changing passwords on Windows 7 and Windows Servers

Use the proper Windows operating system procedure to change a password as instructed in this topic. Failure to do so causes subsequent problems in the SiteConfig application and when doing other configuration tasks. Do not use Computer | Manage and set the password for Local Users and Groups. Do not attempt to change the password on an account that is not your currently logged in account.

1. Ensure that you are logged in to the Windows operating system with the account for which you are changing the password.
2. In the Windows operating system **Control Panel**, open **User Accounts**.
3. Select the account (your currently logged in account) for which you are changing the password.
4. Press **Ctrl + Alt + Delete**.
5. Select **Change a Password**.
6. When prompted, enter the existing (current) password and the new password.
7. If the PC hosts the SiteConfig application, do the following:
   a) Close SiteConfig.
   b) Log out of the Windows operating system.
   c) Log in to the Windows operating system.

If a message regarding loss of data appears, it means you are not using the proper Windows operating system procedure. Do not proceed with attempting to change the password.

If the PC hosts the SiteConfig application and you change the password using an improper procedure, you must change the password back to the original password. Failure to do so renders SiteConfig inoperable. If it is not possible to change the password, a workaround is to switch to a different administrator account on the PC and run SiteConfig from that account.

Ports and services mapping

Software components run as Windows services, which communicate over designated ports. Do not create your own convention for port usage. Designate ports as specified in the following:

80	Protocol: TCP. Traffic: HTTP. Used by any GV STRATUS server, MediaFrame server, and Flexera server for EDIUS Workgroup license activation.
443	Protocol: TCP. Used by SNFS for GUI (Java). Used by GV STRATUS applications for HTTPS secure communication with GV STRATUS Core Server. Used by EDIUS Workgroup applications for HTTPS secure communication with Flexera server for license activation.
445	Protocol: TCP. Used by SDB and XMOS Server and NAS. Used by SiteConfig. File and printer sharing. Used by SMB.
1223	TCP: Used by EDIUS XRE Server.
1433	TCP: Used by DSM.
2000	Protocol: TCP. Used by SDB Server incoming, and by GV STRATUS and GV STRATUS Rundown clients outgoing.
2001	Protocol: TCP. Used by SDB Server incoming, and by GV STRATUS and GV STRATUS Rundown clients outgoing.

2002	Protocol: TCP. Used by backup SDB Server incoming, and by GV STRATUS and GV STRATUS Rundown clients outgoing.
2003	Protocol: TCP. Used by backup SDB Server incoming, and by GV STRATUS and GV STRATUS Rundown clients outgoing.
3000	Protocol: TCP. Used by XMOS Server incoming, and by GV STRATUS and GV STRATUS Rundown clients outgoing.
3001	Protocol: TCP. Used by XMOS Server incoming, and by GV STRATUS and GV STRATUS Rundown clients outgoing.
3811	Protocol: TCP. Used by SDB Server incoming, and by GV STRATUS and GV STRATUS Rundown clients outgoing.
3838	Protocol: TCP. Used by GV STRATUS Ingest services.
3839	Protocol: TCP. Used by GV STRATUS Ingest services.
7213	Protocol: TCP. Used by GV STRATUS Router Controller service.
7144	Protocol: TCP. Traffic: HTTP. Used by GV STRATUS Router Config service for configuration.
7145	Protocol: TCP. Traffic: HTTP. Used by router config data service.
8000 - 8032	Protocol: TCP. Traffic: HTTP. Port 8000 used as follows: GV STRATUS Common Services, including preferences, licensing, authorization; Proxy config, Web Monitor data service; Ignite for Radamec SCP and Shotoku, IP to 422 Serial Communication (Camera Preset Recall). Ports 8000 to 8032 used by Ignite as follows: Digicart, IP to 422 Serial Communication; MDS-B5 and MDS-E11, IP to 422 Serial Communication (Audio Deck Control); Chyron Aprisa SSX, Chyron Duet, Inscriber MOS, and Multi Deko, IP to 232 Serial Communication (CG Graphic Load and Playout); GV Cameraman, IP to 232 Serial Communication (Camera Preset Recall); Under Monitor Display, IP to 422 Serial Communication (Sends Clip +/- time to external device); CalrecMixer, IP to 422 or 232 Serial Communication (Audio Mixer Control); VCR (BVW), IP to 422 Serial Communication (Deck Control); VDCP, IP to 422 Serial Communication (Deck/Video Server Control). Ports 8000 - 8032 used by Comtrol Devicemaster RTS.
8080	Protocol: TCP. Traffic: HTTP. Used by GV STRATUS Summit Services. Used by WCF service provided by the GV STRATUS Workflow Engine. Used by WCF service provided by the GV STRATUS Rules Engine.
8100	HTTP/TCP: Used by Macintosh systems for the SabreTooth licensing web service to check out licenses
8190	Protocol: TCP. Traffic: HTTP. Used by WCF service provided by DeviceKey Service.
8511	Protocol: TCP. Traffic: HTTP. Used by playout config data service.
8732	Protocol: TCP. Traffic: HTTP. Used by Site Config data service .
8733	Protocol: TCP. Traffic: HTTP. Used by K2 Config data service .
8734	Protocol: TCP. Traffic: HTTP. Used by Site Config data service .
8735	Protocol: TCP. Traffic: HTTP. Used by K2 Config data service.

8737	Protocol: TCP. Traffic: HTTP. Used by GV STRATUS Ingest Config service for configuration. Used by GV STRATUS Control Panel Services for K2 Remote storage configuration. Used by GV STRATUS Core Server.
8740	Protocol: TCP. Traffic: HTTP. Used by general config data service.
8742	Protocol: TCP. Traffic: HTTP. Used by Send destination config data service.
8744	Protocol: TCP. Traffic: HTTP. Used by RMI config data service.
9010	TCP: Used by GV Ask service.
9012	TCP: Used by GV License Manager.
9014	TCP: Used by GV Metadata. Not visible on a configuration page.
9016	TCP: Used by GV Resolver. Not visible on a configuration page.
9018	TCP: Used by GV RulesWizard. Not visible on a configuration page.
9019	TCP: Used by GV RulesWizard. Not visible on a configuration page.
9020	TCP: Used by GV Transfer Manager.
9024	TCP: Used by GV Subscription Manager.
9110	TCP: Used by GV Proxy MDI.
9115	TCP: Used by GV NTFS MDI.
9122	TCP: Used by GV DIVA MDI.
9124	TCP: Used by GV FlashNet MDI.
9129	TCP: Used by GV Masstech MDI.
9130	TCP: Used by GV Profile MDI. The service manages one host process for each managed Profile. These host processes require ports 9130-9139. Stopping/starting the service stops/starts all of the host processes.
9140	TCP: Used by GV MSeries MDI. The service manages one host process for each managed M-Series iVDR. These host processes require ports 9140 - 9149. Stopping/starting the service stops/starts all of the host processes.
9150	TCP: Used by GV News Share MDI.
9160	TCP: Used by GV K2 MDI and GV K2 Summit MDI Service. The service manages a number of host processes, one for each K2 system that is being managed. These host processes require ports 9160 - 9169. Stopping/starting the service stops/starts all of the host processes.
9170	TCP: Used by GV FTP MDI in the GV STRATUS workflow, which can use a range of ports, starting with this port number.
10540	TCP: Used by XMOS Server incoming and outgoing MOS communication.
10541	TCP: Used by XMOS Server incoming and outgoing MOS communication.
12345	Protocol: TCP. Used by Ingest Router Port. Used by Ignite for VCP Server (ESPN).
16210 - 16215	Protocol: TCP. Ports 16210 to 16215 used by GV STRATUS Send Message tool.
31820	Protocol: UDP. Used for live streaming from K2 Summit/Solo systems. This is the default base for UDP ports, with the range being 31820 to 31827. Other ranges are possible, depending on the UDP port base configured on the K2 Summit/Solo system.

49168	HTTP/TCP: Used by Grass Valley K2 Config for K2Config application connection between a control point PC and the K2 system device configured. Used for most functions.
49169	TCP: Used by Grass Valley K2 Config for K2Config application connection between a control point PC and the K2 system device configured. Used for a few functions that require longer time periods.

The system also depends upon Microsoft Internet Information Services (IIS) and SQL services.

Related Topics

Devices components: Roles, cab files, services, and licenses on page 444

Set firewall for application ports on page 257

Embedded Security modes and policies

The Embedded Security solution protects against viruses and other unauthorized programs on the following Grass Valley systems:

- K2 Summit system system
- All types/roles of K2 Media Server
- All types/roles of GV STRATUS server

Embedded Security prevents any unauthorized programs from running on the system. It contains a whitelist of programs that are authorized to run. Whenever a program attempts to run, it is checked against the whitelist. If the program is not on the whitelist, Embedded Security blocks the program from running. SiteConfig, and any software deployed by SiteConfig, is on the whitelist, so you do not need to manage Embedded Security in any way when using SiteConfig to deploy software. All versions of SiteConfig are compatible with Embedded Security.

When installing software manually (without SiteConfig) it might be necessary to manage Embedded Security. When necessary, you can put Embedded Security in Update mode. This mode allows you to manually install software that is not on the whitelist. Do not confuse Update mode with the idea that Embedded Security is "disabled". When in Update mode, Embedded Security is still active. While in Update mode, Embedded Security keeps track of any software you run or install and adds it to the whitelist. When you are done installing software and any required restarts, you must take Embedded Security out of Update mode so that it can protect the system. For software that requires a restart after installation, such as K2 system software and SNFS media file system software, Embedded Security must remain in Update mode until after the restart is complete.

No system restarts are required for entering or leaving Update mode, and a restart does not change the Update mode status. If in Update mode before a restart, the system remains in Update mode after a restart. You use the Embedded Security Manager to enter and leave Update mode.

The following policies apply to the Embedded Security:

- Use Update mode only as instructed by Grass Valley product documentation or as directed by Grass Valley Support. Do not do any other operations with Embedded Security Manager, unless under the direct supervision of Grass Valley Support.
- Do not keep Embedded Security in Update mode long-term, as Embedded Security does extra processing while in Update mode and eventually problems arise when attempting to run software.

- Make sure that Embedded Security is not in Update mode when using SiteConfig to install software. Update mode interferes with SiteConfig's automatic management of Embedded Security and causes problems running the software installed.
- Leave Embedded Security enabled for normal operation of your Grass Valley system. Do not disable Embedded Security except as instructed by Grass Valley product documentation or as directed by Grass Valley Support. Enabling and disabling Embedded Security requires a restart.
- Do not install any programs or modify any operating system settings unless approved by Grass Valley. By design, Embedded Security prevents any programs from being installed or from running that are not present when you receive the system new from Grass Valley. These Grass Valley systems are not general purpose Windows workstations. The applications and configuration have been specifically optimized on each system for its intended use as part of the Grass Valley system.
- While Embedded Security is the key anti-virus component on these systems, you should still follow the Grass Valley anti-virus scan policy and scan all the devices in your Grass Valley system to ensure viruses are not propagated between machines.

Embedded Security is part of the K2 Summit system generic disk image and the K2 Media Server generic disk image compatible with K2 software version 9.0 or higher. Both K2 Media Servers and GV STRATUS servers use the same generic disk image, so GV STRATUS servers inherit the Embedded Security solution. On K2 Summit systems, the Embedded Security solution introduced with K2 software version 9.0 replaces the write filter from previous versions.

Related Topics

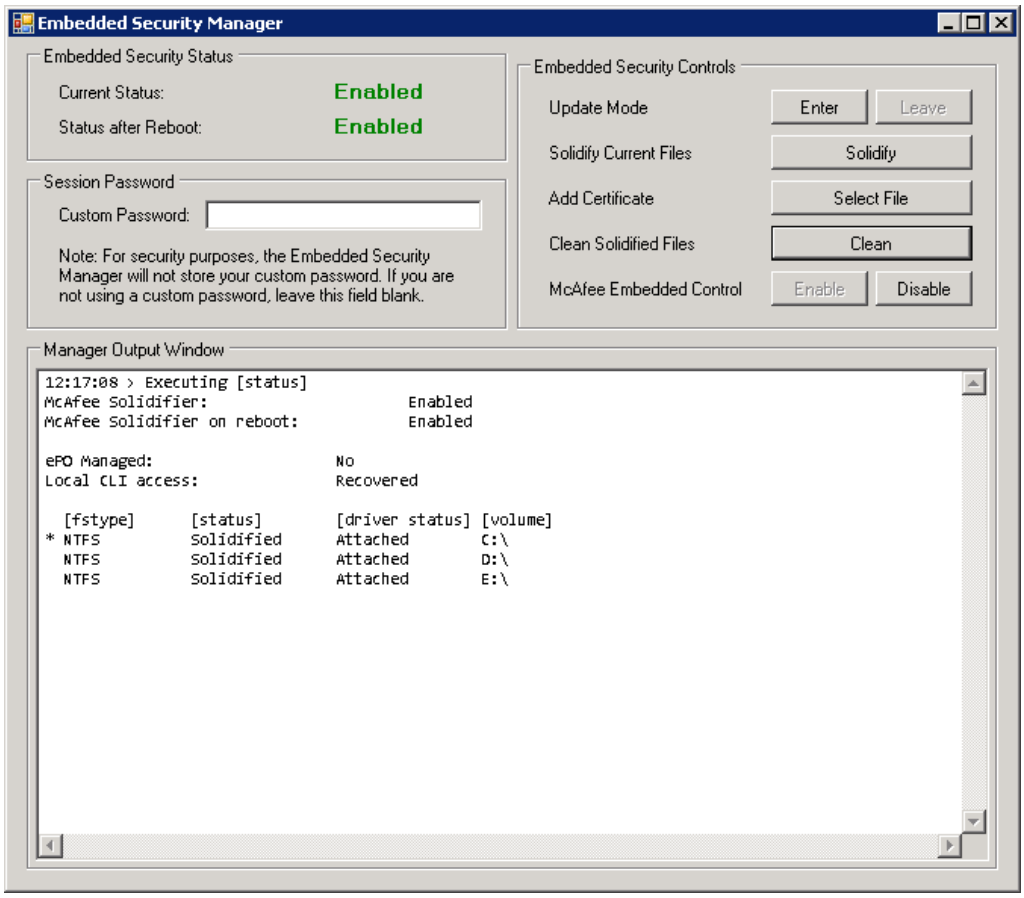
Manage Embedded Security Update mode on page 720
Grass Valley anti-virus scan policy on page 428

Manage Embedded Security Update mode

Update mode is only needed when modifying system software when not using SiteConfig. Be sure the Embedded Security Manager is set to Enabled after software updates are complete for proper operation.

1. From the Windows desktop, click **Start | All Programs | Grass Valley | Embedded Security Manager**.

   Embedded Security Manager opens.



   Interpret Current Status as follows:

   - **Enabled**: Embedded Security is enabled but is not in Update mode.
   - **Update**: Embedded Security is enabled and is in Update mode, ready for software installation.

2. Manage the Update mode as follows:

   - If Embedded Security is not in Update mode, click **Enter** to put it in Update mode.
   - If Embedded Security is already in Update mode, click **Leave** to take it out of Update mode.

   A restart is not required after you change the Update mode.

Complete system set up and configuration

Complete system installation process

Use the following list if you must change the system configuration or if there are system setup or configuration processes that are incomplete. Browse this process and do the appropriate items.

1. *Rack, cable, and power on process* on page 232. All systems require this process.
2. *SiteConfig software deployment process* on page 857. All systems require this process when updating to new versions of Grass Valley product software.
3. *K2 system set up process* on page 722. All systems require this process.
4. *Express/Core server set up process* on page 724. All systems require this process. Use SiteConfig for network setup and software install. On the GV STRATUS server with role of Common Services, use SabreTooth and install GV STRATUS licenses.
5. *Proxy Server/Storage set up process* on page 738. Only systems with proxy on the K2 SAN (A1) or with proxy on dedicated Proxy Storage (B1, C1) require this process. Use SiteConfig for network setup and software install, then use K2Config for SAN setup.
6. *Render Engine Server set up process* on page 768. Only systems with a Render Engine Server require this process. On the GV STRATUS Core server, use SabreTooth and install the STRATUS-CONFORM license. Use SiteConfig for network setup and software install. Then use K2Config for SAN setup.
7. *Standalone Database Server set up process* on page 829. Only systems with a Standalone Database Server require this process. Use SiteConfig for network setup and software install.
8. *Workflow Server set up process* on page 898. Only systems with a Workflow Server require this process. Use SiteConfig for network setup and software install. On the GV STRATUS Core server, use SabreTooth and install the STRATUS-RULES license optional transfer/transcode licenses.
9. *GV STRATUS Control Panel system configuration process* on page 839. All systems require this process. Use GV STRATUS Control Panel to configure the GV STRATUS system for your site's workflow.
10. *Customer network, licenses, and roles process* on page 250. All systems require this process. Set up the GV STRATUS Core server on the customer's network and assign GV STRATUS licenses and roles to the customer's groups and users.
11. *Client PC set up process* on page 253. All systems require this process. Add the customer's GV STRATUS client PCs to the system.
12. *Archive system set up process* on page 874. Only systems with an archive system require this process. Configure the archive system with the K2 Summit/SAN system, use SabreTooth to install the STRATUS-ARCHIVE license, and in GV STRATUS Control Panel configure an archive MDI.

K2 system set up process

All systems require this process.

If you received your K2 system already set up from Grass Valley, skip set up tasks and do the test task only.

1. *Installing SiteConfig* on page 485. All system require this process.
2. *Create a SiteConfig system description* on page 722. All systems require this process.
3. *Set up K2 systems* on page 722. All systems require this process.
4. *Test K2 systems* on page 248. All systems require this process.

Create a SiteConfig system description

All systems require this process.

If you already have a system description supplied by Grass Valley, you can skip this task.

To create a system description for K2 SAN systems, refer to "K2 10G SAN Installation and Service Manual" for instructions.

To create a system description for K2 standalone systems, refer to the "Configuring the K2 System" section of the K2 Topic Library for instructions.

Related Topics

About developing a system description on page 435

Set up K2 systems

All systems require this process.

If you received your K2 systems already set up by Grass Valley, you can skip this task.

Prerequisites for this task are as follows:

- K2 system devices are racked, cabled, and powered on.

- The K2 System has a SiteConfig system description.

This topic applies to the K2 systems that store and serve your high-resolution assets.

1. Set up K2 systems as follows:

   - If you have standalone K2 Summit systems, do the following:

Do these tasks...	Using these tools...	As instructed in the following:
Discover, modify network interfaces, propagate hosts files	SiteConfig	the "Configuring the K2 System" section of the K2 Topic Library
License the K2 Summit system for proxy	SabreTooth License Manager	the "Release Notes" section of the K2 Topic Library
Enable proxy file recording and live network streaming	K2 AppCenter Configuration Manager	the "Configuring the K2 System" section of the K2 Topic Library

   - If you have an online or production K2 SAN, do the following:

Do these tasks...	Using these tools...	As instructed in the following:
Discover, modify network interfaces, propagate hosts files	SiteConfig	"K2 10G SAN Installation and Service Manual"
License the K2 SAN	SabreTooth License Manager	
Import SiteConfig system description into K2Config	K2Config	
Configure the K2 SAN	K2Config	
Configure SAN-attached K2 Summit systems	K2Config	
License SAN-attached K2 Summit systems for proxy	SabreTooth License Manager	the "Release Notes" section of the K2 Topic Library
Enable proxy file recording and live network streaming	K2 AppCenter Configuration Manager	the "Configuring the K2 System" section of the K2 Topic Library

2. Install GV STRATUS support on K2 systems using SiteConfig as follows:
   a) In SiteConfig, add the following role(s) to standalone K2 Summit systems and to K2 Media Servers on K2 SANs that provide the high-resolution assets for the GV STRATUS system:
      - GV STRATUS Summit Service
   b) To the deployment group that contains the K2 systems, add the following:
      - *GrassValley_K2system_x.x.x.cab*, which contains the following cab files that apply to this device:
        - *GrassValley_STRATUS_SummitServices_x.x.x.cab*

      NOTE: Whenever installing or upgrading K2 systems for compatibility with GV STRATUS software, use GrassValley_K2system_x.x.x.cab. This cab file contains the compatible versions of all the K2 software and all the GV STRATUS software required on K2 systems.

      Refer to release notes for version numbers.
   c) Do the SiteConfig **Check Software** operation on the K2 systems.

      NOTE: If an "Unable to copy ... to target" error appears for a device that has the Grass Valley Embedded Security solution, apply the* Embedded Security *solution one-time initial deployment process to the device. After the one-time process is complete the error does not appear and it is no longer necessary to put* Embedded Security *in Update mode.
   d) Verify that deployment tasks are set to **Install** for the file(s) listed above.
   e) Deploy software to the K2 systems.
   f) Restart as prompted.

Test K2 systems

All systems require this process.

Whether you received your K2 system already set up from Grass Valley or you set up your K2 system on site, you should test the K2 system before proceeding.

This topic applies to the K2 systems that store and serve your high-resolution assets.

Test basic record and play operations using K2 AppCenter.

Refer to the "Using K2 AppCenter" section of the K2 Topic Library.

Related Topics

Identify test applications and setup on page 246

Express/Core server set up process

All systems require this process. Use SiteConfig for network setup and software install. On the GV STRATUS server with role of Common Services, use SabreTooth and install GV STRATUS licenses.

If you received your GV STRATUS server already set up from Grass Valley, skip set up tasks and do the test task only.

NOTE: Do not change or rename GV STRATUS core server except under the supervision of qualified Grass Valley Support personnel. Extensive system configuration is required to achieve a working GV STRATUS system.

In an operational GV STRATUS system, GV STRATUS servers must be running and logged on to the Windows operating system. The logon account must be the GV STRATUS system internal system account. The internal system account is the account that the GV STRATUS system uses to access assets and some internal system functions. By default this is the GVAdmin account. If the GVAdmin account does not exist, GV STRATUS Control Panel will be unusable.

The GVAdmin account can be disabled or removed when delegate account credentials had been reconfigured after the software install. For the delegate account on an existing system, it is important that the new password must be configured in GV STRATUS Control Panel *first*, and then changed for the corresponding workgroup or domain user. If not done in this order, GV STRATUS Control Panel will be unusable until the password for the currently configured delegate user is reverted to its previous value, at which point the credentials can be modified in the correct order.

1. *SiteConfig Express/Core server network set up* on page 725. All systems require this process.
2. *SiteConfig Express/Core server software install* on page 727. All systems require this process.
3. *SabreTooth GV STRATUS license process* on page 736. Only the GV STRATUS server with role of Common Services requires this process. Typically, this is the GV STRATUS Core server.
4. *Setting the SQL server memory limit* on page 687. All systems require this process.

NOTE: The operating system on all GV STRATUS server must be configured for English locale (en-US). However, localization options are available on GV STRATUS clients.

SiteConfig Express/Core server network set up

All systems require this process.

If you received your system already set up from Grass Valley, your Express or Core servers are already included in the SiteConfig system description and set up on the network, so you can skip these tasks. Otherwise, work through the topics in this section.

Adding an Express/Core server to the SiteConfig system description

- The system description must contain a group.

This topic applies to a GV STRATUS server that is an Express server or a Core server.

1. In the **Network Configuration | Devices** tree view, right-click a group and select **Add Device**.

2. Configure settings for the device you are adding as follows:
   - Family – Select **STRATUS**.
   - Type – Select **STRATUS Server**.
   - Model – Select one of the following:
     - If an Express server on the GV STRATUS system, select **STRATUS Core Server Express**.
     - If a Core server on the GV STRATUS system, select **STRATUS Core Server**.
   - Name – This is the device name, as displayed in the SiteConfig device tree view and device list view. This name can be different than the host name (network name). You can accept the default name or enter a name of your choice. Devices in the tree view are sorted alphabetically.
   - Amount — Select **1**.
   - Platform — Select **x64**.
   - Control network– Select the control network.
   - Starting Address – Select from the list of available addresses on the selected control network. If adding multiple devices, this is the starting address, with addresses assigned sequentially to each device added.
3. Click **OK** to save settings and close.

   SiteConfig adds the server to the system description as a placeholder device.
4. Verify that unmanaged control network interface is configured correctly and modify if necessary.

Next, add the GV STRATUS server to the control network.

Related Topics

About developing a system description on page 435
Modifying unassigned (unmanaged) control network interface on page 488

Adding a GV STRATUS server to the control network with SiteConfig

Use SiteConfig to configure network settings on a separate GV STRATUS server.

Before doing this task, make sure the GV STRATUS server is added as a placeholder device to the SiteConfig system description.

The following steps are the standard tasks for adding a device to the control network using SiteConfig. Use these steps for the GV STRATUS server you are adding.

1. Discover the device using SiteConfig device discovery.
2. Assign the discovered device to the placeholder device in the SiteConfig system description.
3. Modify the control network interface to ensure communication on the control network.
4. Modify the host name and/or device name as desired.
5. Ping the device to verify network communication.
6. Verify credentials to ensure SiteConfig can install software on the device.
7. Generate and/or add to host tables as appropriate for your network.

Related Topics

Adding a device to a network with SiteConfig on page 490
Adding a device to a network with SiteConfig on page 490

SiteConfig Express/Core server software install

All systems require this process.

If you received your system pre-configured from Grass Valley, software is already installed, so you can skip these tasks. Otherwise, work through the tasks in this section as follows:

- If your GV STRATUS system has a single GV STRATUS Express server, install software on the Express server.
- If your GV STRATUS system has multiple GV STRATUS servers, install software on the GV STRATUS Core server.

Related Topics

GV STRATUS servers logon account on page 245

Setting deployment options

- A software package must be assigned to the deployment group and applicable deployment tasks must be displayed in the Tasks area.

1. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.
2. In the Tasks list view, view tasks and determine if you must set deployment options.

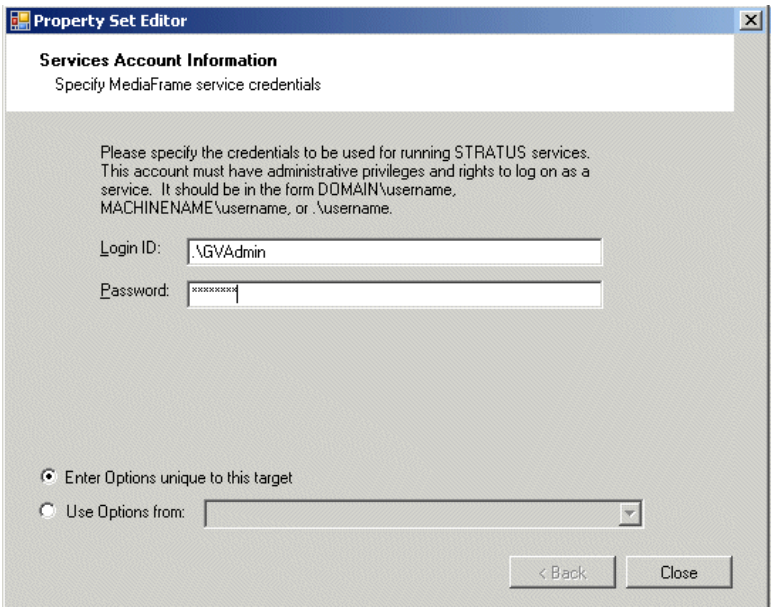
   Tasks that need to have deployment options set display in the Details column a message stating "Deployment options required."

   If you select a task that needs to have its deployment options set, the Start Deployment button is disabled and the message is displayed next to the button.
3. Do one of the following to set deployment options:

   - Double-click the task.
   - Select the task and click the **Options** button.

   A wizard opens.

4. Work through wizards and set deployment options for GV STRATUS software as follows:

Software	Deployment options
GrassValley_STRATUS_CommonServices GrassValley_STRATUS_ControlPanelService GrassValley_STRATUS_CoreServices GrassValley_STRATUS_CRArchive_MDI GrassValley_STRATUS_Databases GrassValley_STRATUS_DataMover GrassValley_STRATUS_DIVA_MDI GrassValley_STRATUS_ExternalMedia GrassValley_STRATUS_FlashNet_MDI GrassValley_STRATUS_GFTP_MDI GrassValley_STRATUS_HttpProxyServer GrassValley_STRATUS_IngestServices GrassValley_STRATUS_Masstech_MDI GrassValley_STRATUS_MediaFlow GrassValley_STRATUS_MEWS GrassValley_STRATUS_Proxy_MDI GrassValley_STRATUS_ProxyStreamingService GrassValley_STRATUS_RenderEngine GrassValley_STRATUS_Rules GrassValley_STRATUS_ScheduledTransferEngine GrassValley_STRATUS_SocialMedia GrassValley_STRATUS_Summit_MDI GrassValley_STRATUS_TrafficGateway GrassValley_STRATUS_Transcode GrassValley_STRATUS_WebApps GrassValley_STRATUS_WebClient GrassValley_DeviceKeyService GrassValley_LogManager GrassValley_LogViewer	 Use the local system account if your system is on a workgroup or if it's on a domain but uses the local system account in SQL. Use a domain\admin account if the account was previously mapped in SQL to the MediaFrame, MediaFlow, RulesEngine and WFPersistence databases. Entering account credentials allows you to use the **Use options from** feature for all other devices of the same type. Once you enter the account credentials this way on the first device, it becomes the template from which options for other devices are copied.

5. If you have multiple devices of the same type, you can enter deployment options for one of them using the wizard. Then, when you bring up the same wizard on every device, you can choose the **Use options from** radio button and select the first device for which you set options.

   SiteConfig copies the options you set for the first device and fills in the blanks on the wizard.

Installing software on a GV STRATUS Express server

Only systems with a single GV STRATUS Express server require this process. Use SiteConfig to install software on the server.

- The server on which you are installing software must be in the SiteConfig system description and communicating on the control network.

- The server on which you are installing software must have its credentials set in SiteConfig to allow access.

1. Verify the SiteConfig roles currently assigned to the server. If the roles are not correct for your system design, add or remove roles accordingly. Roles are as follows:

   - GV STRATUS Ingest Services (Required)
   - GV STRATUS Control Panel Service (Required)
   - GV STRATUS Common Services (Required)
   - License Manager (Required)
   - GV STRATUS Data Mover Engine (Required)
   - GV STRATUS Proxy Express Server (Required on Express server)
   - GV STRATUS Control Panel (Required)
   - GV STRATUS Core Services (Required)
   - GV STRATUS Database (Required)
   - GV STRATUS Summit MDI (Required)
   - GV STRATUS Common RESTful Archive MDI (Optional)
   - GV STRATUS Diva MDI (Optional)
   - GV STRATUS FlashNet MDI (Optional)
   - GV STRATUS Masstech MDI (Optional)
   - GV STRATUS Generic FTP MDI (Optional)
   - GV STRATUS Proxy Streaming Service (Optional)
   - GV STRATUS Rules Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
   - GV STRATUS Scheduled Transfer Engine (Optional)
   - GV STRATUS Scheduled Ingest Engine (Not used in this GV STRATUS release)
   - GV STRATUS Scheduled Ingest Manager (Not used in this GV STRATUS release)
   - GV STRATUS SocialMedia Engine (Optional)
   - GV STRATUS ExternalMedia Engine (Optional)
   - GV STRATUS Traffic Gateway (Optional)
   - GV STRATUS Topic Service Bus (Not used in this GV STRATUS release)
   - GV STRATUS Web Apps (Required. Must be assigned to Express/Core server to display Statistics panel via Dashboard)
   - GV STRATUS Web Client (Optional)
   - GV STRATUS Workflow Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
   - GV STRATUS Xcode Control Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
   - GV Log Manager (Required)
   - GV Log Viewer (Required)
   - GV STRATUS Rundown Server Components (Optional)
   - GV STRATUS Application (Use for test purposes only)
   - If optionally used as a Render Engine, these additional roles:
     - GV STRATUS Render Engine

2. Add the server to a deployment group, such as the GV STRATUS deployment group.

3. Add the following files to the deployment group:

   - *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:

     - *GrassValley_STRATUS_IngestServices_x.x.x.cab*
     - *GrassValley_STRATUS_ControlPanelService_x.x.x.cab*
     - *GrassValley_STRATUS_CommonServices_x.x.x.cab*
     - *GrassValley_STRATUS_CoreServices_x.x.x.cab*
     - *GrassValley_STRATUS_ControlPanel_x.x.x.cab*
     - *GrassValley_STRATUS_Databases_x.x.x.cab*
     - *GrassValley_STRATUS_DataMover_x.x.x.cab*
     - *GrassValley_STRATUS_ExternalMedia_x.x.x.cab*
     - *GrassValley_STRATUS_HttpProxyServer_x.x.x.cab*
     - *GrassValley_STRATUS_Mediaflow_x.x.x.cab*
     - *GrassValley_STRATUS_CRArchive_MDI_x.x.x.cab*
     - *GrassValley_STRATUS_DIVA_MDI_x.x.x.cab*
     - *GrassValley_STRATUS_FlashNet_MDI_x.x.x.cab*
     - *GrassValley_STRATUS_Masstech_MDI_x.x.x.cab*
     - *GrassValley_STRATUS_GFTP_MDI_x.x.x.cab*
     - *GrassValley_STRATUS_Summit_MDI_x.x.x.cab*
     - *GrassValley_STRATUS_Proxy_MDI_x.x.x.cab*
     - *GrassValley_STRATUS_ProxyStreamingService_x.x.x.cab*
     - *GrassValley_STRATUS_RenderEngine_x.x.x.cab*
     - *GrassValley_STRATUS_Rules_x.x.x.cab*
     - *GrassValley_STRATUS_ScheduledTransferEngine_x.x.x.cab*
     - *GrassValley_STRATUS_SocialMedia_x.x.x.cab*
     - *GrassValley_STRATUS_Transcode_x.x.x.cab*
     - *GrassValley_STRATUS_TrafficGateway_x.x.x.cab*
     - *GrassValley_STRATUS_WebApps_x.x.x.cab*
     - *GrassValley_STRATUS_WebClient_x.x.x.cab*
     - *GrassValley_Sabretooth_Application_x.x.x.cab*
     - *GrassValley_DeviceKeyService_x.x.x.cab*
     - *GrassValley_LogManager_x.x.x.cab*
     - *GrassValley_LogViewer_x.x.x.cab*
     - *GV_STRATUS_Rundown_x.x.x.cab*

   - *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:

     - *GrassValley_STRATUS_ControlPanel_x.x.x.cab*
     - *GrassValley_STRATUS_Application_x.x.x.cab* (Use for test purposes only)

   - *GrassValley_K2system_x.x.x.cab* for K2 9.8.x systems.
   - *GrassValley_K2Plus_x.x.x.cab* for K2 10.x systems.

   Refer to release notes for version numbers.

4. Do the SiteConfig **Check Software** operation on the server.

   NOTE: If an "Unable to copy ... to target" error appears for a device that has the Grass Valley Embedded Security solution, apply the* Embedded Security *solution one-time initial deployment process to the device. After the one-time process is complete the error does not appear and it is no longer necessary to put* Embedded Security *in Update mode.

5. Set deployment tasks to **Install** for all the files listed above except when installing Render Engine software, do not install the Render Engine cab file yet.

   If a WFRegMon install task appears, install it as well. It is required to support Grass Valley software installers. There is no uninstall task.

6. Deploy software that is not Render Engine software to the server.
7. Restart as prompted.
8. When installing Render Engine software, do the following:
   a) Set deployment tasks to **Install** for the Render Engine cab file.
   b) Deploy Render Engine software to the server.

      NOTE: Expect long deployment times when installing Render Engine software. It can take several minutes to install. Allow the installation to complete. Do not attempt to stop the installation.

9. Restart as prompted.

Related Topics

Adding a software role to a device on page 490
Configuring deployment groups on page 80
Check all currently installed software on GV STRATUS devices on page 278
Add software package to deployment group for GV STRATUS and other devices on page 111
Devices components: Roles, cab files, services, and licenses on page 444
GV STRATUS servers logon account on page 245

Installing software on a GV STRATUS Core server

Only systems with multiple GV STRATUS servers require this process. Use SiteConfig to install software on the GV STRATUS server that has the role of Core Server.

- The server on which you are installing software must be in the SiteConfig system description and communicating on the control network.

- The server on which you are installing software must have its credentials set in SiteConfig to allow access.

1. Verify the SiteConfig roles currently assigned to the server. If the roles are not correct for your system design, add or remove roles accordingly. Roles are as follows:
   - GV STRATUS Ingest Services (Required)
   - GV STRATUS Control Panel Service (Required)
   - GV STRATUS Common Services (Required)
   - License Manager (Required)
   - GV STRATUS Control Panel (Required)
   - GV STRATUS Core Services (Required)
   - GV STRATUS Database (Required)
   - GV STRATUS Data Mover Engine (Required)
   - GV STRATUS Summit MDI (Required)
   - GV STRATUS Common RESTful Archive MDI (Optional)
   - GV STRATUS Diva MDI (Optional)
   - GV STRATUS FlashNet MDI (Optional)
   - GV STRATUS Masstech MDI (Optional)
   - GV STRATUS Generic FTP MDI (Optional)
   - GV STRATUS Proxy Streaming Service (Optional)
   - GV STRATUS Rules Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
   - GV STRATUS Scheduled Transfer Engine (Optional)
   - GV STRATUS Scheduled Ingest Engine (Not used in this GV STRATUS release)
   - GV STRATUS Scheduled Ingest Manager (Not used in this GV STRATUS release)
   - GV STRATUS SocialMedia Engine (Optional)
   - GV STRATUS ExternalMedia Engine (Optional)
   - GV STRATUS Traffic Gateway (Optional)
   - GV STRATUS Topic Service Bus (Not used in this GV STRATUS release)
   - GV STRATUS Workflow Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
   - GV STRATUS Xcode Control Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
   - GV Log Manager (Required)
   - GV Log Viewer (Required)
   - GV STRATUS Web Apps (Required. Must be assigned to Express/Core server to display Statistics panel via Dashboard)
   - GV STRATUS Web Client (Optional)
   - GV STRATUS Rundown Server Components (Optional)
   - GV STRATUS Application (Use for test purposes only)
2. Add the server to a deployment group, such as the GV STRATUS deployment group.

3. Add the following files to the deployment group:

   - *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:

     - *GrassValley_STRATUS_IngestServices_x.x.x.cab*
     - *GrassValley_STRATUS_ControlPanelService_x.x.x.cab*
     - *GrassValley_STRATUS_CommonServices_x.x.x.cab*
     - *GrassValley_STRATUS_CoreServices_x.x.x.cab*
     - *GrassValley_STRATUS_ControlPanel_x.x.x.cab*
     - *GrassValley_STRATUS_Databases_x.x.x.cab*
     - *GrassValley_STRATUS_DataMover_x.x.x.cab*
     - *GrassValley_STRATUS_ExternalMedia_x.x.x.cab*
     - *GrassValley_STRATUS_CRArchive_MDI_x.x.x.cab*
     - *GrassValley_STRATUS_DIVA_MDI_x.x.x.cab*
     - *GrassValley_STRATUS_FlashNet_MDI_x.x.x.cab*
     - *GrassValley_STRATUS_Masstech_MDI_x.x.x.cab*
     - *GrassValley_STRATUS_GFTP_MDI_x.x.x.cab*
     - *GrassValley_STRATUS_Summit_MDI_x.x.x.cab*
     - *GrassValley_STRATUS_Proxy_MDI_x.x.x.cab*
     - *GrassValley_STRATUS_ProxyStreamingService_x.x.x.cab*
     - *GrassValley_STRATUS_Mediaflow_x.x.x.cab*
     - *GrassValley_STRATUS_Rules_x.x.x.cab*
     - *GrassValley_STRATUS_ScheduledTransferEngine_x.x.x.cab*
     - *GrassValley_STRATUS_SocialMedia_x.x.x.cab*
     - *GrassValley_STRATUS_Transcode_x.x.x.cab*
     - *GrassValley_STRATUS_TrafficGateway_x.x.x.cab*
     - *GrassValley_STRATUS_WebApps_x.x.x.cab*
     - *GrassValley_STRATUS_WebClient_x.x.x.cab*
     - *GrassValley_Sabretooth_Application_x.x.x.cab*
     - *GrassValley_DeviceKeyService_x.x.x.cab*
     - *GrassValley_LogManager_x.x.x.cab*
     - *GrassValley_LogViewer_x.x.x.cab*
     - *GV_STRATUS_Rundown_x.x.x.cab*

   - *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:

     - *GrassValley_STRATUS_ControlPanel_x.x.x.cab*
     - *GrassValley_STRATUS_Application_x.x.x.cab* (Use for test purposes only)

   - *GrassValley_K2system_x.x.x.cab* for K2 9.8.x systems.
   - *GrassValley_K2Plus_x.x.x.cab* for K2 10.x systems.

   Refer to release notes for version numbers.

4. Do the SiteConfig **Check Software** operation on the server.

   NOTE: If an "Unable to copy ... to target" error appears for a device that has the Grass Valley Embedded Security solution, apply the* Embedded Security *solution one-time initial deployment process to the device. After the one-time process is complete the error does not appear and it is no longer necessary to put* Embedded Security *in Update mode.

5. Verify that deployment tasks are set to **Install** for the files listed above.

   If a WFRegMon install task appears, install it as well. It is required to support Grass Valley software installers. There is no uninstall task.

6. Deploy software to the server.
7. Restart as prompted.

Related Topics

Adding a software role to a device on page 490
Configuring deployment groups on page 80
Check all currently installed software on GV STRATUS devices on page 278
Add software package to deployment group for GV STRATUS and other devices on page 111
Devices components: Roles, cab files, services, and licenses on page 444
GV STRATUS servers logon account on page 245

SabreTooth GV STRATUS license process

Only the GV STRATUS server with role of Common Services requires this process. Typically, this is the GV STRATUS Core server.

If you received your system pre-configured from Grass Valley, licenses are already installed, so you can skip these tasks. Otherwise, do the following:

1. Refer to the license sheet that you received with your GV STRATUS license. The license sheet has the Sales Order number that you need.
2. On the GV STRATUS server with role of Common Services, run the SabreTooth License Manager, generate a unique ID, and send the email to Grass Valley requesting your license or licenses.

   Refer to this Topic Library for detailed licensing procedures.

3. When you receive your license file, use SabreTooth License Manager and install it on the GV STRATUS server with role of Common Services.

Related Topics

Licensing a GV STRATUS system on page 61
Requesting a license on page 63
Adding a license on page 64

SabreTooth Multisite license process

The Multisite license is installed on the GV STRATUS server with role of Common Services. Typically the GV STRATUS Core server has the role of Common Services.

One STRATUS-MULTISITE license is required to access a remote GV STRATUS. Once installed, multisite access rights can be assigned to groups and users.

If you received your system pre-configured from Grass Valley, licenses are already installed, so you can skip these tasks. Otherwise, do the following:

1. Refer to the license sheet that you received with your GV STRATUS license. The license sheet has the Sales Order number that you need.
2. On the GV STRATUS server with role of Common Services, run the SabreTooth License Manager, generate a unique ID, and send the email to Grass Valley requesting your license or licenses.

   Refer to this Topic Library for detailed licensing procedures.
3. When you receive your license file, use SabreTooth License Manager and install it on the server.

SabreTooth Web Client license process

Only the GV STRATUS server with role of Common Services requires this process. Typically the GV STRATUS Core server has the role of Common Services.

Only one license is required to use Web Client in your GV STRATUS system. It is a SabreTooth floating license, and not restricted to a single computer.

- STRATUS-WEB-CLIENT

If you received your system pre-configured from Grass Valley, licenses are already installed, so you can skip these tasks. Otherwise, do the following:

1. Refer to the license sheet that you received with your GV STRATUS license. The license sheet has the Sales Order number that you need.
2. On the GV STRATUS server with role of Common Services, run the SabreTooth License Manager, generate a unique ID, and send the email to Grass Valley requesting your license or licenses.

   Refer to this Topic Library for detailed licensing procedures.
3. When you receive your license file, use SabreTooth License Manager and install it on the server.

Setting the SQL server memory limit

The SQL server depends on memory to cache information from databases on disk for fast access. If more data exists on disk than can be held in memory, the SQL server performance will degrade.

To avoid low memory issues on the GV STRATUS Core server or the standalone Database server, the memory that should be assigned to SQL server depends on the memory size of the physical device.

Grass Valley recommends the setting of SQL server memory limit according to the table below:

Physical Memory	SQL server memory limit	Approximate number of assets supported
12 GB	5120 MB	200,000 – 350,000
16 GB	8192 MB	320,000 – 560,000
32 GB	18,432 MB	720,000 – 1,260,000
48 GB	32,768 MB	1,280,000 – 2,240,000
64 GB	47,104 MB	1,900,000 – 3,360,000

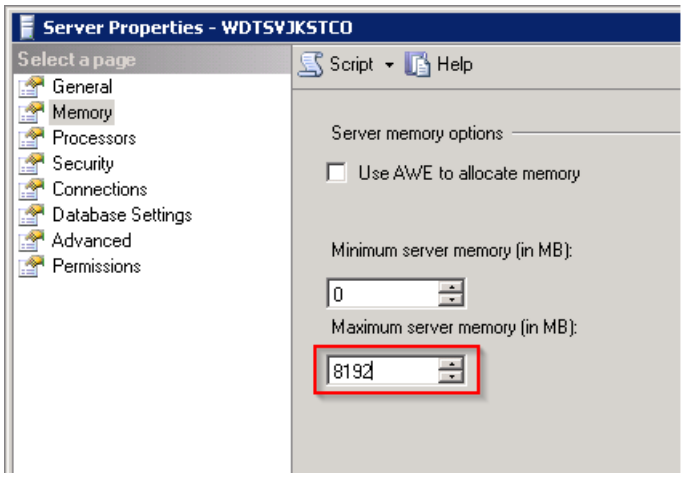
Set the SQL server memory limit as follows:

1. From the Windows desktop click **Start | All Programs | Microsoft SQL Server** and select **Microsoft SQL Server Management Studio**.

   Microsoft SQL Server Management Studio opens.
2. Log on as an Administrator.
3. Right-click on the SQL server name and select **Properties** from the context menu.

   The **Server Properties** dialog opens.
4. Click **Memory**.

   The Memory page opens.



5. In the **Maximum server memory** setting, enter your SQL server memory limit in MB.
6. Click **OK**.

A restart of the server is not necessary, but recommended.

Proxy Server/Storage set up process

Only systems with proxy on the K2 SAN (A1) or with proxy on dedicated Proxy Storage (B1, C1) require this process. Use SiteConfig for network setup and software install, then use K2Config for SAN setup.

If you received your proxy system already set up from Grass Valley, skip set up tasks and do the test task only.

1. *SiteConfig Proxy Server/Storage network set up* on page 739. Only systems with proxy on the K2 SAN (A1) or with proxy on a dedicated Proxy Storage system (B1, C1) require this process.
2. *SiteConfig Proxy Server/Storage software install* on page 741. Only systems with proxy on the K2 SAN (A1) or with proxy on a dedicated Proxy Storage system (B1, C1) require this process.
3. *K2Config Proxy server set up* on page 747. Only systems with proxy on the K2 SAN (A1) require this process.

4. *K2Config Proxy Storage set up* on page 751. Only systems with proxy on a dedicated Proxy Storage system (B1, C1) require this process.

SiteConfig Proxy Server/Storage network set up

Only systems with proxy on the K2 SAN (A1) or with proxy on a dedicated Proxy Storage system (B1, C1) require this process.

If you received your system pre-configured from Grass Valley, your Proxy server or Proxy Storage system is already included in the SiteConfig system description and set up on the network, so you can skip these tasks. Otherwise, work through the tasks in this section as follows:

- If your proxy assets are on an online or production K2 SAN (A1), start by adding the K2 SAN's Proxy server to the SiteConfig system description.
- If your proxy assets are on a dedicated Proxy Storage system (B1, C1), start by adding the Proxy Storage system to the SiteConfig system description.

Adding a Proxy server to the SiteConfig system description

- The system description must contain a group.

This topic applies to a K2 SAN's Proxy server, which is the GV STRATUS server with role of Proxy Server attached to an online or production K2 SAN.

1. In the **Network Configuration | Devices** tree view, right-click a group and select **Add Device**.
2. Configure settings for the device you are adding as follows:
   - Family – Select **STRATUS**.
   - Type – Select **STRATUS Server**.
   - Model – Select **STRATUS Proxy Server**.
   - Name – This is the device name, as displayed in the SiteConfig device tree view and device list view. This name can be different than the host name (network name). You can accept the default name or enter a name of your choice. Devices in the tree view are sorted alphabetically.
   - Amount — Select **1**.
   - Platform — Select **x64**.
   - Control network– Select the control network.
   - Starting Address – Select from the list of available addresses on the selected control network. If adding multiple devices, this is the starting address, with addresses assigned sequentially to each device added.
3. Click **OK** to save settings and close.

   SiteConfig adds the Proxy server to the system description as a placeholder device.
4. Verify that the unmanaged control network interface is configured correctly and modify if necessary.

Next, add the GV STRATUS server to the control network.

Related Topics

About developing a system description on page 435

Modifying unassigned (unmanaged) control network interface on page 488

Adding a Proxy Storage file system server to the SiteConfig system description

Do this if you have a Proxy Storage system and it is not yet included in the SiteConfig system description.

- The Proxy Storage system must be cabled and powered on.
- The system description must contain a group.

This procedure assumes that your online or production K2 SAN is already added to the system description. If you have not yet added your online or production K2 SAN to the system description, you can add both the K2 SAN and the Proxy Storage system at the same time. To do so, make the appropriate selection on the first page of the New Site Wizard, then refer to "K2 10G SAN Installation and Service Manual" for more information.

1. In the **Network Configuration | Devices** tree view, right-click a group and select **Add Device**.
2. Configure settings for the device you are adding as follows:
   - Family – Select **STRATUS**.
   - Type – Select **STRATUS Server**.
   - Model – Select **STRATUS Proxy Storage File System Server**.
   - Name – This is the device name, as displayed in the SiteConfig device tree view and device list view. This name can be different than the host name (network name). You can accept the default name or enter a name of your choice. Devices in the tree view are sorted alphabetically.
   - Amount — Select **1**.
   - Platform — Select **x64**.
   - Control network– Select the control network.
   - Starting Address – Select from the list of available addresses on the selected control network. If adding multiple devices, this is the starting address, with addresses assigned sequentially to each device added.
3. Click **OK** to save settings and close.

   SiteConfig adds the Proxy Storage file system server to the system description as a placeholder device.
4. Verify that the unmanaged control network interface is configured correctly and modify if necessary.

Next, add the GV STRATUS server to the control network.

Related Topics

About developing a system description on page 435
Modifying unassigned (unmanaged) control network interface on page 488

Adding a GV STRATUS server to the control network with SiteConfig

Use SiteConfig to configure network settings on a separate GV STRATUS server.

Before doing this task, make sure the GV STRATUS server is added as a placeholder device to the SiteConfig system description.

The following steps are the standard tasks for adding a device to the control network using SiteConfig. Use these steps for the GV STRATUS server you are adding.

1. Discover the device using SiteConfig device discovery.
2. Assign the discovered device to the placeholder device in the SiteConfig system description.
3. Modify the control network interface to ensure communication on the control network.
4. Modify the host name and/or device name as desired.
5. Ping the device to verify network communication.
6. Verify credentials to ensure SiteConfig can install software on the device.
7. Generate and/or add to host tables as appropriate for your network.

Related Topics

Adding a device to a network with SiteConfig on page 490
Adding a device to a network with SiteConfig on page 490

SiteConfig Proxy Server/Storage software install

Only systems with proxy on the K2 SAN (A1) or with proxy on a dedicated Proxy Storage system (B1, C1) require this process.

If you received your system pre-configured from Grass Valley, software is already installed, so you can skip these tasks. Otherwise, work through the tasks in this section as follows:

- If your proxy assets are on an online or production K2 SAN (A1), you have a Proxy server, which is a GV STRATUS server with role of Proxy Server that is attached to your online or production K2 SAN. Install software on the Proxy server.
- If your proxy assets are on a Proxy Storage SAN (B1, C1), you have a Proxy Storage file system server, which is a GV STRATUS server with role of Proxy Server that is attached to your Proxy Storage system. Install software on the Proxy Storage file system server.

Related Topics

GV STRATUS servers logon account on page 245

Setting deployment options

- A software package must be assigned to the deployment group and applicable deployment tasks must be displayed in the Tasks area.

1. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.

2. In the Tasks list view, view tasks and determine if you must set deployment options.

   Tasks that need to have deployment options set display in the Details column a message stating "Deployment options required."

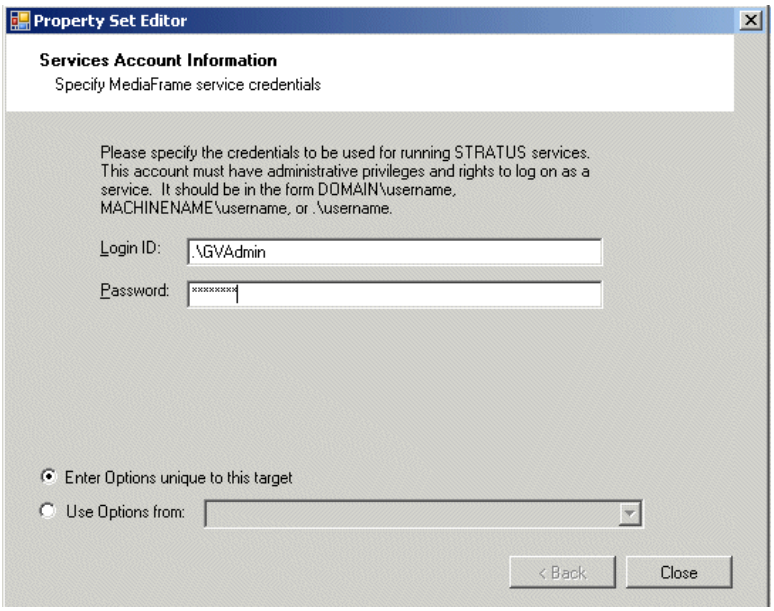
   If you select a task that needs to have its deployment options set, the Start Deployment button is disabled and the message is displayed next to the button.

3. Do one of the following to set deployment options:

   - Double-click the task.
   - Select the task and click the **Options** button.

   A wizard opens.

4. Work through wizards and set deployment options for GV STRATUS software as follows:

Software	Deployment options
GrassValley_STRATUS_CommonServices GrassValley_STRATUS_ControlPanelService GrassValley_STRATUS_CoreServices GrassValley_STRATUS_CRArchive_MDI GrassValley_STRATUS_Databases GrassValley_STRATUS_DataMover GrassValley_STRATUS_DIVA_MDI GrassValley_STRATUS_ExternalMedia GrassValley_STRATUS_FlashNet_MDI GrassValley_STRATUS_GFTP_MDI GrassValley_STRATUS_HttpProxyServer GrassValley_STRATUS_IngestServices GrassValley_STRATUS_Masstech_MDI GrassValley_STRATUS_MediaFlow GrassValley_STRATUS_MEWS GrassValley_STRATUS_Proxy_MDI GrassValley_STRATUS_ProxyStreamingService GrassValley_STRATUS_RenderEngine GrassValley_STRATUS_Rules GrassValley_STRATUS_ScheduledTransferEngine GrassValley_STRATUS_SocialMedia GrassValley_STRATUS_Summit_MDI GrassValley_STRATUS_TrafficGateway GrassValley_STRATUS_Transcode GrassValley_STRATUS_WebApps GrassValley_STRATUS_WebClient GrassValley_DeviceKeyService GrassValley_LogManager GrassValley_LogViewer	 Use the local system account if your system is on a workgroup or if it's on a domain but uses the local system account in SQL. Use a domain\admin account if the account was previously mapped in SQL to the MediaFrame, MediaFlow, RulesEngine and WFPersistence databases. Entering account credentials allows you to use the **Use options from** feature for all other devices of the same type. Once you enter the account credentials this way on the first device, it becomes the template from which options for other devices are copied.

5. If you have multiple devices of the same type, you can enter deployment options for one of them using the wizard. Then, when you bring up the same wizard on every device, you can choose the **Use options from** radio button and select the first device for which you set options.

   SiteConfig copies the options you set for the first device and fills in the blanks on the wizard.

Installing software on a Proxy server

Only systems with proxy on the K2 SAN require this process. Use SiteConfig to install software on the GV STRATUS server with role of Proxy Server that is attached to the K2 SAN.

- The server on which you are installing software must be in the SiteConfig system description and communicating on the control network.
- The server on which you are installing software must have its credentials set in SiteConfig to allow access.

1. Verify the SiteConfig roles currently assigned to the server. If the roles are not correct for your system design, add or remove roles accordingly. Roles are as follows:
   - GV STRATUS Proxy K2 SAN Server
   - GV Log Manager
   - StorNext File System Client
2. Add the server to a deployment group, such as the GV STRATUS deployment group.
3. Add the following files to the deployment group:
   - *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
     - *GrassValley_STRATUS_HttpProxyServer_x.x.x.cab*
     - *GrassValley_LogManager_x.x.x.cab*
   - *GrassValley_STRATUSClient_x.x.x.cab*.
   - For K2 9.8.x systems; use *GrassValley_K2system_x.x.x.cab*, which contains the following cab files that apply to this device:
     - *GrassValleyK2Server_x64_9.8.x.x.cab*
     - *SNFS_x64_4.7.x.xxx.cab*
   - For K2 10.x systems; use *GrassValley_K2Plus_x.x.x.cab*, which contains the following cab files that apply to this device:
     - *GrassValleyK2Server_x64_10.x.x.cab*
     - *SNFS_x64_6.0.x.xxx.cab*

   Refer to release notes for version numbers.
4. Do the SiteConfig **Check Software** operation on the server.

   NOTE: If an "Unable to copy ... to target" error appears for a device that has the Grass Valley Embedded Security solution, apply the* Embedded Security *solution one-time initial deployment process to the device. After the one-time process is complete the error does not appear and it is no longer necessary to put* Embedded Security *in Update mode.

5. Verify that deployment tasks are set to **Install** for the files listed above.

   If a WFRegMon install task appears, install it as well. It is required to support Grass Valley software installers. There is no uninstall task.

6. Deploy software to the server.
7. Restart as prompted.

Next, use K2Config and set up the Proxy server on the K2 SAN.

Related Topics

Adding a software role to a device on page 490
Configuring deployment groups on page 80
Check all currently installed software on GV STRATUS devices on page 278
Add software package to deployment group for GV STRATUS and other devices on page 111
Devices components: Roles, cab files, services, and licenses on page 444
GV STRATUS servers logon account on page 245

Installing software on a Proxy Storage file system server

Only systems with proxy on a dedicated Proxy Storage system require this process. Use SiteConfig to install software on the Proxy Storage file system server, which is the GV STRATUS server on a Proxy Storage system.

- The server on which you are installing software must be in the SiteConfig system description and communicating on the control network.
- The server on which you are installing software must have its credentials set in SiteConfig to allow access.

1. Verify the SiteConfig roles currently assigned to the server. If the roles are not correct for your system design, add or remove roles accordingly. Roles are as follows:

   - GV STRATUS Proxy Storage Server
   - GV Log Manager
   - StorNext File System Server
   - StorNext File System Client

2. Add the server to a deployment group, such as the GV STRATUS deployment group.

3. Add the following files to the deployment group:
   - *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
     - *GrassValley_STRATUS_HttpProxyServer_x.x.x.cab*
     - *GrassValley_LogManager_x.x.x.cab*
   - *GrassValley_STRATUSClient_x.x.x.cab*.
   - For K2 9.8.x systems; use *GrassValley_K2system_x.x.x.cab*, which contains the following cab files that apply to this device:
     - *GrassValleyK2Server_x64_9.8.x.x.cab*
     - *SNFS_x64_4.7.x.xxx.cab*
   - For K2 10.x systems; use *GrassValley_K2Plus_x.x.x.cab*, which contains the following cab files that apply to this device:
     - *GrassValleyK2Server_x64_10.x.x.cab*
     - *SNFS_x64_6.0.x.xxx.cab*

   Refer to release notes for version numbers.
4. Do the SiteConfig **Check Software** operation on the server.

   NOTE: If an "Unable to copy ... to target" error appears for a device that has the Grass Valley Embedded Security solution, apply the* Embedded Security *solution one-time initial deployment process to the device. After the one-time process is complete the error does not appear and it is no longer necessary to put* Embedded Security *in Update mode.
5. Verify that deployment tasks are set to **Install** for the files listed above.

   If a WFRegMon install task appears, install it as well. It is required to support Grass Valley software installers. There is no uninstall task.
6. Deploy software to the server.
7. Restart as prompted.

Next, use K2Config and set up the Proxy Storage system as a K2 SAN.

Related Topics

Adding a software role to a device on page 490
Configuring deployment groups on page 80
Check all currently installed software on GV STRATUS devices on page 278
Add software package to deployment group for GV STRATUS and other devices on page 111
Devices components: Roles, cab files, services, and licenses on page 444
GV STRATUS servers logon account on page 245

K2Config Proxy server set up

Only systems with proxy on the K2 SAN (A1) require this process.

If you received your system pre-configured from Grass Valley, your Proxy server is already set up on your K2 SAN, so you can skip these tasks. Otherwise, work through the tasks in this section sequentially to add a GV STRATUS server as a Proxy server to your online or production K2 SAN.

Related Topics

Synchronizing K2Config information to GV STRATUS Control Panel on page 523

K2 SAN prerequisites for adding devices

The following K2 SAN preparations are required to support adding a device to the SAN:

- All K2 Media Servers and/or K2 RAID storage devices must be installed and cabled.
- The control network must be operational with K2 devices communicating. At the command prompt, use the ping command to verify.
- The media network (non-redundant) or networks (redundant) must be operational. You can check this with the K2Config application.
- K2 RAID devices must have disks bound and be configured as required for operation on the K2 SAN.
- K2 Media Servers must be configured such that an operational media file system is present.
- K2 Ethernet switches must be configured and have V-LANs set up.
- The K2 Media Server with role of file system server must be licensed as appropriate for the design of your K2 SAN.

Verify license on K2 Media Server

The K2 SAN license is installed on K2 Media Servers with role of iSCSI bridge. If a redundant system and/or a large system with multiple servers, the license must be installed on each K2 Media Server with role of iSCSI bridge. Use the following steps to verify the license on each K2 Media Server with role of iSCSI bridge.

1. On the K2 Media Server, open SabreTooth License Manager.
2. Verify that a license identified as K2-ISCSI-SVR is installed.

If the license for your K2 SAN license is not installed, you must install it before proceeding.

Adding a GV STRATUS server to a SAN

You can add a GV STRATUS server to a SAN as follows:

1. If you have not already done so, in SiteConfig, add the server to the appropriate group and verify that it is communicating correctly on networks.
2. In the K2Config application tree view, select the name of the K2 SAN, which is the top node of the storage system tree.
3. Click **Add Device**. The Add Device dialog box opens.

4. Select **GV STRATUS Core Services Server**.

   This is the correct selection for the following GV STRATUS servers:

   - Proxy server (A1)
   - Proxy Storage file system server (B1, C1)

5. Click **OK**. The new server appears in the tree view.

Next, if the server is a redundant iSCSI client on a K2 SAN, install MPIO software. Then configure the server.

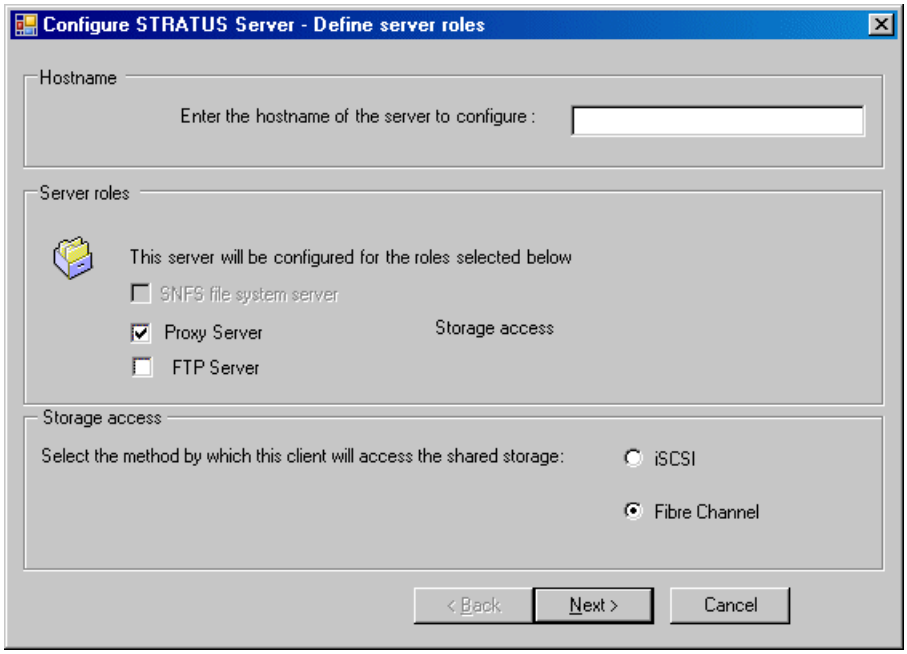
Configuring a GV STRATUS Proxy server

This section applies to a GV STRATUS server with role of Proxy server on an online or production K2 SAN (A1).

1. In the K2Config application tree view, select the GV STRATUS server you are configuring.
2. Click the **Configure** button.

The Configure K2 Server wizard opens to the Define server roles page.

Configure Define Server Roles page - GV STRATUS Proxy server



1. Enter the name of the server, as currently configured on the machine.

   SNFS file system server is not selected by default and disabled.

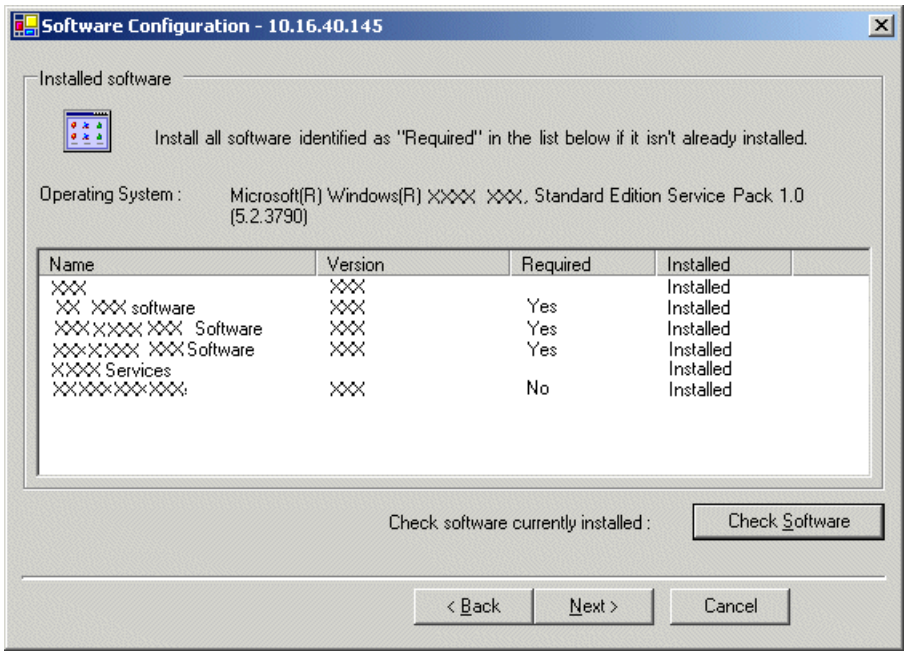
   For a Proxy server, select **Proxy storage server**.

   There is no Media Database Server in a Proxy Storage system.

2. Click **Next**.

The Software Configuration page opens.

Configure Software Configuration page

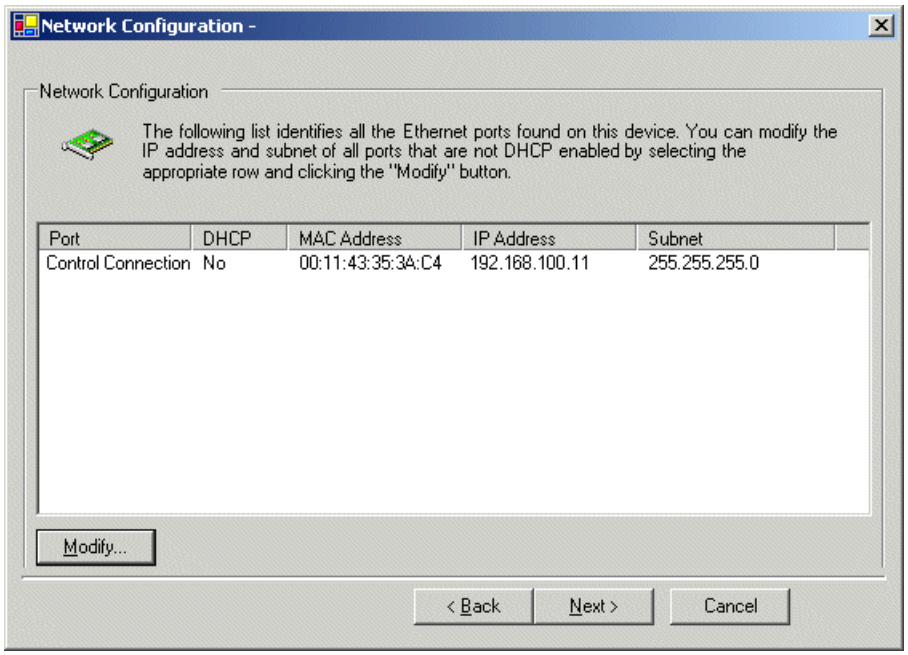


This page checks for the software required to support the roles you selected on the previous page.
NOTE: MPIO software is required on servers in redundant systems.

1. If software with **Yes** in the Required column reports as **Not Installed**, install the software.
2. Click **Check Software**.
3. When all required software reports as **Installed**, click **Next**.

The Network Configuration page opens.

Configure Network Configuration page - GV STRATUS server



This server has a control network connection only, so if it is configured correctly, there is no other configuration to do on this page.

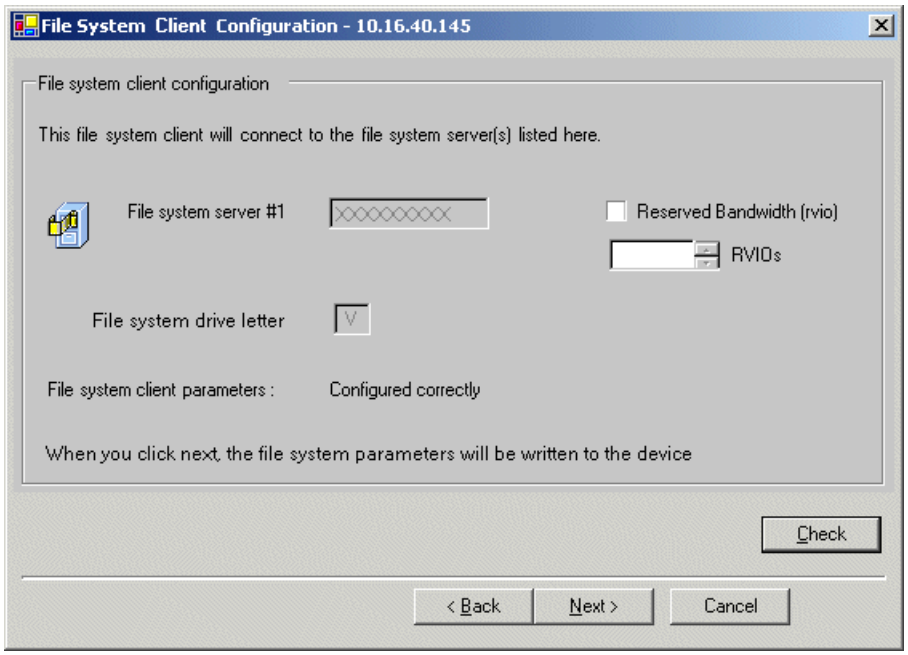
1. Verify that the top port is configured correctly.

   The top port is the port over which the K2Config application is communicating. If correctly configured, it is already assigned the control network IP address, as displayed on this page.

2. Click **Next**.

The File System Server Configuration page opens.

Configure File System Client Configuration page - GV STRATUS Proxy server



This system does not function as a file system server. It does function as a file system client, which is validated from this page.

1. Do not select **Reserved Bandwidth** unless instructed to do so by Grass Valley. This system is usually not configured for RVIO.
2. Click **Check**.
3. When the wizard reports that the configuration is correct, click **Next**.

   If you get a "The V: will not be available until this device is rebooted…" message, you can safely continue now and reboot later when instructed to do so.

GV STRATUS server configuration is complete.

Related Topics

Synchronizing K2Config information to GV STRATUS Control Panel on page 523

K2Config Proxy Storage set up

Only systems with proxy on a dedicated Proxy Storage system (B1, C1) require this process.

If you received your system pre-configured from Grass Valley, your Proxy Storage system is already set up, so you can skip these tasks. Otherwise, work through the tasks in this section sequentially to configure a non-redundant Proxy Storage system. This corresponds to a Tier 3 K2 SAN.

Related Topics

Synchronizing K2Config information to GV STRATUS Control Panel on page 523

Prerequisites for initial configuration - Basic Proxy Storage

Before beginning your initial configuration, make sure the devices of the Proxy Storage system meet the following prerequisites.

Control point PC

- Ethernet cable connected
- Control Point software must be installed
- Control network IP address must be assigned
- There must be network communication over the control network with all other K2 devices
- Power must be on

Ethernet switch

- Ethernet cables connected
- Control network IP address must be assigned
- VLANs must be set up
- Trunks must be set up
- Power must be on

Core Services server

- Ethernet cables connected
- Fibre Channel cable must be connected
- Softwaremust be installed, as from the factory, including QuickTime 7
- Control network IP address must be assigned
- Power must be on for all servers

K2 RAID chassis

- Fibre Channel cable(s) must be connected
- Ethernet cable(s) must be connected
- Power must be on

K2 RAID Expansion chassis (optional)

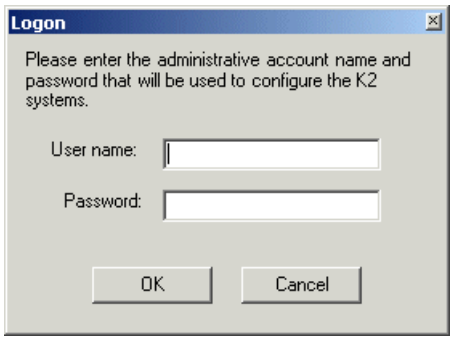
- Fibre channel cable(s) must be connected
- Power must be on

Defining a new Proxy Storage system

If you import a SiteConfig system description file in which the Proxy Storage system is defined, you do not need to define a new Proxy Storage system. You can skip this task and instead start by configuring the Proxy Storage file system server.

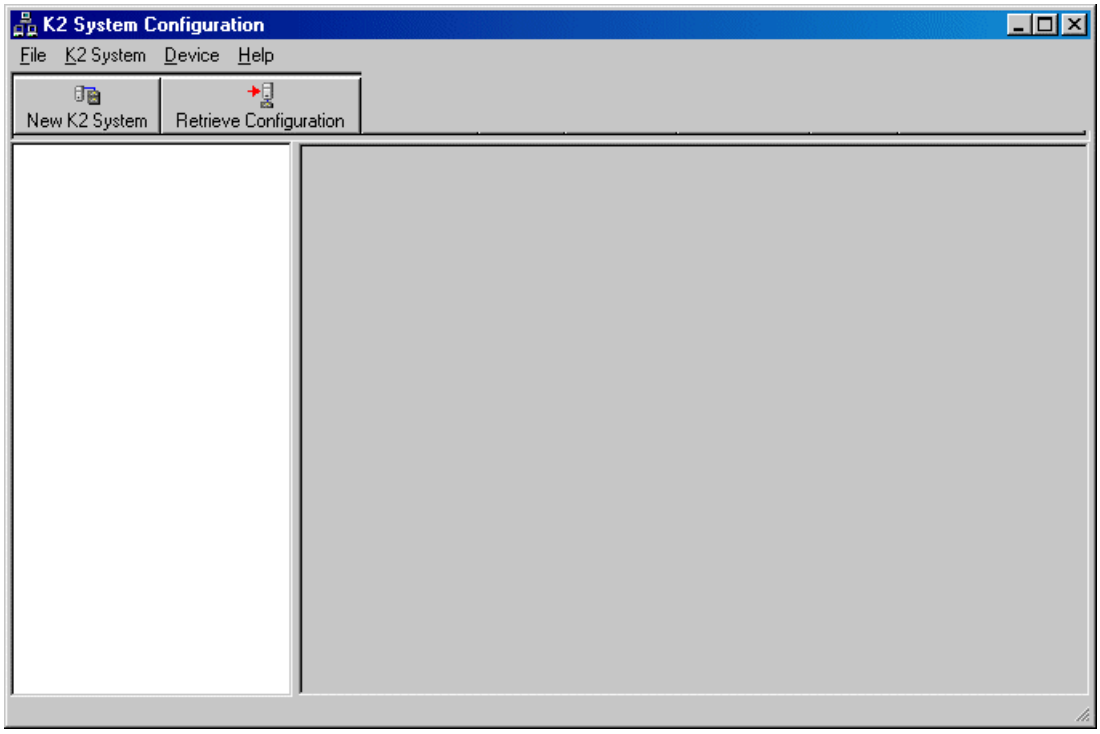
1. On the control point PC, open the K2Config application.

   A log on dialog box opens.



2. Log on to the K2Config application with the Windows administrator account.

   The K2Config application opens.



3. Click **New K2 System**.

The New K2 System wizard opens to page 1.

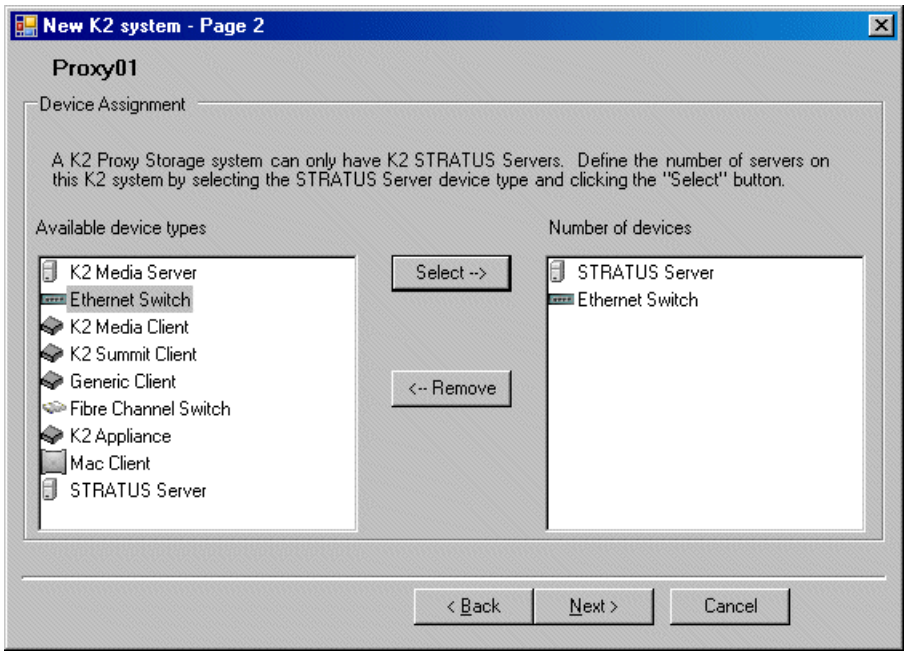
Configure New K2 System page 1 - Proxy Storage system

1. Create a name for your system and type it in the Name box.
2. Select **Proxy Storage**.

   The Server redundancy option is not selected and is disabled. This option applies to media database redundancy. Since the Proxy Storage system has no media database, this setting is correct for both redundant and non-redundant Proxy Storage systems.
3. Click **Next**.

Page 2 opens.

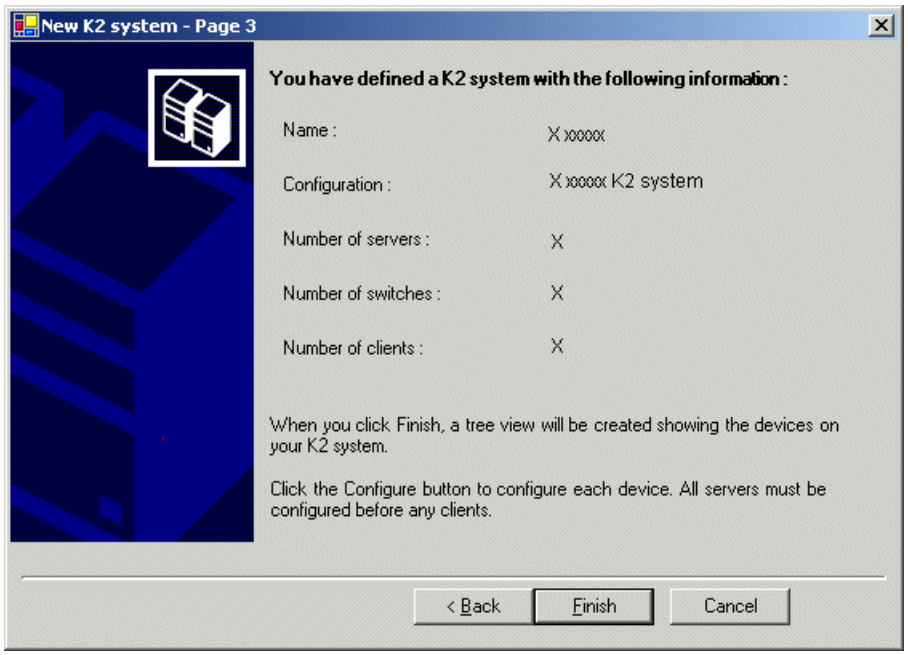
Configure New K2 System page 2 - Proxy Storage system



1. Move the following into the Number of devices box:
   - One STRATUS server
   - One Ethernet switch
2. Click **Next**.

Page 3 opens.

Configure New K2 System page 3 - Proxy Storage system



1. Review the information on this page and verify that you have correctly defined your SAN.
   For a Proxy Storage system you should have the following:
   - One Gigabit Ethernet switch
   - One GV STRATUS server
2. Click **Finish**.
   The Define New K2 Storage System wizard closes.

Your storage system appears in the tree view of the K2Config application.

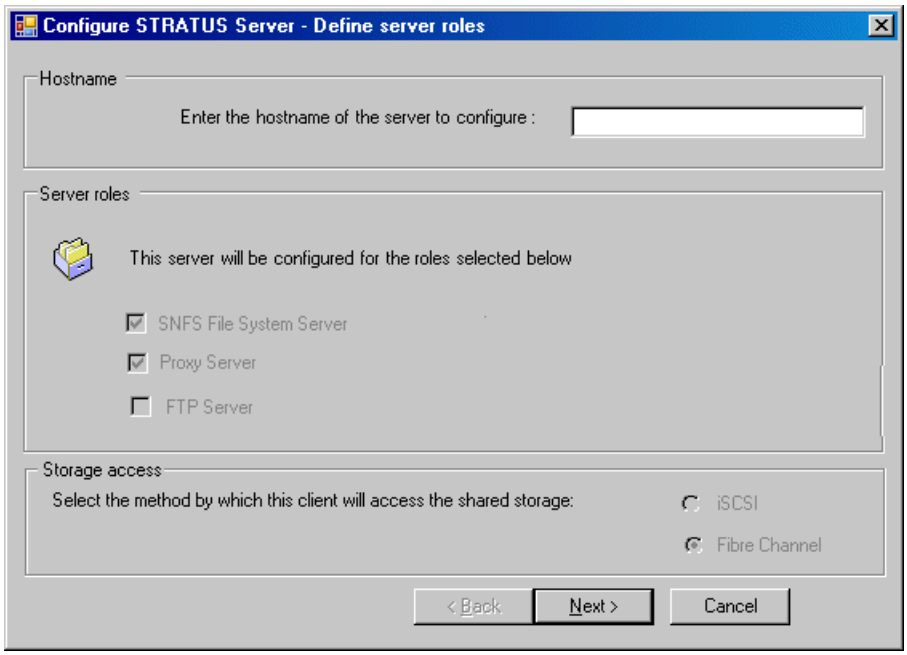
Next, configure the server.

Configuring GV STRATUS Proxy Storage file system server - Part 1

1. In the K2Config application tree view, select **[STRATUS Server1]**.
   For Proxy Storage, this is the only server.
2. Click the **Configure** button.

The Configure K2 Server wizard opens to the Define server roles page.

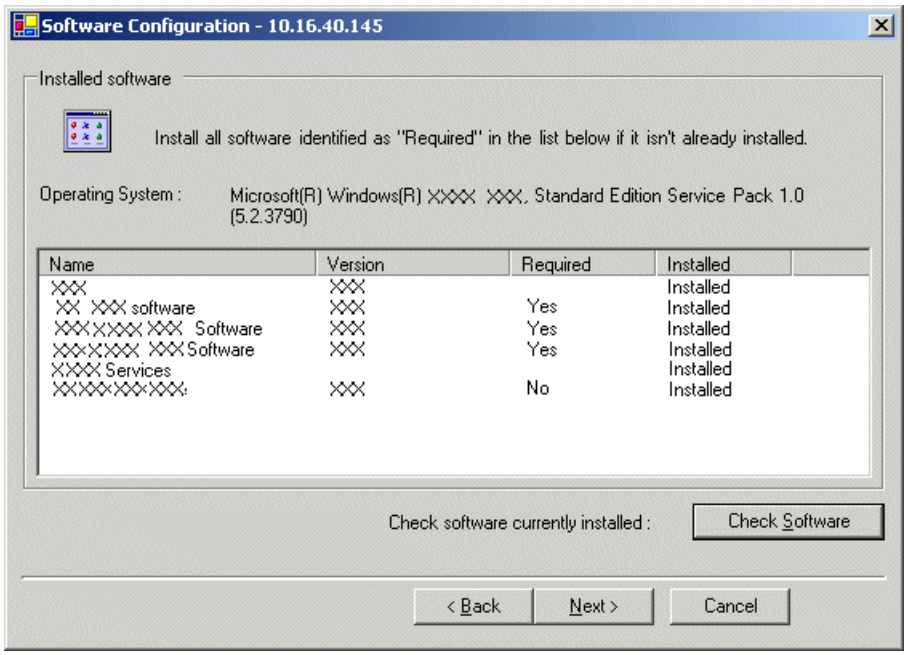
Configure Define Server Roles page - GV STRATUS Proxy Storage file system server



1. Enter the name of the server, as currently configured on the machine.
   SNFS file system server is selected by default and disabled.
   For a Proxy Storage file system server, select **Proxy storage server**.
   There is no Media Database Server in a Proxy Storage system.
2. Click **Next**.

The Software Configuration page opens.

Configure Software Configuration page

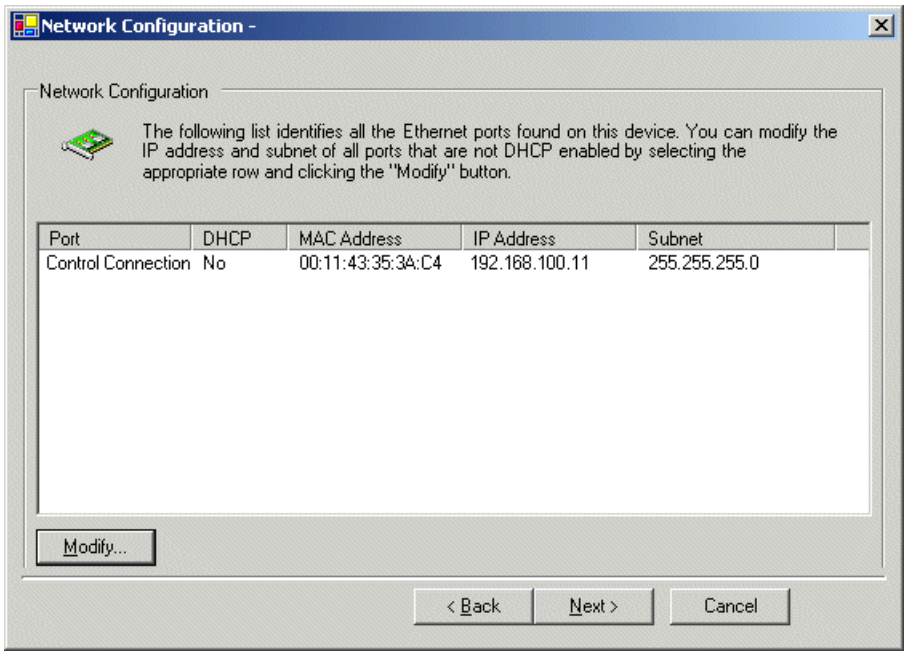


This page checks for the software required to support the roles you selected on the previous page.
NOTE: MPIO software is required on servers in redundant systems.

1. If software with **Yes** in the Required column reports as **Not Installed**, install the software.
2. Click **Check Software**.
3. When all required software reports as **Installed**, click **Next**.

The Network Configuration page opens.

Configure Network Configuration page - GV STRATUS server



This server has a control network connection only, so if it is configured correctly, there is no other configuration to do on this page.

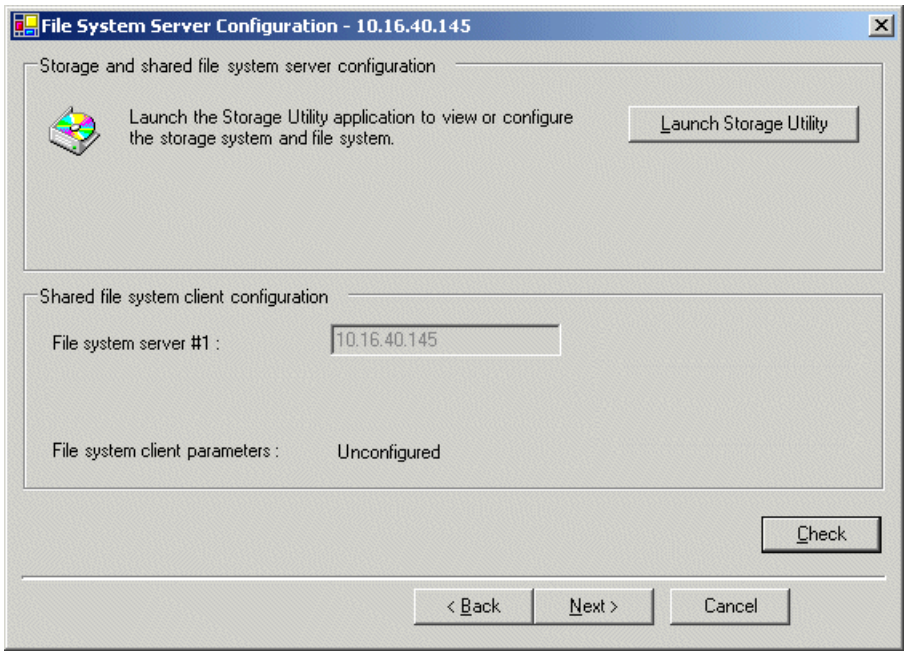
1. Verify that the top port is configured correctly.

   The top port is the port over which the K2Config application is communicating. If correctly configured, it is already assigned the control network IP address, as displayed on this page.

2. Click **Next**.

The File System Server Configuration page opens.

Configure File System Server Configuration page - GV STRATUS Proxy Storage file system server



This page checks on the file system server role. The server also functions as a file system client, which is also checked from this page.

1. Click **Launch Storage Manager**.

   Storage Utility opens.

2. Leave the Configure K2 Server wizard open while you use Storage Utility.

   When you are done with Storage Utility, you continue with the wizard.

Next, use Storage Utility to configure the RAID storage and file system.

Configuring RAID

Use Storage Utility to complete the configuration of the K2 RAID storage devices, as explained in the following topics.

Configuring RAID network and SNMP settings - Basic

- Fibre Channel cable(s) must be connected
- Ethernet cable(s) must be connected
- Power must be on

- Fibre channel cable(s) must be connected
- Power must be on

Use the Storage Utility to configure the following settings for the K2 RAID controller:

- IP address
- Subnet mask
- Gateway Address

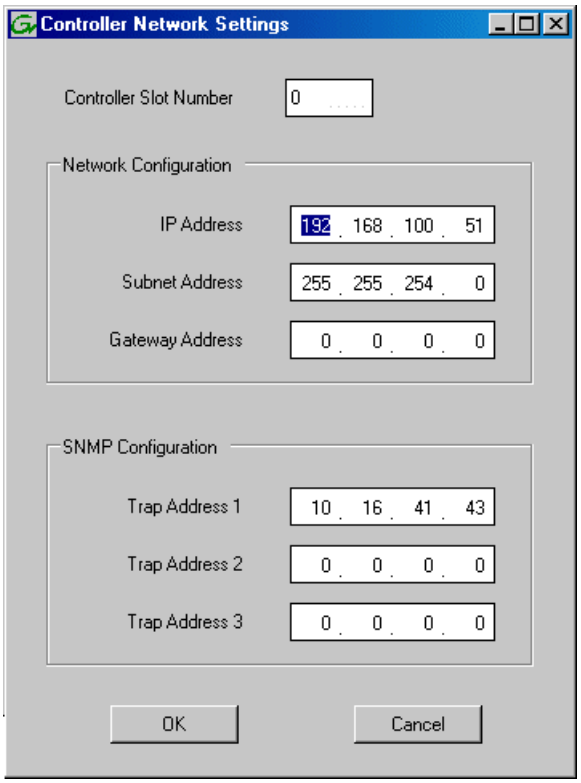
- SNMP trap destinations

For K2 RAID, network and SNMP settings are set and stored on the RAID controller module, so the combined RAID storage devices, including the optional Expansion chassis, exist as a single entity on the control network.

The RAID storage device is configured by default for the SNMP community name “public”. If your site’s policies require using a different SNMP community name, contact your Grass Valley representative.

1. Launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.
3. In Storage Utility tree view, expand the node for the K2 RAID, right-click the icon for a RAID controller, and select **Configuration | Network Properties**.

   The Controller Network Settings dialog box opens.



4. In the Controller Slot Number field enter **0** and then press **Enter**.

   The settings from controller 0 are loaded into the Controller Network Settings dialog box and are available for you to modify.

5. Enter the control network IP address and other network settings.

6. For SNMP Configuration, enter the IP address of the SNMP manager PC.

   You can also enter IP addresses for other SNMP managers to which you want to send SNMP trap messages.

   Refer to related topics about Grass Valley recommended deployment and monitoring solutions in the "Release Notes" section of the K2 Topic Library.

7. Click **OK** to save settings and close.
8. In Storage Utility click **View | Refresh**.

Next, bind disk modules.

Binding disk modules - Proxy Storage

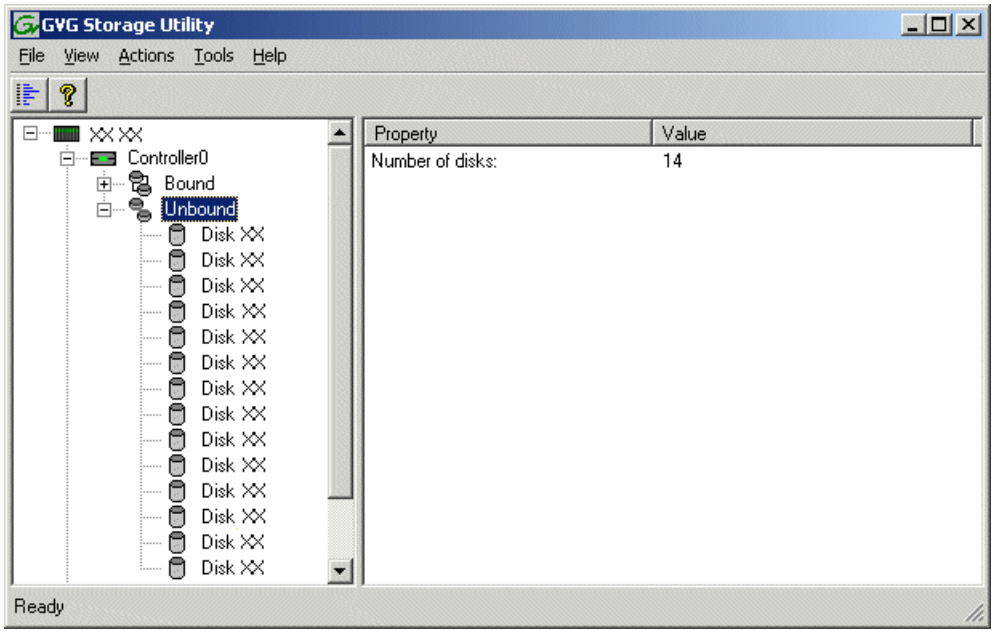
- Fibre Channel cable(s) must be connected
- Ethernet cable(s) must be connected
- Power must be on

- Fibre channel cable(s) must be connected
- Power must be on

NOTE: Binding destroys all user data on the disks.

1. If you have not already done so, launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.

3. In the Storage Utility main window, identify bound RANKs and unbound disks by their placement in the hierarchy of the tree view. In the following illustration, disk numbers are represented by "XX".



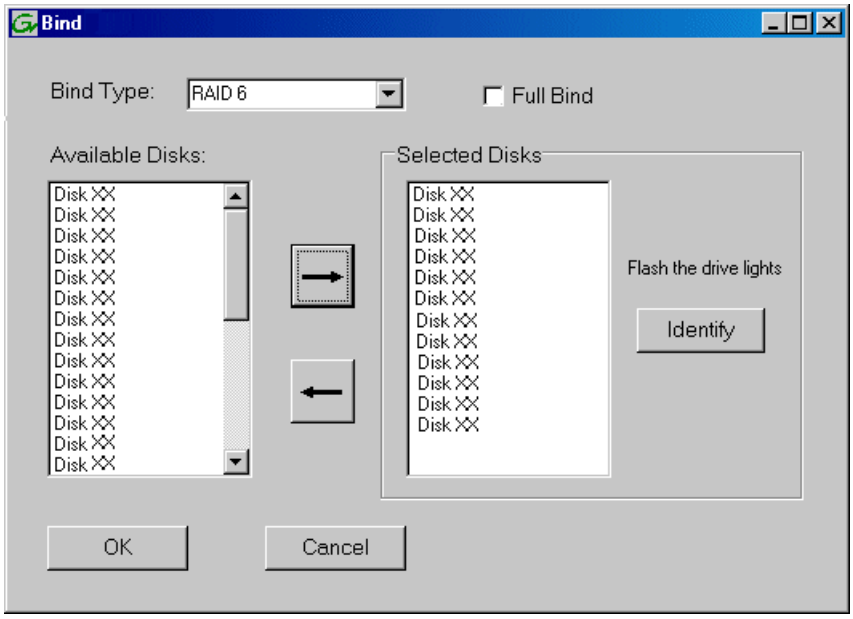
Proxy systems store media files across both the primary RAID chassis and the optional Expansion chassis. In addition, file system metadata files and journal files are mixed in with the media files.

The RAID configuration is the same on all chassis. Each chassis contains disks, which are bound as RAID 6 in a RANK of twelve disks. One twelve disk RANK fills one chassis.

4. Right-click the **Unbound** node for a controller, then select **Bind** in the context menu.

   If the RAID chassis has two controllers, both controllers are represented by the single “Controller” node.

   The Bind dialog box opens showing all unbound disks for the controller listed in the Available Disk list.



5. Leave **Full Bind** unchecked.
6. In the **Bind Type** drop down box, select **RAID 6**.
7. In the Available Disks box, select twelve contiguous disks at the top of the list.

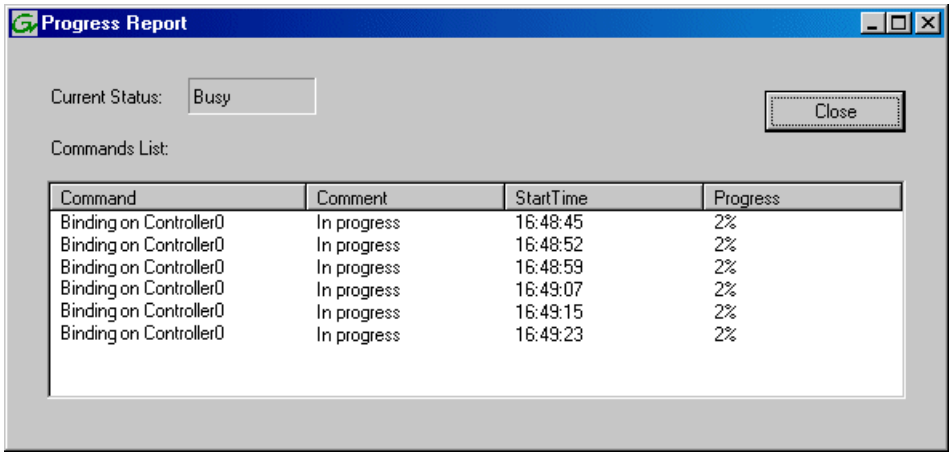
   Use ‘shift-click’ or ‘control-click’ to select disks.

8. Click the add (arrow) button to add disks to the Selected Disks list.

   NOTE: As an aid in identifying a disk module’s physical location, select it in the Selected Disks list, then click Identify Disks. This causes the disk drive light to flash.

9. Click **OK** to close the Bind dialog box and begin the binding process.

   The Progress Report dialog box opens, showing the status of the binding process.



10. Close the Progress Report and repeat these steps for other unbound disks.

    If specified by your system design, you can bind some disks as Hot Spares.

    When you are done, if you did not bind any extra Hot Spares, you should have the following results:

    The disks in the primary RAID chassis and in optional Expansion chassis should be bound as RAID 6 RANKs, with twelve disks to a RANK.

11. Click **Close** in Progress Report window.
12. Restart the GV STRATUS server.

    NOTE: Make sure start up processes on the server are complete before proceeding.

Next, create a new file system.

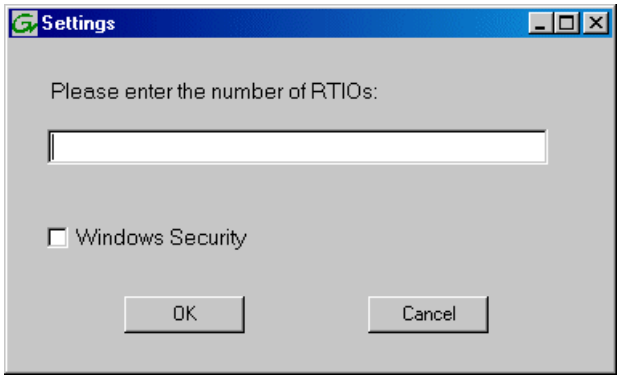
Creating a new file system - Proxy Storage

- Fibre Channel cable(s) must be connected
- Ethernet cable(s) must be connected
- Power must be on
- Disks must be bound

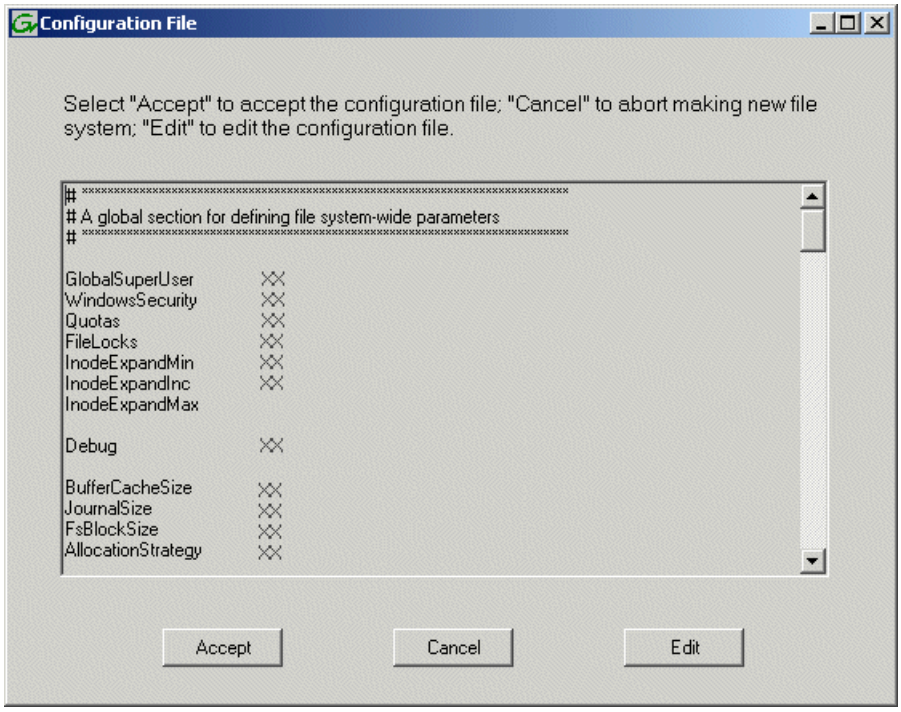
- Fibre channel cable(s) must be connected
- Power must be on
- Disks must be bound

1. If you have not already done so, launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.

3. In Storage Utility, click **Tools | Make New File System**.
   The Setting dialog box opens.



4. For a Proxy Storage system, enter zero as the Real Time Input/Output (RTIO) rate.
5. Leave Windows Security unchecked.
6. Click **OK**.
   The Configuration File dialog box opens.



   The configuration file for the media file system is displayed.

7. Verify media file system parameters.
   Do not edit the configuration file for the media file system.

8. Click **Accept**.

   A "…Please wait…" message box displays progress and a "…succeeded…" message confirms the process is complete.

   A message informs you that you must restart the server, however the restart at the end of the Configure K2 Server wizard suffices, so you do not need to restart now.

9. Close the Storage Utility.

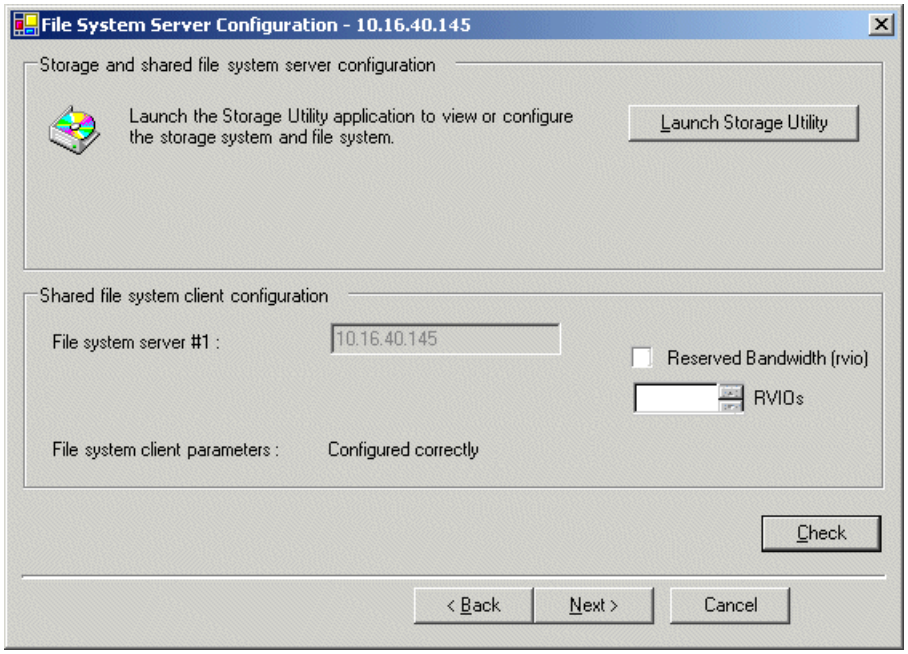
   NOTE: Do not attempt to start SAN-attached systems or otherwise bring the SAN online until instructed to do so by the documented procedure.

Next, continue with configuring the server using the K2Config application.

Configuring GV STRATUS Proxy Storage file system server - Part 2

Configure File System Server Configuration page - GV STRATUS Proxy Storage file system server

- Network and SNMP must be settings configured
- Disks must be bound
- A new file system must be made



This page checks on the file system server role. The server also functions as a file system client, which is also checked from this page.

1. In K2Config open the server's File System Server Configuration page, if the page is not already open.
2. Do not select **Reserved Bandwidth** unless instructed to do so by Grass Valley. This system is usually not configured for RVIO.
3. Click **Check**.

4. When the wizard reports that the configuration is correct, click **Next**.

   If you get a "The V: will not be available until this device is rebooted…" message, you can safely continue now and reboot later when instructed to do so.

GV STRATUS server configuration is complete.

Related Topics

Synchronizing K2Config information to GV STRATUS Control Panel on page 523

Render Engine Server set up process

Only systems with a Render Engine Server require this process. On the GV STRATUS Core server, use SabreTooth and install the STRATUS-CONFORM license. Use SiteConfig for network setup and software install. Then use K2Config for SAN setup.

If you received your Render Engine already set up from Grass Valley, skip set up tasks and do the test task only.

1. *SiteConfig Render Engine Server network set up* on page 768. Only systems with a Render Engine require this process.
2. *SiteConfig Render Engine Server software install* on page 770. Only systems with an Render Engine require this process.
3. *SabreTooth Render Engine server license process* on page 559. Only systems with an Render Engine require this process. The process is on the GV STRATUS server with role of Common Services.
4. *K2Config Render Engine Server setup* on page 775. Only GV STRATUS systems with a Render Engine server require this process.
5. *Configure Render Engine Server* on page 784. Only systems with an Render Engine require this process.

Related Topics

CIFS storage configuration

SiteConfig Render Engine Server network set up

Only systems with a Render Engine require this process.

If you received your system already set up from Grass Valley, your Render Engine or Servers are already included in the SiteConfig system description and set up on the network, so you can skip these tasks. Otherwise, work through the topics in this section.

Adding a Render Engine Server to the SiteConfig system description

- Render Engines must be racked, cabled, and powered on.

- The system description must contain a group.

This topic applies to an Render Engine server.

1. In the **Network Configuration | Devices** tree view, right-click a group and select **Add Device**.
2. Configure settings for the device you are adding as follows:
   - Family: GV STRATUS
   - Device Type: GV STRATUS Server
   - Model: GV STRATUS Render Engine
   - Name – This is the device name, as displayed in the SiteConfig device tree view and device list view. This name can be different than the host name (network name). You can accept the default name or enter a name of your choice. Devices in the tree view are sorted alphabetically.
   - Amount — Select the number of Render Engines, according to your system design.
   - Platform — Select **x64**.
   - Control network– Select the control network.
   - Starting Address – Select from the list of available addresses on the selected control network. If adding multiple devices, this is the starting address, with addresses assigned sequentially to each device added.
3. Click **OK** to save settings and close.

   SiteConfig adds the Render Engine to the system description as a placeholder device.
4. Verify that unmanaged control network interface is configured correctly and modify if necessary.

Next, add the GV STRATUS server to the control network.

Adding a GV STRATUS server to the control network with SiteConfig

Use SiteConfig to configure network settings on a separate GV STRATUS server.

Before doing this task, make sure the GV STRATUS server is added as a placeholder device to the SiteConfig system description.

The following steps are the standard tasks for adding a device to the control network using SiteConfig. Use these steps for the GV STRATUS server you are adding.

1. Discover the device using SiteConfig device discovery.
2. Assign the discovered device to the placeholder device in the SiteConfig system description.
3. Modify the control network interface to ensure communication on the control network.
4. Modify the host name and/or device name as desired.
5. Ping the device to verify network communication.
6. Verify credentials to ensure SiteConfig can install software on the device.
7. Generate and/or add to host tables as appropriate for your network.

Related Topics

Adding a device to a network with SiteConfig on page 490
Adding a device to a network with SiteConfig on page 490

SiteConfig Render Engine Server software install

Only systems with an Render Engine require this process.

If you received your system pre-configured from Grass Valley, software is already installed, so you can skip these tasks. Otherwise, work through the tasks in this section as follows:

- If your GV STRATUS system has one or more GV STRATUS servers that are Render Engines, install software on those servers.

Setting deployment options

- A software package must be assigned to the deployment group and applicable deployment tasks must be displayed in the Tasks area.

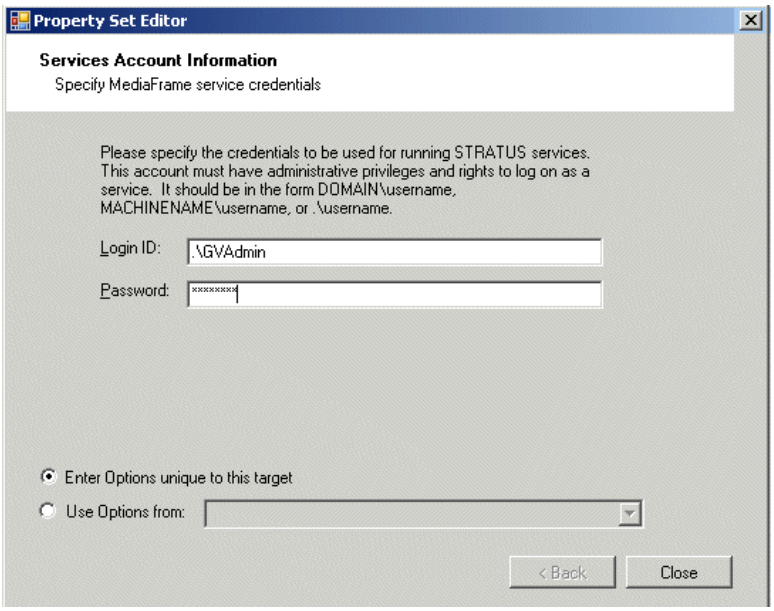
1. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.
2. In the Tasks list view, view tasks and determine if you must set deployment options.

   Tasks that need to have deployment options set display in the Details column a message stating "Deployment options required."

   If you select a task that needs to have its deployment options set, the Start Deployment button is disabled and the message is displayed next to the button.
3. Do one of the following to set deployment options:
   - Double-click the task.
   - Select the task and click the **Options** button.

   A wizard opens.

4. Work through wizards and set deployment options for GV STRATUS software as follows:

Software	Deployment options
GrassValley_STRATUS_CommonServices GrassValley_STRATUS_ControlPanelService GrassValley_STRATUS_CoreServices GrassValley_STRATUS_CRArchive_MDI GrassValley_STRATUS_Databases GrassValley_STRATUS_DataMover GrassValley_STRATUS_DIVA_MDI GrassValley_STRATUS_ExternalMedia GrassValley_STRATUS_FlashNet_MDI GrassValley_STRATUS_GFTP_MDI GrassValley_STRATUS_HttpProxyServer GrassValley_STRATUS_IngestServices GrassValley_STRATUS_Masstech_MDI GrassValley_STRATUS_MediaFlow GrassValley_STRATUS_MEWS GrassValley_STRATUS_Proxy_MDI GrassValley_STRATUS_ProxyStreamingService GrassValley_STRATUS_RenderEngine GrassValley_STRATUS_Rules GrassValley_STRATUS_ScheduledTransferEngine GrassValley_STRATUS_SocialMedia GrassValley_STRATUS_Summit_MDI GrassValley_STRATUS_TrafficGateway GrassValley_STRATUS_Transcode GrassValley_STRATUS_WebApps GrassValley_STRATUS_WebClient GrassValley_DeviceKeyService GrassValley_LogManager GrassValley_LogViewer	 Use the local system account if your system is on a workgroup or if it's on a domain but uses the local system account in SQL. Use a domain\admin account if the account was previously mapped in SQL to the MediaFrame, MediaFlow, RulesEngine and WFPersistence databases. Entering account credentials allows you to use the **Use options from** feature for all other devices of the same type. Once you enter the account credentials this way on the first device, it becomes the template from which options for other devices are copied.

5. If you have multiple devices of the same type, you can enter deployment options for one of them using the wizard. Then, when you bring up the same wizard on every device, you can choose the **Use options from** radio button and select the first device for which you set options.

   SiteConfig copies the options you set for the first device and fills in the blanks on the wizard.

Installing software on a Render Engine Server

Only systems with one or more GV STRATUS servers that are Render Engines require this process. Use SiteConfig to install software on the server.

- The server on which you are installing software must be in the SiteConfig system description and communicating on the control network.
- The server on which you are installing software must have its credentials set in SiteConfig to allow access.
- Windows High Priority updates are required and must be installed. For more details, refer to *Install Important Windows updates for EDIUS* on page 148.
- QuickTime must be installed on the server to which you are installing the GV STRATUS Render Engine software.

1. Verify the SiteConfig roles currently assigned to the server. If the roles are not correct for your system design, add or remove roles accordingly. Roles are as follows:
   - GV STRATUS Control Panel
   - GV Log Manager
   - StorNext File System Client
   - GV Embedded Security Manager
   - GV STRATUS Render Engine
2. Add the server to a deployment group.

3. Add the following files to the deployment group:

   - *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
     - *GrassValley_STRATUS_RenderEngine_x.x.x.cab*
     - *GVEmbeddedSecurityManager_x.x.x.cab*
     - *GrassValley_Sabretooth_Application_x.x.x.cab*
     - *GrassValley_LogManager_x.x.x.cab*
   - For K2 9.8.x systems; use *GrassValley_K2system_x.x.x.cab*, which contains the following cab files that apply to this device:
     - *GrassValleyK2Server_x64_9.8.x.x.cab*
     - *SNFS_x64_4.7.x.xxx.cab*
   - For K2 10.x systems; use *GrassValley_K2Plus_x.x.x.cab*, which contains the following cab files that apply to this device:
     - *GrassValleyK2Server_x64_10.x.x.cab*
     - *SNFS_x64_6.0.x.xxx.cab*
   - *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:
     - *GrassValley_STRATUS_Application_x.x.x.cab*
     - *GrassValley_STRATUS_ControlPanel_x.x.x.cab*

   Refer to release notes for version numbers.

4. Do the SiteConfig **Check Software** operation on the server.

   NOTE: If an "Unable to copy ... to target" error appears for a device that has the Grass Valley Embedded Security solution, apply the* Embedded Security *solution one-time initial deployment process to the device. After the one-time process is complete the error does not appear and it is no longer necessary to put* Embedded Security *in Update mode.

5. Set deployment tasks to **Install** for all the files listed above except when installing Render Engine software, do not install the Render Engine cab file yet.

   If a WFRegMon install task appears, install it as well. It is required to support Grass Valley software installers. There is no uninstall task.

6. Deploy software that is not Render Engine software to the server.
7. Restart as prompted.
8. When installing Render Engine software, do the following:
   a) Set deployment tasks to **Install** for the Render Engine cab file.
   b) Deploy Render Engine software to the server.

      NOTE: Expect long deployment times when installing Render Engine software. It can take several minutes to install. Allow the installation to complete. Do not attempt to stop the installation.

9. Restart as prompted.

Related Topics

GV STRATUS servers logon account on page 245

Configure GVAdmin account

This task applies to a computer on which the following software is installed:

- GV STRATUS/EDIUS client PC
- EDIUS XRE Server
- Render Engine Server

Verify the following before doing this task:

- EDIUS or Render Engine software must be installed on the computer.

  Add the internal system account, which by default is GVAdmin, to the Administrators group on the computer.

Related Topics

GV STRATUS servers logon account on page 245

SabreTooth Render Engine server license process

Only systems with an Render Engine require this process. The process is on the GV STRATUS server with role of Common Services.

The Render Engine license is installed on the GV STRATUS server with role of Common Services. Typically the GV STRATUS Core server has the role of Common Services. Each license below is a SabreTooth floating license.

STRATUS-CONFORM: This is the current license for the GV STRATUS Render Engine. One STRATUS-CONFORM license is required for each GV STRATUS server running Render Engine software in your GV STRATUS system. Each Render Engine server runs Render Engine software as the Conform Server and Proxy Encoder, so each server requires a license.

STRATUS-GVRE: This is the new license for the GV STRATUS Render Engine. One STRATUS-GVRE license is required for each GV STRATUS server running Render Engine software in your GV STRATUS system as the Conform Server and Proxy Encoder. Only one license is checked out by GV STRATUS Render Engine for conform and proxy functionality, therefore you must either have the **STRATUS-CONFORM** or the **STRATUS-GVRE** license in your GV STRATUS server.

STRATUS-TRANSCODE: This is the new license for the GV STRATUS Render Engine. One STRATUS-TRANSCODE license is required for each GV STRATUS server running Render Engine software in your GV STRATUS system as the Generic Transcoder. This license only enables Transcode jobs, with the maximum number of 10 jobs per server.

The type of license to be installed is determined by the usage of Render Engine in your system by setting the number of maximum concurrent job per functionality for the Render Engine on the Engines tab of GV STRATUS Control Panel.

If you received your system pre-configured from Grass Valley, licenses are already installed, so you can skip these tasks. Otherwise, do the following:

1. Refer to the license sheet that you received with your GV STRATUS license. The license sheet has the Sales Order number that you need.
2. On the GV STRATUS server with role of Common Services, run the SabreTooth License Manager, generate a unique ID, and send the email to Grass Valley requesting your license or licenses.

   Refer to this Topic Library for detailed licensing procedures.
3. When you receive your license file, use SabreTooth License Manager and install it on the server.

K2Config Render Engine Server setup

Only GV STRATUS systems with a Render Engine server require this process.

If you received your system pre-configured from Grass Valley, your server is already set up on the K2 SAN, so you can skip these tasks. Otherwise, work through the topics in this section sequentially to add a server to your online or production K2 SAN.

K2 SAN prerequisites for adding devices

The following K2 SAN preparations are required to support adding a device to the SAN:

- All K2 Media Servers and/or K2 RAID storage devices must be installed and cabled.
- The control network must be operational with K2 devices communicating. At the command prompt, use the ping command to verify.
- The media network (non-redundant) or networks (redundant) must be operational. You can check this with the K2Config application.
- K2 RAID devices must have disks bound and be configured as required for operation on the K2 SAN.
- K2 Media Servers must be configured such that an operational media file system is present.
- K2 Ethernet switches must be configured and have V-LANs set up.
- The K2 Media Server with role of file system server must be licensed as appropriate for the design of your K2 SAN.

Verify license on K2 Media Server

The K2 SAN license is installed on K2 Media Servers with role of iSCSI bridge. If a redundant system and/or a large system with multiple servers, the license must be installed on each K2 Media Server with role of iSCSI bridge. Use the following steps to verify the license on each K2 Media Server with role of iSCSI bridge.

1. On the K2 Media Server, open SabreTooth License Manager.
2. Verify that a license identified as K2-ISCSI-SVR is installed.

If the license for your K2 SAN license is not installed, you must install it before proceeding.

Adding an Render Engine Server to a SAN

Before doing this task, verify the following:

- On the Render Engine, in Windows Services Control Panel, **Microsoft iSCSI Initiator Service** must be started and set to startup type Automatic.
- If adding the Render Engine to a redundant K2 SAN, MPIO software must be installed on the Render Engine.

1. If you have not already done so, in SiteConfig, add the server to the appropriate group and verify that it is communicating correctly on networks.
2. In the K2Config application tree view, select the name of the K2 SAN, which is the top node of the storage system tree.
3. Click **Add Device**. The Add Device dialog box opens.
4. Select **GV STRATUS Core Services Server**.

   This is the correct selection for the any of the following types of GV STRATUS servers:

   - Render Engine

5. Click **OK**. The new server appears in the tree view.

Next, if the server is a redundant iSCSI client on a K2 SAN, install MPIO software. Then configure the server.

Installing Multi-Path I/O Software

This task applies only to 64-bit systems.

The following procedure is required for devices that are clients to a K2 SAN clients that have their Gigabit Media ports connected to the two iSCSI Media networks. This configuration is used for redundant K2 SANs.

The files for the Multi-Path I/O software are copied on to the system when the K2 software is installed.

1. Access the Windows desktop on the computer on which you are installing MPIO.

   You can do this locally with a connected keyboard, mouse, and monitor or remotely via the Windows Remote Desktop Connection.

2. Stop all media access. If AppCenter is open, close it.
3. Click **Start | Run**, type `cmd` and press **Enter**.

   The MS-DOS command prompt window opens.

4. From the command prompt, navigate to the *`C:\profile\mpio`* directory.
5. Type the following at the command prompt:

   ```
   gdsminstall64.exe -i
   ```

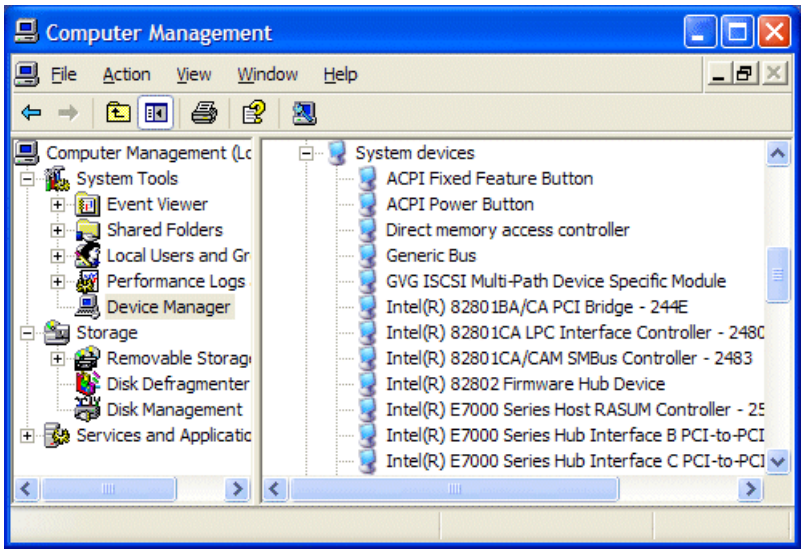
6. Press **Enter**.

   The software is installed. The command prompt window reports progress.

7. Restart the computer on which you installed MPIO.

8. After restart, to verify that the software is installed, on the Windows desktop right-click **My Computer** and select **Manage**.

   The Computer Management window opens.



9. In the left pane select **Device Manager**.
10. In the right pane open the **System devices** node and verify that **GVG ISCSI Multi-Path Device Specific Module** is listed.

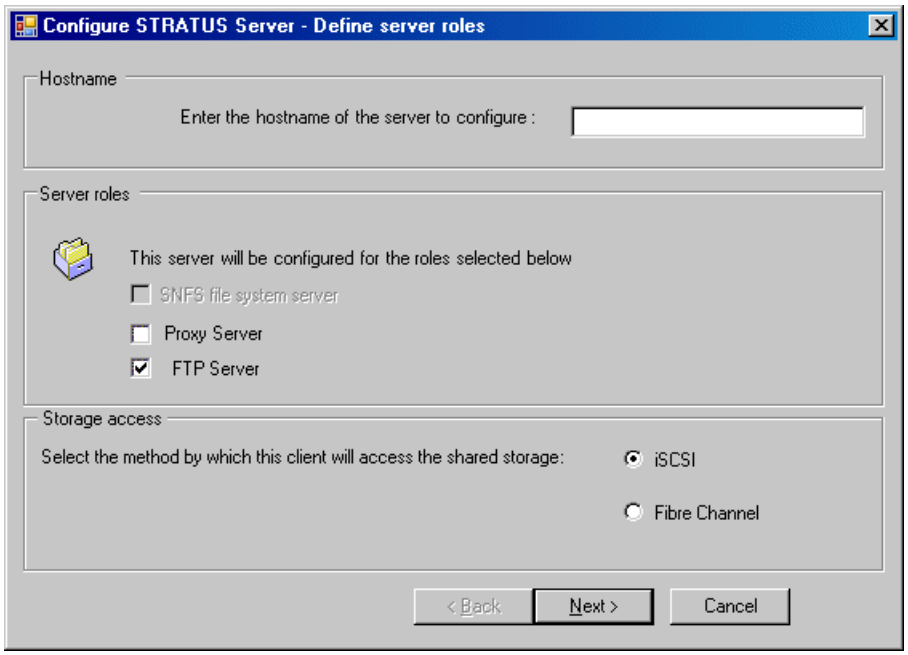
Configuring a GV STRATUS server on a K2 SAN

This section applies to a GV STRATUS server on an online or production K2 SAN.

1. In the K2Config application tree view, select the GV STRATUS server you are configuring.
2. Click the **Configure** button.

The Configure K2 Server wizard opens to the Define server roles page.

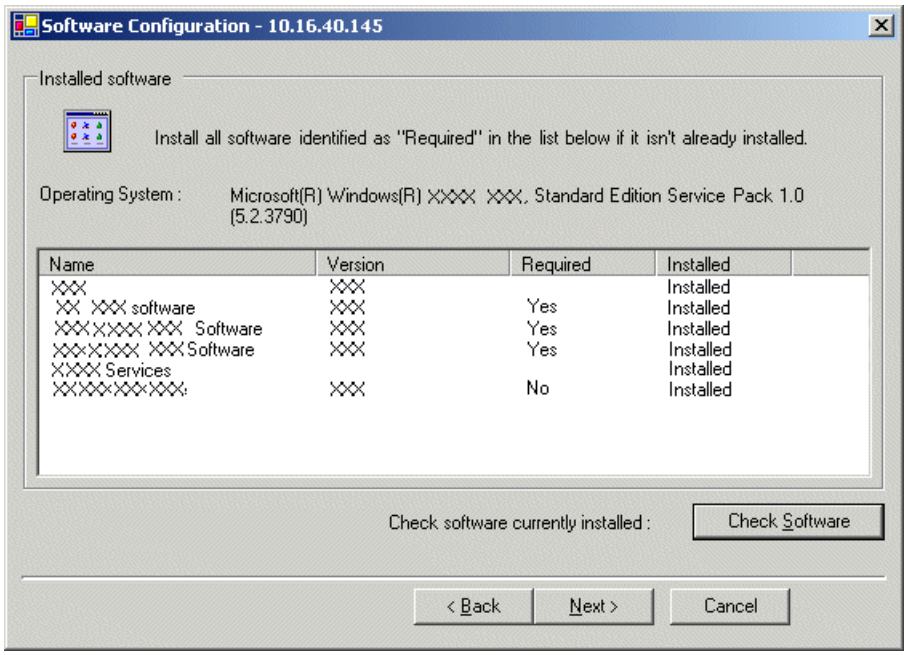
Configure Define Server Roles page



1. Enter the name of the server, as currently configured on the machine.
   SNFS file system server is not selected by default and disabled.
   For a Render Engine, select **FTP Server**.
2. Click **Next**.

The Software Configuration page opens.

Configure Software Configuration page

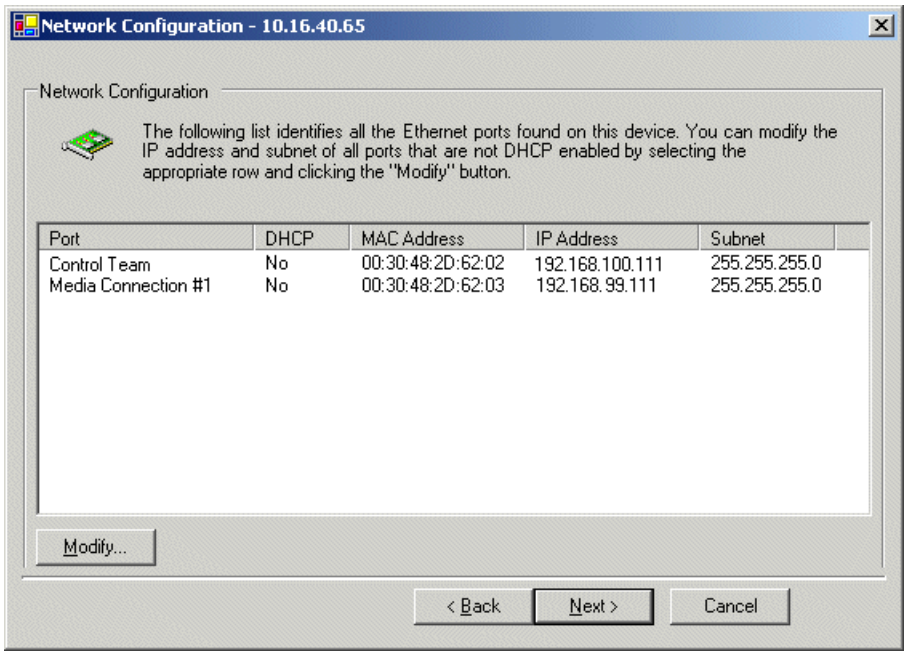


This page checks for the software required to support the roles you selected on the previous page.
NOTE: MPIO software is required on servers in redundant systems.

1. If software with **Yes** in the Required column reports as **Not Installed**, install the software.
2. Click **Check Software**.
3. When all required software reports as **Installed**, click **Next**.

The Network Configuration page opens.

Configure Network Configuration page



This page configures both control and media (iSCSI) network connections.

1. Verify that the top port is configured correctly.

   The top port is the port over which the K2Config application is communicating. If correctly configured, it is already assigned the control network IP address, as displayed on this page.

2. Select **Media Connection #1** and then click **Modify**.

   A network configuration dialog box opens.

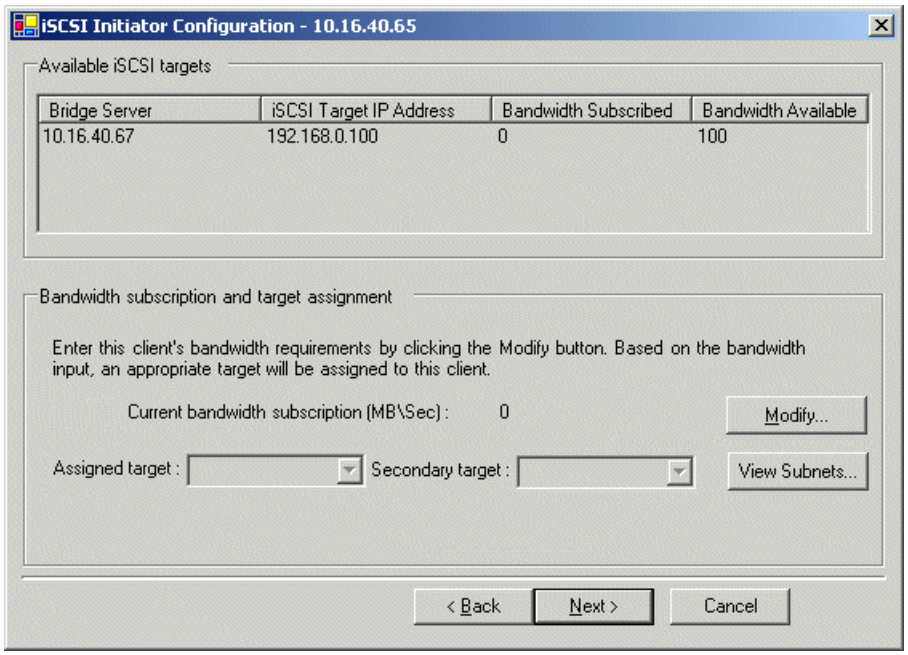
3. Verify or configure the media connection as follows:

   - Verify or enter the media network IP address. Also enter the subnet mask.

4. Click **Next**.

The iSCSI Initiator Configuration page opens.

Configure iSCSI Initiator Configuration page



This page lists the iSCSI adapter on your K2 Media Server as an iSCSI target. The K2Config application subscribes the SAN client to the iSCSI target and allocates bandwidth, based on the bandwidth values that you enter. The K2Config application keeps track of each SAN client's bandwidth, and when the total amount allowed by the K2 SAN license is consumed, the K2Config application displays an informative message and then disables your ability to add more SAN clients. For large systems the K2Config application can load balance SAN clients across multiple iSCSI targets.

If a custom K2 SAN, qualified system designers can view subnets to help assign iSCSI targets.

1. Click **Modify**.

   The Bandwidth Input dialog box opens.

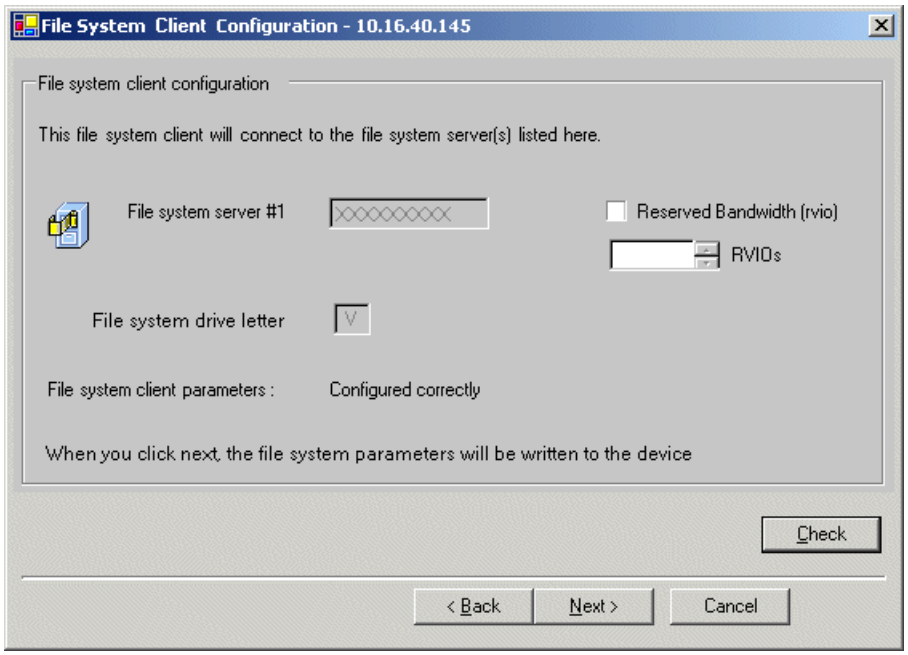
2. In the Bandwidth Input dialog box, enter the bandwidth value specified in your system design and then click **OK**.

   If the server has the role of encoder, you can calculate encoder bandwidth to determine the value to enter.

3. Click **Next**.

The File System Client Configuration page opens.

Configure File System Client Configuration page



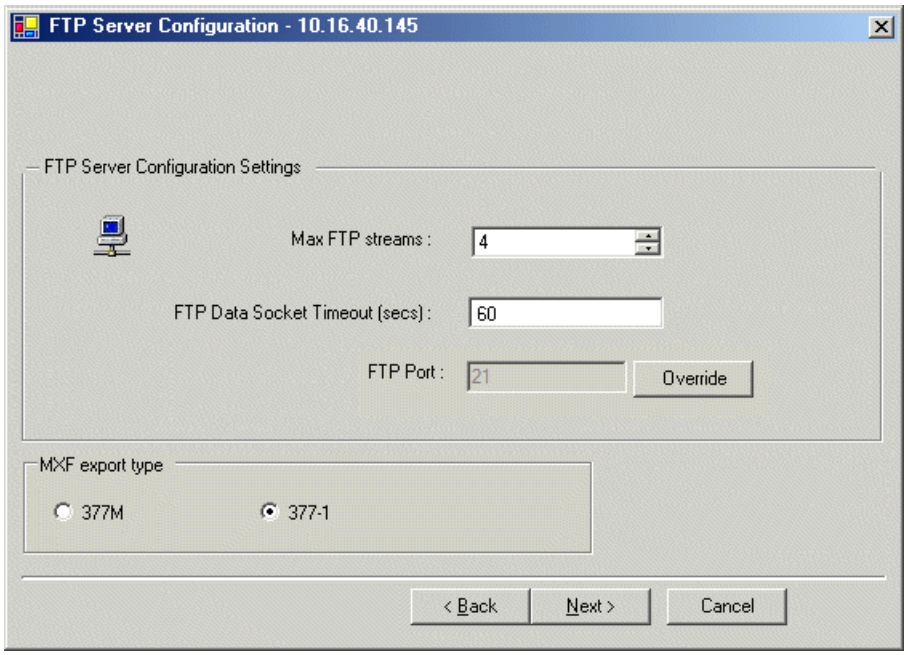
This system does not function as a file system server. It does function as a file system client, which is validated from this page.

1. Do not select **Reserved Bandwidth** unless instructed to do so by Grass Valley. This system is usually not configured for RVIO.
2. Click **Check**.
3. When the wizard reports that the configuration is correct, click **Next**.

   If you get a "The V: will not be available until this device is rebooted…" message, you can safely continue now and reboot later when instructed to do so.

The FTP Server Configuration page opens.

Configure FTP Server Configuration page



This page appears only if the server has the role of FTP server.

Do not modify these settings. Leave at default values of Max FTP streams = 4, FTP Data Socket Timeout = 60, and FTP Port = 21. Only qualified Grass Valley personnel should specify other values, as these settings are intended for use only with custom systems designed by Grass Valley.

1. Select MXF export type as follows:

   - **377M**: Original SMPTE 377M style. Ensures compatibility with older products.
   - **377-1**: Newer SMPTE 377-1 style.

   Refer to related topics in the "Configuring the K2 System" section of the K2 Topic Library for more information.

2. Click **Next**.

   The Completing the Configuration Wizard page opens.

3. Click **Finish**.

   The wizard closes. The server restarts.

Wait until all startup processes have completed before continuing.

Configure Render Engine Server

Only systems with a Render Engine require this process.

If you received your system already set up from Grass Valley, your Render Engine or Servers are already configured, so you can skip these tasks. Otherwise, work through the topics in this section.

Configuring settings: Render Engine

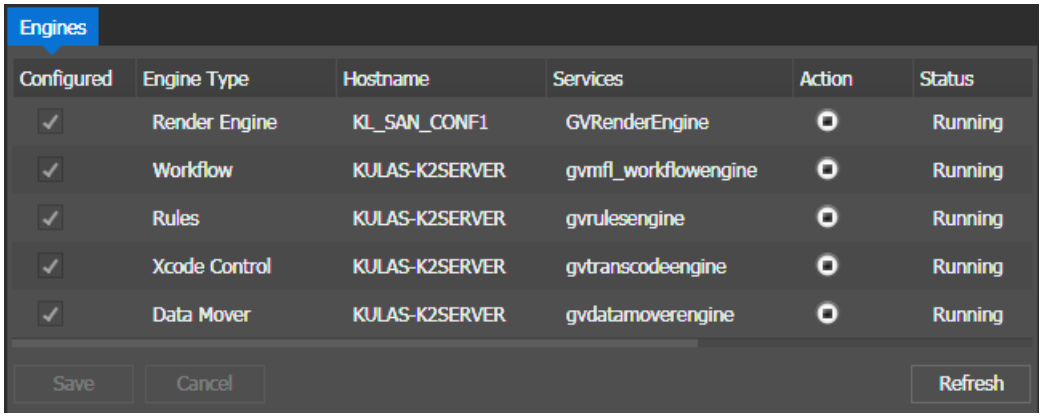
Only systems with a Render Engine require this process.

If you received your system pre-configured from Grass Valley, your Engines settings are already configured so you can skip these tasks. Otherwise, work through this section to configure your Engines settings.

To locate these settings, click **Core | Engines**

Depending on the workflow and bandwidth requirements of your system, Grass Valley may provide a system design in which multiple engines of the same type run on one or more servers. Configure engines as specified by your system design.

1. In the Control Panel application, open Engines settings.



Settings are described as follows:

Setting or button	Description
Configured	Selects an Engine for which settings are saved.
Hostname	The name of a GV STRATUS server that hosts the Engine.
Engine Type	The Engine components installed on the GV STRATUS server.
Status	Indicates if the Engine service is running or stopped.
Action	Starts and stops the Engine service.
Save	Saves current settings to selected GV STRATUS servers.
Cancel	Returns settings to their last saved state.
Refresh	Updates the list.

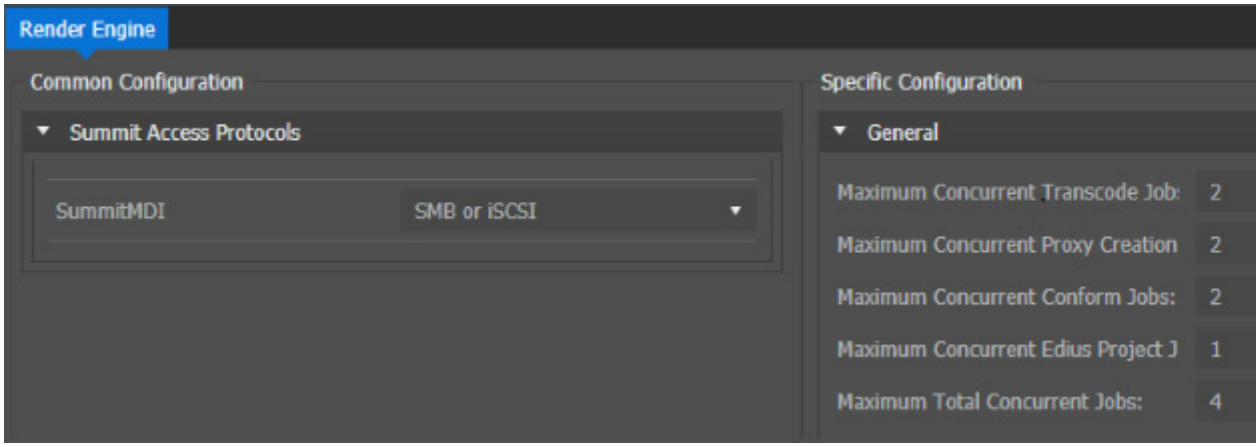
2. Click **Refresh** to make sure the list has the latest information from SiteConfig.
3. Verify that GV STRATUS servers with role of Render Engine are listed, and that those servers are set to Engine Type **Render Engine**.
4. In the **Configured** column, select each server with role of Render Engine, with Engine Type **Render Engine**.

   You must save settings at initial install/config and any time a GV STRATUS server with an Engine Type role is added, removed, or modified in SiteConfig.
5. Click **Save**.

   Settings are saved to the selected GV STRATUS servers.

6. Select the Render Engine and click **Modify**.

   The Render Engine configuration page displays.



7. Configure settings as follows:

Setting or button	Description
Summit Access Protocols	The Summit Access protocol is a common configuration that must be the same for all GV Render Engine servers. Different K2 Summit servers might be accessed via different protocols. Select the Summit Access Protocol for your Render Engine server from the following: • **FTP**: Setting for FTP protocol to be used by Render Engine to access K2 Summits. • **SMB or iSCSI**: Setting for SMB or iSCSI protocol to be used by Render Engine to access K2 Summits. ***NOTE: When a Render Engine accesses high-res media on a standalone K2 Summit or a K2 Central server, FTP is ALWAYS the preferred method. It is recommended to use iSCSI with K2 SAN configurations, and SMB with Isilon shared storage configurations.***
Maximum Concurrent Transcode Jobs	Setting to specify the maximum number of concurrent transcode jobs allowed on the Render Engine server.
Maximum Concurrent Proxy Creation Jobs	Setting to specify the maximum number of concurrent proxy encoder jobs allowed on the Render Engine server.
Maximum Concurrent Conform Jobs	Setting to specify the maximum number of concurrent conform jobs allowed on the Render Engine server.
Maximum Concurrent EDIUS Project Jobs	Setting to specify the maximum number of concurrent EDIUS project jobs allowed on the Render Engine server.
Maximum Total Concurrent Jobs	Setting to specify the maximum number of total concurrent jobs allowed on the Render Engine server. ***NOTE: The maximum number for the setting is up to 4 concurrent jobs in total.***

Use these settings to balance resource load on the GV STRATUS server hosting the engine.

NOTE: The total number of maximum concurrent jobs is limited by the number of available simultaneous connections with K2 Summits. If set to zero, the Render Engine does not process jobs of that type.

8. Click **Save**.

Render Engine settings are saved to the selected server.

Configuring Proxy Config settings: Required

All systems, all workflows, require this process.

If you are configuring Grass Valley Media Server MDI settings, you must make those settings first before doing this procedure.

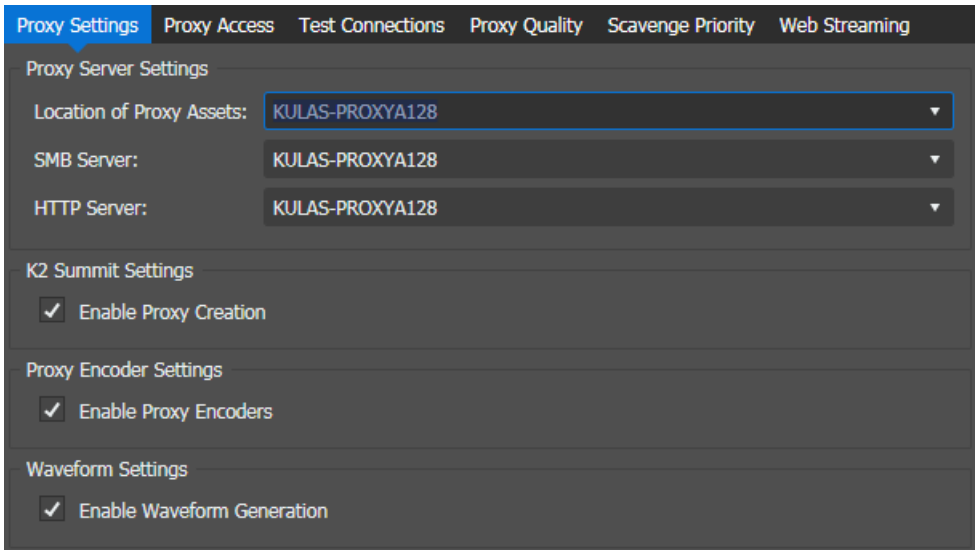
If you received your system pre-configured from Grass Valley, your Proxy Config settings are already configured so you can skip these tasks. Otherwise, work through this section sequentially to configure your Proxy Config settings.

NOTE: A GV STRATUS system must have only one proxy location and server, so these settings apply to all K2 Summit systems, both standalone and SAN.

NOTE: On an operational system, consult with Grass Valley Support before attempting to change Location of Proxy Assets, SMB Server, or HTTP Server settings. Changing these settings requires a purge of the GV STRATUS database and a new K2 storage file system, which results in a loss of high-resolution and low-resolution media. Grass Valley Support can provide methods to avoid this loss of media.

To locate these settings, click **Core | Proxy Config**

1. In the Control Panel application, open Proxy Config settings.



NOTE: GV STRATUS versions lower than 3.0 had only one Proxy Server setting. With version 3.0 and higher, the SMB Server and HTTP Server settings must be configured to replace the Proxy Server setting.

2. If your GV STRATUS system stores its proxy on a GV STRATUS Express server, configure as follows:

Setting or button	Description
Location of Proxy Assets	The name of the system that stores proxy files generated by K2 Summit and GV STRATUS systems, as follows: • For proxy stored on the GV STRATUS Express server, this is the network name of the server with role GV STRATUS Core Server Express, as configured in SiteConfig.
SMB Server	The network machine name of the device hosting the server to which proxy files are written, as follows: • For proxy stored on the GV STRATUS Express server, this is the network name of the server with role GV STRATUS Core Server Express, as configured in SiteConfig.
HTTP Server	The network machine name of the device hosting the server from which GV STRATUS clients read proxy files. Typically the SMB Server and the HTTP Server are hosted by the same device. • For proxy stored on the GV STRATUS Express server, this is the network name of the server with role GV STRATUS Core Server Express, as configured in SiteConfig.

3. If your GV STRATUS system stores its proxy on an online or production K2 SAN (A1), configure as follows:

Setting or button	Description
Location of Proxy Assets	The name of the system that stores proxy files generated by K2 Summit and GV STRATUS systems, as follows: • For proxy stored on the K2 SAN (A1), this is the name of the K2 SAN, as named in K2Config.
SMB Server	The network machine name of the device hosting the server to which proxy files are written, as follows: • For proxy stored on the K2 SAN (A1), this is the network name of the GV STRATUS Proxy server attached to the K2 SAN, as configured in K2Config.
HTTP Server	The network machine name of the device hosting the server from which GV STRATUS clients read proxy files. Typically the SMB Server and the HTTP Server are hosted by the same device. • For proxy stored on the K2 SAN (A1), this is the network name of the GV STRATUS Proxy server attached to the K2 SAN, as configured in K2Config.

4. If your GV STRATUS system stores its proxy on a dedicated Proxy Storage system (B1, C1), configure as follows:

Setting or button	Description
Location of Proxy Assets	The name of the system that stores proxy files generated by K2 Summit and GV STRATUS systems, as follows: • For proxy stored on the dedicated Proxy Storage system (B1, C1), this is the name of the Proxy Storage system, as named in K2Config.
SMB Server	The network machine name of the device hosting the server to which proxy files are written, as follows: • For proxy stored on the dedicated Proxy Storage system (B1, C1), this is the network name of the GV STRATUS Proxy Storage file system server, as configured in K2Config.
HTTP Server	The network machine name of the device hosting the server from which GV STRATUS clients read proxy files. Typically the SMB Server and the HTTP Server are hosted by the same device. • For proxy stored on the dedicated Proxy Storage system (B1, C1), this is the network name of the GV STRATUS Proxy Storage file system server, as configured in K2Config.

5. On the **Test Connections** tab, click **Test Connections**.

   The GV STRATUS system populates a list of K2 Storage devices. Verify that this list is correct.

6. Select **Enable Proxy Creation**.

   This allows K2 Summit systems to create proxy assets when high resolution assets are recorded.

7. Select **Enable Proxy Encoders**.

   This allows the system to create proxy assets for any high resolution assets that do not currently have a corresponding low-resolution proxy asset. This setting applies to proxy created by Render Engine servers. If your system instead has Proxy Encoder servers, which are no longer supported, the setting then applies to proxy created by your Proxy Encoder servers.

8. Click **Save**.
9. If you changed Location of Proxy Assets, SMB Server, or HTTP Server settings, under supervision of Grass Valley Support, you must purge the GV STRATUS database and make a new K2 storage file system.

Related Topics

Proxy Settings on page 343
HTTP server overview on page 226

Configuring settings: Render Engine work directory

Only systems with a Render Engine require this process.

To specify the path of work directory for the Render Engine, do the following:

1. On the Render Engine server at *..\Program Files\Grass Valley\XREServer 9\Settings*, copy the *EdiusRenderer.conf* file.
2. Paste the file into *..\Program Files\Grass Valley\XREServer 9*, and open *EdiusRenderer.conf* in a text editor.

```
# **** Configuration file for EdiusRendrerer.exe ****
  work = c:\temp
```

3. Enter a different **work** directory for your GV STRATUS operation, if applicable.

   The work directory consists of temporary files for the proxy operation.
4. Save and close the *EdiusRenderer.conf* file.
5. Restart the Render Engine server.

Create EDIUS project folder

If you use the Render Engine to render EDIUS projects, you must create a location for the EDIUS projects.

1. On the K2 media file system (the *V:* drive), create a folder.
2. Name the folder with a meaningful name.

   For example create the following folder:

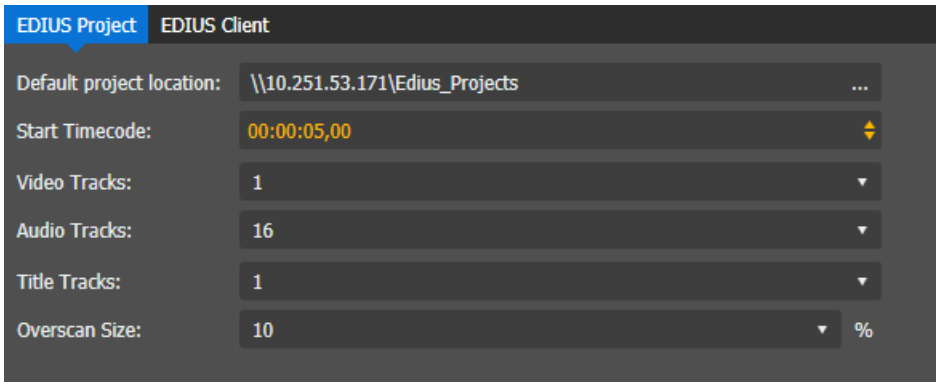
   V:\EDIUS_Projects
3. Make sure the folder is shared with permission granted so that your GV STRATUS/EDIUS XS client PCs, Render Engine Servers, and EDIUS Workgroup client PCs can access the folder.

   On the Render Engine Server, the internal system account, which by default is GVAdmin, accesses the folder.

EDIUS Settings

These settings are only required on GV STRATUS systems with EDIUS.

To locate these settings, in GV STRATUS Control Panel click **Applications | EDIUS | EDIUS Project**



Setting or button	Description
Default project location	The default location for your EDIUS projects. The location is a folder on K2 storage. Make sure this path uses the standard convention of UNC path with hostname (not drive letter) for EDIUS access to K2 storage.
Start timecode	The start timecode of your project or conformed asset. The default is set to 00:00:00,00.
Video Tracks	The number of video tracks for your project.
Audio Tracks	The number of audio tracks for your project.
Title Tracks	The number of title tracks for your project.
Overscan Size	The percentage ratio of overscan size for your project. Set to 0 if you are not using the overscan feature.

Format settings define the format of projects.

Related Topics

Format settings on page 161
If you have trouble launching EDIUS XS on page 169
Access K2 storage for EDIUS using standard convention on page 282
Access K2 storage for EDIUS using standard convention on page 282

Format settings

These settings are required on all GV STRATUS systems.

Format settings let you configure video and audio settings. The GV STRATUS application uses these settings as follows:

Conform When the Render Engine conforms a complex asset, such as a GV STRATUS sequence, into a simple clip, the Format settings define the format of the simple clip.

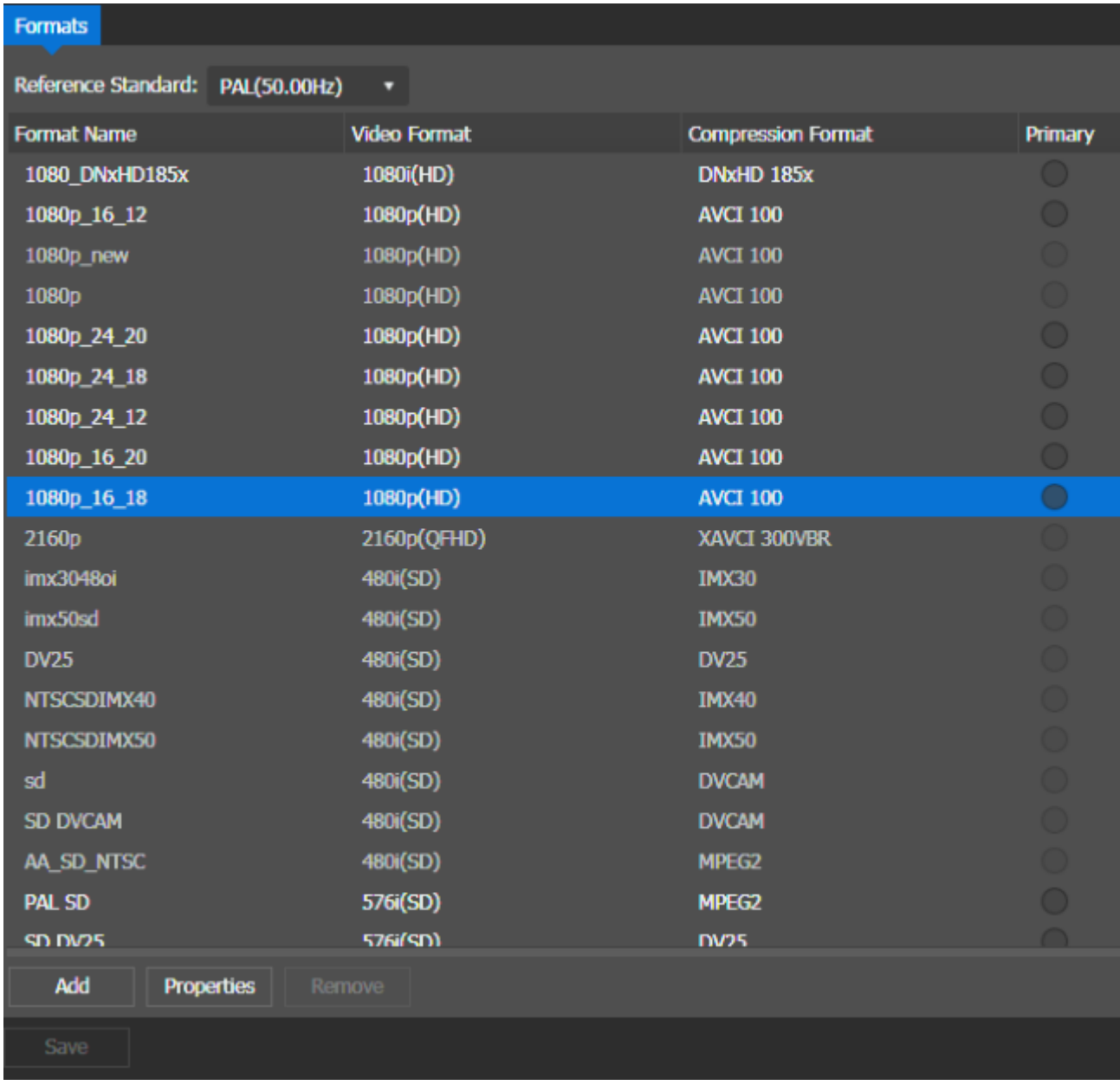
EDIUS XS Format settings are inherited by EDIUS XS when the application is launched and a new project is created.

GV STRATUS Rundown Format settings define the video standard settings, such as PAL or NTSC.

GV I/O Appliance	Format settings define the valid format for configured channels and ingested assets.
Storyboard and Source Viewer	Format settings define the video standard, audio reference, etc.

Access these settings in the GV STRATUS Control Panel application.

To locate these settings, click **General | Format | Formats**



Setting or button	Description
Reference Standard	Sets the GV STRATUS formats available according to their Reference Standard, to match the current Reference Standard on the K2 system. Formats that do not match this setting are disabled in the list. When changing and saving this setting, a corresponding primary format must be selected.
Format Name, Video Format, Compression Format, etc	Format settings, as configured in the **Format Settings** dialog box.
Primary	The default format for configuration. For example, when configuring a Send Destination, the primary format is set by default, but a different format can be selected if desired. ***NOTE: A primary format must be selected. Multiple primary formats are not allowed.***
Locked	Indicates if a format name can be modified. A format that is currently configured in a Send Destination displays a closed lock icon. A dialog box prompts for confirmation before a locked format name can be modified.
Add	Opens the **Format Settings** dialog box for you to add formats.
Properties	Opens the **Format Settings** dialog box for you to view properties of the selected format.
Remove	Removes the selected format. The format currently selected as the primary format can not be removed.
Save	Saves the current configuration of added formats and their order.

Clicking column heads and/or arrow buttons on the right reorders the list of formats.

Related Topics

K2 - Send Destination settings on page 370

Send Destination Add/Modify settings on page 372

Configuring Format settings: Required

EDIUS/GV Render Engine Setup

1. Install/upgrade EDIUS and GV Render Engine software as directed by standard instructions in GV STRATUS customer documentation.

   Make sure you follow the proper sequence for installation and running applications.

2. Verify that the `V:` drives of your K2 Summit system(s) have been shared, in order to allow the GV Render Engine(s) to access them.

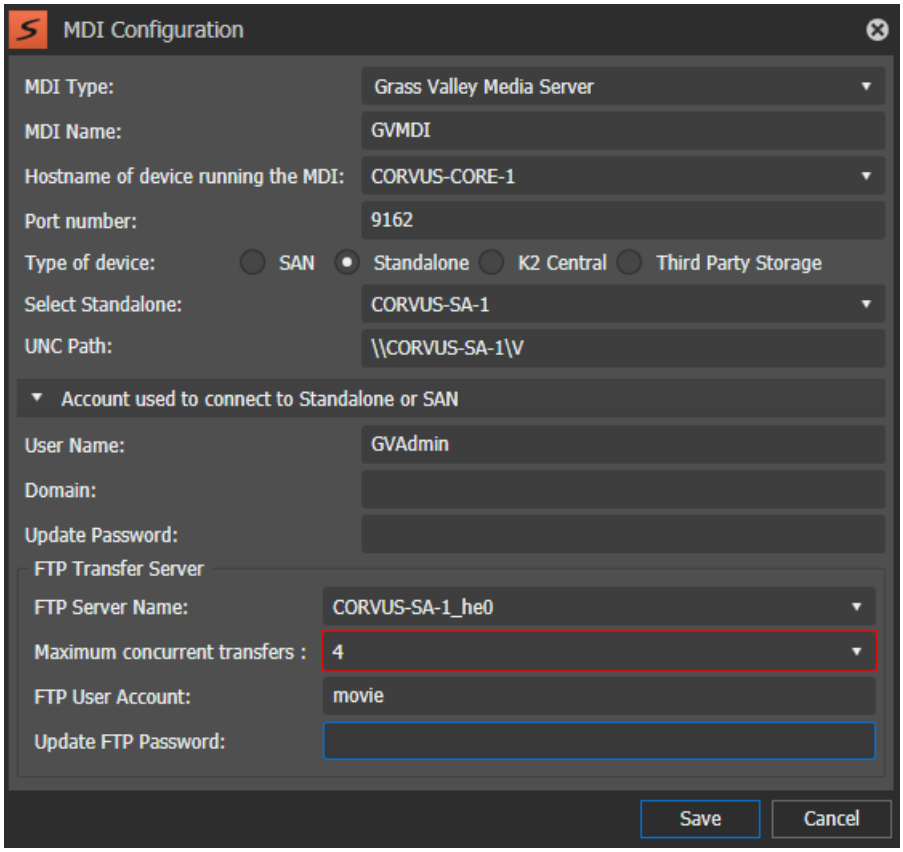
   NOTE: If the GV Render Engines are clients of a K2 SAN, the K2 SAN's V: drive does not need to be shared.

3. Add an EDIUS project folder at the root of the `V:` drive, as directed by standard instructions in GV STRATUS customer documentation.

4. In GV STRATUS Control Panel, set the UNC path as follows:
   - For EDIUS XS and Workgroup, click **Applications | EDIUS | EDIUS Project** and set **Default project location** to the UNC path of the above EDIUS folder. For a GV STRATUS Express system with K2 Summit standalone systems, use a path such as the following:

     `\\K2SummitStandaloneName\V\[EDIUSFolderName]`
   - For the GV Render Engine server, click **Core | MDI Configuration | Add | Grass Valley Media Server** and do the following:
     - Select **Standalone** for the type of K2 device. Then set the UNC path for the K2 Summit standalone system, use a path such as the following:

       `\\standalone_summit\V`



5. If you have EDIUS Workgroup or EDIUS XS workstations; on EDIUS Server Settings, configure as follows:

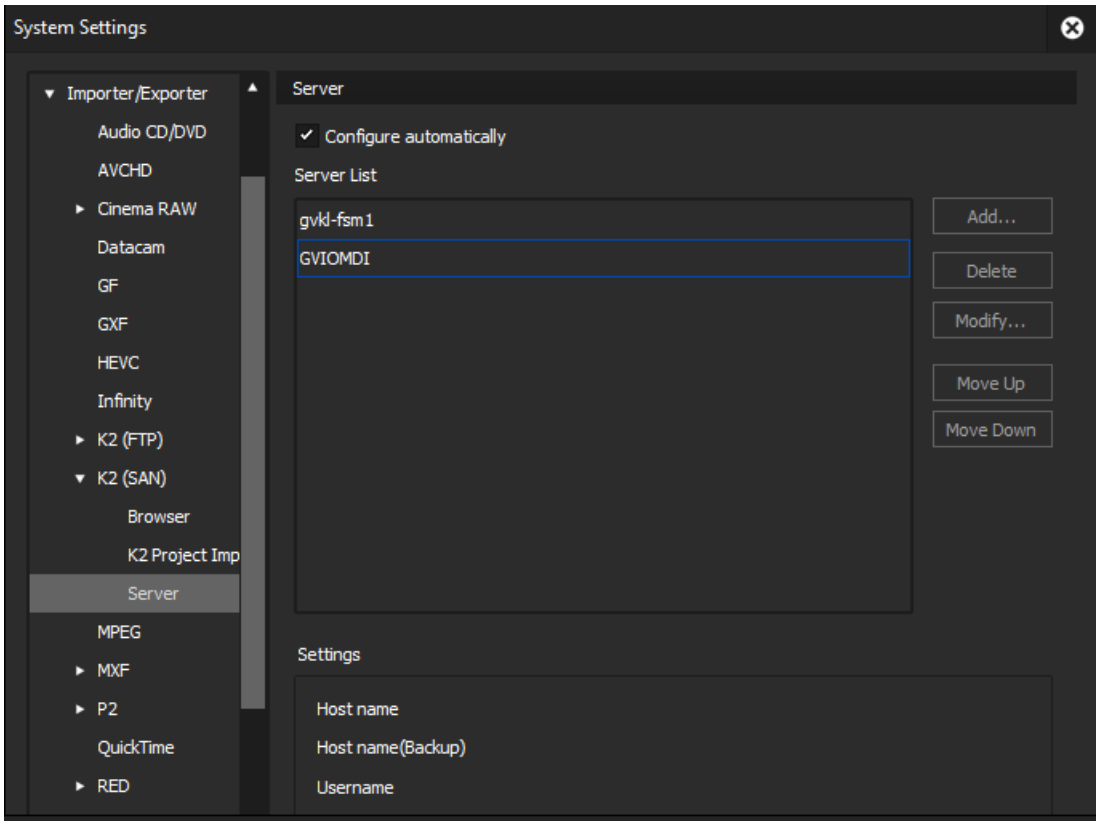
   These settings must be the same as your UNC path already configured on the GV STRATUS Control Panel. The settings identify the storage locations EDIUS accesses. A K2 storage location can be a K2 Summit standalone system or for a K2 SAN, the K2 Media Server with role of file system server (FSM).

   a) From the EDIUS application, click **Settings | System Settings**.

      EDIUS System Settings window opens.

   b) In the Importer/Exporter tree-view, click **K2 (SAN)**.

      Server settings open.



   c) Users are recommended to select the **Configure automatically** check-box.

      For the **Configure automatically** setting, take note of the following:

      - If the **Configure automatically** check-box is selected, the K2(SAN) drives will be automatically populated after each installation or software upgrade.

        NOTE: If the Grass Valley Media Server MDI has UNC path settings configured for third party storage, K2 central, or K2 Summit standalone; each server will be mapped according to its UNC path and not to a drive letter.

      - If the **Configure automatically** check-box is not selected, configure the K2 storage location following these steps below.

   d) In **Server** section, click **Add**.

The **Server Settings** dialog box opens.

e) Verify or make settings as follows.

Table 15: Server Settings

Setting	Value
Name	Enter a name that identifies the K2 storage location to display in the folder view.
Address	Enter the IP address or DNS name of the server that is the K2 storage location.
Address(Backup)	If the K2 storage location is a redundant K2 SAN, the IP address or DNS name of the redundant K2 Media Server with role of file system server (FSM).
Username	Enter the user name required when making the connection to the server configured above. For example, GVAdmin.
Password	Enter the password required for the user name configured above.
Domain	Enter the domain for the user credentials configured above. If not a domain account, leave this setting blank.
Storage Drive	Select the K2 storage location. It must be a drive available on the local system. For a K2 SAN this is typically the `v:` drive. For a K2 Summit standalone system this is typically a mapped network drive.
Show only SNFS drives	For a K2 SAN, select this setting. For a K2 Summit standalone system, clear this setting.
Connection Test	Click this button to test the connection to the server with the settings entered in the **Server settings** dialog box.

f) Click **OK** to save settings and close.

6. Follow the instructions in the this Topic Library to complete EDIUS and GV Render Engine setup.

Related Topics

Configuring CIFS Render Engine settings

EDIUS/XRE Setup for SMB storage

1. Install/upgrade EDIUS and GV Render Engine software as directed by standard instructions in GV STRATUS customer documentation.

   Make sure you follow the proper sequence for installation and running applications.

2. Mount the *V:* drive to your GV Render Engine server and any high resolution STRATUS/EDIUS clients.
   - For SMB storage, mount the Public Media Share, such as the following:

     \\gvstorage-public\mediashare

3. Add an EDIUS project folder at the root of the *V:* drive, as directed by standard instructions in GV STRATUS customer documentation.
4. In GV STRATUS Control Panel, click **Applications | EDIUS | EDIUS Project** and set **Default project location** to the UNC path of the above EDIUS folder, as follows:
   - For SMB storage, use a path to the Public Media Share, such as the following:

     \\gvstorage-public\mediashare\EDIUS

EDIUS/GV Render Engine Setup for K2 Central

1. Install/upgrade EDIUS and GV Render Engine software as directed by standard instructions in GV STRATUS customer documentation.

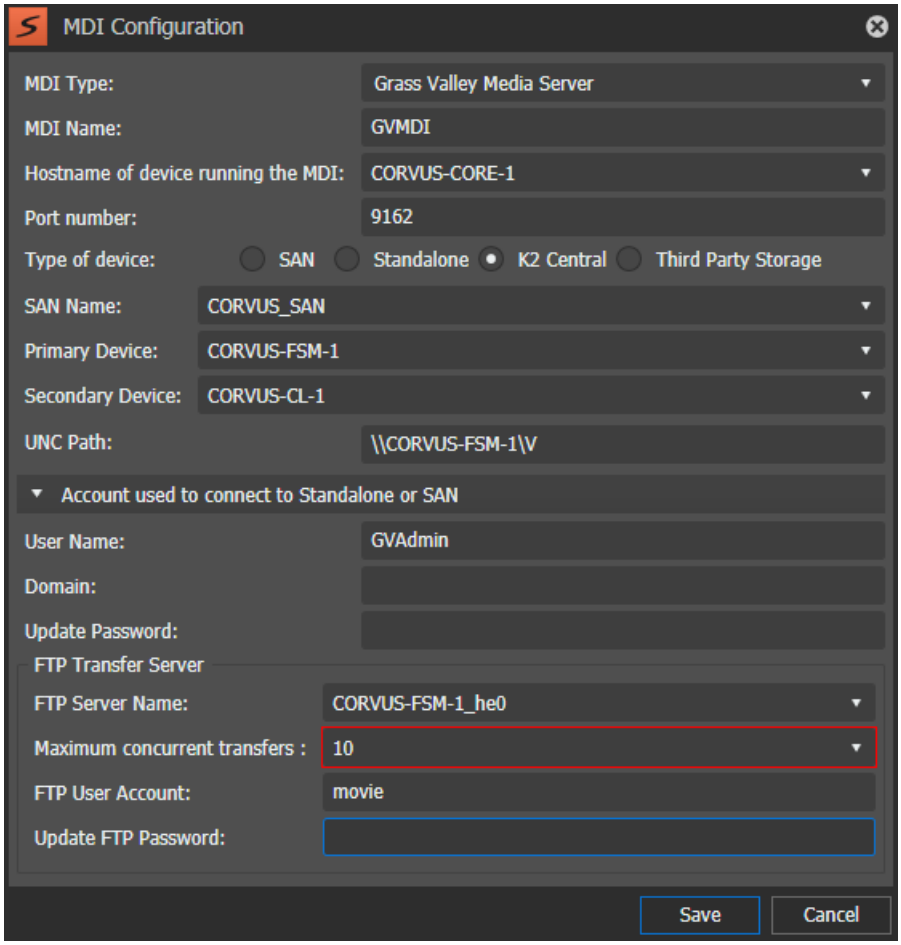
   Make sure you follow the proper sequence for installation and running applications.
2. On the K2 Central server, share the V: drive.
3. To configure the EDIUS share folder, contact Grass Valley Support for the qualified setup and configuration with all GV STRATUS system types.
4. Mount the *V:* drive to your GV Render Engine server and any high resolution GV STRATUS/EDIUS clients.
5. In GV STRATUS Control Panel, click **Applications | EDIUS | EDIUS Project** and set **Default project location** to the UNC path of the above EDIUS folder, as follows:
   - For K2 Central, use a path to the EDIUS folder on the K2 Central server, such as the following:

     \\[K2CentralServerName]\V\[EdiusFolderName]

   NOTE: If there are multiple K2s on the* GV STRATUS *system besides the K2Central, then the EDIUS project folder may be located on a different K2.

6. Click **Core | MDI Configuration | Add | Grass Valley Media Server** and set **K2 Central** for the type of K2 device. Select the K2 Central system as the SAN Name, Primary Device, Secondary Device, and set the UNC path to the K2 Central system.

   NOTE: For system performance, is it recommended that if there are K2 Summit Clients use them for the primary and secondary device. If there is only one client, use the client as the primary device and the FSM/Storage Manager as the secondary device.



   Complete the MDI configuration and click **Save**.

7. In the **Core | Engines** settings, verify that each GV Render Engine is displayed, desired streams configured, and the engine status is running.

8. If you have EDIUS Workgroup or EDIUS XS workstations; on EDIUS Server Settings, configure as follows:

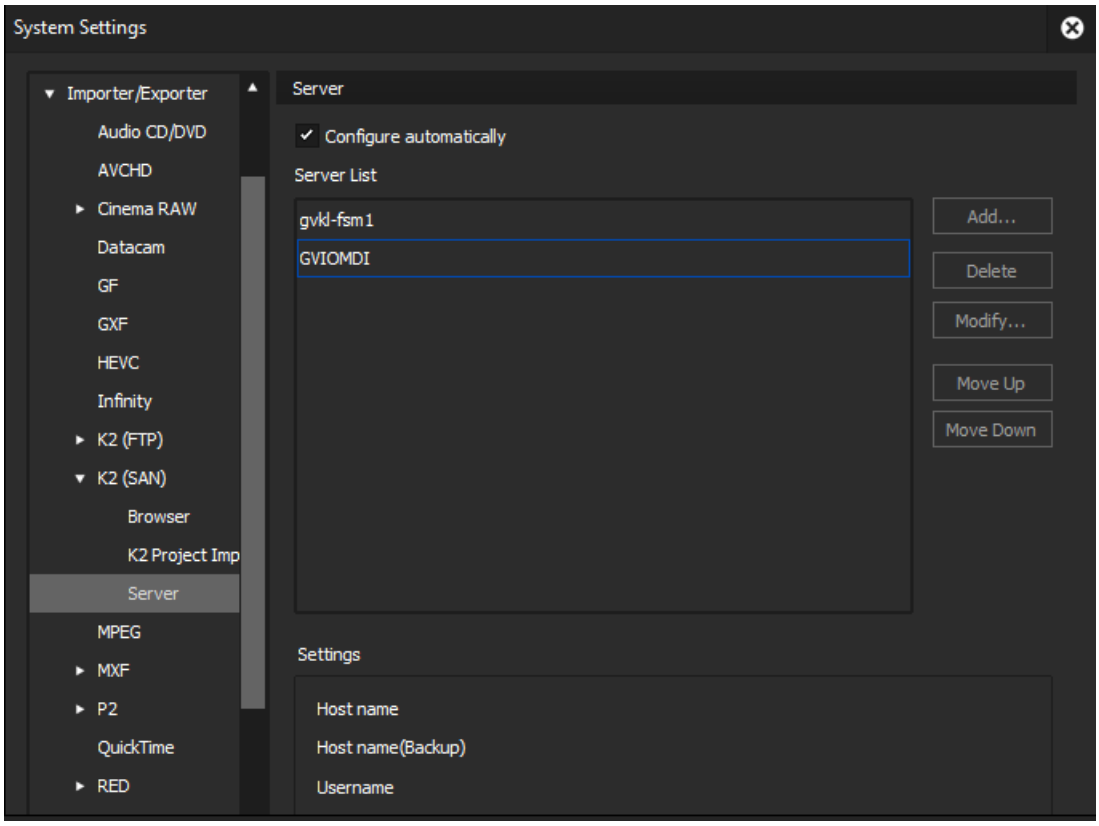
   These settings must be the same as your UNC path already configured on the GV STRATUS Control Panel. The settings identify the storage locations EDIUS accesses. A K2 storage location can be a K2 Summit standalone system or for a K2 SAN, the K2 Media Server with role of file system server (FSM).

   a) From the EDIUS application, click **Settings | System Settings**.

      EDIUS System Settings window opens.

   b) In the Importer/Exporter tree-view, click **K2 (SAN)**.

      Server settings open.



   c) Users are recommended to select the **Configure automatically** check-box.

      For the **Configure automatically** setting, take note of the following:

      - If the **Configure automatically** check-box is selected, the K2(SAN) drives will be automatically populated after each installation or software upgrade.

        NOTE: If the Grass Valley Media Server MDI has UNC path settings configured for third party storage, K2 central, or K2 Summit standalone; each server will be mapped according to its UNC path and not to a drive letter.

      - If the **Configure automatically** check-box is not selected, configure the K2 storage location following these steps below.

   d) In **Server** section, click **Add**.

The **Server Settings** dialog box opens.

e) Verify or make settings as follows.

Table 16: Server Settings

Setting	Value
Name	Enter a name that identifies the K2 storage location to display in the folder view.
Address	Enter the IP address or DNS name of the server that is the K2 storage location.
Address(Backup)	If the K2 storage location is a redundant K2 SAN, the IP address or DNS name of the redundant K2 Media Server with role of file system server (FSM).
Username	Enter the user name required when making the connection to the server configured above. For example, GVAdmin.
Password	Enter the password required for the user name configured above.
Domain	Enter the domain for the user credentials configured above. If not a domain account, leave this setting blank.
Storage Drive	Select the K2 storage location. It must be a drive available on the local system. For a K2 SAN this is typically the `v:` drive. For a K2 Summit standalone system this is typically a mapped network drive.
Show only SNFS drives	For a K2 SAN, select this setting. For a K2 Summit standalone system, clear this setting.
Connection Test	Click this button to test the connection to the server with the settings entered in the **Server settings** dialog box.

f) Click **OK** to save settings and close.

9. Restart the entire GV STRATUS system in the following order:

   - B1 proxy server (if applicable)
   - K2 Central servers, Stand-alones, primary FSMs
   - Secondary FSMs (if applicable)
   - All K2 Summits, iSCSI clients, GVREs, PCs
   - Core/Workflow/DME servers

10. Open Embedded Security Managers on the K2 Central and K2 Summit clients, and put them in Enabled mode.

Social Media Engine Server set up process

Only systems with a Social Media Engine require this process. Use SiteConfig for network setup and software install.

GV STRATUS supports the deployment of Social Media Engine on the GV STRATUS Core server, Workflow Server, or a separate server. The Workflow Server or a separate server allows the separation of GV STRATUS Engines (Workflow-, Rules-, XCodeControl- and optional DataMover-Engine) away from the Core Server for large system setups where rules and workflows are used intensively paired with lots of file exports.

If you received your Social Media Engine server already set up from Grass Valley, skip set up tasks and do the test task only.

1. *SiteConfig Workflow Server network set up* on page 802. Only systems with a Workflow Server or separate server require this process.
2. *SiteConfig Social Media Engine software install* on page 803. Only systems with a Social Media Engine require this process.
3. *SabreTooth Social Media Engine license process* on page 805. Only systems with a Social Media Engine require this process. The process is on the GV STRATUS Core server, Workflow Server, or a separate server.
4. *Configure Social Media Engine* on page 805. Only systems with a Social Media Engine with supported Social Media Platforms require this process.

SiteConfig Workflow Server network set up

Only systems with a Workflow Server require this process.

If you received your system already set up from Grass Valley, your Workflow Server or Servers are already included in the SiteConfig system description and set up on the network, so you can skip these tasks. Otherwise, work through the topics in this section.

Adding a Workflow Server to the SiteConfig system description

- Workflow Servers are racked, cabled, and powered on.
- The system description must contain a group.

This topic applies to a GV STRATUS server that is a Workflow Server.

1. In the **Network Configuration | Devices** tree view, right-click a group and select **Add Device**.

2. Configure settings for the device you are adding as follows:
   - Family: GV STRATUS
   - Device Type: GV STRATUS Server
   - Model: GV STRATUS Workflow Server
   - Name – This is the device name, as displayed in the SiteConfig device tree view and device list view. This name can be different than the host name (network name). You can accept the default name or enter a name of your choice. Devices in the tree view are sorted alphabetically.
   - Amount — Select the number of Workflow Servers, according to your system design.
   - Platform — Select **x64**.
   - Control network– Select the control network.
   - Starting Address – Select from the list of available addresses on the selected control network. If adding multiple devices, this is the starting address, with addresses assigned sequentially to each device added.
3. Click **OK** to save settings and close.

   SiteConfig adds the Workflow Server to the system description as a placeholder device.
4. Verify that unmanaged control network interface is configured correctly and modify if necessary.

Next, add the GV STRATUS server to the control network.

Adding a GV STRATUS server to the control network with SiteConfig

Use SiteConfig to configure network settings on a separate GV STRATUS server.

Before doing this task, make sure the GV STRATUS server is added as a placeholder device to the SiteConfig system description.

The following steps are the standard tasks for adding a device to the control network using SiteConfig. Use these steps for the GV STRATUS server you are adding.

1. Discover the device using SiteConfig device discovery.
2. Assign the discovered device to the placeholder device in the SiteConfig system description.
3. Modify the control network interface to ensure communication on the control network.
4. Modify the host name and/or device name as desired.
5. Ping the device to verify network communication.
6. Verify credentials to ensure SiteConfig can install software on the device.
7. Generate and/or add to host tables as appropriate for your network.

Related Topics

Adding a device to a network with SiteConfig on page 490
Adding a device to a network with SiteConfig on page 490

SiteConfig Social Media Engine software install

Only systems with a Social Media Engine require this process.

If you received your system pre-configured from Grass Valley, software is already installed, so you can skip these tasks. Otherwise, work through the tasks in this section as follows:

Add software role for the Social Media Engine

Before doing this task, make sure devices are added to the SiteConfig system description with the correct family and device type. Refer to *Complete listing of device types, roles, and software packages for GV STRATUS devices* on page 194.

1. As appropriate for your system design and licensing, in your SiteConfig system description, configure role as follows:
   - For your Core Server, Workflow Server or a separate server, add the new role as follows:
     - GV STRATUS SocialMedia Engine
2. Save SiteConfig and verify in `C:\ProgramData\Grass Valley\ConfigurationDataFiles\SiteConfig` that .scsd and .config files are saved to the server.

If you want to verify all your currently configured SiteConfig roles, refer to the complete list of roles and software packages.

Installing software for the Social Media Engine

Use SiteConfig to install software for the Social Media Engine.

- The server on which you are installing software is in the SiteConfig system description and communicating on the control network.
- The server on which you are installing software has its credentials set in SiteConfig to allow access.

1. Verify the SiteConfig roles currently assigned to the server. If the roles are not correct for your system design, add or remove roles accordingly. The role should be as follows:
   - GV STRATUS SocialMedia Engine
2. Add the server to a deployment group, such as the GV STRATUS deployment group.
3. Add the following file to the deployment group:
   - `GrassValley_CoreServer_x.x.x.cab`, which contains the following cab file that apply to this device:
     - `GrassValley_STRATUS_SocialMedia_x.x.x.cab`

   Refer to release notes for version numbers.
4. Do the SiteConfig **Check Software** operation on the server.
5. Verify that deployment tasks are set to **Install** for the files listed above.
6. Deploy software to the server.
7. Restart as prompted.
8. After deployment is complete, start the GV STRATUS Social Media Engine Service.

Next, license the Social Media Engine.

SabreTooth Social Media Engine license process

The Social Media Engine license should be installed on the GV STRATUS server with role of Common Services.

One STRATUS-SMNSOCIALMEDIAENGINE license is required for the Social Media Engine software component in your GV STRATUS system. This is a SabreTooth floating license. It is possible to deploy more than one Social Media Engine per system. Each Engine must have its own license.

The Social Media Engine also requires a license for each Social Media Platform it supports. Licenses for each Social Media Platform include the following:

- STRATUS-SMNYOUTUBE
- STRATUS-SMNTWITTER
- STRATUS-SMNFACEBOOK

If you received your system pre-configured from Grass Valley, licenses are already installed, so you can skip these tasks. Otherwise, do the following:

1. Refer to the license sheet that you received with your GV STRATUS license. The license sheet has the Sales Order number that you need.
2. On the GV STRATUS server with role of Common Services, run the SabreTooth License Manager, generate a unique ID, and send the email to Grass Valley requesting your license or licenses.

   Refer to this Topic Library for detailed licensing procedures.
3. When you receive your license file, use SabreTooth License Manager and install it on the server.

Configure Social Media Engine

Only systems with a Social Media Engine require this process.

If you received your system already set up from Grass Valley, your Social Media Engine is already configured, so you can skip these tasks. Otherwise, work through the topics in this section.

Configuring settings: Social Media Engine

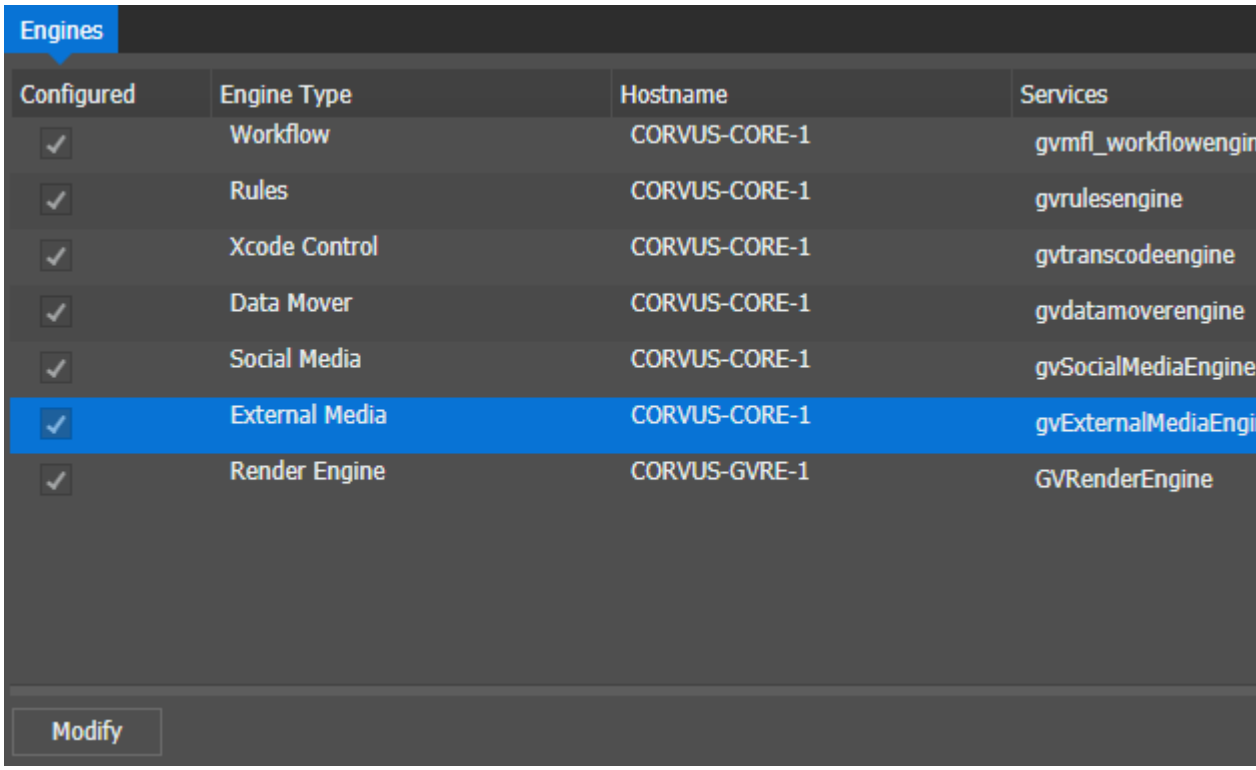
Only systems with a Social Media Engine require this process.

If you received your system pre-configured from Grass Valley, your Engines settings are already configured so you can skip these tasks. Otherwise, work through this section to configure your Engines settings.

To locate these settings, click **Core | Engines**

Depending on the workflow and bandwidth requirements of your system, Grass Valley may provide a system design in which multiple engines of the same type run on one or more servers. Configure engines as specified by your system design.

1. In the Control Panel application, open Engines settings.



Settings are described as follows:

Setting or button	Description
Configured	Selects an Engine for which settings are saved.
Hostname	The name of a GV STRATUS server that hosts the Engine.
Engine Type	The Engine components installed on the GV STRATUS server.
Status	Indicates if the Engine service is running or stopped.
Action	Starts and stops the Engine service.
Save	Saves current settings to selected GV STRATUS servers.
Cancel	Returns settings to their last saved state.
Refresh	Updates the list.

2. Click **Refresh** to make sure the list has the latest information from SiteConfig.
3. Verify that GV STRATUS server with role of Social Media Engine is listed, and that the server's Engine Type is set to **Social Media**.

4. In the **Configured** column, select each server with Engine Type: **Social Media**.

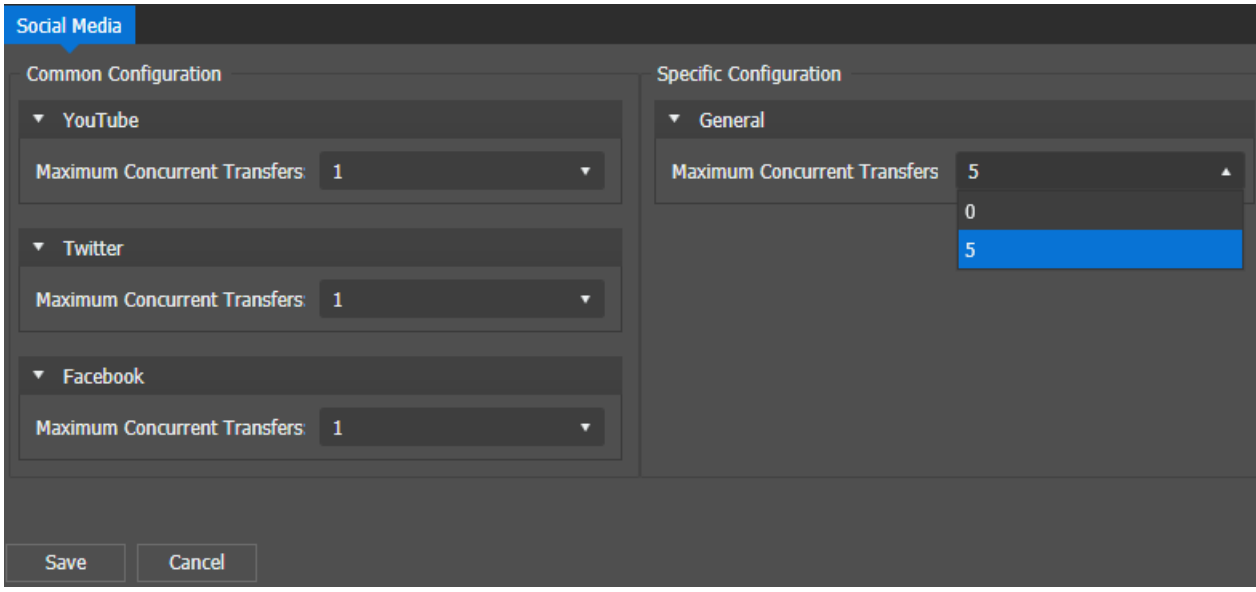
   You must save settings at initial install/config and any time a GV STRATUS server with an Engine Type role is added, removed, or modified in SiteConfig.

5. Click **Save**.

   Settings are saved to the selected GV STRATUS servers.

6. Select the row with **Social Media** engine type and click **Modify**.

   The **Social Media** engine configuration page displays.



7. Configure settings as follows:

Setting or button	Description
YouTube : Maximum Concurrent Transfers	Limits the number of simultaneous transfers performed by the Social Media engine on your configured YouTube account. You can configure the number of maximum concurrent transfers between 0-10 per Social Media Platform type. This setting is set to “0” if the YouTube site license is not installed.
Twitter : Maximum Concurrent Transfers	Limits the number of simultaneous transfers performed by the Social Media engine on your configured Twitter account. You can configure the number of maximum concurrent transfers between 0-10 per Social Media Platform type. This setting is set to “0” if the Twitter site license is not installed.
Facebook : Maximum Concurrent Transfer	Limits the number of simultaneous transfers performed by the Social Media engine on your configured Facebook account. You can configure the number of maximum concurrent transfers between 0-10 per Social Media Platform type. This setting is set to “0” if the Facebook site license is not installed.
General: Maximum Concurrent Transfers	Limits the total number of simultaneous transfers performed by the Social Media engine for all social media platforms. Use to balance resource load on the system hosting the engine. If the engine is deployed without a Social Media Engine license, this setting is set to “0” and cannot be configured. You can set 5 maximum concurrent transfers for each Social Media Engine license.

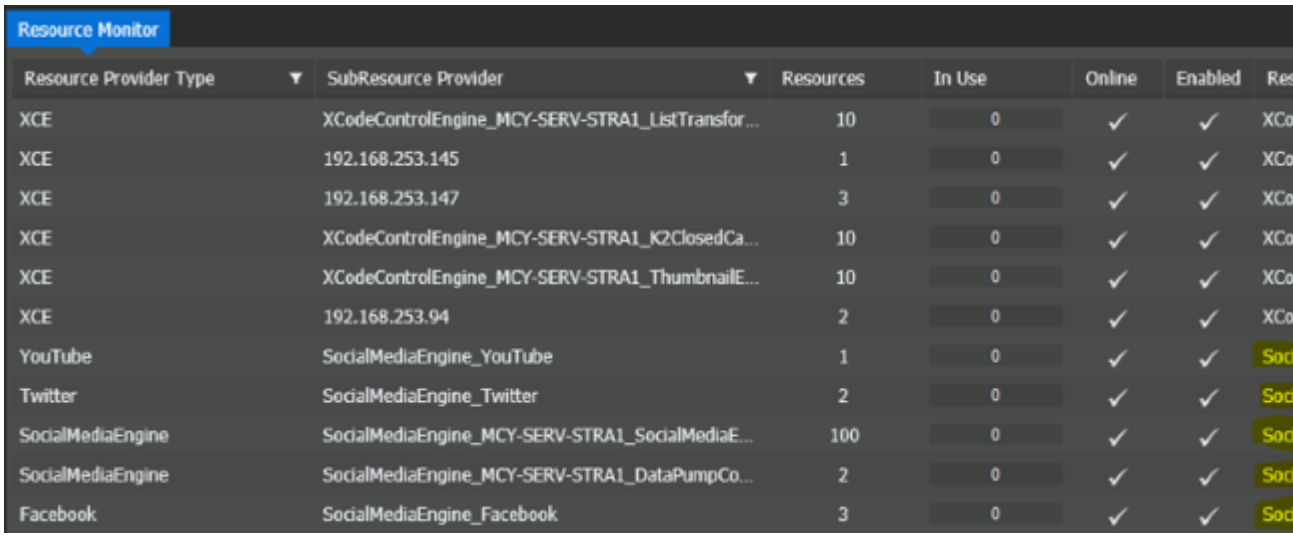
Use these settings to balance resource load on the GV STRATUS server hosting the engine.

NOTE: One volume license for the Social Media Engine limits the maximum concurrent jobs to five (5). It is possible to deploy more than one Engine per system for a bigger operation. Each Engine must have its own license.

8. Click **Save**.

   The Social Media Engine settings are saved to the selected server.

The available resources are registered as individual resources in the Resource Management and listed in the Resource Monitor.



Configure and authenticate Facebook location

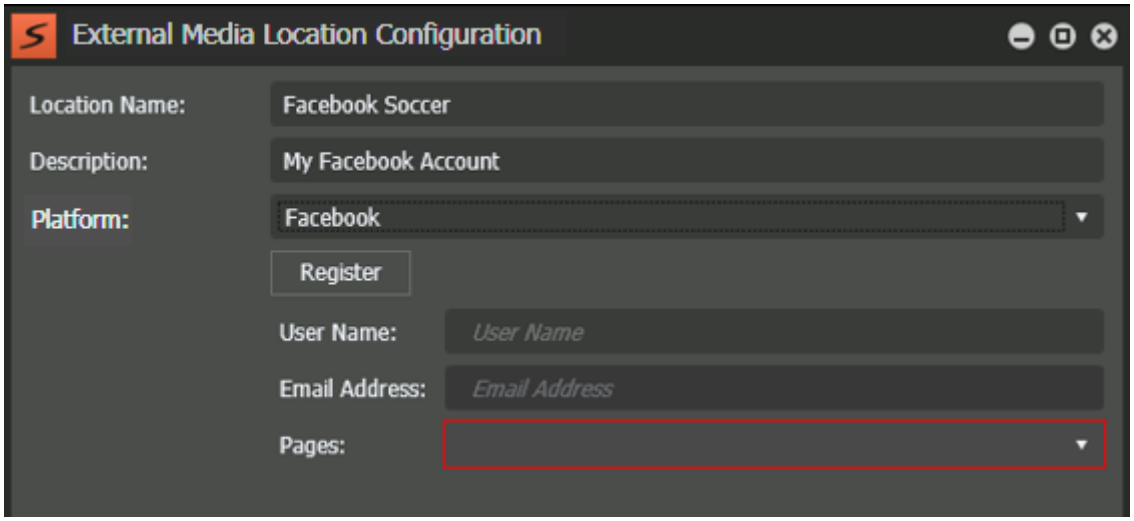
Only systems that publish assets to Facebook require this process.

- The express/core server, workflow server, or separate server must be configured with the GV STRATUS Social Media Engine role and deployed by SiteConfig.
- The Social Media Engine must be running in GV STRATUS Control Panel Engines settings.
- Both "STRATUS-SMNSOCIALMEDIAENGINE" and "STRATUS-SMNFACEBOOK" licenses are installed on the core/express or separate server.

Configure a location as follows:

1. In GV STRATUS Control Panel, navigate to **General | Locations Config | External Media | Add**.

   The **External Media Location Configuration** dialog appears.

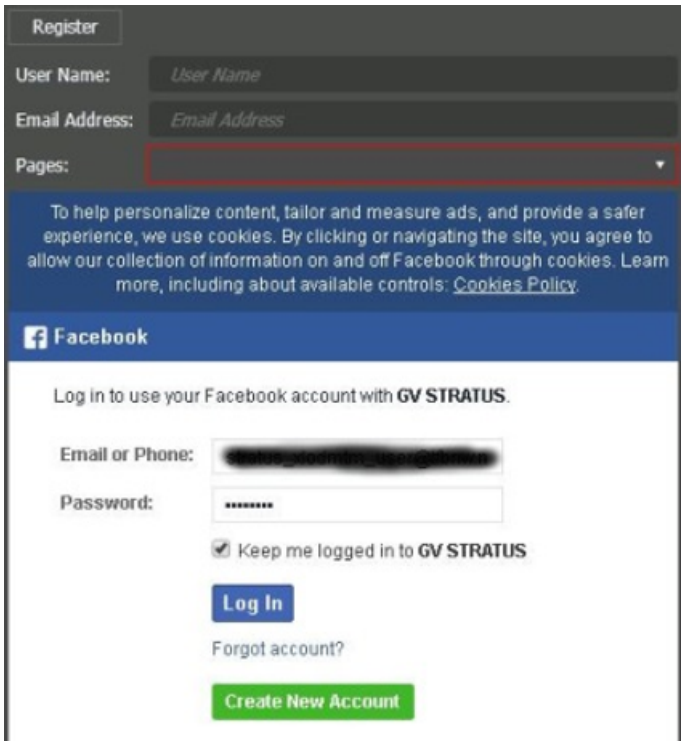


2. Configure as follows:

Setting or button	Description
Location Name	The name of the location, as it appears in the application. This can be any name, as appropriate for your workflow. This identifies the Facebook location when publishing assets to your Facebook account via the GV STRATUS application.
Description	Your description of the location.
Platform	Select **Facebook** from the drop-down list.

3. Click **Register**.

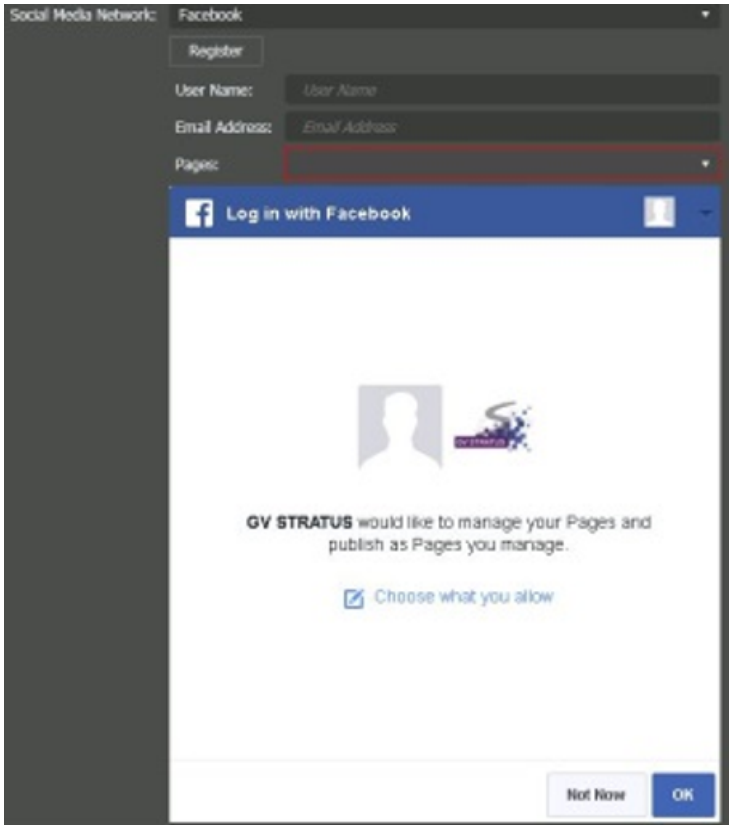
   A web-browser opens automatically for you to enter the account credentials.



4. Enter the e-mail address and password of the Facebook account.

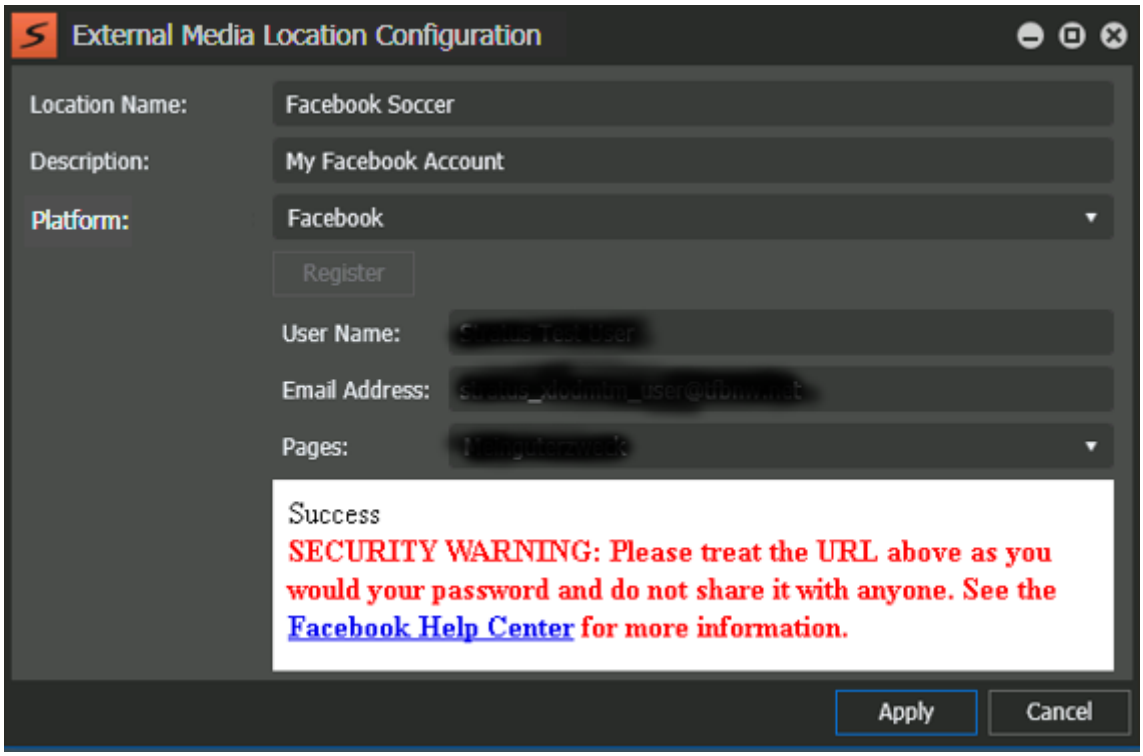
5. Select the **Keep me logged in to GV STRATUS** check-box and click **Log In**.

   The GV STRATUS permission page opens.



6. Click **OK** to allow GV STRATUS system to manage and publish assets on your Facebook account.

   In the Social Media Locations Configuration dialog, your Facebook user name and email address are displayed.



7. Click the **Pages** drop-down list and select your Facebook page.
8. Click **Apply** to save the Facebook location configuration in the GV STRATUS Control Panel.

Next, configure the Publish External Media Network rule.

Related Topics

Adding a publish external media network rule on page 621

Configure and authenticate Twitter location

Only systems that publish assets to Twitter require this process.

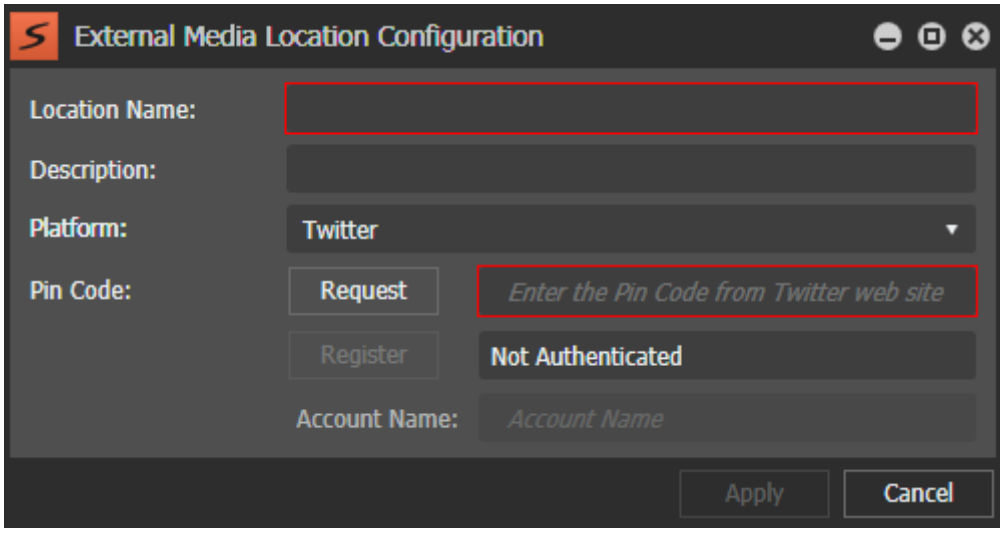
- The express/core server, workflow server, or separate server must be configured with the GV STRATUS Social Media Engine role and deployed by SiteConfig.
- The Social Media Engine must be running in GV STRATUS Control Panel Engines settings.

- Both "STRATUS-SMNSOCIALMEDIAENGINE" and "STRATUS-SMNTWITTER" licenses are installed on the core/express or separate server.

Configure a location as follows:

1. In GV STRATUS Control Panel, navigate to **General | Locations Config | External Media | Add**.

   The **External Media Location Configuration** dialog appears.

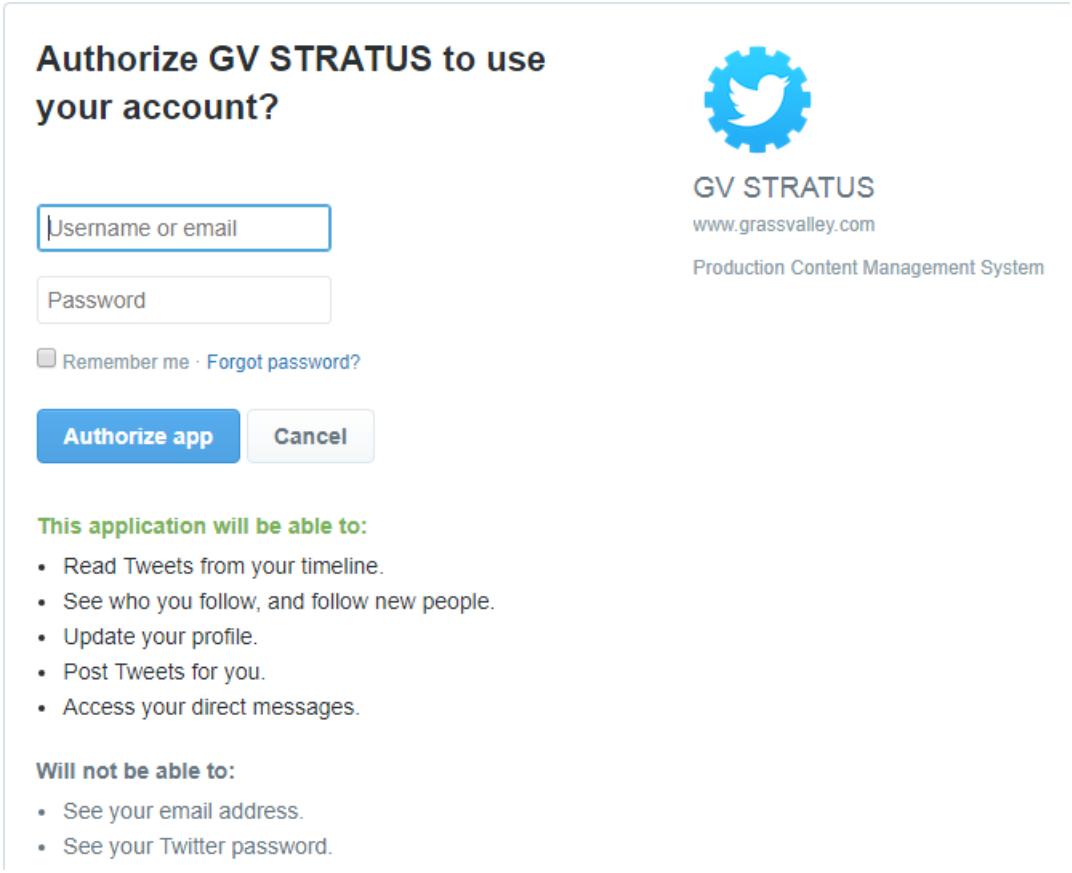


2. Configure as follows:

Setting or button	Description
Location Name	The name of the location, as it appears in the application. This can be any name, as appropriate for your workflow. This identifies the Twitter location when publishing assets to your Twitter account via the GV STRATUS application.
Description	Your description of the location.
Platform	Select **Twitter** from the drop-down list.

3. Click **Request** to get a Pin Code from the Twitter website.

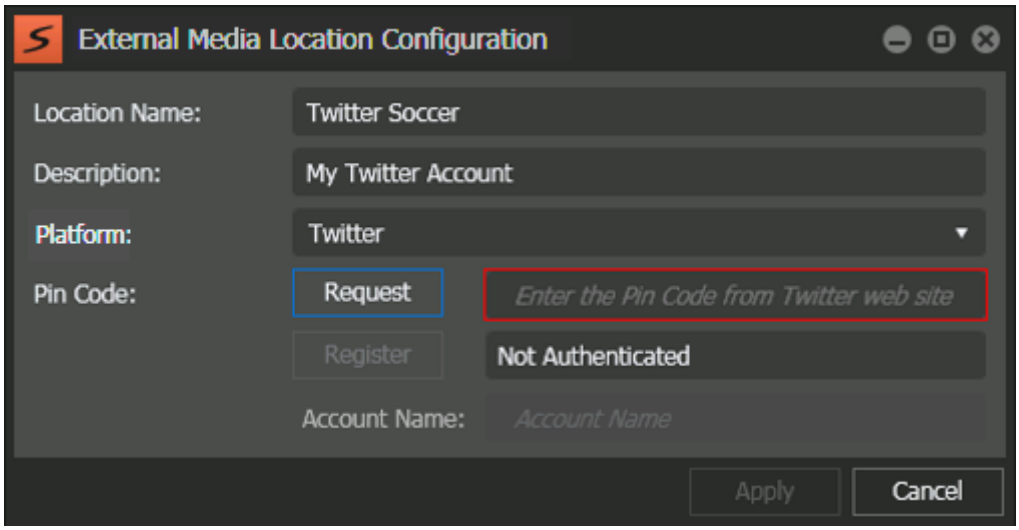
   A web-browser opens automatically for you to enter the account credentials.



4. Enter your User name or email address, and enter the password.
5. Then, click **Authorize app** for GV STRATUS system to access and manage assets on your Twitter account.

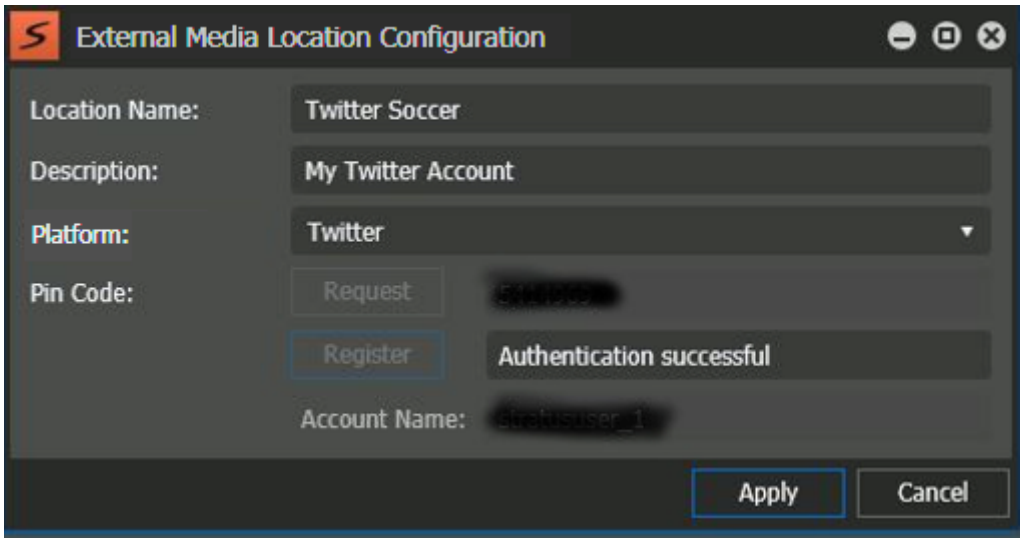
   The request is successful when the web-browser displays a 7 digit Pin Code.

6. Copy the Pin Code and paste it on the Social Media Locations Configuration dialog.



7. Click **Register**.

   The Twitter location configuration is completed when the **Authentication successful** message appears as below:



8. Click **Apply** to save the Twitter location configuration in the GV STRATUS Control Panel.

Next, configure the Publish External Media Network rule.

Related Topics

Adding a publish external media network rule on page 621

Configure and authenticate YouTube location

Only systems that publish assets to YouTube channel require this process.

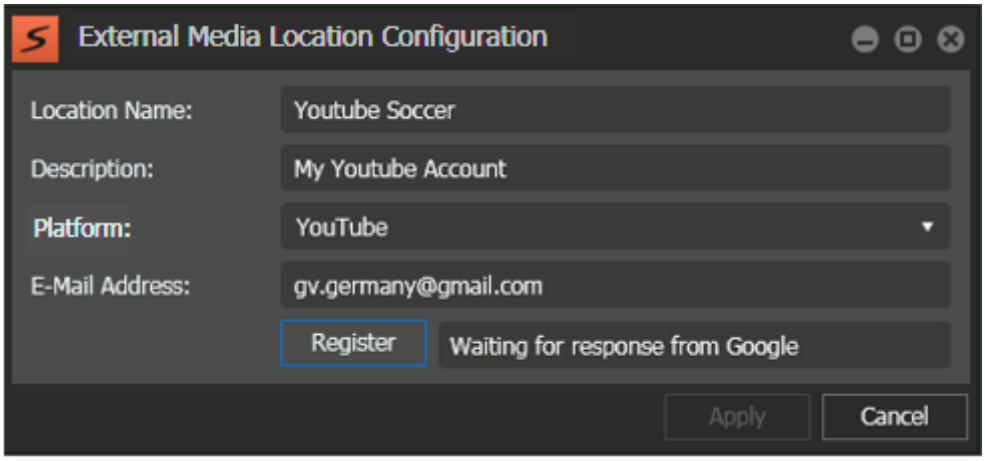
- The express/core server, workflow server, or separate server must be configured with the GV STRATUS Social Media Engine role and deployed by SiteConfig.

- The Social Media Engine must be running in GV STRATUS Control Panel Engines settings.
- Both "STRATUS-SMNSOCIALMEDIAENGINE" and "STRATUS-SMNYOUTUBE" licenses are installed on the core/express or separate server.

Configure a location as follows:

1. In GV STRATUS Control Panel, navigate to **General | Locations Config | External Media | Add**.

   The **External Media Location Configuration** dialog appears.

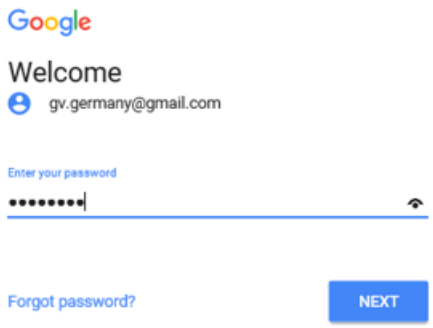


2. Configure as follows:

Setting or button	Description
Location Name	The name of the location, as it appears in the application. This can be any name, as appropriate for your workflow. This identifies the YouTube location when publishing assets to your YouTube channel via the GV STRATUS application.
Description	Your description of the location.
Platform	Select **YouTube** from the drop-down list.
E-mail Address	Enter the email address of the YouTube account.

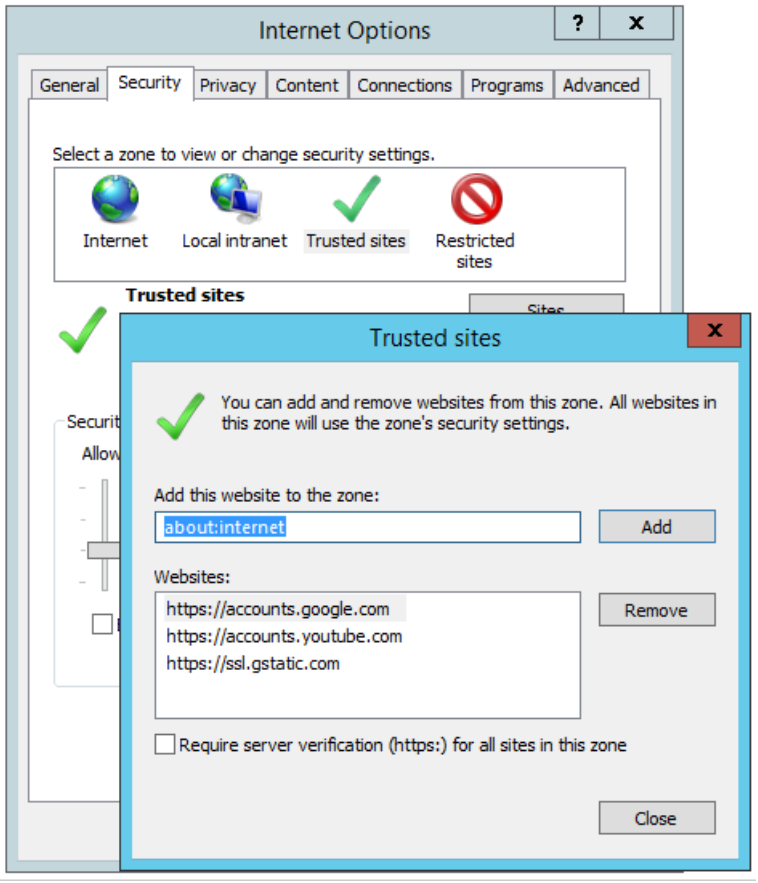
3. Click **Register**.

   A web-browser opens automatically for you to enter the account credentials.



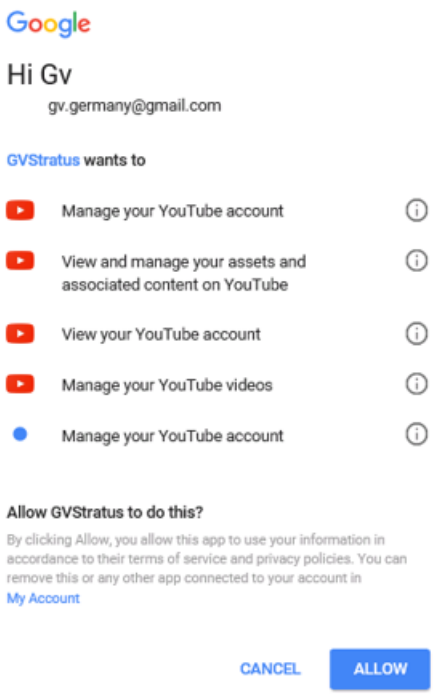
4. If the web-browser opens but does not display the login page, you must add the following sites as “Trusted Sites” in the browser’s “Security” options.

   - *https://accounts.google.com/*
   - *https://accounts.youtube.com/*
   - *https://ssl.gstatic.com/*



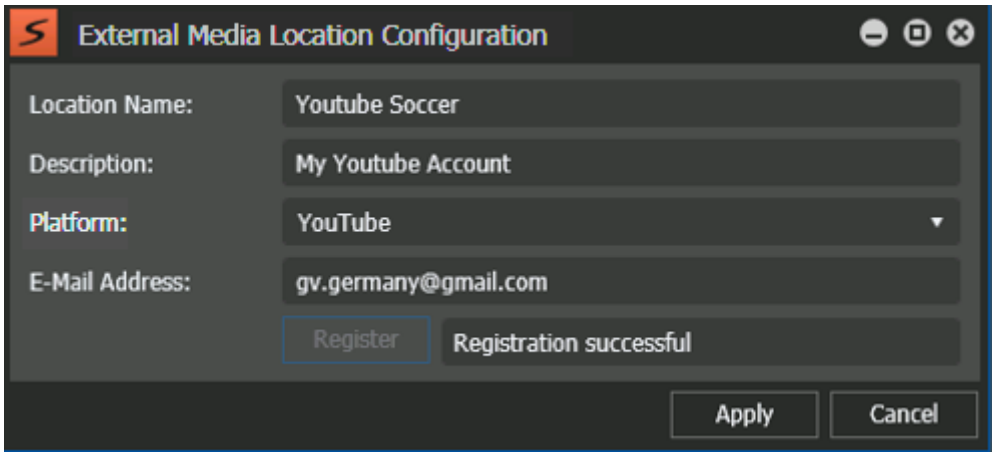
5. Enter your password in the login page, and click **Next**.

   The GV STRATUS configuration page opens.



6. Click **Allow** for GV STRATUS system to access and manage assets on your YouTube account.

   The YouTube location configuration is completed when the **Registration successful** message appears as below:



7. Click **Apply** to save the YouTube location configuration in the GV STRATUS Control Panel.

Next, configure the Publish External Media network rule.

Related Topics

Adding a publish external media network rule on page 621

External Media Engine Server set up process

Only systems with an External Media Engine require this process. Use SiteConfig for network setup and software install.

GV STRATUS supports the deployment of External Media Engine on the GV STRATUS Core server, Workflow Server, or a separate server. The Workflow Server or a separate server allows the separation of GV STRATUS Engines (Workflow-, Rules-, XCodeControl- and optional DataMover-Engine) away from the Core Server for large system setups where rules and workflows are used intensively paired with lots of file exports.

If you received your External Media Engine server already set up from Grass Valley, skip set up tasks and do the test task only.

1. *SiteConfig Workflow Server network set up* on page 802. Only systems with a Workflow Server or separate server require this process.
2. *SiteConfig External Media Engine software install* on page 820. Only systems with an External Media Engine require this process.
3. *SabreTooth External Media Engine license process* on page 822. Only systems with an External Media Engine require this process. The process is on the GV STRATUS Core server, Workflow Server, or a separate server.
4. *Configure External Media Engine* on page 822. Only systems with an External Media Engine with supported content management systems require this process.

SiteConfig Workflow Server network set up

Only systems with a Workflow Server require this process.

If you received your system already set up from Grass Valley, your Workflow Server or Servers are already included in the SiteConfig system description and set up on the network, so you can skip these tasks. Otherwise, work through the topics in this section.

Adding a Workflow Server to the SiteConfig system description

- Workflow Servers are racked, cabled, and powered on.
- The system description must contain a group.

This topic applies to a GV STRATUS server that is a Workflow Server.

1. In the **Network Configuration | Devices** tree view, right-click a group and select **Add Device**.

2. Configure settings for the device you are adding as follows:
   - Family: GV STRATUS
   - Device Type: GV STRATUS Server
   - Model: GV STRATUS Workflow Server
   - Name – This is the device name, as displayed in the SiteConfig device tree view and device list view. This name can be different than the host name (network name). You can accept the default name or enter a name of your choice. Devices in the tree view are sorted alphabetically.
   - Amount — Select the number of Workflow Servers, according to your system design.
   - Platform — Select **x64**.
   - Control network– Select the control network.
   - Starting Address – Select from the list of available addresses on the selected control network. If adding multiple devices, this is the starting address, with addresses assigned sequentially to each device added.
3. Click **OK** to save settings and close.

   SiteConfig adds the Workflow Server to the system description as a placeholder device.
4. Verify that unmanaged control network interface is configured correctly and modify if necessary.

Next, add the GV STRATUS server to the control network.

Adding a GV STRATUS server to the control network with SiteConfig

Use SiteConfig to configure network settings on a separate GV STRATUS server.

Before doing this task, make sure the GV STRATUS server is added as a placeholder device to the SiteConfig system description.

The following steps are the standard tasks for adding a device to the control network using SiteConfig. Use these steps for the GV STRATUS server you are adding.

1. Discover the device using SiteConfig device discovery.
2. Assign the discovered device to the placeholder device in the SiteConfig system description.
3. Modify the control network interface to ensure communication on the control network.
4. Modify the host name and/or device name as desired.
5. Ping the device to verify network communication.
6. Verify credentials to ensure SiteConfig can install software on the device.
7. Generate and/or add to host tables as appropriate for your network.

Related Topics

Adding a device to a network with SiteConfig on page 490
Adding a device to a network with SiteConfig on page 490

SiteConfig External Media Engine software install

Only systems with an External Media Engine require this process.

If you received your system pre-configured from Grass Valley, software is already installed, so you can skip these tasks. Otherwise, work through the tasks in this section as follows:

Add software role for the External Media Engine

Before doing this task, make sure devices are added to the SiteConfig system description with the correct family and device type. Refer to *Complete listing of device types, roles, and software packages for GV STRATUS devices* on page 194.

1. As appropriate for your system design and licensing, in your SiteConfig system description, configure role as follows:
   - For your Core Server, Workflow Server or a separate server, add the new role as follows:
     - GV STRATUS ExternalMedia Engine
2. Save SiteConfig and verify in `C:\ProgramData\Grass Valley\ConfigurationDataFiles\SiteConfig` that .scsd and .config files are saved to the server.

If you want to verify all your currently configured SiteConfig roles, refer to the complete list of roles and software packages.

Installing software for the External Media Engine

Use SiteConfig to install software for the External Media Engine.

- The server on which you are installing software is in the SiteConfig system description and communicating on the control network.
- The server on which you are installing software has its credentials set in SiteConfig to allow access.

1. Verify the SiteConfig roles currently assigned to the server. If the roles are not correct for your system design, add or remove roles accordingly. The role should be as follows:
   - GV STRATUS ExternalMedia Engine
2. Add the server to a deployment group, such as the GV STRATUS deployment group.
3. Add the following file to the deployment group:
   - `GrassValley_CoreServer_x.x.x.cab`, which contains the following cab file that apply to this device:
     - `GrassValley_STRATUS_ExternalMedia_x.x.x.cab`

   Refer to release notes for version numbers.
4. Do the SiteConfig **Check Software** operation on the server.
5. Verify that deployment tasks are set to **Install** for the files listed above.
6. Deploy software to the server.
7. Restart as prompted.
8. After deployment is complete, start the GV STRATUS External Media Engine Service.

Next, license the External Media Engine.

SabreTooth External Media Engine license process

The External Media Engine license should be installed on the GV STRATUS server with role of Common Services.

One STRATUS-EMNEXTERNALMEDIAENGINE license is required for the External Media Engine software component in your GV STRATUS system. This is a SabreTooth floating license. It is possible to deploy more than one External Media Engine per system. Each Engine must have its own license.

The External Media Engine also requires a license for each Social Media - Content Management System it supports. License for the Social Media - CMS system include the following:

- STRATUS-EMNVERIZON

If you received your system pre-configured from Grass Valley, licenses are already installed, so you can skip these tasks. Otherwise, do the following:

1. Refer to the license sheet that you received with your GV STRATUS license. The license sheet has the Sales Order number that you need.
2. On the GV STRATUS server with role of Common Services, run the SabreTooth License Manager, generate a unique ID, and send the email to Grass Valley requesting your license or licenses.

   Refer to this Topic Library for detailed licensing procedures.
3. When you receive your license file, use SabreTooth License Manager and install it on the server.

Configure External Media Engine

Only systems with an External Media Engine require this process.

If you received your system already set up from Grass Valley, your External Media Engine is already configured, so you can skip these tasks. Otherwise, work through the topics in this section.

Configuring settings: External Media Engine

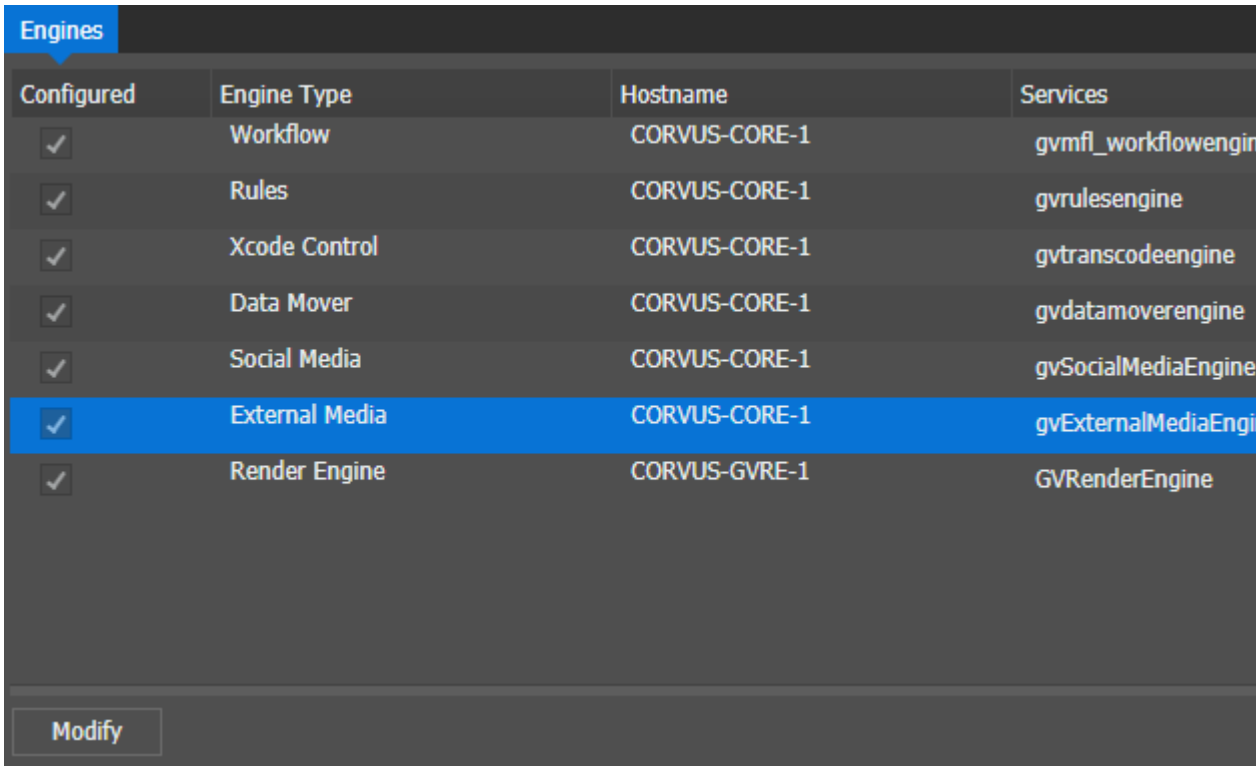
Only systems with an External Media Engine require this process.

If you received your system pre-configured from Grass Valley, your Engines settings are already configured so you can skip these tasks. Otherwise, work through this section to configure your Engines settings.

To locate these settings, click **Core | Engines**

Depending on the workflow and bandwidth requirements of your system, Grass Valley may provide a system design in which multiple engines of the same type run on one or more servers. Configure engines as specified by your system design.

1. In the Control Panel application, open Engines settings.



Settings are described as follows:

Setting or button	Description
Configured	Selects an Engine for which settings are saved.
Engine Type	The Engine components installed on the GV STRATUS server.
Hostname	The name of a GV STRATUS server that hosts the Engine.
Services	The services that support the Engine.
Action	Starts and stops the Engine service.
Status	Indicates if the Engine service is running or stopped.
Save	Saves current settings to selected GV STRATUS servers.
Cancel	Returns settings to their last saved state.
Modify	When an Engine type that is modifiable is selected, opens settings to configure the engine.
Refresh	Updates the list.

2. Click **Refresh** to make sure the list has the latest information from SiteConfig.

3. Verify that GV STRATUS server with role of External Media Engine is listed, and that the server's Engine Type is set to **External Media**.
4. In the **Configured** column, select each server with Engine Type: **External Media**.

   You must save settings at initial install/config and any time a GV STRATUS server with an Engine Type role is added, removed, or modified in SiteConfig.
5. Click **Save**.

   Settings are saved to the selected GV STRATUS servers.
6. Select the column with **External Media** engine type and click **Modify**.

   The **External Media** configuration page displays.

7. Configure settings as follows:

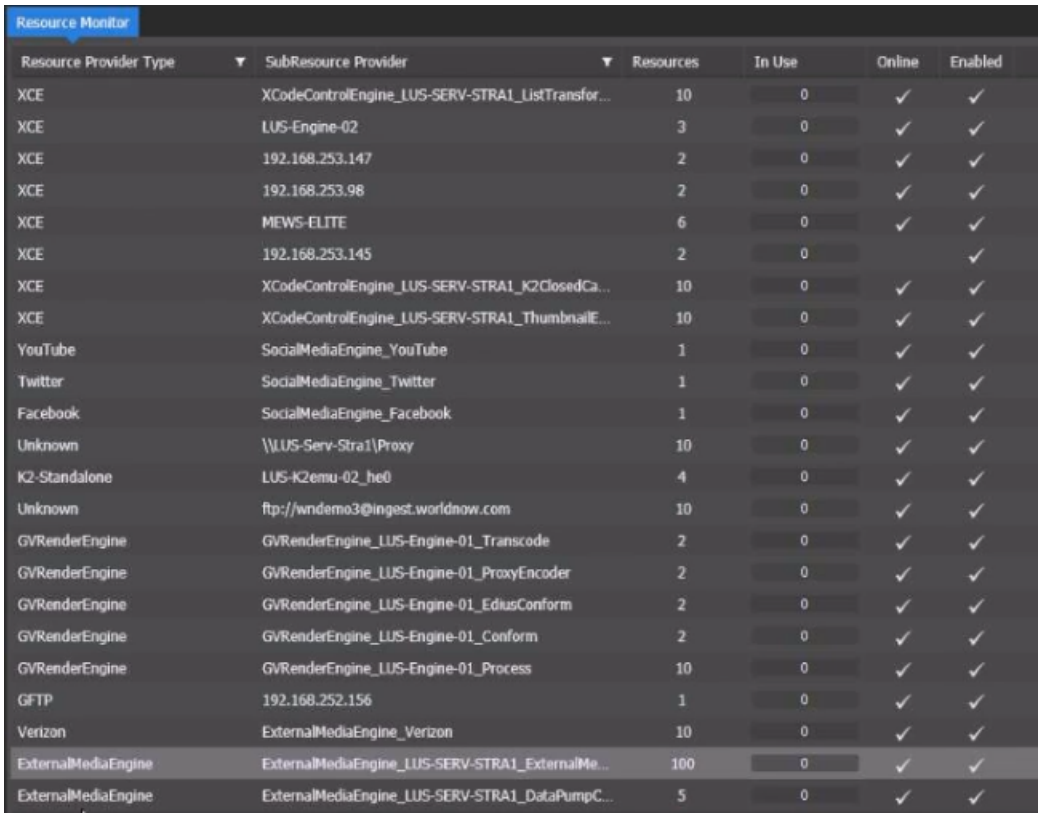
Setting or button	Description
Verizon : Maximum Concurrent Transfers	Limits the number of simultaneous transfers performed by the External Media engine on your configured CMS system account. You can configure the number of maximum concurrent transfers between 0-10 per Social Media - CMS platform. This setting is set to “0” if the Verizon site license is not installed.
General: Maximum Concurrent Transfers	Limits the total number of simultaneous transfers performed by the External Media engine for all Social Media CMS platforms. Use to balance resource load on the system hosting the engine. If the engine is deployed without an External Media Engine license, this setting is set to “0” and cannot be configured. You can set up to 5 maximum concurrent transfers for each External Media Engine volume license.

   Use these settings to balance resource load on the GV STRATUS server hosting the engine.

   NOTE: One volume license for the External Media Engine limits the maximum concurrent jobs to five (5). It is possible to deploy more than one Engine per system for a larger operation. Each Engine must have its own license.
8. Click **Save**.

   The External Media Engine settings are saved to the selected server.

The available resources are registered as individual resources in the Resource Management and listed in the Resource Monitor.



Resource Provider Type	SubResource Provider	Resources	In Use	Online	Enabled
XCE	XCodeControlEngine_LUS-SERV-STRA1_ListTransfor...	10	0	✓	✓
XCE	LUS-Engine-02	3	0	✓	✓
XCE	192.168.253.147	2	0	✓	✓
XCE	192.168.253.98	2	0	✓	✓
XCE	MEWS-ELITE	6	0	✓	✓
XCE	192.168.253.145	2	0		✓
XCE	XCodeControlEngine_LUS-SERV-STRA1_K2ClosedCa...	10	0	✓	✓
XCE	XCodeControlEngine_LUS-SERV-STRA1_ThumbnailE...	10	0	✓	✓
YouTube	SocialMediaEngine_YouTube	1	0	✓	✓
Twitter	SocialMediaEngine_Twitter	1	0	✓	✓
Facebook	SocialMediaEngine_Facebook	1	0	✓	✓
Unknown	\\LUS-Serv-Stra1\Proxy	10	0	✓	✓
K2-Standalone	LUS-K2emu-02_he0	4	0	✓	✓
Unknown	ftp://wndemo3@ingest.worldnow.com	10	0	✓	✓
GVRenderEngine	GVRenderEngine_LUS-Engine-01_Transcode	2	0	✓	✓
GVRenderEngine	GVRenderEngine_LUS-Engine-01_ProxyEncoder	2	0	✓	✓
GVRenderEngine	GVRenderEngine_LUS-Engine-01_EdiusConform	2	0	✓	✓
GVRenderEngine	GVRenderEngine_LUS-Engine-01_Conform	2	0	✓	✓
GVRenderEngine	GVRenderEngine_LUS-Engine-01_Process	10	0	✓	✓
GFTP	192.168.252.156	1	0	✓	✓
Verizon	ExternalMediaEngine_Verizon	10	0	✓	✓
ExternalMediaEngine	ExternalMediaEngine_LUS-SERV-STRA1_ExternalMe...	100	0	✓	✓
ExternalMediaEngine	ExternalMediaEngine_LUS-SERV-STRA1_DataPumpC...	5	0	✓	✓

Configure and authenticate Verizon location

Only systems that publish assets to Verizon CMS system require this process.

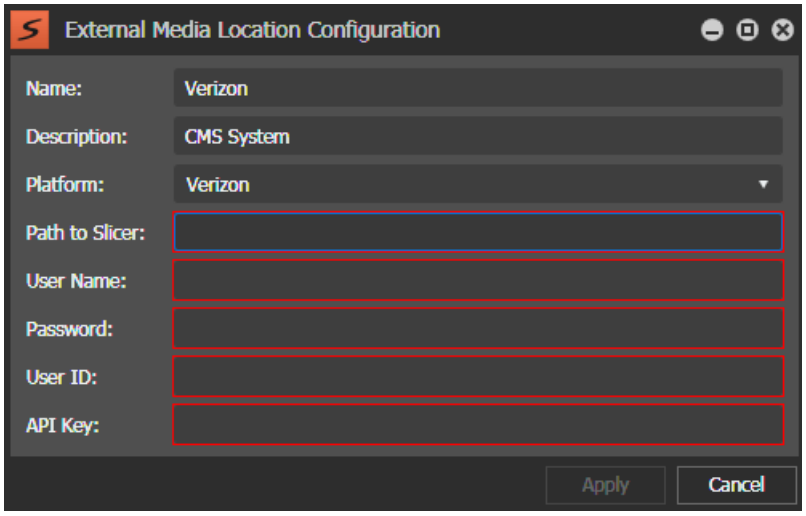
- The express/core server, workflow server, or separate server must be configured with the GV STRATUS External Media Engine role and deployed by SiteConfig.
- The External Media Engine must be running in GV STRATUS Control Panel Engines settings.

- Both "STRATUS-EMNEXTERNALMEDIAENGINE" and "STRATUS-EMNVERIZON" licenses are installed on the core/express or separate server.

Configure a location as follows:

1. In GV STRATUS Control Panel, navigate to **General | Locations Config | External Media | Add**.

   The **External Media Location Configuration** dialog appears.



2. Configure as follows:

Setting or button	Description
Name	The name of the location, as it appears in the application. This can be any name, as appropriate for your workflow. This identifies the Verizon location when publishing assets to your Verizon CMS system via the GV STRATUS application.
Description	Your description of the location.
Platform	Select **Verizon** from the drop-down list.

3. Enter the path to Slicer, the required software to upload content to Verizon platform.

   Verizon Content Management System requires its own encoder to be used in order to upload content to Verizon platform. Slicer is the software required for upload and must always be installed on the server where the External Media Engine is running. It must be downloaded from the Verizon web site by logging in to your Verizon Account, and click the download button to download the Slicer software at the bottom left of the screen.

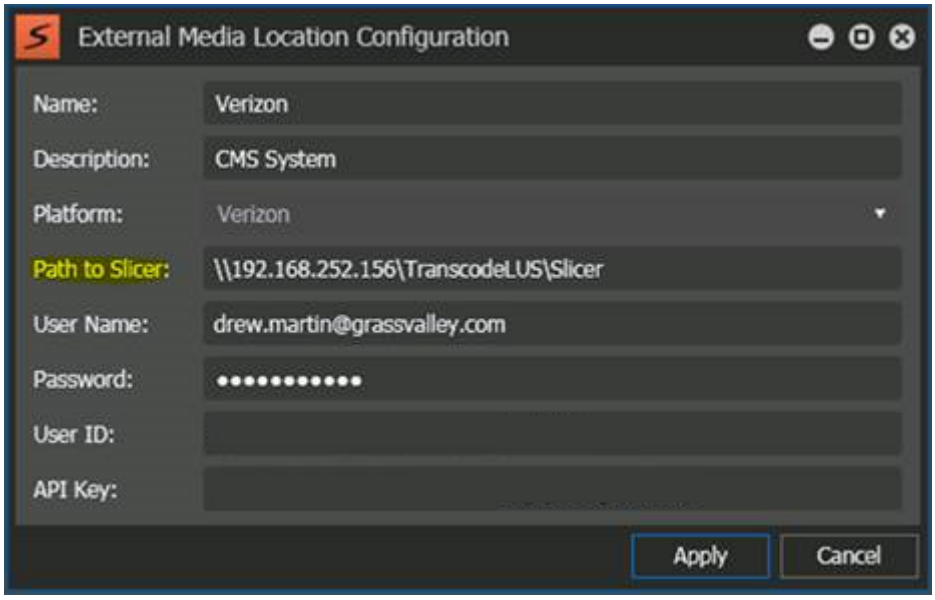
   The Slicer software should be installed where the External Media Engine is deployed, which is usually on the GV STRATUS Core Server. It is recommended to install Slicer into the following directory:

   ```
   C:\Program Files\Grass Valley\STRATUS ExternalMedia
   Engine\ExternalMediaExecutorVerizon\Slicer
   ```

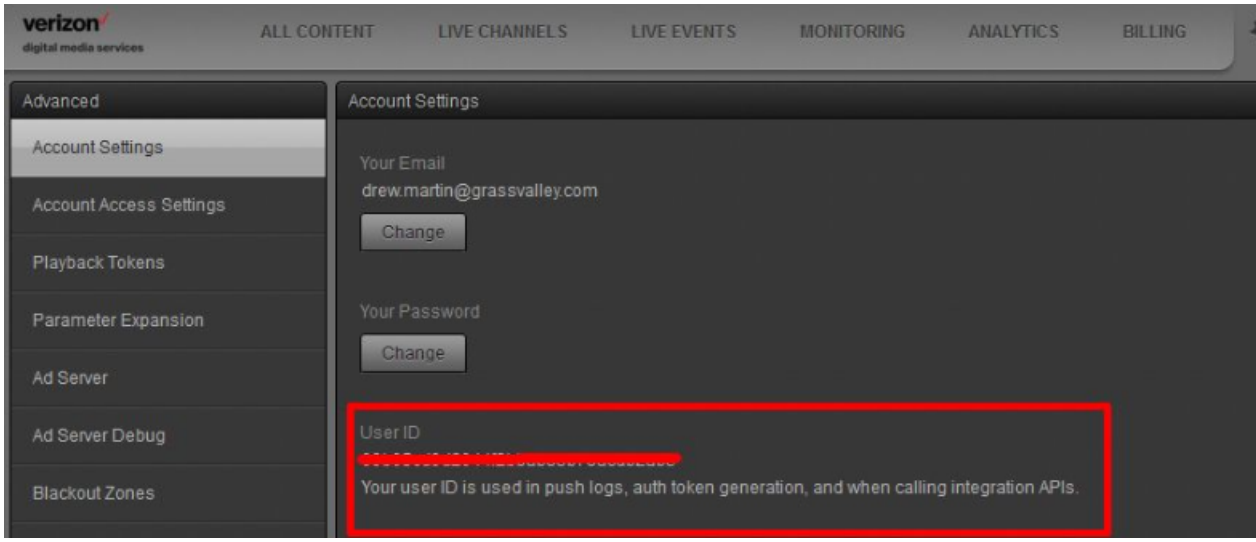
   After copying the Slicer software to the directory above, you must enter the path to Slicer in the **External Media Location Configuration** dialog. The Slicer software will be used by the External Media Engine for each upload.

   NOTE: If more than one External Media Engines exist, Slicer must be installed in the same directory on all servers where External Media Engine is installed.

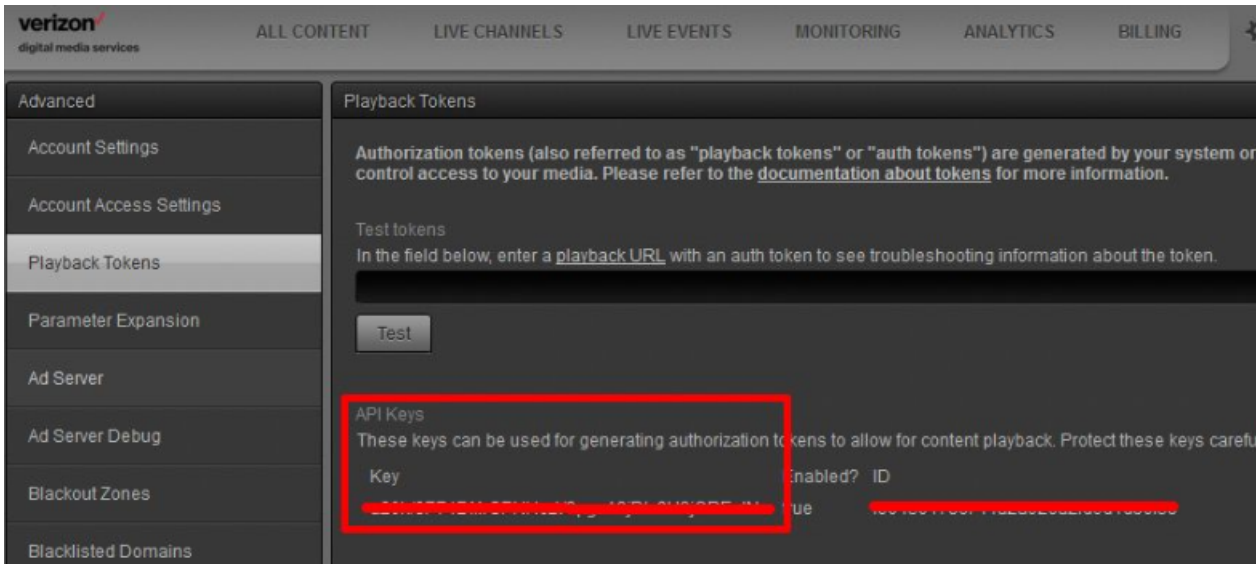
4. Enter your User name or email address, and enter the password.



5. To enter the User ID, you must procure it from your account on the Verizon web site.



6. Go to **Settings** and on the left hand side, select the **Account Settings** tab.
7. Copy the **User ID** and paste it into the **External Media Location Configuration** dialog.
8. To get the API Key, select the **Playback Tokens** tab.



9. Copy the **API Key** and paste it into the **External Media Location Configuration** dialog.
10. Click **Apply** to save the Verizon location configuration in the GV STRATUS Control Panel.

Next, configure the Publish External Media Network rule.

Related Topics

Adding a publish external media network rule on page 621

Standalone Database Server set up process

Only systems with a Standalone Database Server require this process. Use SiteConfig for network setup and software install.

If you received your system already set up from Grass Valley, your Standalone Database Server is already included in the SiteConfig system description and set up on the network, so you can skip these tasks. Otherwise, work through the topics in this section.

1. *SiteConfig Standalone Database Server network set up* on page 829. Only systems with a Standalone Database Server require this process.
2. *SiteConfig Standalone Database Server software install* on page 831. Only systems with a Standalone Database Server require this process.
3. *Backing up a database* on page 103. Only systems with the role of GV STRATUS Database Server require this process.
4. *Restoring a database* on page 706. Only systems with the role of GV STRATUS Database Server require this process.
5. *Setting the SQL server memory limit* on page 687. Only systems with the role of GV STRATUS Database Server require this process.

SiteConfig Standalone Database Server network set up

Only systems with a Standalone Database Server require this process.

If you received your system already set up from Grass Valley, your Standalone Database Server is already included in the SiteConfig system description and set up on the network, so you can skip these tasks. Otherwise, work through the topics in this section.

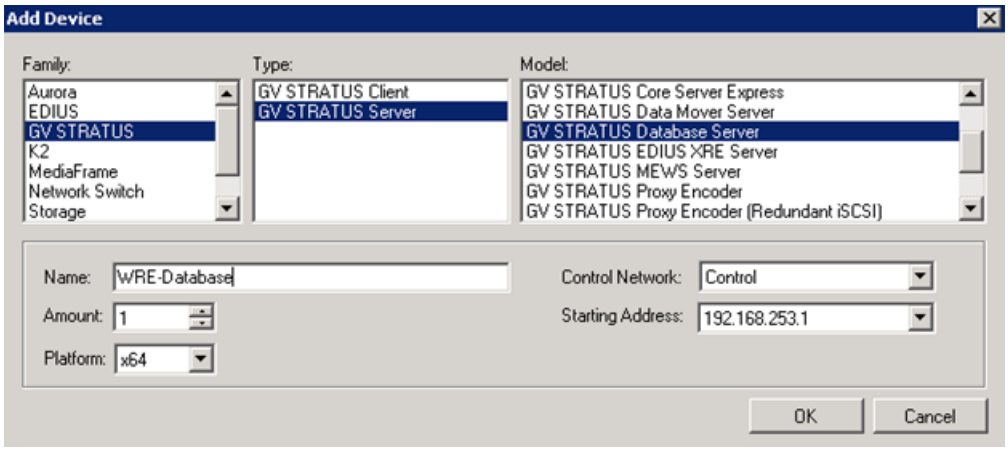
Adding a Standalone Database Server to the SiteConfig system description

- The system description must contain a group.

This topic applies to a Standalone Database Server.

1. In the **Network Configuration | Devices** tree view, right-click a group and select **Add Device**.

   The Add Device dialog opens.



2. Configure settings for the device you are adding as follows:

   - Family: GV STRATUS
   - Device Type: GV STRATUS Server
   - Model: GV STRATUS Database Server
   - Name – This is the device name, as displayed in the SiteConfig device tree view and device list view. This name can be different than the host name (network name). You can accept the default name or enter a name of your choice. Devices in the tree view are sorted alphabetically.
   - Amount — Select the number of databases, according to your system design.
   - Platform — Select **x64**.
   - Control network– Select the control network.
   - Starting Address – Select from the list of available addresses on the selected control network. If adding multiple devices, this is the starting address, with addresses assigned sequentially to each device added.

3. Click **OK** to save settings and close.

   SiteConfig adds the standalone database server to the system description as a placeholder device.

4. Verify that unmanaged control network interface is configured correctly and modify if necessary.

Next, add the standalone database server to the control network.

Adding a GV STRATUS server to the control network with SiteConfig

Use SiteConfig to configure network settings on a separate GV STRATUS server.

Before doing this task, make sure the GV STRATUS server is added as a placeholder device to the SiteConfig system description.

The following steps are the standard tasks for adding a device to the control network using SiteConfig. Use these steps for the GV STRATUS server you are adding.

1. Discover the device using SiteConfig device discovery.
2. Assign the discovered device to the placeholder device in the SiteConfig system description.
3. Modify the control network interface to ensure communication on the control network.
4. Modify the host name and/or device name as desired.
5. Ping the device to verify network communication.
6. Verify credentials to ensure SiteConfig can install software on the device.
7. Generate and/or add to host tables as appropriate for your network.

Related Topics

Adding a device to a network with SiteConfig on page 490
Adding a device to a network with SiteConfig on page 490

SiteConfig Standalone Database Server software install

Only systems with a Standalone Database Server require this process.

If you received your system pre-configured from Grass Valley, software is already installed, so you can skip these tasks. Otherwise, work through the tasks in this section as follows:

Setting deployment options

- A software package must be assigned to the deployment group and applicable deployment tasks must be displayed in the Tasks area.

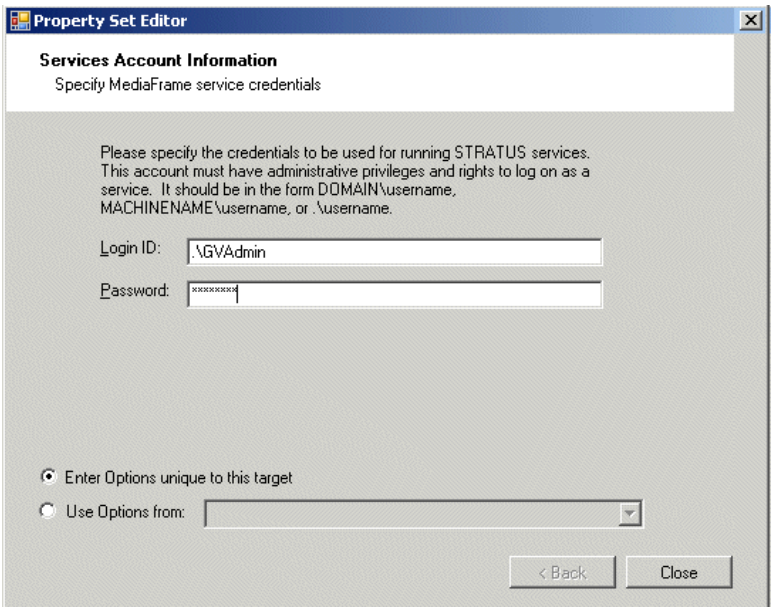
1. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.
2. In the Tasks list view, view tasks and determine if you must set deployment options.

   Tasks that need to have deployment options set display in the Details column a message stating "Deployment options required."

   If you select a task that needs to have its deployment options set, the Start Deployment button is disabled and the message is displayed next to the button.
3. Do one of the following to set deployment options:
   - Double-click the task.
   - Select the task and click the **Options** button.

   A wizard opens.

4. Work through wizards and set deployment options for GV STRATUS software as follows:

Software	Deployment options
GrassValley_STRATUS_CommonServices GrassValley_STRATUS_ControlPanelService GrassValley_STRATUS_CoreServices GrassValley_STRATUS_CRArchive_MDI GrassValley_STRATUS_Databases GrassValley_STRATUS_DataMover GrassValley_STRATUS_DIVA_MDI GrassValley_STRATUS_ExternalMedia GrassValley_STRATUS_FlashNet_MDI GrassValley_STRATUS_GFTP_MDI GrassValley_STRATUS_HttpProxyServer GrassValley_STRATUS_IngestServices GrassValley_STRATUS_Masstech_MDI GrassValley_STRATUS_MediaFlow GrassValley_STRATUS_MEWS GrassValley_STRATUS_Proxy_MDI GrassValley_STRATUS_ProxyStreamingService GrassValley_STRATUS_RenderEngine GrassValley_STRATUS_Rules GrassValley_STRATUS_ScheduledTransferEngine GrassValley_STRATUS_SocialMedia GrassValley_STRATUS_Summit_MDI GrassValley_STRATUS_TrafficGateway GrassValley_STRATUS_Transcode GrassValley_STRATUS_WebApps GrassValley_STRATUS_WebClient GrassValley_DeviceKeyService GrassValley_LogManager GrassValley_LogViewer	 Use the local system account if your system is on a workgroup or if it's on a domain but uses the local system account in SQL. Use a domain\admin account if the account was previously mapped in SQL to the MediaFrame, MediaFlow, RulesEngine and WFPersistence databases. Entering account credentials allows you to use the **Use options from** feature for all other devices of the same type. Once you enter the account credentials this way on the first device, it becomes the template from which options for other devices are copied.

5. If you have multiple devices of the same type, you can enter deployment options for one of them using the wizard. Then, when you bring up the same wizard on every device, you can choose the **Use options from** radio button and select the first device for which you set options.

   SiteConfig copies the options you set for the first device and fills in the blanks on the wizard.

Installing software on a standalone Database Server

Use SiteConfig to install software on the standalone Database server.

- The server on which you are installing software must be in the SiteConfig system description and communicating on the control network.
- The server on which you are installing software must have its credentials set in SiteConfig to allow access.

1. Verify the SiteConfig roles currently assigned to the server. If the roles are not correct for your system design, add or remove roles accordingly. Roles are as follows:
   - GV STRATUS Database
   - GV Log Manager
   - GV Embedded Security Manager
2. Add the server to a deployment group, such as the GV STRATUS deployment group.
3. Add the following files to the deployment group:
   - *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
     - *GrassValley_STRATUS_Databases_x.x.x.cab*
     - *GrassValley_LogManager_x.x.x.cab*
     - *GVEmbeddedSecurityManager_x.x.x.cab*

   Refer to release notes for version numbers.
4. Do the SiteConfig **Check Software** operation on the server.

   NOTE: If an "Unable to copy ... to target" error appears for a device that has the Grass Valley Embedded Security solution, apply the* Embedded Security *solution one-time initial deployment process to the device. After the one-time process is complete the error does not appear and it is no longer necessary to put* Embedded Security *in Update mode.
5. Verify that deployment tasks are set to **Install** for the files listed above.

   If a WFRegMon install task appears, install it as well. It is required to support Grass Valley software installers. There is no uninstall task.
6. Deploy software to the server.
7. Restart as prompted.

Next, go to **Core | STRATUS Core Services | Primary Site** in the GV STRATUS Control Panel and select the standalone Database Server from the **STRATUS Database Server** setting.

Related Topics

STRATUS Core Services settings on page 296

Configure GVAdmin account

This task applies to a computer on which the following is installed:

- GV STRATUS Database Server
- GV STRATUS/EDIUS client PC

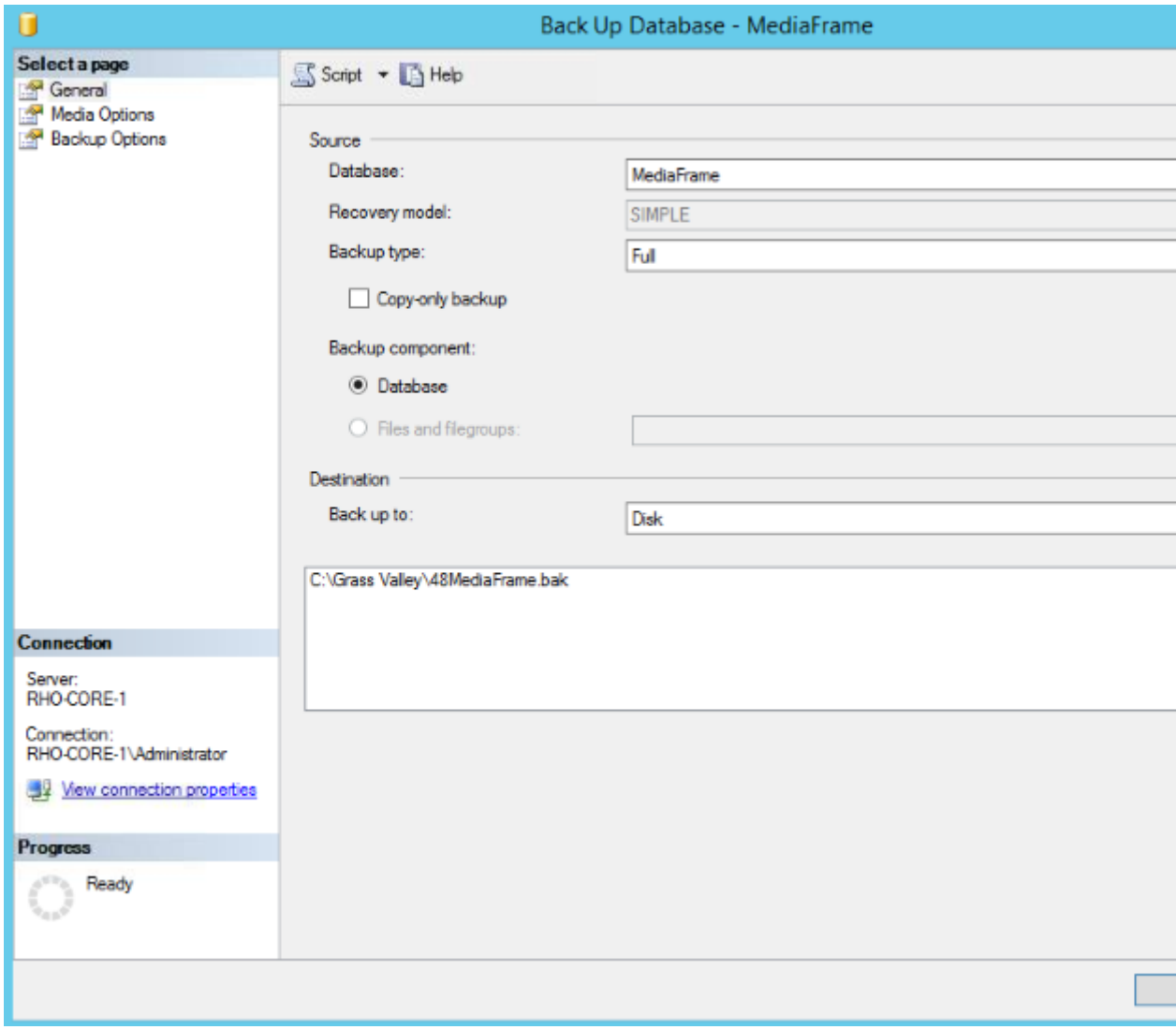
Add the internal system account, which by default is GVAdmin, to the Administrators group on the computer.

Backing up a database

Grass Valley recommends that you back up all the databases of the GV STRATUS system before upgrading to the latest version of the software or before moving your databases from the GV STRATUS Core server to a standalone Database Server. With a database backup, you can avoid any lost of feed schedules and the need to key in everything again in case of a system crash. The backup could also be placed on another machine or an external drive for extra precaution.

1. Open and log in to Microsoft SQL Server Management Studio.
2. In the tree-view expand the **Databases** node and identify the databases of the GV STRATUS system to backup, which are the following:
   - ISDB
   - MediaFlow
   - MediaFrame
   - RulesEngine
   - WfPersistence

3. Right-click on a database and select **Tasks | Back Up**.



4. On the General page, select a database to be backed up from the **Database** drop-down list.
5. Select **Full** on the **Backup type** drop-down list.
6. In the Destination section, click **Add** and select the backup destination.
7. On the Media Options page, select **Back up to the existing media set** and **Overwrite all existing backup sets**.
8. On the Backup Options page, enter the name of the backup database.
9. Click **OK**.
10. Repeat for other databases of the GV STRATUS system that you are backing up.

Restoring a database

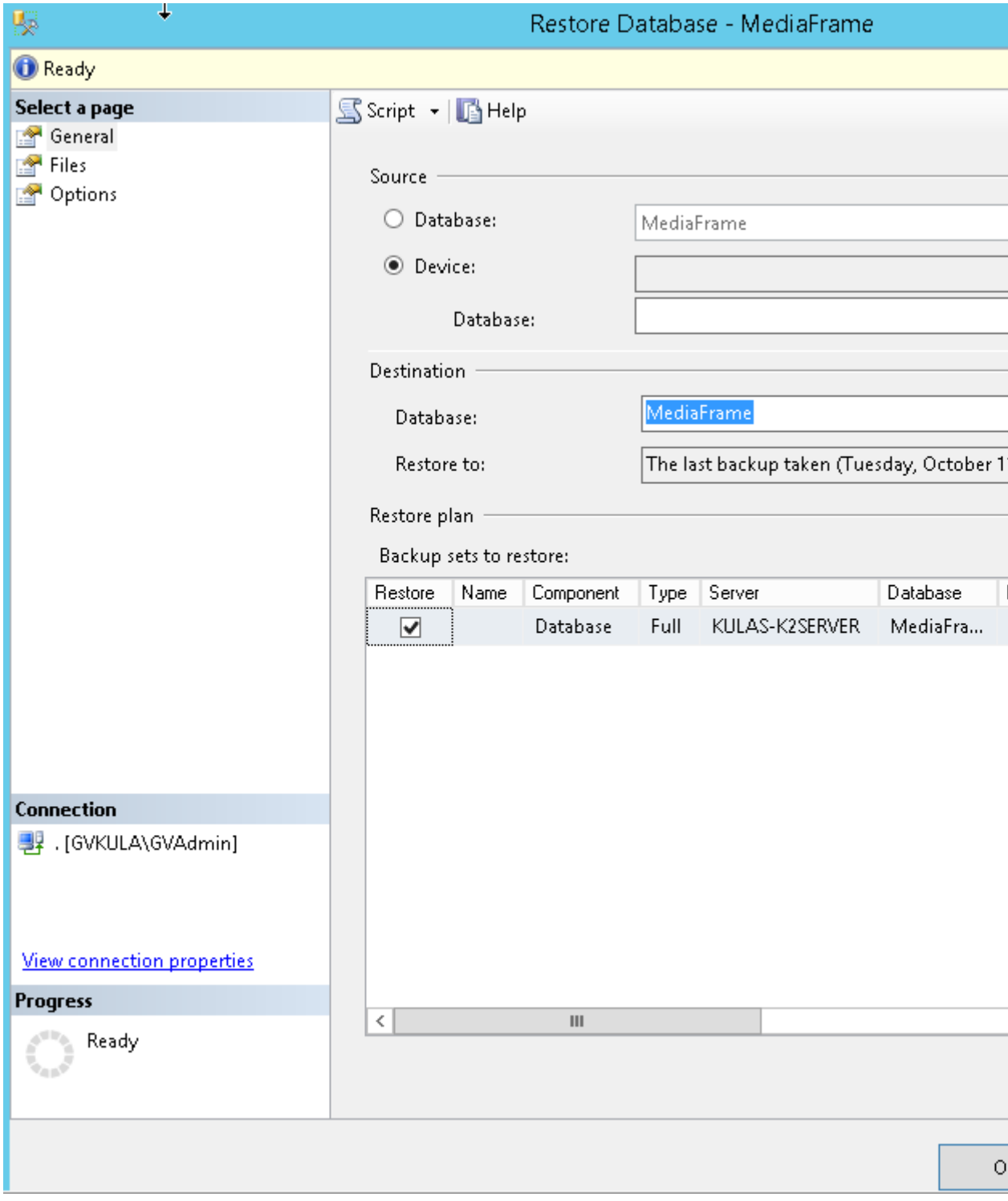
- The back up process of all GV STRATUS databases have been completed and backup locations already identified.

- Ensure that previously existing databases with the same name have been deleted from the restore destination.
- For the restore at a new standalone Database server, delete the previously installed GV STRATUS databases because they were automatically created during the initial installation via SiteConfig.

1. On the GV STRATUS Core server do the following:
   a) In Internet Information Services (IIS) Manager, stop the IIS Web server.
   b) In the Windows operating system Control Panel, stop all of the GV services.
2. Open and log in to Microsoft SQL Server Management Studio.
3. In the tree-view expand the **Databases** node and identify the databases of the GV STRATUS system to restore, which are the following:
   - ISDB
   - MediaFlow
   - MediaFrame
   - RulesEngine
   - WfPersistence

4. Right-click on a database, and select **Tasks | Restore | Database**.

   The Restore Database window opens.



5. In the **Source** section, select **Device** and click **...**.

6. Click **Add**, navigate to the database backup location, select the backup file, click **OK** and **OK**.

   If there are multiple backup files, check the date of the file and make sure you are selecting the correct file.

7. In the **Destination** section, select the database.
8. In the **Restore plan** section, select the checkbox under the **Restore** column to select the backup database to be restored.
9. In the **Options** page, do the following steps:
   - In the Restore options section, check the box to **Overwrite the existing database**.
   - In the Server connections section, check the box to **Close existing connections to destination database**, if possible.
10. Click **OK**.
11. Restart the GV STRATUS Core server.

    The GV STRATUS database is now restored.

12. If you are switching database servers, start the IIS Web server in Internet Information Services (IIS) Manager.
13. On the GV STRATUS Control Panel, click **Core | STRATUS Core Services | Primary Site** and select the Database Server Machine from the **STRATUS Database Server** drop-down list.

    Changing the **STRATUS Database Server** setting on the GV STRATUS Control Panel starts the switch over process to the newly added standalone Database Server.

14. If there were changes to assets/metadata on the system since the database backup, select **Core | Search Index Config** in the GV STRATUS Control Panel and click **Reset Index**.

Related Topics

STRATUS Core Services settings on page 296

Setting the SQL server memory limit

The SQL server depends on memory to cache information from databases on disk for fast access. If more data exists on disk than can be held in memory, the SQL server performance will degrade.

To avoid low memory issues on the GV STRATUS Core server or the standalone Database server, the memory that should be assigned to SQL server depends on the memory size of the physical device.

Grass Valley recommends the setting of SQL server memory limit according to the table below:

Physical Memory	SQL server memory limit	Approximate number of assets supported
12 GB	5120 MB	200,000 – 350,000
16 GB	8192 MB	320,000 – 560,000
32 GB	18,432 MB	720,000 – 1,260,000
48 GB	32,768 MB	1,280,000 – 2,240,000
64 GB	47,104 MB	1,900,000 – 3,360,000

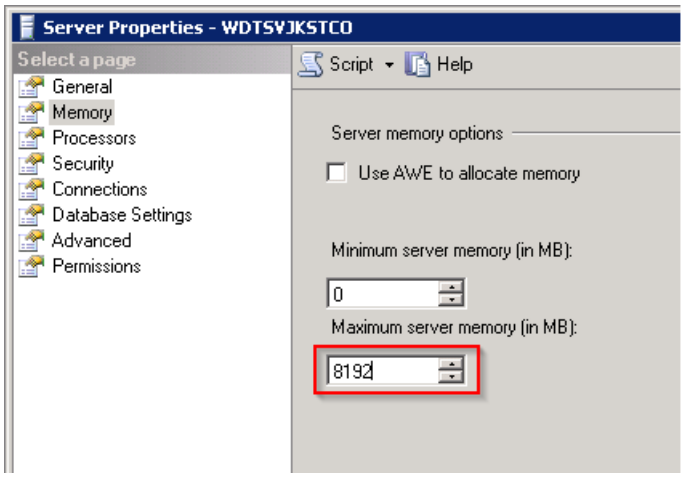
Set the SQL server memory limit as follows:

1. From the Windows desktop click **Start | All Programs | Microsoft SQL Server** and select **Microsoft SQL Server Management Studio**.

   Microsoft SQL Server Management Studio opens.
2. Log on as an Administrator.
3. Right-click on the SQL server name and select **Properties** from the context menu.

   The **Server Properties** dialog opens.
4. Click **Memory**.

   The Memory page opens.



5. In the **Maximum server memory** setting, enter your SQL server memory limit in MB.
6. Click **OK**.

A restart of the server is not necessary, but recommended.

GV STRATUS Control Panel system configuration process

All systems require this process. Use GV STRATUS Control Panel to configure the GV STRATUS system for your site's workflow.

Grass Valley recommends the GV STRATUS Control Panel is only configured on the Core server and multiple copies are not opened simultaneously on different machines.

In an operational GV STRATUS system, GV STRATUS servers must be running and logged on to the Windows operating system. The logon account must be the GV STRATUS system internal system account. The internal system account is the account that the GV STRATUS system uses to access assets and some internal system functions. By default this is the GVAdmin account. If the GVAdmin account does not exist, GV STRATUS Control Panel will be unusable.

The GVAdmin account can be disabled or removed when delegate account credentials had been reconfigured after the software install. For the delegate account on an existing system, it is important that the new password must be configured in GV STRATUS Control Panel *first*, and then changed for the corresponding workgroup or domain user. If not done in this order, GV STRATUS Control Panel will be unusable until the password for the currently configured delegate user is reverted to its previous value, at which point the credentials can be modified in the correct order.

If you received your GV STRATUS system pre-configured from Grass Valley, skip configuration tasks and do the test tasks only.

1. *Configure Control Panel Service Host in applications* on page 840. All systems require this process. Configure SiteConfig and K2Config to reference the Control Panel Service Host.
2. *Install the GV STRATUS Control Panel application with SiteConfig* on page 841. All systems require this process.
3. *Configuring GV STRATUS Control Panel: Required settings* on page 842. All systems, all workflows, require this process. Configure GV STRATUS Database, proxy, K2 Summit, and other settings that the GV STRATUS system requires regardless of the site's unique workflow or system design.
4. *Test GV STRATUS configuration settings* on page 856. All systems require this process.
5. *Reference to settings: Required and optional* on page 296. All systems require GV STRATUS Control Panel settings, as appropriate for the site's unique workflow and GV STRATUS licenses.

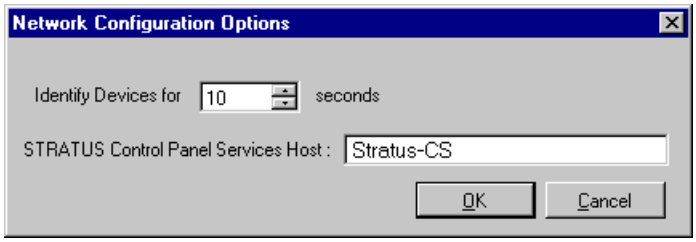
Configure Control Panel Service Host in applications

All systems require this process. Configure SiteConfig and K2Config to reference the Control Panel Service Host.

The GV STRATUS server with the SiteConfig role of Common Services hosts the Control Panel Service. Typically, this is the GV STRATUS Core server. To communicate configuration information, multiple applications must be configured to reference this GV STRATUS server.

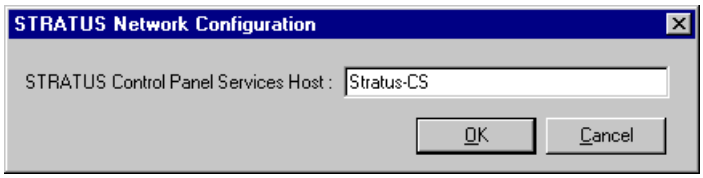
1. Enter the GV STRATUS Core server name in SiteConfig as follows:

   In the SiteConfig application, click **Tools | Options | Network Configuration**.



2. Enter the GV STRATUS Core server name in K2Config as follows:

   In the K2Config application, click **STRATUS | Network Configuration**.



Install the GV STRATUS Control Panel application with SiteConfig

All systems require this process.

- The devices to which you are installing software must be in a deployment group.
- For the software you are installing, the managed package must be added to the deployment group.
- The SiteConfig "Check Software" operation must have been recently done on the devices to which you are installing software.
- The PC to which you are installing the application must meet system requirements.
- The PC to which you are installing the application must have the SiteConfig role of GV STRATUS Control Panel.
- The `GrassValley_STRATUS_ControlPanel_`x.x.x.cab must be added to the deployment group. Refer to release notes for version information.

With the installation instructions in this section, you use SiteConfig from a network connected control point PC and remotely install/upgrade software simultaneously on your system devices. This is the recommended process for software installation and upgrades. When installing the GV STRATUS application or the GV STRATUS Control Panel application, if SiteConfig installation is not possible, you may install manually on the local PC. You must uninstall before installing.

1. In the **Software Deployment | Deployment Groups** tree view, select the device or the group of devices to which you are installing software. You can select a Device node, a Deployment Group node, or the All Deployment Groups node.

   The corresponding software deployment tasks are displayed in the Tasks list view.

2. Identify one or more deployment tasks listed as "Install" in the Action column.
3. For the software you are installing, select the **Deploy** check box in the row for the install task.

   If a WFRegMon install task appears, install it as well. It is required to support Grass Valley software installers. There is no uninstall task.

4. Before starting the deployment session, verify the following for the installation deployment tasks:

   - The Deploy checkbox is selected.
   - The software package is the correct version.
   - The Action column reports Install.
   - The Status column indicates the planned icon.
   - The Details column does not indicate that deployment options are required.

5. Click the **Start Deployment** button.

   Deployment tasks run and software is installed. Progress is reported in both the Status and Details columns.

   NOTE: If an "Unable to copy ... to target" error appears for a device that has the Grass Valley Embedded Security solution, apply the* Embedded Security *solution one-time initial deployment process to the device. After the one-time process is complete the error does not appear and it is no longer necessary to put* Embedded Security *in Update mode.

6. Monitor progress as indicated by both the Status and Details column. When finished, the Status column indicates complete.

Related Topics

System requirements for GV STRATUS client PC on page 52

Logging on to the GV STRATUS Control Panel application

When you log on, use administrator credentials that give you access to all your GV STRATUS system devices.

Grass Valley recommends the GV STRATUS Control Panel is only configured on the Core server.

1. From the Windows desktop, do one of the following:
   - Open the **STRATUS Control Panel** icon shortcut.
   - Click **Start | All Programs | Grass Valley** and click the **STRATUS Control Panel** icon.

   A Log On dialog box opens.
2. Enter your user name.

   If you use domain credentials, enter in format `<domain>\<username>`. For example, if your domain is "gv" and your username is "GVuser", enter `gv\GVuser`.

   If you have successfully logged on before, select your user name from the drop-down list.
3. Enter your password.
4. Verify that the application is correctly referencing the Control Panel Services Host as follows:
   a) If not already showing, click the **Options** button to show settings.
   b) Verify or enter the hostname (do not enter the IP address) of the GV STRATUS server with the SiteConfig role of GV STRATUS Control Panel Service. This is the Control Panel Services Host. In most systems this is the main GV STRATUS Core server.

      If you have successfully logged on before, your hostname is automatically populated. You can select a hostname from the drop-down list if you have previously logged on to multiple hosts in your operation.
5. Click **Log On**.

The application opens.

Related Topics

About groups and users on a GV STRATUS system on page 37

Configuring GV STRATUS Control Panel: Required settings

All systems, all workflows, require this process. Configure GV STRATUS Database, proxy, K2 Summit, and other settings that the GV STRATUS system requires regardless of the site's unique workflow or system design.

If you received your system pre-configured from Grass Valley, your required settings are already configured, so you can skip these tasks. Otherwise, work through the topics in this section.

This section provides the configuration steps that are required for all systems. Follow the topics in the section sequentially to configure the required settings.

Related Topics

About Control Panel, SiteConfig, and K2Config settings on page 433

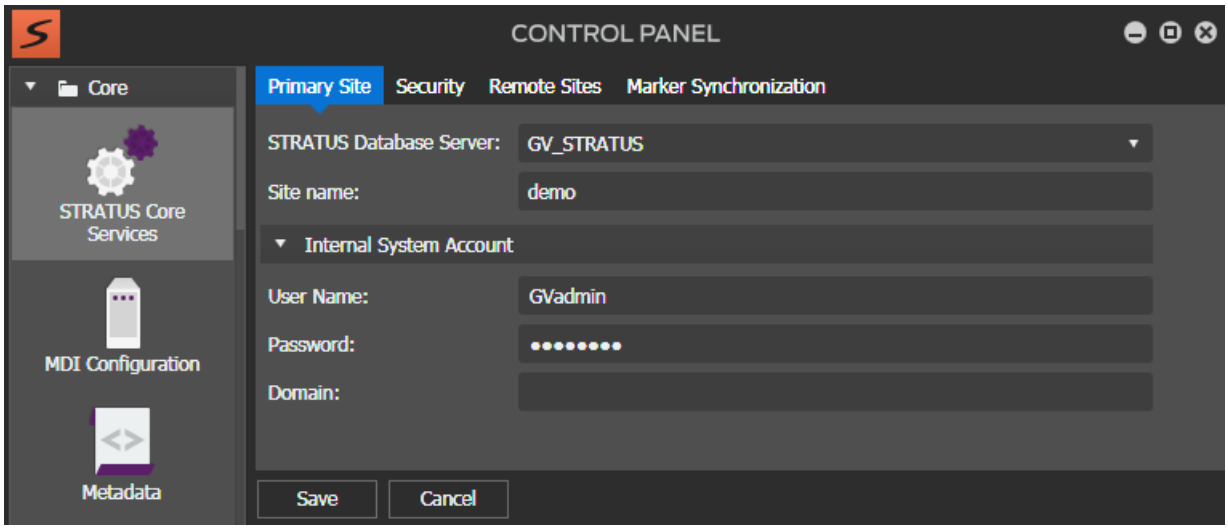
Configuring STRATUS Core Services settings: Required

All systems, all workflows, require this process.

If you received your system pre-configured from Grass Valley, your STRATUS Core Services settings are already configured so you can skip these tasks. Otherwise, work through this section sequentially to configure your STRATUS Core Services.

To locate these settings, click **Core | STRATUS Core Services | Primary Site**

1. In the Control Panel application, open General settings.



2. Configure as follows:

Setting or button	Description
GV STRATUS Core Server	The GV STRATUS server with SiteConfig role of GV STRATUS Core Services. In a typical system, select the server from the drop-down list. The server or servers available on this drop-down list are provided by SiteConfig. For some system configurations, you can also enter the GV STRATUS server manually.
GV STRATUS Database Server	The GV STRATUS server with SiteConfig role of GV STRATUS Database. In a typical system, select the server from the drop-down list. The server or servers available on this drop-down list are provided by SiteConfig. The GV STRATUS Database Server is currently supported on the GV STRATUS Express, Core, and separate standalone servers.
Site name	Customizable name that can be set for the local GV STRATUS site.
Internal System Account User Name, Password, Domain	The internal system account is the account that the GV STRATUS system uses to access assets and some internal system functions. By default this is the GVAdmin account. If your site policies require a different account, such as a fully qualified domain account, that account must be configured here and throughout the GV STRATUS system. ***NOTE: Do not enter a domain or otherwise modify account settings except under the supervision of qualified Grass Valley Support personnel. Extensive system configuration is required to achieve a working GV STRATUS system.***
Save	Saves current settings.
Cancel	Returns settings to their last saved state.

3. Click **Save**.
4. If you changed Marker Synchronization settings, restart the GV STRATUS Core server and the K2 system.

Next, configure Proxy Config settings.

Related Topics

STRATUS Core Services settings on page 296
About Control Panel, SiteConfig, and K2Config settings on page 433
Rules engine settings on page 334
Enabling and disabling rules on page 636

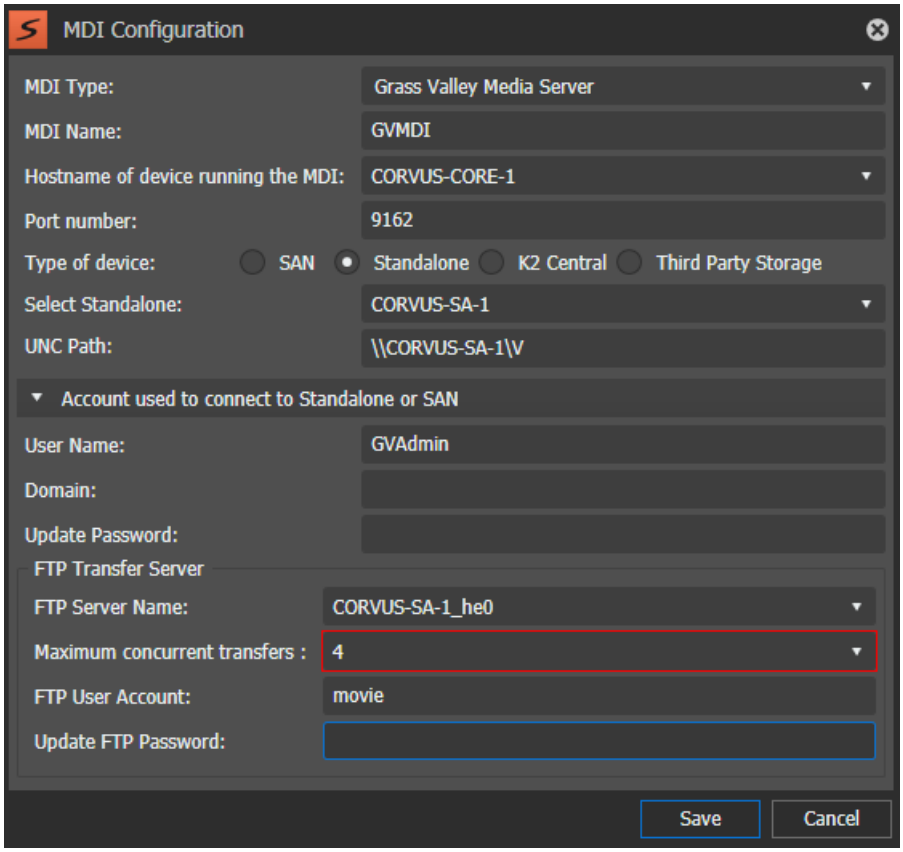
Configuring Grass Valley Media Server MDI settings: Required for standalone

All systems with one or more standalone K2 Summit systems require this process.

If you received your system pre-configured from Grass Valley, your Grass Valley Media Server MDI settings are already configured so you can skip these tasks. Otherwise, work through this section sequentially to configure your Grass Valley Media Server MDI settings.

To locate these settings, click **Core | MDI Configuration | Add | Grass Valley Media Server**

1. In the Control Panel application, open Grass Valley Media Server MDI Configuration settings.



2. Configure one Summit MDI for each standalone K2 Summit system on your GV STRATUS system.

   When you have multiple Grass Valley Media Server MDIs, they must each have their own process port number. For this purpose, numbers 9160 - 9169 increment in the **Port** field.

3. Configure as follows:

Setting or button	Description
MDI Type	The Managed Device Interface (MDI) type to which these settings apply.
MDI Name	A name for this instance of the MDI type. Do not use spaces in the MDI name. The MDI name could be renamed later, if desired. ***NOTE: After renaming the MDI, you must restart the Render Engine server and its services. Then, reconfigure other settings on the Control Panel (such as Send Destinations, Rules, K2 Central storage, etc.) to use the new Grass Valley Media Server MDI name.***
Hostname of device running the MDI	The name of the GV STRATUS server that hosts this MDI.
Port number	The process port for this instance of the MDI type. Each instance must have its own process port. Port numbers must be in range 9160-9169.
Type of K2 device	Specifies either SAN-attached K2 Summit system , Standalone K2 Summit system, K2 Central system, or Third Party Storage system. When Standalone is selected, settings are as follows.
Select Standalone	The standalone K2 Summit system that this MDI accesses.
UNC Path	The UNC path to the standalone K2 Summit system.
User Name	The user name that this MDI uses to access the K2 Summit system. This is the internal system account, which by default is GVAdmin.
Domain	If on a domain, the domain that manages the account that this MDI uses to access the K2 Summit system. ***NOTE: Do not enter a domain or otherwise modify account settings except under the supervision of qualified Grass Valley Support personnel. Extensive system configuration is required to achieve a working GV STRATUS system.***
Update Password	The password that this MDI uses to access the K2 Summit system.
FTP Server Name	The FTP server name for the remote K2 Summit system. For the typical system where there is a separate FTP network, this is the name of the K2 SAN's FTP server with the `_he0` suffix added. The `_he0` suffix specifies the FTP network.
Maximum concurrent transfers	The maximum number of concurrent transfers allowed. The maximum is set in K2Config. You may select the maximum or a lesser number as designed for your system. The number of concurrent transfers as well as the device status can be checked once the system is configured in Resource Monitor of the GV STRATUS Control Panel.
FTP User Account	The FTP user name for the K2 Summit system this MDI accesses. Typically this is `movie`.

Setting or button	Description
Update FTP Password	The FTP password for the K2 Summit system this MDI accesses. When this field is blank the system automatically uses the default password.

4. Click **Save**.
5. If you changed a standalone MDI setting, you must restart the GV STRATUS Core server system and the K2 Summit system. If SAN MDI settings, you must restart the entire K2 SAN system, including K2 Media Servers, attached K2 Summit systems, and other SAN clients.

   If you are changing multiple Grass Valley Media Server MDI settings, you can make all those settings first before restarting these systems. Restarting the systems once is sufficient for multiple Grass Valley Media Server MDI settings changes.
6. Repeat steps to configure an MDI for each standalone K2 Summit system on your GV STRATUS system.

Next, if your GV STRATUS system accesses a K2 SAN, configure Grass Valley Media Server MDI SAN settings.

Related Topics

MDI and Encoder logical names convention on page 442

Grass Valley Media Server MDI standalone settings on page 304

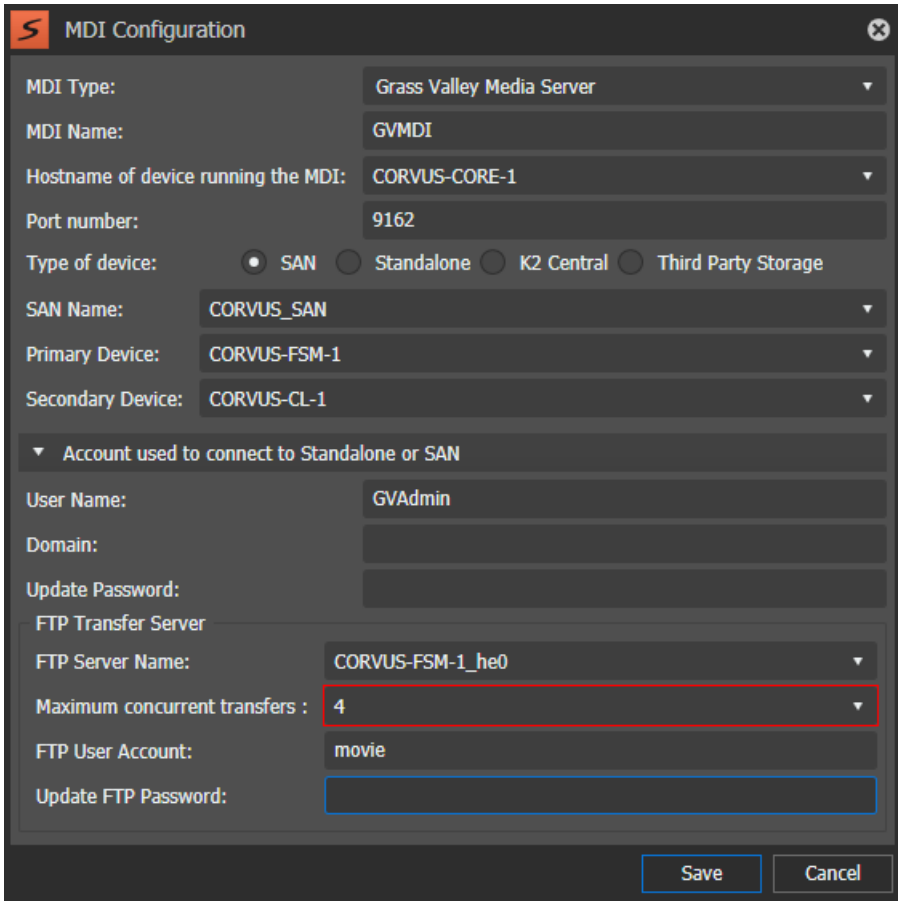
Configuring Grass Valley Media Server MDI settings: Required for SAN

All systems with one or more K2 SANs require this process.

If you received your system pre-configured from Grass Valley, your Grass Valley Media Server MDI settings are already configured so you can skip these tasks. Otherwise, work through this section sequentially to configure your Grass Valley Media Server MDI settings.

To locate these settings, click **Core | MDI Configuration | Add | Grass Valley Media Server**

1. In the Control Panel application, open **Grass Valley Media Server** MDI Configuration settings.



2. Designate SAN-attached K2 Summit systems to be the primary and secondary device for the entire K2 SAN storage system. Configure a Grass Valley Media Server MDI for those K2 Summit systems on the K2 SAN.

   - If you have no other K2 Summit systems, neither standalone systems nor K2 SAN systems, when you configure the **Port** field, accept the default value. If required by your system design, you can configure a port number in the allowed range.
   - If you have multiple standalone K2 Summit systems, multiple K2 SAN systems, a combination of standalone and K2 SAN systems, a K2 Central system, or a SMB storage system, each system must have its own Grass Valley Media Server MDI.

3. Configure as follows:

Setting or button	Description
MDI Type	The Managed Device Interface (MDI) type to which these settings apply.
MDI Name	A name for this instance of the MDI type. Do not use spaces in the MDI name. The MDI name could be renamed later, if desired. ***NOTE: After renaming the MDI, you must restart the Render Engine server and its services. Then, reconfigure other settings on the* GV STRATUS Control Panel *(such as Send Destinations, Rules, K2 Central storage, etc.) to use the new Grass Valley Media Server MDI name.***
Hostname of device running the MDI	The name of the GV STRATUS server that hosts this MDI.
Port number	The process port for this instance of the MDI type. Each instance must have its own process port. Port numbers must be in range 9160-9169.
Type of K2 device	Specifies either SAN-attached K2 Summit system , Standalone K2 Summit system, K2 Central system, or Third Party Storage system.
SAN Name	The name of the K2 SAN, as named in K2Config. You can also enter the name of K2 Central system or third party storage device, if you have them in your operation.
Primary Device	The Summit client or server designated to be the primary managed device for the entire K2 SAN, K2 Central or Third Party Storage system. For optimum system performance it is recommended that if there are K2 Summit Clients, use them for the primary and secondary device. If there is only one client, use the client as the primary device and the FSM/Storage Manager as the secondary device. If it is a shared storage with no attached K2 Summit clients, configure the primary FSM or Storage Manager as the primary device and the secondary FSM (if exists) or FTP Server as the secondary device.
Secondary Device	The Summit client or server designated to the secondary managed device for the entire K2 SAN, K2 Central or Third Party Storage system.
UNC Path	The UNC path for a connection to the K2 Central and SMB Storage. The field for UNC path is only available for **K2 Central** and **Third Party Storage** settings.
User Name	The user name that this MDI uses to access the K2 Summit system. This is the internal system account, which by default is GVAdmin.

Setting or button	Description
Domain	If on a domain, it must be a fully qualified domain that this MDI uses to access the designated managed device. This field should only be set for fully qualified domain of third party storage system in your operation.
Update Password	The password that this MDI uses to access the K2 Summit system. ***NOTE: Do not enter a domain or otherwise modify account settings except under the supervision of qualified Grass Valley Support personnel. Extensive system configuration is required to achieve a working GV STRATUS system.***
FTP Server Name	The FTP server name for the remote K2 Summit system. The drop-down list consists of all FTP servers belonging to the Summit SAN. For the typical system where there is a separate FTP network, this is the name of the K2 SAN's FTP server with the `_he0` suffix added. The `_he0` suffix specifies the FTP network.
Maximum concurrent transfers	The maximum number of concurrent transfers allowed. The maximum is set in K2Config. You may select the maximum or a lesser number as designed for your system. The number of concurrent transfers as well as the device status can be checked once the system is configured in Resource Monitor of the GV STRATUS Control Panel.
FTP User Account	The FTP user name for the K2 Summit system this MDI accesses. Typically this is `movie`.
Update FTP Password	The FTP password for the K2 Summit system this MDI accesses. When this field is blank the system automatically uses the default password.

4. Click **Save**.
5. If you changed a standalone MDI setting, you must restart the GV STRATUS Core server system and the K2 Summit system. If SAN MDI settings, you must restart the entire K2 SAN system, including K2 Media Servers, attached K2 Summit systems, and other SAN clients.

   If you are changing multiple Grass Valley Media Server MDI settings, you can make all those settings first before restarting these systems. Restarting the systems once is sufficient for multiple Grass Valley Media Server MDI settings changes.
6. If you have multiple K2 SAN systems, repeat steps to configure an MDI for each K2 SAN system on your GV STRATUS system.

Related Topics

MDI and Encoder logical names convention on page 442
Grass Valley Media Server MDI SAN settings on page 306

Configuring Proxy Config settings: Required

All systems, all workflows, require this process.

If you are configuring Grass Valley Media Server MDI settings, you must make those settings first before doing this procedure.

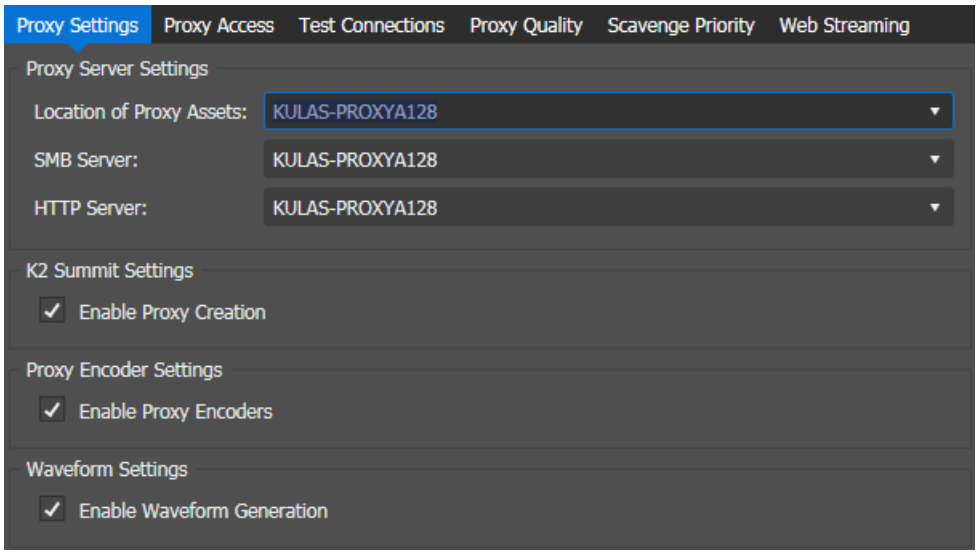
If you received your system pre-configured from Grass Valley, your Proxy Config settings are already configured so you can skip these tasks. Otherwise, work through this section sequentially to configure your Proxy Config settings.

NOTE: A GV STRATUS system must have only one proxy location and server, so these settings apply to all K2 Summit systems, both standalone and SAN.

NOTE: On an operational system, consult with Grass Valley Support before attempting to change Location of Proxy Assets, SMB Server, or HTTP Server settings. Changing these settings requires a purge of the GV STRATUS database and a new K2 storage file system, which results in a loss of high-resolution and low-resolution media. Grass Valley Support can provide methods to avoid this loss of media.

To locate these settings, click **Core | Proxy Config**

1. In the Control Panel application, open Proxy Config settings.



NOTE: GV STRATUS versions lower than 3.0 had only one Proxy Server setting. With version 3.0 and higher, the SMB Server and HTTP Server settings must be configured to replace the Proxy Server setting.

2. If your GV STRATUS system stores its proxy on a GV STRATUS Express server, configure as follows:

Setting or button	Description
Location of Proxy Assets	The name of the system that stores proxy files generated by K2 Summit and GV STRATUS systems, as follows: • For proxy stored on the GV STRATUS Express server, this is the network name of the server with role GV STRATUS Core Server Express, as configured in SiteConfig.
SMB Server	The network machine name of the device hosting the server to which proxy files are written, as follows: • For proxy stored on the GV STRATUS Express server, this is the network name of the server with role GV STRATUS Core Server Express, as configured in SiteConfig.
HTTP Server	The network machine name of the device hosting the server from which GV STRATUS clients read proxy files. Typically the SMB Server and the HTTP Server are hosted by the same device. • For proxy stored on the GV STRATUS Express server, this is the network name of the server with role GV STRATUS Core Server Express, as configured in SiteConfig.

3. If your GV STRATUS system stores its proxy on an online or production K2 SAN (A1), configure as follows:

Setting or button	Description
Location of Proxy Assets	The name of the system that stores proxy files generated by K2 Summit and GV STRATUS systems, as follows: • For proxy stored on the K2 SAN (A1), this is the name of the K2 SAN, as named in K2Config.
SMB Server	The network machine name of the device hosting the server to which proxy files are written, as follows: • For proxy stored on the K2 SAN (A1), this is the network name of the GV STRATUS Proxy server attached to the K2 SAN, as configured in K2Config.
HTTP Server	The network machine name of the device hosting the server from which GV STRATUS clients read proxy files. Typically the SMB Server and the HTTP Server are hosted by the same device. • For proxy stored on the K2 SAN (A1), this is the network name of the GV STRATUS Proxy server attached to the K2 SAN, as configured in K2Config.

4. If your GV STRATUS system stores its proxy on a dedicated Proxy Storage system (B1, C1), configure as follows:

Setting or button	Description
Location of Proxy Assets	The name of the system that stores proxy files generated by K2 Summit and GV STRATUS systems, as follows: • For proxy stored on the dedicated Proxy Storage system (B1, C1), this is the name of the Proxy Storage system, as named in K2Config.
SMB Server	The network machine name of the device hosting the server to which proxy files are written, as follows: • For proxy stored on the dedicated Proxy Storage system (B1, C1), this is the network name of the GV STRATUS Proxy Storage file system server, as configured in K2Config.
HTTP Server	The network machine name of the device hosting the server from which GV STRATUS clients read proxy files. Typically the SMB Server and the HTTP Server are hosted by the same device. • For proxy stored on the dedicated Proxy Storage system (B1, C1), this is the network name of the GV STRATUS Proxy Storage file system server, as configured in K2Config.

5. On the **Test Connections** tab, click **Test Connections**.

   The GV STRATUS system populates a list of K2 Storage devices. Verify that this list is correct.

6. Select **Enable Proxy Creation**.

   This allows K2 Summit systems to create proxy assets when high resolution assets are recorded.

7. Select **Enable Proxy Encoders**.

   This allows the system to create proxy assets for any high resolution assets that do not currently have a corresponding low-resolution proxy asset. This setting applies to proxy created by Render Engine servers. If your system instead has Proxy Encoder servers, which are no longer supported, the setting then applies to proxy created by your Proxy Encoder servers.

8. Click **Save**.
9. If you changed Location of Proxy Assets, SMB Server, or HTTP Server settings, under supervision of Grass Valley Support, you must purge the GV STRATUS database and make a new K2 storage file system.

Related Topics

Proxy Settings on page 343
HTTP server overview on page 226

Verify that devices are configured properly

Within the Control Panel application, do the following to verify systems and tools are ready for configuration. Grass Valley recommends the GV STRATUS Control Panel is only configured on the Core server:

- In the GV STRATUS Control Panel, do one or both of the following:
  - If your system has a K2 SAN, click **Core | K2 Storage | K2 SAN Storage** and verify that the information for the K2 SAN is the same information that is in K2Config. If the information is the same, it means that the Control Panel application is correctly reading the information from the K2Config application.
  - If your system has a standalone K2 Summit system, K2 SAN, K2 Central or Third Party Storage system, you must reconfigure MDI settings of all K2 Summit Standalone, K2 SAN, K2 Central, and Third Party Storage systems in this release. The Summit MDI Type has been renamed to **Grass Valley Media Server** in the MDI Configuration settings within GV STRATUS Control Panel.
  - If your system has a K2 SAN, K2 Central or Third Party Storage system, you must enter the Secondary Device in the MDI configuration. For optimum system performance it is recommended that if there are K2 Summit Clients, use them for the primary and secondary device. If there is only one client, use the client as the primary device and the FSM/Storage Manager as the secondary device. If it is shared storage with no attached K2 Summit clients, configure the primary FSM or Storage Manager as the primary device and the secondary FSM (if exists) or FTP Server as the secondary device.
  - If your system has a standalone K2 Summit system, verify the UNC Path in the standalone Grass Valley Media Server MDI configuration in **Core | MDI Configuration | Managed Devices**. Then, click **Core | K2 Storage | K2 Standalone Storage** and verify that the information for the K2 Summit system is the same information that is in SiteConfig. If the information is the same, it means that the Control Panel application is correctly reading the information from the SiteConfig application.
  - If your system has a GV I/O Live Ingest and Playback Server, configure the GV I/O channel formats in **General | Channels | GV I/O** to the desired formats configured in the **General | Format | Formats** settings.
- From each machine in the GV STRATUS system, verify that you can ping all the devices that the GV STRATUS server needs to communicate with over the control network.
- For the machines that need to communicate with a Proxy server, verify you can log in to that Proxy server using the credentials that the system will be using.
- If you exported an XML file backup of your GV STRATUS Rules before the upgrade, those rules cannot be used anymore once you upgrade to version 6.8 due to the new encryption support. You must import the XML file backup into GV STRATUS system after the upgrade. Then, export your rules again and re-import them to enable the encryption.
- The GV STRATUS database is automatically indexed to support enhanced search features. During this time, Search features and Rules are not fully functional. In GV STRATUS Control Panel, click **Core | Search Index Config** to view indexing progress.
- Begin by configuring STRATUS Core Services settings and move on to other settings.

After automatic re-index completes, reboot system in the correct order and verify that the GV STRATUS-EDIUS system is working.

NOTE: If prompted for a Java update, upgrade to the latest version of Java software to ensure you have the latest security updates.

Related Topics

About Control Panel, SiteConfig, and K2Config settings on page 433

Configuring licenses and roles settings: Required

All systems require this process. Assign GV STRATUS licenses and roles to groups and users.

- The groups and users to which you are assigning licenses and roles must be set up, either on a workgroup or on a domain, on the following:
  - The GV STRATUS server with role of Common Services.
- The GV STRATUS server with role of Common Services must have the site's GV STRATUS licenses installed.

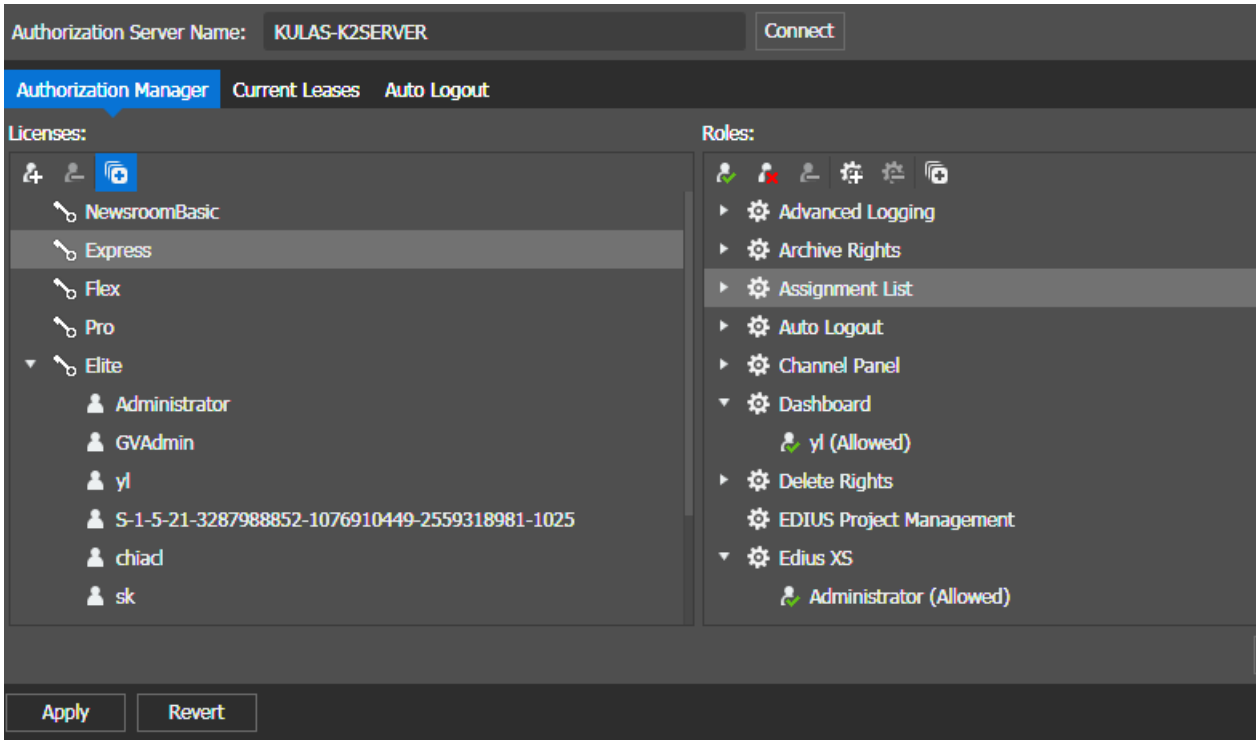
If on a network Workgroup, to configure Authorization Manager settings, you must be running GV STRATUS Control Panel on the GV STRATUS Core server.

When you receive your GV STRATUS system from Grass Valley, it is configured to workgroup, with all licenses and roles assigned to GVAdmin by default. Change the default configuration as appropriate for your site.

If you have temporary GV STRATUS licenses, GV STRATUS Control Panel allows you to configure Authorization Manager settings while you are waiting to install your permanent licenses. Authorization Manager displays indicators informing you of your license status.

To locate these settings, click **General | License Management | Authorization Manager**

1. In the GV STRATUS Control Panel application, open **License Management** settings.



2. On the Authorization Manager tab, enter the following:
   - **Authorization Server Name**: The name of GV STRATUS server with role of Common Services.
3. Click the following:
   - **Connect**: Connects to the GV STRATUS server and populates settings. If the Connect button is disabled, it means you are already connected.
4. Assign licenses according to the following description:
   - **Licenses**: Settings to assign licenses to user groups. When you select a license and click **Assign**, you can use standard Windows operating system processes to assign a group to the license. This can be either Workgroup or Domain, as appropriate for your site's user accounts. When you first assign a license to a group, all users in the group are assigned all of that license's roles. These are floating license so you may over-assign. If you over-assign you must ensure that the number of licenses checked out at any one time does not exceed the number of licenses available.
5. Assign roles according to the following description:
   - **Roles**: Settings to assign tools and other functionality to users or groups. When you expand a node and select one of its groups or users, you can allow or deny the group or user the use of that operation. You can also remove the group or user from the node. If a tool is not assigned to a user, when that user logs into the GV STRATUS application, the tool does not appear in the GV STRATUS application. If a new version of GV STRATUS software adds a role to a license, make sure it is assigned correctly to existing users.

   You can click the **Expand All** button to expand all licenses and roles on the **Authorization Manager** tab.
6. Click **Apply** to save your current settings, or click **Revert** to return to the last saved settings.

Related Topics

Identify test applications and setup on page 246
GV STRATUS roles matrix on page 37
Adding a custom role on page 466

Test GV STRATUS configuration settings

All systems require this process.

Whether you received your system pre-configured from Grass Valley or you configured your system on site, you should test the system operation before proceeding.

Related Topics

GV STRATUS client test on page 249
GV STRATUS proxy encoding test on page 250

Configure optional GV STRATUS Control Panel settings

All systems require GV STRATUS Control Panel settings, as appropriate for the site's unique workflow and GV STRATUS licenses.

If you received your system pre-configured from Grass Valley, your site's settings are already configured, so the system should not need any additional settings. Otherwise, refer to topics about Control Panel settings and configure as needed.

Control Panel settings are categorized as follows:

- Required settings — These are settings that must be configured for all GV STRATUS systems, regardless of the site's unique workflow and GV STRATUS license requirements.
- Optional settings — These are settings that might or might not be necessary, depending on the site's unique workflow and GV STRATUS license requirements.

Topics about configuring required settings provide the proper sequence and specific instructions for the required settings.

Topics that reference Control Panel settings describe all settings on all Control Panel configuration pages, including both required and optional settings. Choose the optional settings that are relevant to your site's unique workflow and GV STRATUS license requirements.

Related Topics

Custom Metadata settings on page 318
Engines settings on page 328
Rules settings on page 368
Locations Config settings on page 370
Web Monitor Config settings on page 377
EDIUS Settings on page 159
Ingest settings on page 380
Rundown settings on page 390
RMI settings on page 396
Router settings on page 397
Segmentation settings on page 403

SiteConfig software deployment process

All systems require this process when updating to new versions of Grass Valley product software.

1. *Verify software roles* on page 858. All systems require this process.
2. *Distribute devices into deployment groups* on page 858. All systems require this process.
3. *Stage software for deployment* on page 860. All systems require this process.
4. *Deploy software to GV STRATUS devices* on page 871. All systems require this process.

Verify software roles

All systems require this process.

Verify that the roles assigned to your GV STRATUS devices in SiteConfig are correct for your system design.

1. In the **Software Deployment | Devices** tree view, expand a device's node to expose the roles currently assigned to the device.
2. If the roles are not correct for your system design, add or remove roles accordingly.

Related Topics

Devices components: Roles, cab files, services, and licenses on page 444
Adding a software role to a device on page 490
Removing a software role from a device on page 490

Distribute devices into deployment groups

All systems require this process.

You can gather devices of different types into a SiteConfig deployment group. This allows you to deploy software to all the devices in the deployment group at the same time, as part of the same deployment session. Based on the roles you have assigned to the devices, SiteConfig deploys the proper software to each device. This increases the efficiency of your software deployment with SiteConfig.

If you have not already done so, configure your deployment groups. The recommended deployment group distribution is as follows. Depending on your system design, your system might not have all the device types listed.

- In a deployment group named "STRATUS", place the following devices:
  - GV STRATUS client PC connected on the corporate LAN for low-resolution (proxy) workflow
  - GV STRATUS client PC connected on the media (iSCSI) network for high-resolution workflow
  - GV STRATUS servers as follows:
    - Express server
    - Core server
    - Proxy server (A1)
    - Proxy Storage file system server (B1, C1)
    - Render Engine
    - Workflow Server
- In a deployment group named "EDIUS", place the following devices:
  - GV STRATUS/EDIUS XS client PC connected on the corporate LAN for low-resolution (proxy) workflow
  - GV STRATUS/EDIUS Workgroup client PC connected on the media (iSCSI) network for high-resolution workflow

- If you have GV STRATUS Rundown, in a deployment group named "GV STRATUS Rundown", place the following devices:
  - IEP
  - GV STRATUS Rundown

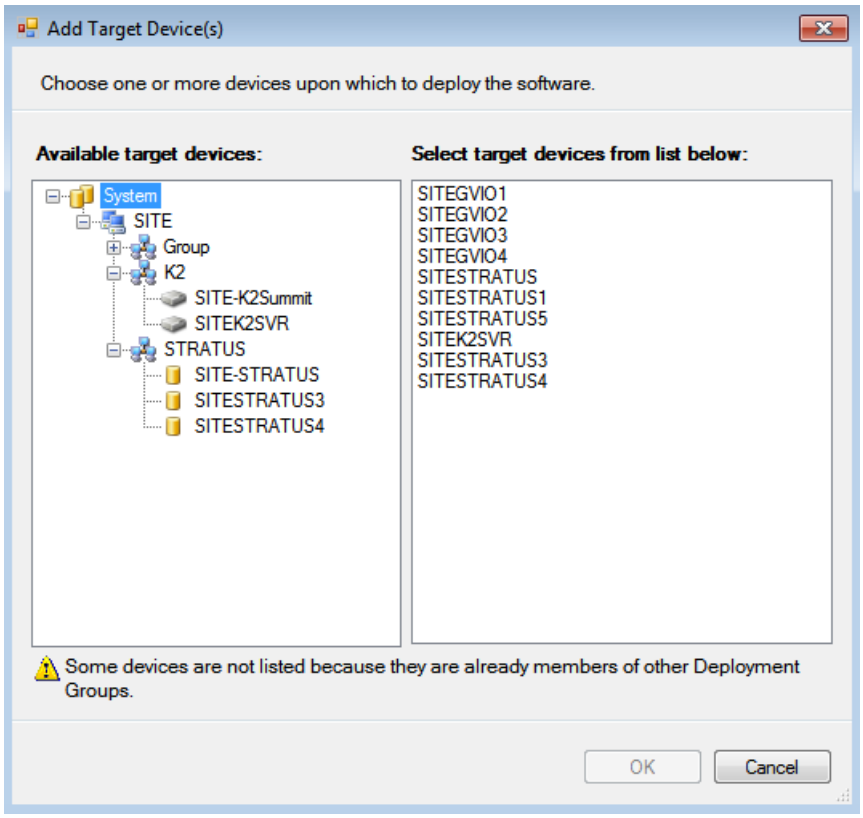
Configuring deployment groups

- The device must be assigned in the SiteConfig system description and network connectivity must be present.
- GV STRATUS systems containing mixed K2 Summit versions of 9.8 and 10.1 will require at least two separate deployment groups, one for K2 Summit 9.8.x system and one for K2 Summit 10.x system.

1. In the **Software Deployment | Deployment Groups** tree view, right-click the top node and select **Add Deployment Group**.

   A deployment group appears in the tree view.
2. Right-click the deployment group, select **Rename**, and enter a name for the deployment group.
3. Right-click the deployment group and select **Add Target Device**.

   The Add Target Device(s) wizard opens.



4. In the Available Target Devices tree view, select the node that displays the devices that you are combining as a deployment group.

5. In the right-hand pane, select the devices that you are combining as a deployment group.

   To select multiple devices, you can drag through the devices, use Ctrl + Click, or use Shift + Click.

6. Click **OK**.

The devices appear in the Deployment Groups tree view under the deployment group. Before you perform a software deployment, you must check software on the devices that will be receiving new software. If you have already added packages to the group, on the Deployment Groups tab you will also see deployment tasks generated for every device with roles that match the package contents.

Stage software for deployment

All systems require this process.

About deploying software

You must control the sequence of tasks and device restarts as you install or upgrade software. The exact steps can vary from software version to version. The following sequence of SiteConfig tasks is typical:

1. Check currently installed software.
2. Add software package(s) to deployment group(s).
3. Set deployment options.
4. Deploy (install or upgrade) software.

Your product's release notes or other upgrade instructions have the specific task flow for the version of software you are installing. If you are installing software for the first time or you are upgrading existing software, the steps are essentially the same. The primary difference is that when installing software for the first time, the SiteConfig "uninstall" deployment tasks are not displayed.

NOTE: Make sure you follow the documented task flow for the version of software you are installing or to which you are upgrading.

Check all currently installed software on GV STRATUS devices

Check software on GV STRATUS devices.

- The device must be assigned in the SiteConfig system description and network connectivity must be present.
- SiteConfig must be able to log in to the device using the username/password credentials assigned to the device.

- The SiteConfig PC must not have a network drive mapped to an administrative share (such as C$) on a device on which you are checking software.
- Put devices that run Embedded Security into Update Mode. Refer to the related topic on the Embedded Security one-time initial deployment process.

  NOTE: A re-image of the computer might be necessary if the Embedded Security one-time process is done incorrectly. Follow instructions carefully.

Do the following steps on the devices on which you are installing or upgrading software.

1. In the **Software Deployment | Deployment Groups** tree view, right-click the top-most node for the group or any individual device and select **Check Software**.

   NOTE: If you have access problems, verify that the administrator account on the device has credentials as currently configured in SiteConfig.

   NOTE: If an "Unable to copy ... to target" error appears for a device that has the Grass Valley Embedded Security solution, apply the* Embedded Security *solution one-time initial deployment process to the device. After the one-time process is complete the error does not appear and it is no longer necessary to put* Embedded Security *in Update mode.

   The Check Software dialog box appears. SiteConfig searches for software on the selected device or devices and gathers information. Progress is reported.
2. When the check is complete, close the Check Software dialog box.

An updated list of all currently installed software is displayed in the **Software Deployment | Devices | Installed Software** list view. If software is a SiteConfig managed software package, information is displayed in the Managed Package and Deployment Group columns.

Related Topics

Complete listing of device types, roles, and software packages for GV STRATUS devices on page 194

Deploy Embedded Security solution - One-time process

Complete listing of device types, roles, and software packages for GV STRATUS devices

Software packages are SiteConfig `*.cab` files. You add packages to a SiteConfig deployment group in order to make the software available for deployment to the devices in the group. When a correctly added device has its SiteConfig roles assigned correctly, SiteConfig installs the appropriate package.

GV STRATUS Client PC low-resolution (proxy):

- SiteConfig "Add Device":
  - Family: GV STRATUS

    NOTE: Do not select the EDIUS family.
  - Device Type: GV STRATUS Client
  - Model: GV STRATUS PC or GV STRATUS/EDIUS PC (if using EDIUS XS)
- SiteConfig roles:
  - GV STRATUS Application
  - EDIUS (Required for EDIUS XS)

- Software packages:
  - *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValley_STRATUS_Application_x.x.x.cab*
    - *EDIUS_x.x.x.cab* (Required for EDIUS XS)

GV STRATUS Client PC high-resolution (iSCSI):

- SiteConfig "Add Device":
  - Family: GV STRATUS

    NOTE: Do not select the EDIUS family.
  - Device Type: GV STRATUS Client
  - Model: GV STRATUS PC - SAN Client or GV STRATUS/EDIUS PC - SAN Client (if using EDIUS Workgroup)
- SiteConfig Roles:
  - GV STRATUS Application
  - StorNext File System Client (non K2 only)
  - Generic iSCSI Client (non K2 only)

    NOTE: First install StorNext File System Client, then install Generic iSCSI Client via SiteConfig for the following:
    - ***First installation of GV STRATUS application into a system.***
    - ***When there is an upgrade of the StorNext File System Client.***
  - EDIUS (Required for EDIUS Workgroup)
- Software packages:
  - *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValley_STRATUS_Application_x.x.x.cab*
    - *GenericISCSI_x64_ x.x.x.cab*
    - *SNFS_nonK2_x64_x.x.x.cab*
    - *EDIUS_x.x.x.cab* (Required for EDIUS Workgroup).

GV STRATUS Express server:

- SiteConfig "Add Device":
  - Family: GV STRATUS
  - Device Type: GV STRATUS Server
  - Model: GV STRATUS Core Server Express

- SiteConfig Roles:
  - GV STRATUS Ingest Services (Required)
  - GV STRATUS Control Panel Service (Required)
  - GV STRATUS Common Services (Required)
  - License Manager (Required)
  - GV STRATUS Data Mover Engine (Required)
  - GV STRATUS Proxy Express Server (Required on Express server)
  - GV STRATUS Control Panel (Required)
  - GV STRATUS Core Services (Required)
  - GV STRATUS Database (Required)
  - GV STRATUS Summit MDI (Required)
  - GV STRATUS Common RESTful Archive MDI (Optional)
  - GV STRATUS Diva MDI (Optional)
  - GV STRATUS FlashNet MDI (Optional)
  - GV STRATUS Masstech MDI (Optional)
  - GV STRATUS Generic FTP MDI (Optional)
  - GV STRATUS Proxy Streaming Service (Optional)
  - GV STRATUS Rules Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV STRATUS Scheduled Transfer Engine (Optional)
  - GV STRATUS Scheduled Ingest Engine (Not used in this GV STRATUS release)
  - GV STRATUS Scheduled Ingest Manager (Not used in this GV STRATUS release)
  - GV STRATUS SocialMedia Engine (Optional)
  - GV STRATUS ExternalMedia Engine (Optional)
  - GV STRATUS Traffic Gateway (Optional)
  - GV STRATUS Topic Service Bus (Not used in this GV STRATUS release)
  - GV STRATUS Web Apps (Required. Must be assigned to Express/Core server to display Statistics panel via Dashboard)
  - GV STRATUS Web Client (Optional)
  - GV STRATUS Workflow Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV STRATUS Xcode Control Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV Log Manager (Required)
  - GV Log Viewer (Required)
  - GV STRATUS Rundown Server Components (Optional)
  - GV STRATUS Application (Use for test purposes only)
  - If optionally used as a Render Engine, these additional roles:
    - GV STRATUS Render Engine

- Software packages:
  - *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValley_STRATUS_IngestServices_x.x.x.cab*
    - *GrassValley_STRATUS_ControlPanelService_x.x.x.cab*
    - *GrassValley_STRATUS_CommonServices_x.x.x.cab*
    - *GrassValley_STRATUS_CoreServices_x.x.x.cab*
    - *GrassValley_STRATUS_ControlPanel_x.x.x.cab*
    - *GrassValley_STRATUS_Databases_x.x.x.cab*
    - *GrassValley_STRATUS_DataMover_x.x.x.cab*
    - *GrassValley_STRATUS_ExternalMedia_x.x.x.cab*
    - *GrassValley_STRATUS_HttpProxyServer_x.x.x.cab*
    - *GrassValley_STRATUS_Mediaflow_x.x.x.cab*
    - *GrassValley_STRATUS_CRArchive_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_DIVA_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_FlashNet_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_Masstech_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_GFTP_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_Summit_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_Proxy_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_ProxyStreamingService_x.x.x.cab*
    - *GrassValley_STRATUS_RenderEngine_x.x.x.cab*
    - *GrassValley_STRATUS_Rules_x.x.x.cab*
    - *GrassValley_STRATUS_ScheduledTransferEngine_x.x.x.cab*
    - *GrassValley_STRATUS_SocialMedia_x.x.x.cab*
    - *GrassValley_STRATUS_Transcode_x.x.x.cab*
    - *GrassValley_STRATUS_TrafficGateway_x.x.x.cab*
    - *GrassValley_STRATUS_WebApps_x.x.x.cab*
    - *GrassValley_STRATUS_WebClient_x.x.x.cab*
    - *GrassValley_Sabretooth_Application_x.x.x.cab*
    - *GrassValley_DeviceKeyService_x.x.x.cab*
    - *GrassValley_LogManager_x.x.x.cab*
    - *GrassValley_LogViewer_x.x.x.cab*
    - *GV_STRATUS_Rundown_x.x.x.cab*
  - *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValley_STRATUS_ControlPanel_x.x.x.cab*
    - *GrassValley_STRATUS_Application_x.x.x.cab* (Use for test purposes only)
  - *GrassValley_K2system_x.x.x.cab* for K2 9.8.x systems.
  - *GrassValley_K2Plus_x.x.x.cab* for K2 10.x systems.

GV STRATUS Core server:

- SiteConfig "Add Device":
  - Family: GV STRATUS
  - Device Type: GV STRATUS Server
  - Model: GV STRATUS Core Server
- SiteConfig Roles:
  - GV STRATUS Ingest Services (Required)
  - GV STRATUS Control Panel Service (Required)
  - GV STRATUS Common Services (Required)
  - License Manager (Required)
  - GV STRATUS Control Panel (Required)
  - GV STRATUS Core Services (Required)
  - GV STRATUS Database (Required)
  - GV STRATUS Data Mover Engine (Required)
  - GV STRATUS Summit MDI (Required)
  - GV STRATUS Common RESTful Archive MDI (Optional)
  - GV STRATUS Diva MDI (Optional)
  - GV STRATUS FlashNet MDI (Optional)
  - GV STRATUS Masstech MDI (Optional)
  - GV STRATUS Generic FTP MDI (Optional)
  - GV STRATUS Proxy Streaming Service (Optional)
  - GV STRATUS Rules Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV STRATUS Scheduled Transfer Engine (Optional)
  - GV STRATUS Scheduled Ingest Engine (Not used in this GV STRATUS release)
  - GV STRATUS Scheduled Ingest Manager (Not used in this GV STRATUS release)
  - GV STRATUS SocialMedia Engine (Optional)
  - GV STRATUS ExternalMedia Engine (Optional)
  - GV STRATUS Traffic Gateway (Optional)
  - GV STRATUS Topic Service Bus (Not used in this GV STRATUS release)
  - GV STRATUS Workflow Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV STRATUS Xcode Control Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV Log Manager (Required)
  - GV Log Viewer (Required)
  - GV STRATUS Web Apps (Required. Must be assigned to Express/Core server to display Statistics panel via Dashboard)
  - GV STRATUS Web Client (Optional)
  - GV STRATUS Rundown Server Components (Optional)
  - GV STRATUS Application (Use for test purposes only)

- Software packages:
  - *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValley_STRATUS_IngestServices_x.x.x.cab*
    - *GrassValley_STRATUS_ControlPanelService_x.x.x.cab*
    - *GrassValley_STRATUS_CommonServices_x.x.x.cab*
    - *GrassValley_STRATUS_CoreServices_x.x.x.cab*
    - *GrassValley_STRATUS_ControlPanel_x.x.x.cab*
    - *GrassValley_STRATUS_Databases_x.x.x.cab*
    - *GrassValley_STRATUS_DataMover_x.x.x.cab*
    - *GrassValley_STRATUS_ExternalMedia_x.x.x.cab*
    - *GrassValley_STRATUS_CRArchive_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_DIVA_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_FlashNet_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_Masstech_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_GFTP_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_Summit_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_Proxy_MDI_x.x.x.cab*
    - *GrassValley_STRATUS_ProxyStreamingService_x.x.x.cab*
    - *GrassValley_STRATUS_Mediaflow_x.x.x.cab*
    - *GrassValley_STRATUS_Rules_x.x.x.cab*
    - *GrassValley_STRATUS_ScheduledTransferEngine_x.x.x.cab*
    - *GrassValley_STRATUS_SocialMedia_x.x.x.cab*
    - *GrassValley_STRATUS_Transcode_x.x.x.cab*
    - *GrassValley_STRATUS_TrafficGateway_x.x.x.cab*
    - *GrassValley_STRATUS_WebApps_x.x.x.cab*
    - *GrassValley_STRATUS_WebClient_x.x.x.cab*
    - *GrassValley_Sabretooth_Application_x.x.x.cab*
    - *GrassValley_DeviceKeyService_x.x.x.cab*
    - *GrassValley_LogManager_x.x.x.cab*
    - *GrassValley_LogViewer_x.x.x.cab*
    - *GV_STRATUS_Rundown_x.x.x.cab*
  - *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValley_STRATUS_ControlPanel_x.x.x.cab*
    - *GrassValley_STRATUS_Application_x.x.x.cab* (Use for test purposes only)
  - *GrassValley_K2system_x.x.x.cab* for K2 9.8.x systems.
  - *GrassValley_K2Plus_x.x.x.cab* for K2 10.x systems.

GV STRATUS Proxy server:

- SiteConfig "Add Device":
  - Family: GV STRATUS
  - Device Type: GV STRATUS Server
  - Model: GV STRATUS Proxy Server
- SiteConfig Roles:
  - GV STRATUS Proxy K2 SAN Server
  - GV Log Manager
  - StorNext File System Client
- Software packages:
  - *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValley_STRATUS_HttpProxyServer_x.x.x.cab*
    - *GrassValley_LogManager_x.x.x.cab*
  - *GrassValley_STRATUSClient_x.x.x.cab*.
  - For K2 9.8.x systems; use *GrassValley_K2system_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValleyK2Server_x64_9.8.x.x.cab*
    - *SNFS_x64_4.7.x.xxx.cab*
  - For K2 10.x systems; use *GrassValley_K2Plus_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValleyK2Server_x64_10.x.x.cab*
    - *SNFS_x64_6.0.x.xxx.cab*

GV STRATUS Proxy Storage file system server:

- SiteConfig "Add Device":
  - Family: GV STRATUS
  - Device Type: GV STRATUS Server
  - Model: GV STRATUS Proxy Storage File System Server
- SiteConfig Roles:
  - GV STRATUS Proxy Storage Server
  - GV Log Manager
  - StorNext File System Server
  - StorNext File System Client

- Software packages:
  - *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValley_STRATUS_HttpProxyServer_x.x.x.cab*
    - *GrassValley_LogManager_x.x.x.cab*
  - *GrassValley_STRATUSClient_x.x.x.cab*.
  - For K2 9.8.x systems; use *GrassValley_K2system_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValleyK2Server_x64_9.8.x.x.cab*
    - *SNFS_x64_4.7.x.xxx.cab*
  - For K2 10.x systems; use *GrassValley_K2Plus_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValleyK2Server_x64_10.x.x.cab*
    - *SNFS_x64_6.0.x.xxx.cab*

GV STRATUS Render Engine Server:

- SiteConfig "Add Device":
  - Family: GV STRATUS
  - Device Type: GV STRATUS Server
  - Model: GV STRATUS Render Engine
- SiteConfig Roles:
  - GV STRATUS Control Panel
  - GV Log Manager
  - StorNext File System Client
  - GV Embedded Security Manager
  - GV STRATUS Render Engine

- Software packages:
  - *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValley_STRATUS_RenderEngine_x.x.x.cab*
    - *GVEmbeddedSecurityManager_x.x.x.cab*
    - *GrassValley_Sabretooth_Application_x.x.x.cab*
    - *GrassValley_LogManager_x.x.x.cab*
  - For K2 9.8.x systems; use *GrassValley_K2system_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValleyK2Server_x64_9.8.x.x.cab*
    - *SNFS_x64_4.7.x.xxx.cab*
  - For K2 10.x systems; use *GrassValley_K2Plus_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValleyK2Server_x64_10.x.x.cab*
    - *SNFS_x64_6.0.x.xxx.cab*
  - *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValley_STRATUS_Application_x.x.x.cab*
    - *GrassValley_STRATUS_ControlPanel_x.x.x.cab*

GV STRATUS Workflow Server:

- SiteConfig "Add Device":
  - Family: GV STRATUS
  - Device Type: GV STRATUS Server
  - Model: GV STRATUS Workflow Server
- SiteConfig Roles:
  - GV STRATUS Workflow Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV STRATUS Rules Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV STRATUS SocialMedia Engine (Optional)
  - GV STRATUS ExternalMedia Engine (Optional)
  - GV STRATUS Xcode Control Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV STRATUS Control Panel
  - GV Log Manager

- Software packages:
  - *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValley_STRATUS_Mediaflow_x.x.x.cab*
    - *GrassValley_STRATUS_Rules_x.x.x.cab*
    - *GrassValley_STRATUS_SocialMedia_x.x.x.cab*
    - *GrassValley_STRATUS_ExternalMedia_x.x.x.cab*
    - *GrassValley_STRATUS_Transcode_x.x.x.cab*
    - *GrassValley_STRATUS_TrafficGateway_x.x.x.cab*
    - *GrassValley_Sabretooth_Application_x.x.x.cab*
    - *GrassValley_LogManager_x.x.x.cab*
  - *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:
    - *GrassValley_STRATUS_ControlPanel_x.x.x.cab*
  - *GrassValley_K2system_x.x.x.cab* for K2 9.8.x systems.
  - *GrassValley_K2Plus_x.x.x.cab* for K2 10.x systems.

Add software package to deployment group for GV STRATUS and other devices

- The GV STRATUS devices to which you are deploying software must have their SiteConfig roles correctly configured.
- The GV STRATUS devices to which you are deploying software must be in a deployment group.
- The following software upgrade system cab files apply to all deployment groups.
  - *GrassValley_STRATUSClient_X.X.X.XXX.cab*
  - *GrassValley_CoreServer_X.X.X.XXX.cab*
- The following software upgrade system cab files apply to K2 Summit 9.8.x devices. For each deployment group, choose the one that applies.
  - *GrassValley_K2system_X.X.X.XXX.cab*
- The following software upgrade system cab file apply to K2 Summit 10.x devices. For each deployment group, choose the one that applies.
  - *GrassValley_K2Plus_X.X.X.XXX.cab*
- The following software upgrade system cab files apply to GV I/O devices, if already added as a standalone device or a shared storage client with Dell EMC Isilon network-attached storage system.
  - *GrassValley_GVIO_X.X.X.XXX.cab*

  NOTE: Next, you must manually run the GVEngineInstaller-x.x.x.xxx_xxxxx_xxx.exe and MPIcore on each GV I/O device in your operation. The installation files can be procured from the Grass Valley FTP site.

1. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.

2. Click the **Add** button.

   The Add Package(s) dialog box opens.

3. Do one of the following to select the software package:

   - Select from the list of packages then click **OK**.
   - Click **Browse**, browse to and select the package, then click **Open**.

4. If one or more EULAs are displayed, accept them to proceed. If you do not accept a EULA, the associated software is not assigned to the deployment group.

   SiteConfig adds the package to the deployment group.

The package appears in the Managed Packages list for the selected deployment group. SiteConfig creates new software deployment tasks for the package and displays them in the Tasks list view.

Related Topics

Complete listing of device types, roles, and software packages for GV STRATUS devices on page 194

Complete listing of device types, roles, and software packages for GV STRATUS devices on page 194

Deploy software to GV STRATUS devices

All systems require this process.

About deploying software for the K2 SAN

You must control the sequence of software deployment tasks and device restarts as you upgrade software across the K2 SAN. The general sequence is to upgrade K2 Media Servers first then the SAN-attached K2 systems. The exact steps can vary from software version to version. Make sure you follow the task flow in the *K2 Release Notes* for the version of software to which you are upgrading.

Related Topics

Installing GV STRATUS application with SiteConfig on page 280

About deploying software for GV STRATUS devices

You must control the sequence of software deployment tasks and device restarts as you upgrade software across the devices of your GV STRATUS system. The general sequence is to upgrade K2 systems first, then GV STRATUS servers and GV STRATUS client PCs. The exact steps can vary from software version to version. Make sure you follow the task flow in release notes or other upgrade instructions for the version of software to which you are upgrading.

Related Topics

Installing GV STRATUS application with SiteConfig on page 280

Setting deployment options

- A software package must be assigned to the deployment group and applicable deployment tasks must be displayed in the Tasks area.

1. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.
2. In the Tasks list view, view tasks and determine if you must set deployment options.

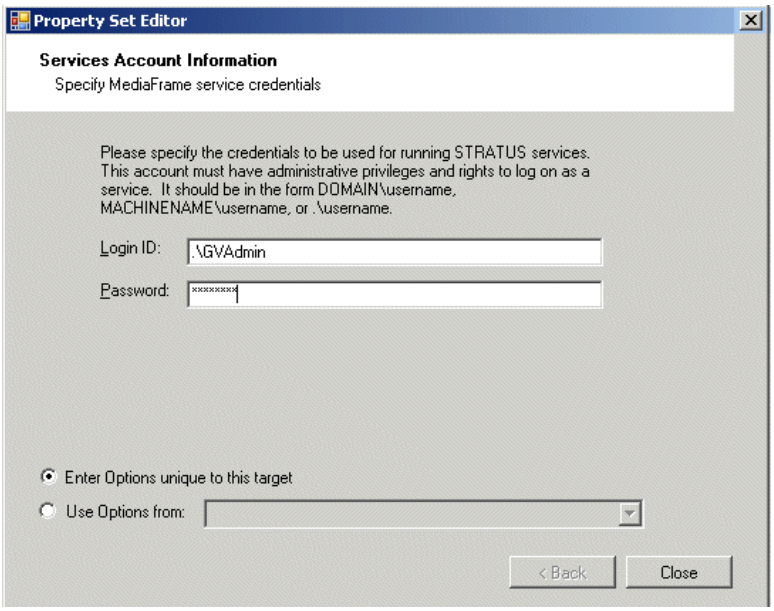
   Tasks that need to have deployment options set display in the Details column a message stating "Deployment options required."

   If you select a task that needs to have its deployment options set, the Start Deployment button is disabled and the message is displayed next to the button.
3. Do one of the following to set deployment options:

   - Double-click the task.
   - Select the task and click the **Options** button.

   A wizard opens.

4. Work through wizards and set deployment options for GV STRATUS software as follows:

Software	Deployment options
GrassValley_STRATUS_CommonServices GrassValley_STRATUS_ControlPanelService GrassValley_STRATUS_CoreServices GrassValley_STRATUS_CRArchive_MDI GrassValley_STRATUS_Databases GrassValley_STRATUS_DataMover GrassValley_STRATUS_DIVA_MDI GrassValley_STRATUS_ExternalMedia GrassValley_STRATUS_FlashNet_MDI GrassValley_STRATUS_GFTP_MDI GrassValley_STRATUS_HttpProxyServer GrassValley_STRATUS_IngestServices GrassValley_STRATUS_Masstech_MDI GrassValley_STRATUS_MediaFlow GrassValley_STRATUS_MEWS GrassValley_STRATUS_Proxy_MDI GrassValley_STRATUS_ProxyStreamingService GrassValley_STRATUS_RenderEngine GrassValley_STRATUS_Rules GrassValley_STRATUS_ScheduledTransferEngine GrassValley_STRATUS_SocialMedia GrassValley_STRATUS_Summit_MDI GrassValley_STRATUS_TrafficGateway GrassValley_STRATUS_Transcode GrassValley_STRATUS_WebApps GrassValley_STRATUS_WebClient GrassValley_DeviceKeyService GrassValley_LogManager GrassValley_LogViewer	 Use the local system account if your system is on a workgroup or if it's on a domain but uses the local system account in SQL. Use a domain\admin account if the account was previously mapped in SQL to the MediaFrame, MediaFlow, RulesEngine and WFPersistence databases. Entering account credentials allows you to use the **Use options from** feature for all other devices of the same type. Once you enter the account credentials this way on the first device, it becomes the template from which options for other devices are copied.

5. If you have multiple devices of the same type, you can enter deployment options for one of them using the wizard. Then, when you bring up the same wizard on every device, you can choose the **Use options from** radio button and select the first device for which you set options.

   SiteConfig copies the options you set for the first device and fills in the blanks on the wizard.

Installing software on the GV STRATUS system with SiteConfig

- The devices to which you are installing software must be in a deployment group.
- For the software you are installing, the managed package must be added to the deployment group.
- The SiteConfig "Check Software" operation must have been recently done on the devices to which you are installing software.

1. In the **Software Deployment | Deployment Groups** tree view, select the device or the group of devices to which you are installing software. You can select a Device node, a Deployment Group node, or the All Deployment Groups node.

   The corresponding software deployment tasks are displayed in the Tasks list view.
2. Identify one or more deployment tasks listed as "Install" in the Action column.
3. For the software you are installing, select the **Deploy** check box in the row for the install task.

   If a WFRegMon install task appears, install it as well. It is required to support Grass Valley software installers. There is no uninstall task.
4. Before starting the deployment session, verify the following for the installation deployment tasks:
   - The Deploy checkbox is selected.
   - The software package is the correct version.
   - The Action column reports Install.
   - The Status column indicates the planned icon.
   - The Details column does not indicate that deployment options are required.
5. Click the **Start Deployment** button.

   Deployment tasks run and software is installed. Progress is reported in both the Status and Details columns.

   NOTE: If an "Unable to copy ... to target" error appears for a device that has the Grass Valley Embedded Security solution, apply the* Embedded Security *solution one-time initial deployment process to the device. After the one-time process is complete the error does not appear and it is no longer necessary to put* Embedded Security *in Update mode.
6. Monitor progress as indicated by both the Status and Details column. When finished, the Status column indicates complete.

Archive system set up process

Only systems with an archive system require this process. Configure the archive system with the K2 Summit/SAN system, use SabreTooth to install the STRATUS-ARCHIVE license, and in GV STRATUS Control Panel configure an archive MDI.

Use the topics in this section that are appropriate for the type of archive system you are using with your GV STRATUS system.

Configuring DIVA

Before you begin, verify the following:

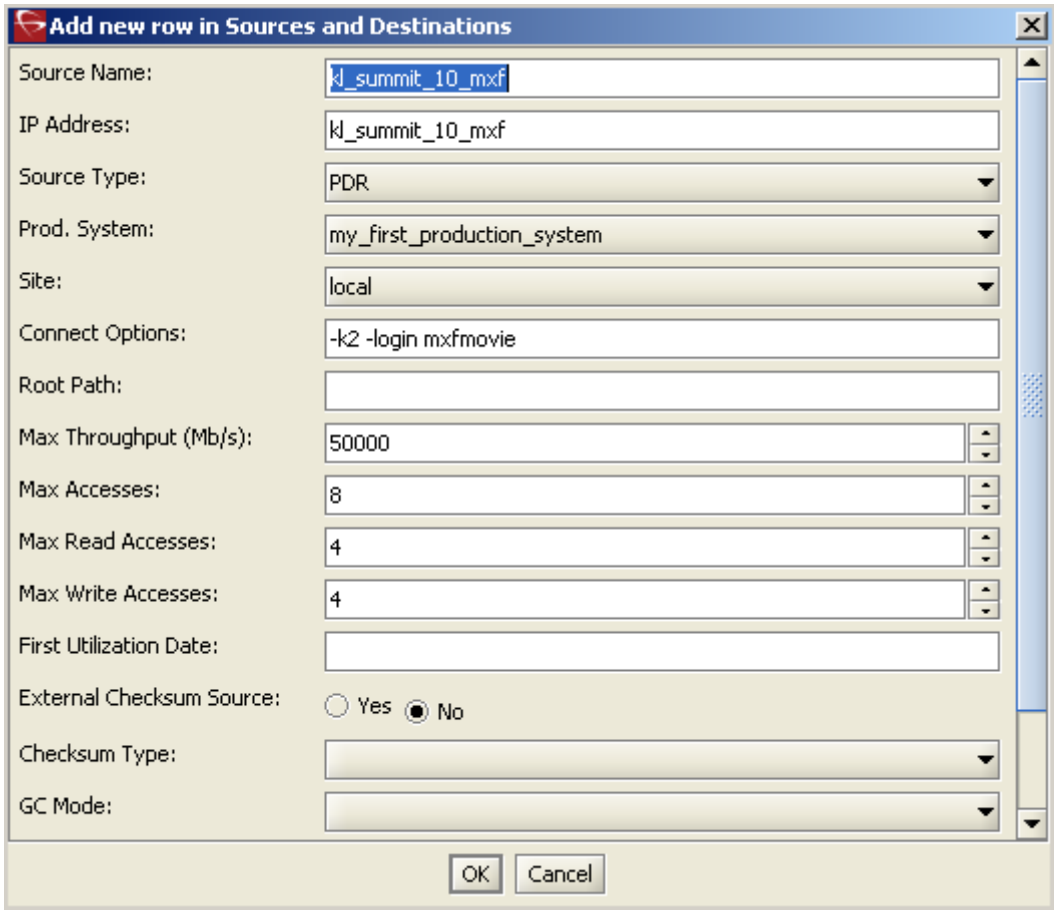
- The DIVA server must have sufficient storage for archived clips.
- The DIVA server must be connected to the Control and streaming/FTP networks.
- The K2 system must be assigned with the role of FTP Server.
- The K2 systems, GV STRATUS Core server, and the archive device must be able to communicate with each other on the streaming/FTP network.
- All FTP servers of K2 Summit SAN must be configured as individual entry in the Configuration Utility on the DIVA server.
- Two separate entries of the K2 server name must be configured to archive both GXF and MXF formats from a K2 server.

1. Launch the MS-DOS command prompt and use the `ping` command to test each K2 system, GV STRATUS Core server, and the archive device's streaming/FTP network name, which includes the `_he0` suffix.
2. Log on to the DIVA server.
3. Launch the Configuration Utility on the DIVA server.
4. Click the **Open connection** button on the toolbar to connect to the DIVA database.

   The log on dialog box opens.
5. Enter your user name and password, and click **OK**.

6. Click the **Add source** button + to add K2 server to the DIVA system configuration.

   The configuration dialog opens.



7. Fill in the following information:
   a) Source name – Name of the K2 server that the DIVA server connects to. If applicable, enter the server name including the `_he0` and `_mxf` suffixes. For MXF archive, the `_mxf` suffix must be at the end of the server name.

      NOTE: To archive both GXF and MXF formats from a K2 server, make 2 entries of the K2 server name with `_he0` suffix for GXF and `_he0_mxf` suffix for MXF.

   b) IP Address – IP address of the K2 server.
   c) Source Type – Select **PDR**.
   d) Production System – Select the production system in your operation.
   e) Site – Select the site in your operation.
   f) Connect Options – Enter one of the following:

      - For GXF archive, enter **-k2 -login movie**.
      - For MXF archive, enter **-k2 -login mxfmovie**.

   g) Root Path – You can leave this blank.
   h) Max Throughput (Mb/s) – Enter **50000** for the maximum throughput.
   i) Max Accesses – Enter **8**, the sum of max read and write accesses for the total number of maximum access.
   j) Max Read Accesses – Enter **4** for the total number of maximum read access.
   k) Max Write Accesses – Enter **4** for the total number of maximum write access.

   NOTE: The same number of maximum concurrent archive and restore operations should be entered for all FTP servers belonging to the same SAN. The same goes for all other connected K2 Summit stand-alone servers in one system.

8. If you're configuring DIVA version 7, go to `C:\Diva70\Program\conf\actor\partial_restore.conf` and set the following setting:

   - GXF_PROGRESSIVE_TIMECODE_TRANSLATION=1
   - MXF_IGNORE_START_TIMECODE=0

9. Restart the DIVArchive Actor Service, DIVArchive Manager Service, and DIVArchive Robot Manager Service on the DIVA server to enable the new settings.
10. Verify that you can FTP from the DIVA server to the K2 server using the *movie* or *mxfmovie* user account.

NOTE: DIVA file names are case sensitive, therefore make sure you selected the correct file name in lowercase or uppercase letters before archiving.

Related Topics

Configuring the GV STRATUS system for DIVA, FlashNET, Masstech, and Common RESTful archives on page 890

Configuring the GV STRATUS system for DIVA, FlashNET, Masstech, and Common RESTful archives on page 890

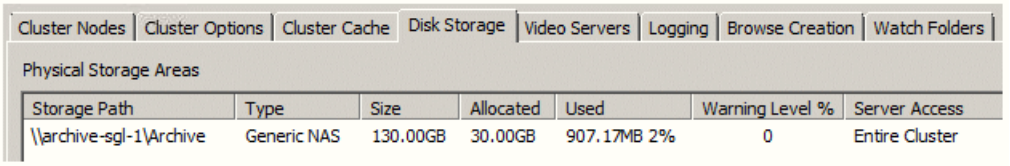
DIVA Archive MDI settings on page 309

Configuring FlashNet

Before you begin, verify the following:

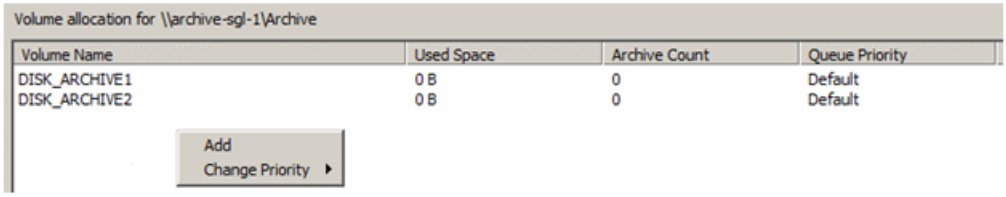
- The FlashNet server must have sufficient storage for archived clips.
- The FlashNet server must be connected to the Control and streaming/FTP networks.
- The K2 system must be assigned with the role of FTP Server.
- Verify that K2 systems, GV STRATUS Core server, and the FlashNet device can all communicate with each other on the streaming/FTP network. Use the `ping` command at the MS-DOS command prompt to test each device's streaming/FTP network name, which includes the `_he0` and `_mxf` suffixes.

1. Log on to the FlashNet server.
2. Make sure the FlashNet services are up and running.
3. Launch the FlashNet Administration application.
4. Click the **Configuration Settings** button to open the FlashNet Configurator.
5. Select the **Disk Storage** tab and add a storage path.



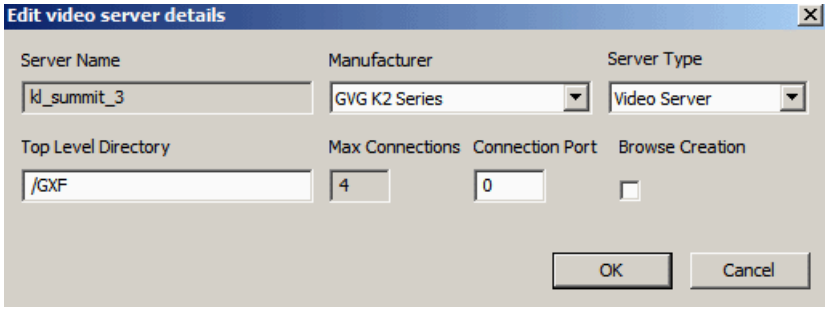
NOTE: : The allocated size should not exceed the size in the license.

6. Right-click on the storage path and select **Add** to add volumes or bins to archive into.



7. Select the **Video Servers** tab.
8. Right-click and select **Add Server**.

   The Edit video server details dialog opens.



9. Fill in the following information:
   a) Server Name - Name of the K2 server that the FlashNet server connects to. If applicable, enter the server name including the `_he0` and `_mxf` suffixes. For MXF archive, the `_mxf` suffix must be at the end of the server name. In case content is being archived/restored from a K2 SAN system, add ALL K2-SAN FTP server as individual entries to the FlashNet configuration.

      NOTE: To archive both GXF and MXF formats from a K2 server, make 2 entries of the K2 server name with `_he0` suffix for GXF and `_he0_mxf` suffix for MXF.

   b) Manufacturer - Select **GVG K2 Series**.
   c) Server Type - Select **Video Server**.
   d) Top Level Directory - Enter **/GXF** or **/MXF** according to your archive MDI setting.
   e) Connection Port - Enter **0**.

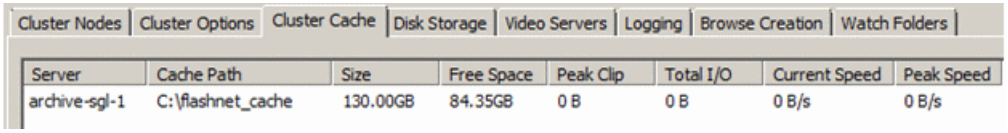
   NOTE: When you add servers, update those server details in host tables of all devices that use them. Make sure server names with `_he0` and `_he0_mxf` suffixes are added to your host tables.

10. Click OK.

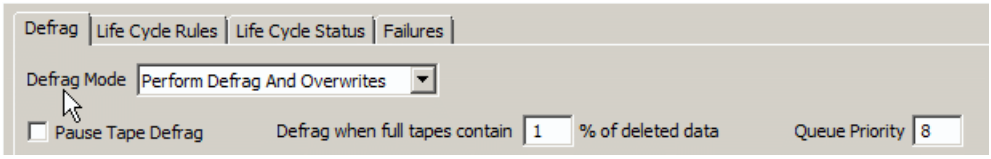
    The K2 server is added to the FlashNet configuration.

    Repeat above steps to add more K2 servers into the configuration.

11. Select the **Cluster Cache** tab, and add the cache path to allow the cleanup and deletion of assets.



12. Launch the FlashNet Storage Manager to continue with the cache cleanup configuration.
13. Select the **Defrag** tab, and set the Defrag Mode to **Perform Defrag And Overwrites**.



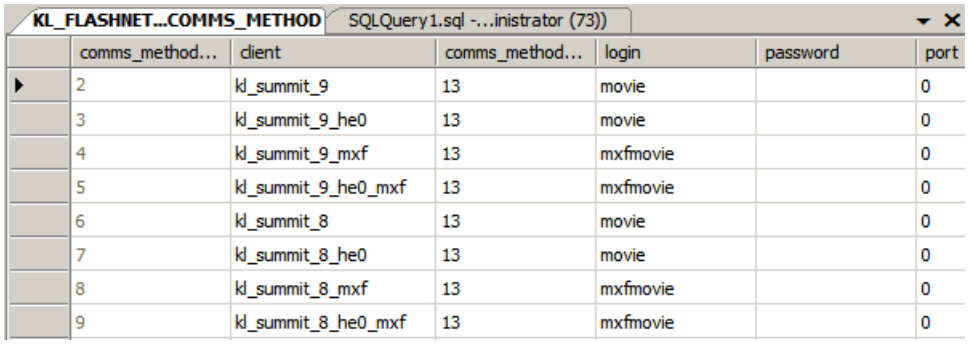
14. Enter **1** in the setting of Defrag when full tapes contain % of deleted data.
15. To set the FTP user account, click **Start | All Programs | Microsoft SQL Server** and select **Microsoft SQL Server Management Studio**.

    Microsoft SQL Server Management Studio opens.

16. Click **Databases | flashnet | Tables**.

17. Right-click on **dbo.COMMS_METHOD** and select **Edit Top 200 Rows**.

    The table for video server opens.



KL_FLASHNET...COMMS_METHOD | SQLQuery1.sql -...inistrator (73))

	comms_method...	client	comms_method...	login	password	port
▶	2	kl_summit_9	13	movie		0
	3	kl_summit_9_he0	13	movie		0
	4	kl_summit_9_mxf	13	mxfmovie		0
	5	kl_summit_9_he0_mxf	13	mxfmovie		0
	6	kl_summit_8	13	movie		0
	7	kl_summit_8_he0	13	movie		0
	8	kl_summit_8_mxf	13	mxfmovie		0
	9	kl_summit_8_he0_mxf	13	mxfmovie		0

18. Check that all your newly added servers are in the table.
19. In the **login** column, do the following:
    - For GXF archive, change from flashnet to **movie**.
    - For MXF archive, change from flashnet to **mxfmovie**.
20. In the **max_connect** column, change the number of maximum connection from 0 to 4.
21. Click **File | Save All** and close the **Microsoft SQL Server Management Studio**.
22. Verify that you can FTP from the FlashNet server to the K2 server using the *movie* or *mxfmovie* user account.

Related Topics

Configuring the GV STRATUS system for DIVA, FlashNET, Masstech, and Common RESTful archives on page 890

Configuring the GV STRATUS system for DIVA, FlashNET, Masstech, and Common RESTful archives on page 890

FlashNET Archive MDI settings on page 313

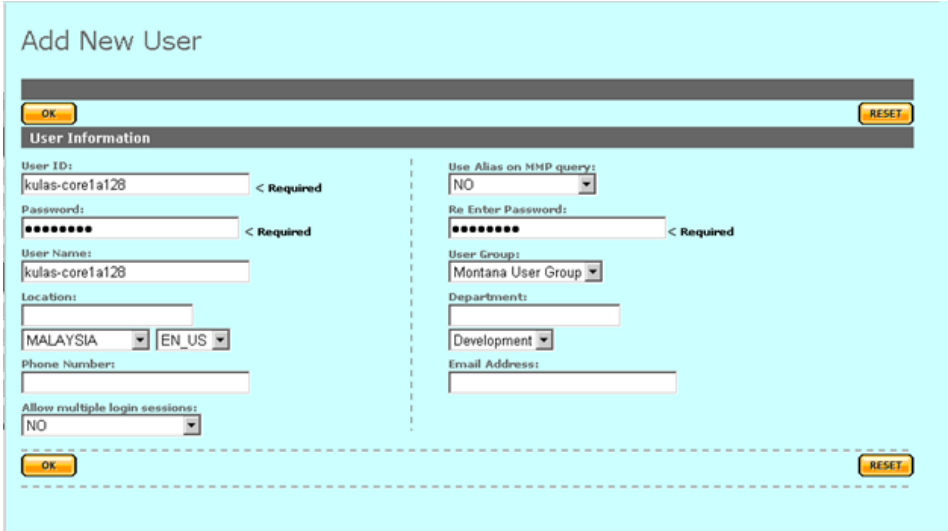
Configuring Masstech

Before you begin, verify the following:

- The Masstech server must have sufficient storage for archived clips.
- The Masstech server must be connected to the Control and streaming/FTP networks.
- The K2 system must be assigned with the role of FTP Server.
- Verify that K2 systems, GV STRATUS Core server, and the archive device can all communicate with each other on the streaming/FTP network. Use the `ping` command at the MS-DOS command prompt to test each device's streaming/FTP network name, which includes the `_he0` suffix.

1. In a web browser, log on to the Masstech server administration page using the administrator account.

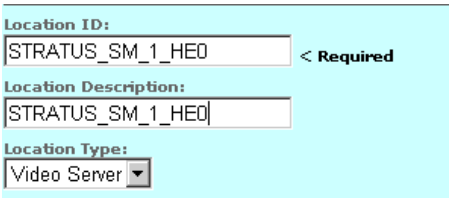
2. Navigate to **Management | Security | User Information** and click **Add New User**.



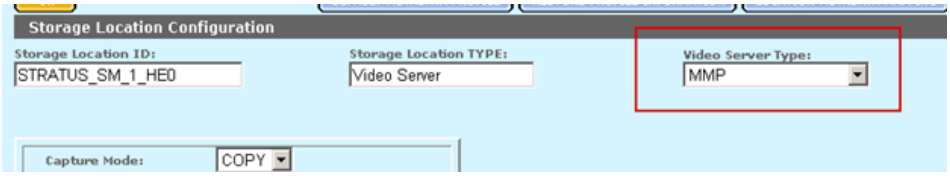
3. Add a user for the Masstech MDI to use to log on to the Masstech system.

   Each MDI must have a unique user for log on.

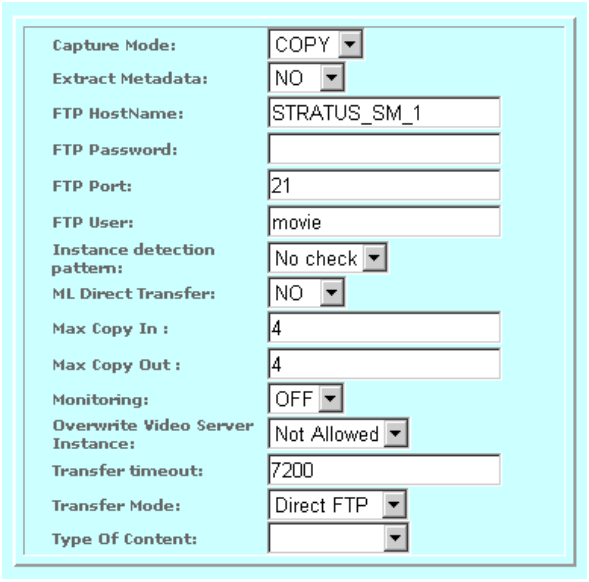
4. Configure settings for K2 Summit systems as follows:
   a) Navigate to **Management | Locations | Storage** and click **Add New Location**.



   b) Configure **Location ID** to be the same as the Grass Valley Media Server MDI **FTP Server Name** configured in GV STRATUS Control Panel. Make sure the server name is in all capital letters.
   c) For **Video Server Type** select **MMP** and then click **OK** and confirm as prompted.



   The screen displays different settings, based on the selection.
   d) For **Transfer Mode** select **Direct FTP** and then click **OK** and confirm as prompted.
   The screen displays different settings, based on the selection.



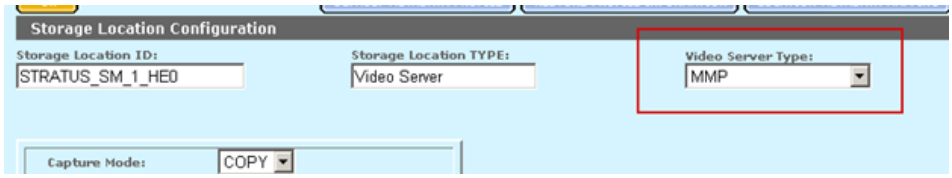
   e) Verify/configure settings as follows:

   - Capture Mode: COPY
   - Extract Metadata: NO

- FTP HostName: Enter the same server name used in the **Location ID** setting, except without the `_HEO` suffix.
- FTP Password: Leave this field blank
- FTP Port: 21
- FTP User: movie
- Instance detection pattern: No check
- ML Direct Transfer: NO
- Max Copy In: 4
- Max Copy Out: 4
- Monitoring: OFF
- Overwrite Video Server Instance: Not Allowed
- Transfer timeout: 7200
- Transfer Mode: Direct FTP
- Type Of Content: Leave this field blank

5. Configure settings for MXF archive restore using similar steps, as follows:
   a) Navigate to **Management | Locations | Storage** and click **Add New Location**.
   b) For **Location ID** and **Location Description**, enter the same value as you did in the previous step, except with a `_MXF` suffix added to the end.

      For example, if you entered `STRATUS_SM_1_HE0` in the previous step, enter `STRATUS_SM_1_HE0_MXF` in this step.
   c) For **Video Server Type** select **MMP** and then click **OK** and confirm as prompted.



      The screen displays different settings, based on the selection.
   d) For **Transfer Mode** select **Direct FTP** and then click **OK** and confirm as prompted.

      The screen displays different settings, based on the selection.
   e) Verify/configure settings as follows:

      - Capture Mode: COPY
      - Extract Metadata: NO
      - FTP HostName: Enter the same server name used in the **Location ID** setting, except without the `_HEO` suffix.
      - FTP Password: Leave this field blank
      - FTP Port: 21
      - FTP User: mxfmovie
      - Instance detection pattern: No check
      - ML Direct Transfer: NO
      - Max Copy In: 4
      - Max Copy Out: 4
      - Monitoring: OFF
      - Overwrite Video Server Instance: Not Allowed
      - Transfer timeout: 7200
      - Transfer Mode: Direct FTP
      - Type Of Content: Leave this field blank

Installing and configuring FileZilla

Before you begin, verify the following:

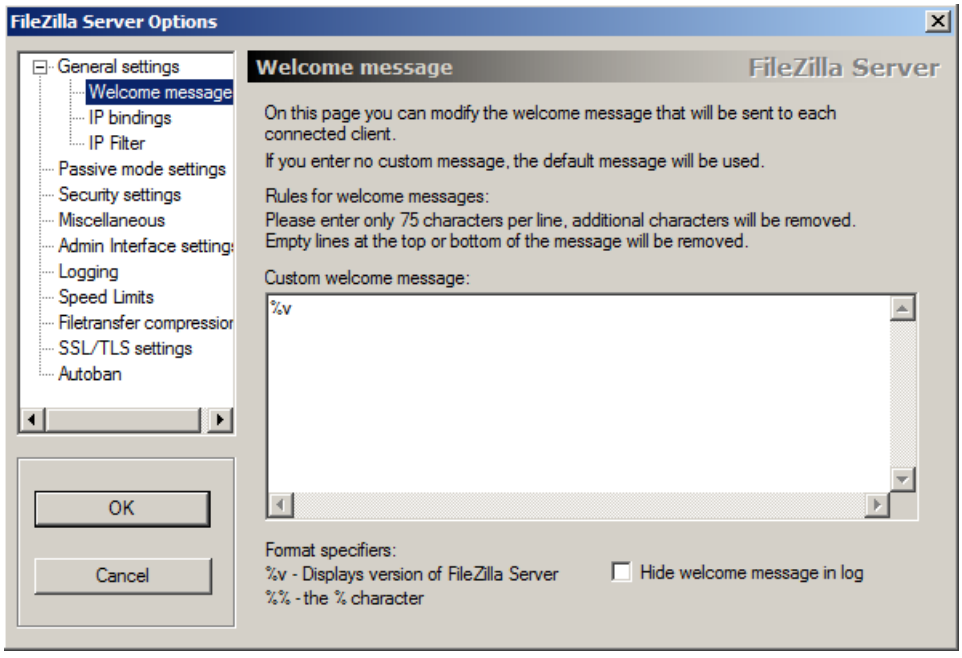
- The server that runs the FileZilla FTP service must have sufficient storage for archived clips.
- The server that runs the FileZilla FTP service must have a connection to the Control network and a connection to the streaming/FTP network.

- If using hosts files, the server's Control and FTP IP addresses must be added to your K2/GV STRATUS system hosts files. Hostnames for FTP IP addresses must have the `_he0` suffix.

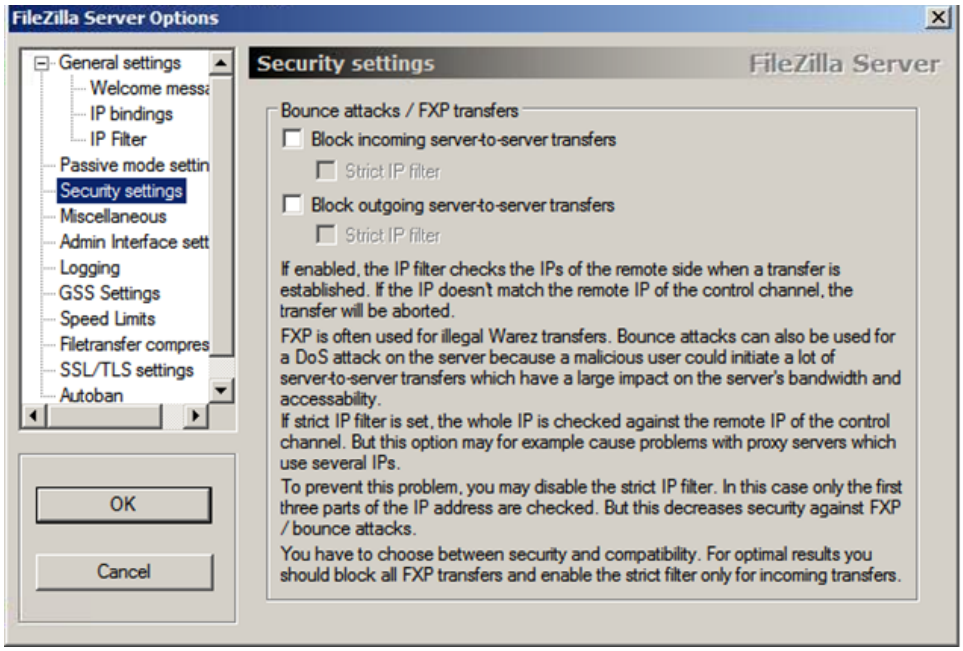
1. Verify that K2 systems, GV STRATUS Core server, and the archive device can all communicate with each other on the streaming/FTP network. Use the `ping` command at the MS-DOS command prompt to test each device's streaming/FTP network name, which includes the `_he0` suffix.
2. On the server that runs the FileZilla FTP service, check to see if IIS is installed. If it is installed, either uninstall it or disable it.
3. On the server that runs the FileZilla FTP service, on the C:\ drive, create a folder and name it *`root`*.
4. It is recommended that you create the internal system account, which by default is GVAdmin, in the Administrators group
5. Install the FileZilla Server software.

   Install the latest version available on the Internet.
6. Open the FileZilla application.
7. When the Connect to Server window opens, do the following:
   a) Verify that the Server Address defaults to 127.0.0.1.
   b) Verify that the port defaults to 14147.
   c) Enter the password for the internal system account, which by default is GVAdmin.
   d) Select **Always connect to this server**.

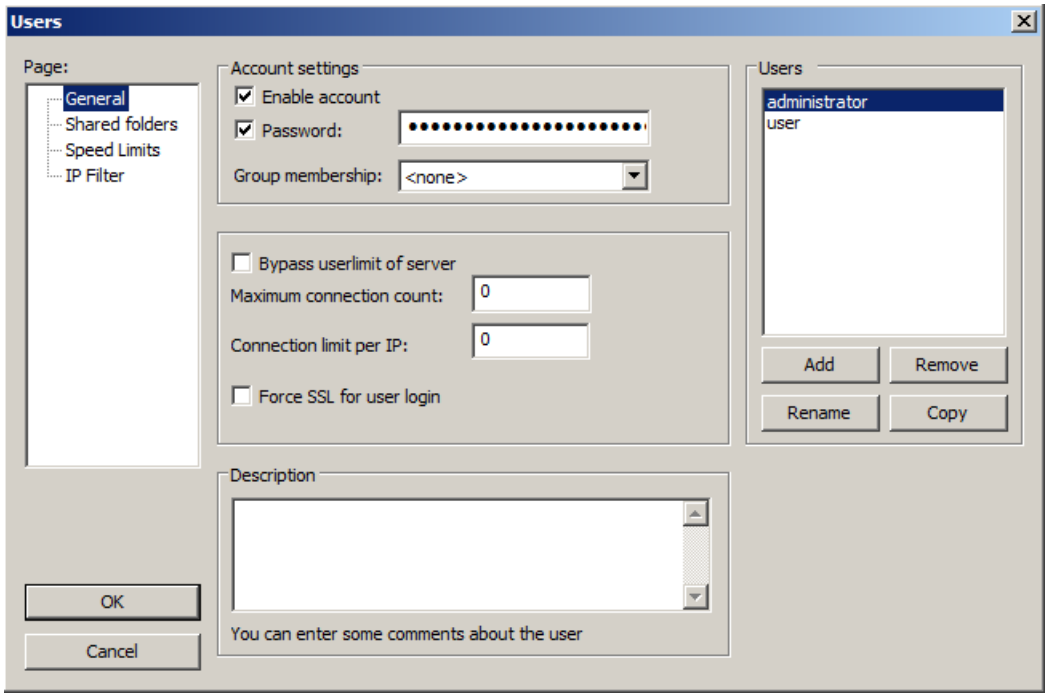
      This disables the automatic opening of the Connect to Server window.
8. Click **Edit | Settings | General Settings**, and configure the Welcome message as follows:
   a) Select **Welcome message**.
   b) Delete all characters except for `%v`.
   c) Click **OK**.



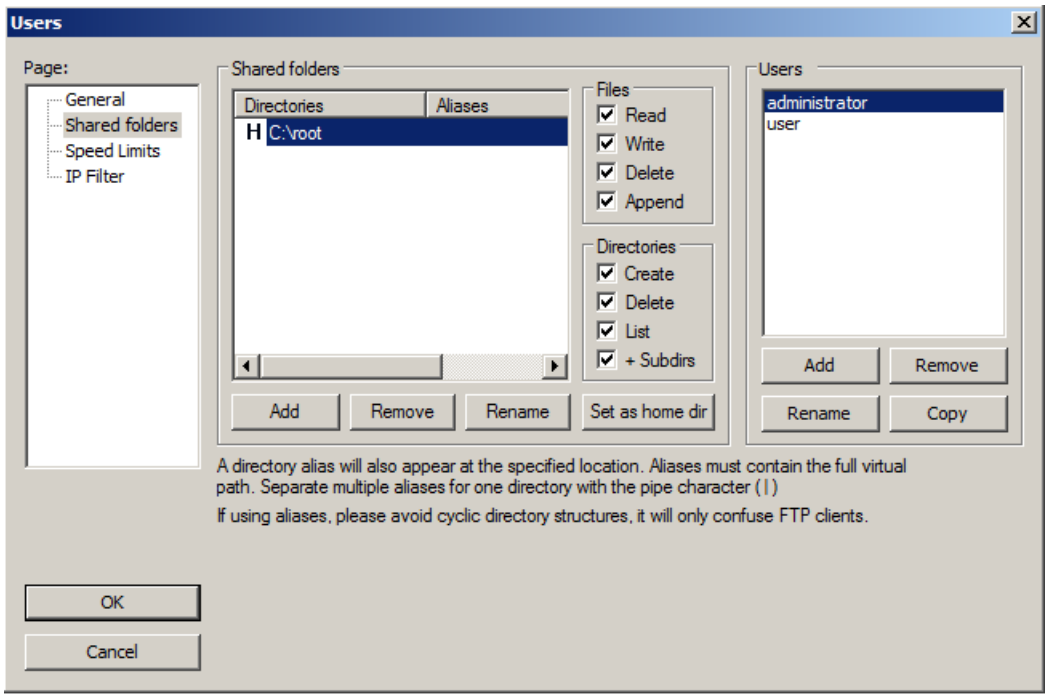
9. If the FileZilla server is not running on the same host as the GFTP MDI, click **Edit | Settings | Security settings** and configure the security settings as follows:
   a) Clear the **Block incoming server-to-server transfers** checkbox.
   b) Clear the **Block outgoing server-to-server transfers** checkbox.
   c) Click **OK**.



10. Click **Edit | Users | General** and configure the internal system account, which by default is GVAdmin, as follows:
    a) Add the account.
    b) Select the account.
    c) Verify that **Enable account** and **Password** are selected.
    d) Enter the account password.
    e) Click **OK**.



11. Click **Edit | Users | Shared folders** and configure the root folder as follows:
    a) Add the `C:\root` folder.
    b) Select the root folder.
    c) Select all **Files** and **Directories** checkboxes.
    d) Click **Set as home dir**
    e) Click **OK**.



12. Click **FileZilla | Server**, verify that **Active** is selected.

Next, configure the GV STRATUS system for FileZilla.

Related Topics

About host files on page 415
Configuring the GV STRATUS system for FileZilla on page 889
Generic FTP MDI settings on page 315

Configuring a Linux archive device

Before you begin, verify the following:

- The Linux archive device must have sufficient storage for archived clips.
- The Linux archive device must be connected to the Control and streaming/FTP networks.
- The K2 system must be assigned with the role of FTP Server.
- Verify that K2 systems, GV STRATUS Core server, and the archive device can all communicate with each other on the streaming/FTP network. Use the `ping` command at the MS-DOS command prompt to test each device's streaming/FTP network name, which includes the `_he0` suffix

- Linux file names are case sensitive, therefore make sure you don't have duplicate file names in lowercase and uppercase letters.

In addition to the instructions in related topics about using generic FTP for archive, the following steps are required for a Linux archive device that is using Very Secure FTP Daemon (vsftpd), which is an FTP server for Unix-like systems, including Linux.

1. Edit */etc/vsftpd.conf* as follows:
   a) Add `pasv_promiscuous=YES`.
      This disables the PASV security check that ensures the data connection originates from the same IP address as the control connection.
   b) Add `chroot_local_user=YES`, if is not already added.
      This locks a user within their root directory and a does not allow them to access anything beyond.
2. Restart vsftpd.
3. If vsftpd version 2.3.5 or higher, remove write permissions on the user's root directory. Use the `chmod` command.
   For example, if a user's home directory is */home/user* the command is `chmod a-w /home/user`.
   Removing write permissions on the user's root directory avoids the following error:

   ```
   500 OOPS: vsftpd: refusing to run with writable root inside chroot ()
   ```

Configuring the GV STRATUS system for FileZilla

1. In SiteConfig, add the GV STRATUS Generic FTP MDI role to the GV STRATUS Core server, if it is not already added.
   NOTE: The server that runs the FileZilla FTP service is not maintained through SiteConfig.
2. If not already installed, use SiteConfig to install the Generic FTP MDI on the GV STRATUS Core server.
3. On the GV STRATUS Core server, in the SabreTooth License Manager, generate a unique Id and request a STRATUS-Archive license. When you receive the license, install it on the GV STRATUS Core server.
4. In GV STRATUS Control Panel application, add a Generic FTP MDI and configure the FTP Server settings as follows:
   - FTP Server Name: The FTP network name of the server that runs the FileZilla FTP service. Make sure the name includes the `_he0` suffix.
   - FTP User Account: GVAdmin
   - FTP Password: The administrator password
5. Save the MDI configuration.
6. Restart the GV STRATUS Core server.
7. In GV STRATUS Control Panel application, in Licensing settings, verify that the desired users are licensed with the **Archive Rights** and **Restore Rights**.
8. To test, log in as one of those users and verify that you are able to Archive and Restore.

9. To add a new archive bin, go to **Devices | FTPMDI** right-click and select **New | Bin**.

   Archive bins are automatically populated under FTPMDI node in the Navigator if those bins already exist on the FTP server.

Related Topics

Adding a software role to a device on page 490
SabreTooth GV STRATUS license process on page 736
Generic FTP MDI settings on page 315
License Management settings on page 365
About Archive/Restore roles on page 465
Installing and configuring FileZilla on page 884
Generic FTP MDI settings on page 315

Configuring the GV STRATUS system for DIVA, FlashNET, Masstech, and Common RESTful archives

1. In SiteConfig, add the GV STRATUS DIVA MDI role, the GV STRATUS FlashNET MDI role, the GV STRATUS Masstech MDI role, or the GV STRATUS Common RESTful Archive MDI role to the GV STRATUS Core server, if it is not already added.
2. If not already installed, use SiteConfig to install the appropriate archive MDI on the GV STRATUS Core server.
3. On the GV STRATUS Core server, in the SabreTooth License Manager, generate a unique ID and request a STRATUS-ARCHIVE license. When you receive the license, install it on the GV STRATUS Core server.
4. In GV STRATUS Control Panel application, add and configure the appropriate archive MDI.
5. Save the MDI configuration.
6. Restart the GV STRATUS Core server.
7. In GV STRATUS Control Panel application, in Licensing settings, verify that the desired users are licensed with the **Archive Rights** and **Restore Rights**.

   Users without the **Archive Rights** or **Restore Rights** are not able to see archive devices under Devices node in the Navigator.

8. To test, log in as one of those users and verify that you are able to Archive and Restore.

Related Topics

About archive MDIs on page 442
DIVA Archive MDI settings on page 309
FlashNET Archive MDI settings on page 313
Masstech MDI settings on page 314
Common RESTful Archive MDI settings on page 316
SabreTooth Archive/Restore license process on page 891
Configuring DIVA on page 875
DIVA Archive MDI settings on page 309
Configuring FlashNet on page 878
FlashNET Archive MDI settings on page 313

Configuring the Generic FTP MDI role for Nearline K2 SAN

1. In SiteConfig, add the GV STRATUS Generic FTP MDI role to the GV STRATUS Core server, if it is not already added.
2. If not already installed, use SiteConfig to install the Generic FTP MDI on the GV STRATUS Core server.
3. On the GV STRATUS Core server, in the SabreTooth License Manager, generate a unique Id and request a STRATUS-ARCHIVE license. When you receive the license, install it on the GV STRATUS Core server.
4. In GV STRATUS Control Panel application, add a Generic FTP MDI and configure the FTP Server settings as follows:
   - FTP Server Name: The FTP network name of the K2 server for the Nearline K2 SAN system. Make sure the name includes the `_he0` suffix.
   - FTP User Account: It is recommended that you use the internal system account, which by default is GVAdmin.
   - FTP Password: The administrator password for the default GVAdmin account.
5. Save the MDI configuration.
6. Restart the GV STRATUS Core server.
7. In GV STRATUS Control Panel application, in Licensing settings, verify that the desired users are licensed with the **Archive Rights** and **Restore Rights**.
8. To test, log in as one of those users and verify that you are able to Archive and Restore.
9. To add a new archive bin, go to **Devices | FTPMDI** right-click and select **New | Bin**.

   Archive bins are automatically populated under FTPMDI node in the Navigator if those bins already exist on the FTP server.

Related Topics

Adding a software role to a device on page 490
SabreTooth GV STRATUS license process on page 736
Generic FTP MDI settings on page 315
License Management settings on page 365
About Archive/Restore roles on page 465
Generic FTP MDI settings on page 315

SabreTooth Archive/Restore license process

The Archive/Restore license is installed on the GV STRATUS server with role of Common Services. Typically the GV STRATUS Core server has the role of Common Services.

One STRATUS-ARCHIVE license is required for archive and restore operations in the GV STRATUS. Once installed, archive and restore rights can be assigned to groups and users.

If you received your system pre-configured from Grass Valley, licenses are already installed, so you can skip these tasks. Otherwise, do the following:

1. Refer to the license sheet that you received with your GV STRATUS license. The license sheet has the Sales Order number that you need.

2. On the GV STRATUS server with role of Common Services, run the SabreTooth License Manager, generate a unique ID, and send the email to Grass Valley requesting your license or licenses.

   Refer to this Topic Library for detailed licensing procedures.

3. When you receive your license file, use SabreTooth License Manager and install it on the server.

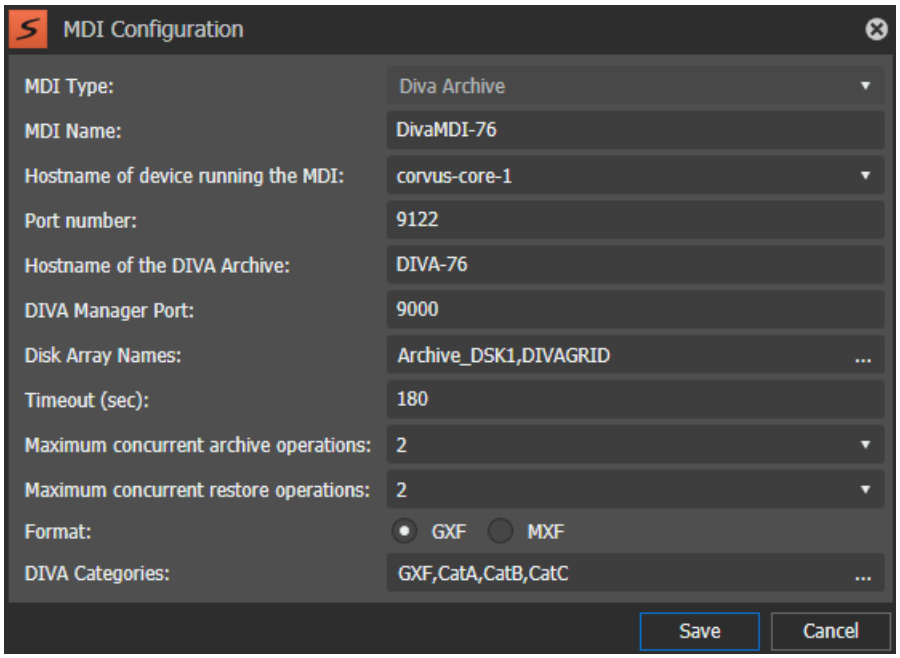
DIVA Archive MDI settings

These settings are optional on GV STRATUS systems.

Before archiving assets, your K2 system must be assigned with the role of FTP Server.

Since DIVA provides direction oriented FTP transfer and port configuration settings, it is recommended to configure the maximum concurrent number of supported archive and restore operations in this Diva Archive MDI setting. They should be identical to the configuration in the DIVA Manager.

To locate these settings, click **Core | MDI Configuration | Managed Devices | Add | Diva Archive**



Setting or button	Description
MDI Type	The Managed Device Interface (MDI) type to which these settings apply.
MDI Name	A name for this instance of the MDI type. Do not use spaces in the MDI name.
Hostname of device running the MDI	The name of the GV STRATUS server that hosts this MDI.
Port number	The port number of the port that this MDI listens to. The default port number is 9122. Other port numbers are also allowed.

Setting or button	Description
Hostname of the DIVA Archive	The hostname or IP address of the DIVA Archive server. ***NOTE: The device status can be monitored in the Resource Monitor of* GV STRATUS Control Panel.**
DIVA Manager Port	The default value for the DIVA Manager Port number is listed below: • DIVA version 7.1 and below: **9000** • DIVA version 7.2: **9072** Other DIVA Manager Port numbers are also allowed. Refer to your DIVA archive server for configuration details.
Disk Array Names	The disk arrays in DIVA that are exposed in GV STRATUS clients.
Timeout (sec)	The default timeout is 180 seconds.
Maximum concurrent archive operations	The maximum number of transfers that the MDI will process at the same time for archive operations. The number of maximum concurrent transfers can be monitored in the Resource Monitor of GV STRATUS Control Panel. The maximum number is set to 5 by default.
Maximum concurrent restore operations	The maximum number of transfers that the MDI will process at the same time for restore operations. The number of maximum concurrent transfers can be monitored in the Resource Monitor of GV STRATUS Control Panel. The maximum number is set to 5 by default.
Format	Specifies the format of the archived asset, either GXF or MXF. ***NOTE: In order for the format change to take effect, you need to click* Save *and restart your GV STRATUS clients.***
DIVA Categories	Specifies multiple DIVA categories for your archived material. All configured categories in DIVA Archive MDI settings will be accessible via the GV STRATUS Navigator. If this setting is empty, GXF category will be used and shown by default in DIVA Archive MDI.

NOTE: These special characters are not allowed to be included in DIVA Category and Disk Array Names: ? < >

Related Topics

Configuring DIVA on page 875

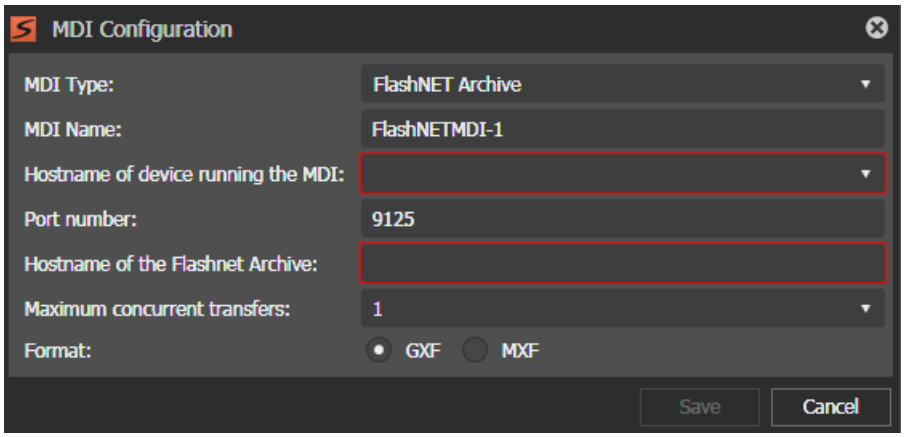
Configuring the GV STRATUS system for DIVA, FlashNET, Masstech, and Common RESTful archives on page 890

FlashNET Archive MDI settings

These settings are optional on GV STRATUS systems.

Before archiving assets, your K2 system must be assigned with the role of FTP Server.

To locate these settings, click **Core | MDI Configuration | Managed Devices | Add | FlashNET Archive**



Setting or button	Description
MDI Type	The Managed Device Interface (MDI) type to which these settings apply.
MDI Name	A name for this instance of the MDI type. Do not use spaces in the MDI name.
Hostname of device running the MDI	The name of the GV STRATUS server that hosts this MDI.
Port number	The port number of the port that this MDI listens to. The default port number is 9124. Other port numbers are also allowed.
Hostname of the FlashNET Archive	The name or IP address of the FlashNET Archive server. ***NOTE: The device status can be monitored in the Resource Monitor of* GV STRATUS Control Panel.**
Maximum concurrent transfers	The maximum number of transfers that the MDI will process at the same time. The number of maximum concurrent transfers can be monitored in the Resource Monitor of GV STRATUS Control Panel.
Format	Specifies the format of the archived asset, either GXF or MXF. ***NOTE: In order for the format change to take effect, you need to click* Save *and restart your GV STRATUS clients.***

Related Topics

Configuring FlashNet on page 878

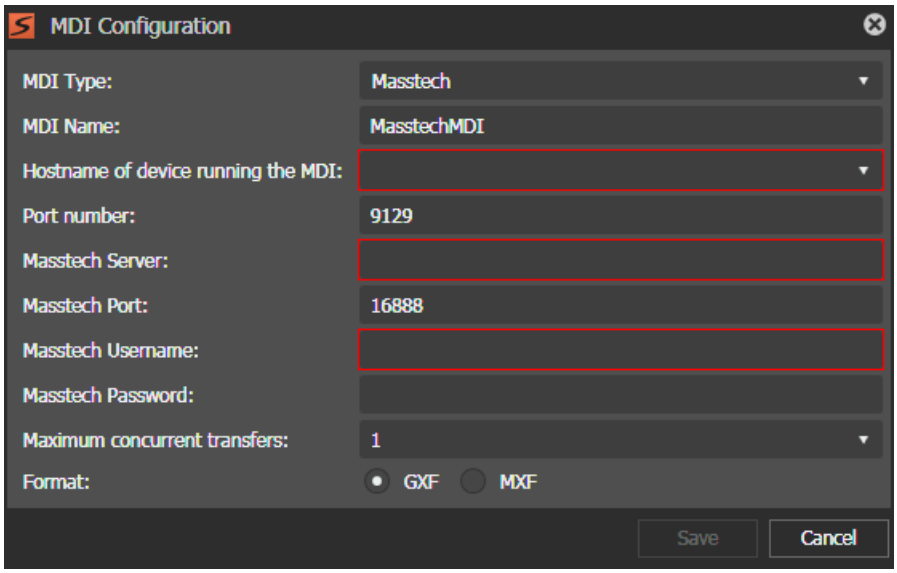
Configuring the GV STRATUS system for DIVA, FlashNET, Masstech, and Common RESTful archives on page 890

Masstech MDI settings

These settings are optional on GV STRATUS systems.

Before archiving assets, your K2 system must be assigned with the role of FTP Server.

To locate these settings, click **Core | MDI Configuration | Managed Devices | Add | Masstech**



Setting or button	Description
MDI Type	The Managed Device Interface (MDI) type to which these settings apply.
MDI Name	A name for this instance of the MDI type. Do not use spaces in the MDI name.
Hostname of device running the MDI	The name of the GV STRATUS server that hosts this MDI.
Port number	The port number of the port that this MDI listens to. The default port number is 9129. Other port numbers are also allowed.
Masstech Server	The name or IP address of the Masstech server. ***NOTE: The device status can be monitored in the Resource Monitor of* GV STRATUS Control Panel.**
Masstech Port	The default value for the Masstech port is 16888.
Masstech Username	The Masstech username.
Masstech Password	The Masstech password.
Maximum concurrent transfers	The maximum number of transfers that the MDI will process at the same time. The number of maximum concurrent transfers can be monitored in the Resource Monitor of GV STRATUS Control Panel.
Format	Specifies the format of the archived asset, either GXF or MXF. ***NOTE: Click Save and restart your GV STRATUS clients to put a format change into effect.***

Related Topics

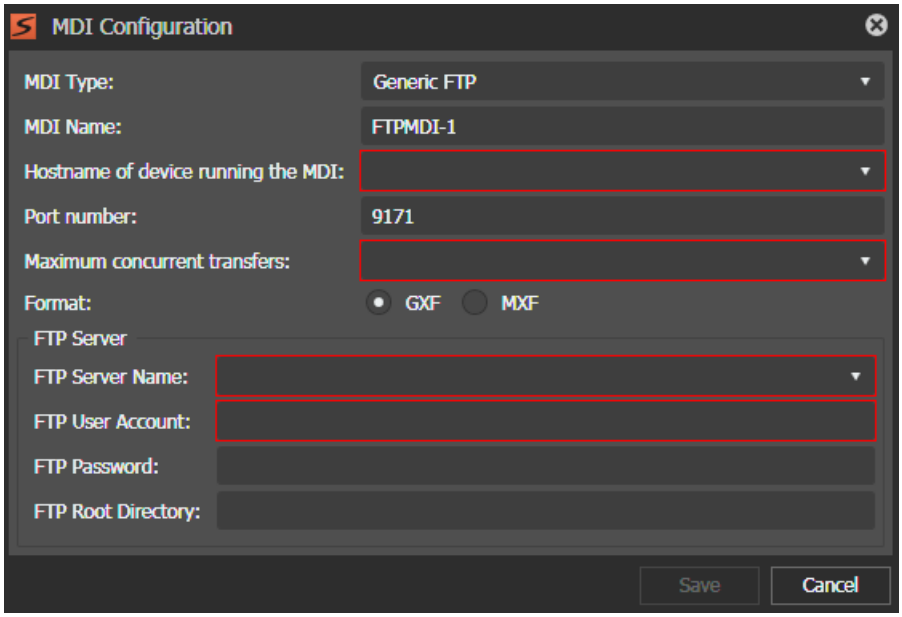
Configuring Masstech on page 880

Configuring the GV STRATUS system for DIVA, FlashNET, Masstech, and Common RESTful archives on page 890

Generic FTP MDI settings

These settings are optional on GV STRATUS systems.

To locate these settings, click **Core | MDI Configuration | Managed Devices | Add | Generic FTP**



Setting or button	Description
MDI Type	The Managed Device Interface (MDI) type to which these settings apply.
MDI Name	A name for this instance of the MDI type. Do not use spaces in the MDI name.
Hostname of device running the MDI	The name of the GV STRATUS server that hosts this MDI.
Port number	The port number of the port that this MDI listens to. The default port number is 9170. Other port numbers are also allowed.
Maximum concurrent transfers	The maximum number of transfers that the MDI will process at the same time. You can configure up to 10 concurrent transfers if you have large resources in your system. The number of maximum concurrent transfers can be monitored in the Resource Monitor of GV STRATUS Control Panel.
Format	Specifies the format of the archived asset, either GXF or MXF. ***NOTE: In order for the format change to take effect, you need to click Save and restart your GV STRATUS clients.***
FTP Server Name	The IP Address or the name resolving to the FTP server on the FTP server network where assets will be transferred to. If using a K2 nearline, configure the Generic FTP MDI to use the K2's nearline FTP. ***NOTE: The device status can be monitored in the Resource Monitor of* GV STRATUS Control Panel.**

Setting or button	Description
FTP User Account	The FTP user name.
FTP Password	The FTP password.
FTP Root Directory	The root directory for the Generic FTP MDI. Once you set the root directory, only folders under the root directory are exposed in the Navigator of GV STRATUS application.

Related Topics

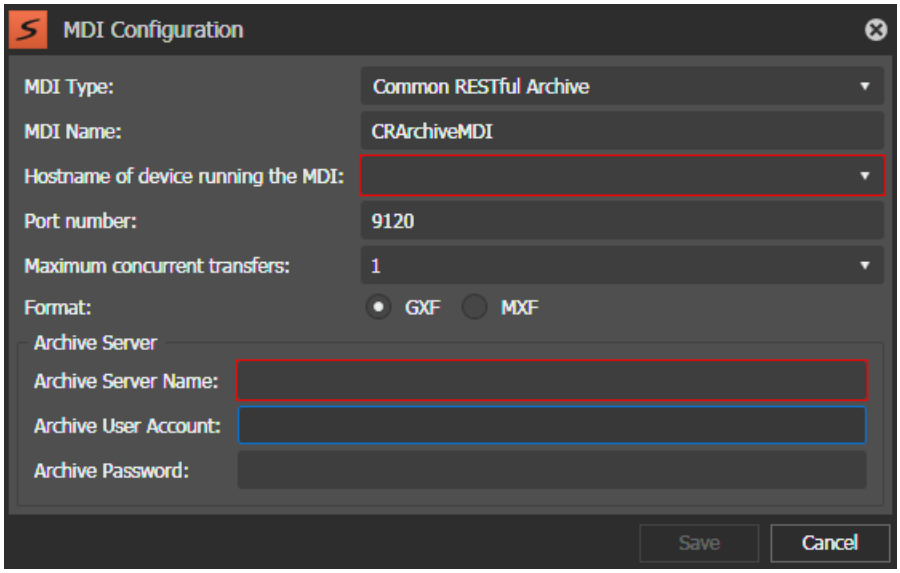
Installing and configuring FileZilla on page 884
Configuring the GV STRATUS system for FileZilla on page 889
Configuring the Generic FTP MDI role for Nearline K2 SAN on page 891

Common RESTful Archive MDI settings

These settings are optional on GV STRATUS systems.

You can configure up to 2 Common RESTful Archive MDIs in the GV STRATUS Control Panel, and both MDIs are able to archive assets in parallel at the same time.

To locate these settings, click **Core | MDI Configuration | Managed Devices | Add | Common RESTful Archive**



Setting or button	Description
MDI Type	The Managed Device Interface (MDI) type to which these settings apply.
MDI Name	A name for this instance of the MDI type. Do not use spaces in the MDI name.
Hostname of device running the MDI	The name of the GV STRATUS server that hosts this MDI.

Setting or button	Description
Port number	The port number of the port that this MDI listens to. The default port number is 9120. Other port numbers are also allowed.
Maximum concurrent transfers	The maximum number of transfers that the MDI will process at the same time. The number of maximum concurrent transfers can be monitored in the Resource Monitor of GV STRATUS Control Panel.
Format	Specifies the format of the archived asset, either GXF or MXF. ***NOTE: In order for the format change to take effect, you need to click Save and restart your GV STRATUS clients.***
Archive Server Name	The name of the Archive Server.
Archive User Account	The user account to access the Archive Server.
Archive Password	The password for the user account.

NOTE: For Common RESTful Archives, transfers between archives are only supported between the Common RESTful Archive and Generic FTP servers.

Related Topics

Configuring the GV STRATUS system for DIVA, FlashNET, Masstech, and Common RESTful archives on page 890

Archiving an asset on page 1123

Workflow Server set up process

Only systems with a Workflow Server require this process. Use SiteConfig for network setup and software install. On the GV STRATUS Core server, use SabreTooth and install the STRATUS-RULES license optional transfer/transcode licenses.

GV STRATUS supports a separate workflow server. The separate workflow server is recommended for B1 (FT) and C1 (FT) configurations.

The separate Workflow Server allows the separation of GV STRATUS Engines (Workflow-, Rules-, XCodeControl- and optional DataMover-Engine) away from the Core Server for large system setups where rules and workflows are used intensively paired with lots of file exports. Since the release of version 5.5, all GV STRATUS Databases are running on one Database Server, which is usually the Core Server.

For very large scaled systems, it is possible to deploy the GV STRATUS Databases on a separate server away from the Core Server. When you want to move engines away from the Core server to a new Workflow Server, there is no need anymore to move the Workflow and Rules Databases. They both remain on the Core server, even when the engines are running on a separate server machine. There is no separate SQL-Server license required for the separate Workflow Server. Just remove the roles from the old server in SiteConfig, assign the roles of the engines (WFE, RUE, XCE, and DME) to the new server machine, deploy the software, and check later on whether those engines are enabled using GV STRATUS Control Panel.

NOTE: Make sure the new separate Workflow Server has the same image as the Core Server.

If your GV STRATUS system has a single GV STRATUS Express server or a GV STRATUS Core server and no Workflow Servers, the GV STRATUS Express server or GV STRATUS Core server has Workflow Server software installed.

If you received your Workflow Server already set up from Grass Valley, skip set up tasks and do the test task only.

1. SiteConfig Workflow Server network set up. Only systems with a Workflow Server require this process.
2. SiteConfig Workflow Server software install. Only systems with a Workflow Server require this process.
3. SabreTooth Rules, Xcode license process. Only the GV STRATUS server with role of Common Services requires this process.

SiteConfig Workflow Server network set up

Only systems with a Workflow Server require this process.

If you received your system already set up from Grass Valley, your Workflow Server or Servers are already included in the SiteConfig system description and set up on the network, so you can skip these tasks. Otherwise, work through the topics in this section.

Adding a Workflow Server to the SiteConfig system description

- Workflow Servers are racked, cabled, and powered on.
- The system description must contain a group.

This topic applies to a GV STRATUS server that is a Workflow Server.

1. In the **Network Configuration | Devices** tree view, right-click a group and select **Add Device**.
2. Configure settings for the device you are adding as follows:
   - Family: GV STRATUS
   - Device Type: GV STRATUS Server
   - Model: GV STRATUS Workflow Server
   - Name – This is the device name, as displayed in the SiteConfig device tree view and device list view. This name can be different than the host name (network name). You can accept the default name or enter a name of your choice. Devices in the tree view are sorted alphabetically.
   - Amount — Select the number of Workflow Servers, according to your system design.
   - Platform — Select **x64**.
   - Control network– Select the control network.
   - Starting Address – Select from the list of available addresses on the selected control network. If adding multiple devices, this is the starting address, with addresses assigned sequentially to each device added.
3. Click **OK** to save settings and close.

   SiteConfig adds the Workflow Server to the system description as a placeholder device.
4. Verify that unmanaged control network interface is configured correctly and modify if necessary.

Next, add the GV STRATUS server to the control network.

Adding a GV STRATUS server to the control network with SiteConfig

Use SiteConfig to configure network settings on a separate GV STRATUS server.

Before doing this task, make sure the GV STRATUS server is added as a placeholder device to the SiteConfig system description.

The following steps are the standard tasks for adding a device to the control network using SiteConfig. Use these steps for the GV STRATUS server you are adding.

1. Discover the device using SiteConfig device discovery.
2. Assign the discovered device to the placeholder device in the SiteConfig system description.
3. Modify the control network interface to ensure communication on the control network.
4. Modify the host name and/or device name as desired.
5. Ping the device to verify network communication.
6. Verify credentials to ensure SiteConfig can install software on the device.
7. Generate and/or add to host tables as appropriate for your network.

Related Topics

Adding a device to a network with SiteConfig on page 490
Adding a device to a network with SiteConfig on page 490

SiteConfig Workflow Server software install

Only systems with a Workflow Server require this process.

If you received your system pre-configured from Grass Valley, software is already installed, so you can skip these tasks. Otherwise, work through the tasks in this section as follows:

- If your GV STRATUS system has one or more GV STRATUS servers that are Workflow Servers, install software on those servers.

If your GV STRATUS system has a single GV STRATUS Express server or a GV STRATUS Core server and no Workflow Servers, the GV STRATUS Express server or GV STRATUS Core server has Workflow Server software installed. Follow software installation instructions for the GV STRATUS Express server or GV STRATUS Core server, rather than the instructions in this section.

Setting deployment options

- A software package must be assigned to the deployment group and applicable deployment tasks must be displayed in the Tasks area.

1. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.
2. In the Tasks list view, view tasks and determine if you must set deployment options.

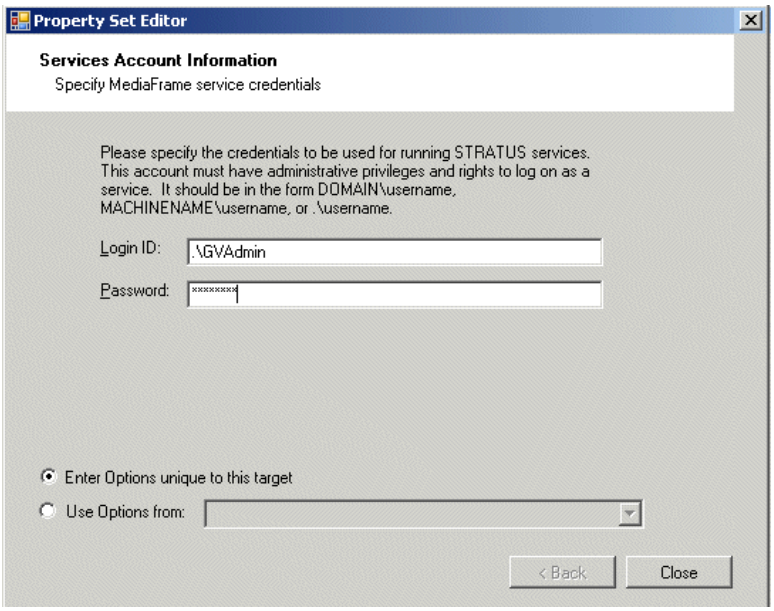
   Tasks that need to have deployment options set display in the Details column a message stating "Deployment options required."

   If you select a task that needs to have its deployment options set, the Start Deployment button is disabled and the message is displayed next to the button.

3. Do one of the following to set deployment options:
   - Double-click the task.
   - Select the task and click the **Options** button.

   A wizard opens.

4. Work through wizards and set deployment options for GV STRATUS software as follows:

Software	Deployment options
GrassValley_STRATUS_CommonServices GrassValley_STRATUS_ControlPanelService GrassValley_STRATUS_CoreServices GrassValley_STRATUS_CRArchive_MDI GrassValley_STRATUS_Databases GrassValley_STRATUS_DataMover GrassValley_STRATUS_DIVA_MDI GrassValley_STRATUS_ExternalMedia GrassValley_STRATUS_FlashNet_MDI GrassValley_STRATUS_GFTP_MDI GrassValley_STRATUS_HttpProxyServer GrassValley_STRATUS_IngestServices GrassValley_STRATUS_Masstech_MDI GrassValley_STRATUS_MediaFlow GrassValley_STRATUS_MEWS GrassValley_STRATUS_Proxy_MDI GrassValley_STRATUS_ProxyStreamingService GrassValley_STRATUS_RenderEngine GrassValley_STRATUS_Rules GrassValley_STRATUS_ScheduledTransferEngine GrassValley_STRATUS_SocialMedia GrassValley_STRATUS_Summit_MDI GrassValley_STRATUS_TrafficGateway GrassValley_STRATUS_Transcode GrassValley_STRATUS_WebApps GrassValley_STRATUS_WebClient GrassValley_DeviceKeyService GrassValley_LogManager GrassValley_LogViewer	 Use the local system account if your system is on a workgroup or if it's on a domain but uses the local system account in SQL. Use a domain\admin account if the account was previously mapped in SQL to the MediaFrame, MediaFlow, RulesEngine and WFPersistence databases. Entering account credentials allows you to use the **Use options from** feature for all other devices of the same type. Once you enter the account credentials this way on the first device, it becomes the template from which options for other devices are copied.

5. If you have multiple devices of the same type, you can enter deployment options for one of them using the wizard. Then, when you bring up the same wizard on every device, you can choose the **Use options from** radio button and select the first device for which you set options.

   SiteConfig copies the options you set for the first device and fills in the blanks on the wizard.

Installing software on a Workflow Server

Only systems with one or more GV STRATUS servers that are Workflow Servers require this process. Use SiteConfig to install software on the Workflow Servers.

Prerequisites:

- The server on which you are installing software is in the SiteConfig system description and communicating on the control network.
- The server on which you are installing software has its credentials set in SiteConfig to allow access.

1. Verify the SiteConfig roles currently assigned to the server. If the roles are not correct for your system design, add or remove roles accordingly. Roles are as follows:
   - GV STRATUS Workflow Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
   - GV STRATUS Rules Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
   - GV STRATUS SocialMedia Engine (Optional)
   - GV STRATUS ExternalMedia Engine (Optional)
   - GV STRATUS Xcode Control Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
   - GV STRATUS Control Panel
   - GV Log Manager
2. Add the server to a deployment group, such as the GV STRATUS deployment group.

3. Add the following files to the deployment group:

   - *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
     - *GrassValley_STRATUS_Mediaflow_x.x.x.cab*
     - *GrassValley_STRATUS_Rules_x.x.x.cab*
     - *GrassValley_STRATUS_SocialMedia_x.x.x.cab*
     - *GrassValley_STRATUS_ExternalMedia_x.x.x.cab*
     - *GrassValley_STRATUS_Transcode_x.x.x.cab*
     - *GrassValley_STRATUS_TrafficGateway_x.x.x.cab*
     - *GrassValley_Sabretooth_Application_x.x.x.cab*
     - *GrassValley_LogManager_x.x.x.cab*
   - *GrassValley_STRATUSClient_x.x.x.cab*, which contains the following cab files that apply to this device:
     - *GrassValley_STRATUS_ControlPanel_x.x.x.cab*
   - *GrassValley_K2system_x.x.x.cab* for K2 9.8.x systems.
   - *GrassValley_K2Plus_x.x.x.cab* for K2 10.x systems.

   Refer to release notes for version numbers.

4. Do the SiteConfig **Check Software** operation on the server.

   NOTE: If an "Unable to copy ... to target" error appears for a device that has the Grass Valley Embedded Security solution, apply the* Embedded Security *solution one-time initial deployment process to the device. After the one-time process is complete the error does not appear and it is no longer necessary to put* Embedded Security *in Update mode.

5. Verify that deployment tasks are set to **Install** for the files listed above.

   If a WFRegMon install task appears, install it as well. It is required to support Grass Valley software installers. There is no uninstall task.

6. Deploy software to the server.
7. Restart as prompted.

When running the Data Mover Engine on the Workflow Server, make sure the Workflow Server can access all potential communication partners for the DME, including the FTP network of the K2 SAN and standalone systems.

Next, license the Workflow Server.

Related Topics

GV STRATUS servers logon account on page 245

Complete listing of device types, roles, and software packages for GV STRATUS devices on page 194

SabreTooth Rules, Xcode license process

Only the GV STRATUS server with role of Common Services requires this process.

The Workflow license is installed on the GV STRATUS server with role of Common Services. Typically the GV STRATUS Core server has the role of Common Services.

One STRATUS-RULES license is required for the Rules Engine software component in your GV STRATUS system. This is a SabreTooth floating license. Optional licenses for associated functionality include the following:

- STRATUS-TRANSCODE
- STRATUS-XCODECONTROLCARBONCODER
- STRATUS-XCODECONTROLVANTAGE
- STRATUS-XCODECONTROLELEMENTAL
- STRATUS-ASPERA
- STRATUS-XCODECONTROLMEWS
- STRATUS-XCODECONTROLMEWSEXT

If you received your system pre-configured from Grass Valley, licenses are already installed, so you can skip these tasks. Otherwise, do the following:

1. Refer to the license sheet that you received with your GV STRATUS license. The license sheet has the Sales Order number that you need.
2. On the GV STRATUS server with role of Common Services, run the SabreTooth License Manager, generate a unique ID, and send the email to Grass Valley requesting your license or licenses.

   Refer to this Topic Library for detailed licensing procedures.
3. When you receive your license file, use SabreTooth License Manager and install it on the server.

Configuring Engines settings: Workflow

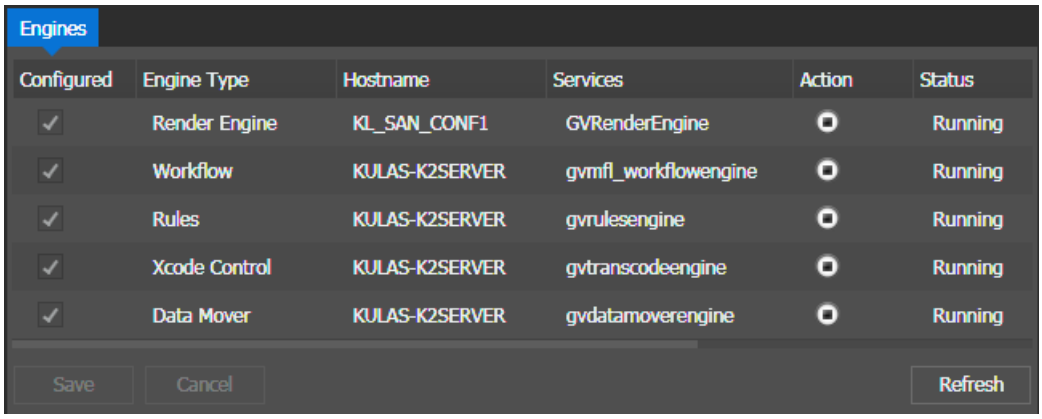
Systems using GV STRATUS rules require this process. This includes systems with and without a separate Workflow Server.

If you received your system pre-configured from Grass Valley, your Engines settings are already configured so you can skip these tasks. Otherwise, work through this section to configure your Engines settings.

To locate these settings, click **Core | Engines**

Depending on the workflow and bandwidth requirements of your system, Grass Valley may provide a system design in which multiple engines of the same type run on one or more servers. Configure engines as specified by your system design.

1. In the Control Panel application, open Engines settings.



Settings are described as follows:

Setting or button	Description
Configured	Selects an Engine for which settings are saved.
Hostname	The name of a GV STRATUS server that hosts the Engine.
Engine Type	The Engine components installed on the GV STRATUS server.
Status	Indicates if the Engine service is running or stopped.
Action	Starts and stops the Engine service.
Save	Saves current settings to selected GV STRATUS servers.
Cancel	Returns settings to their last saved state.
Refresh	Updates the list.

2. Click **Refresh** to make sure the list has the latest information from SiteConfig.
3. Verify that GV STRATUS servers with one or more of the following roles are listed, with corresponding Engine Types:
   - GV STRATUS Workflow Engine
   - GV STRATUS Rules Engine
   - GV STRATUS Xcode Control Engine
4. To save settings, in the **Configured** column, select each GV STRATUS server with one of the Engine Type roles.

   You must save settings at initial install/config and any time a GV STRATUS server with an Engine Type role is added, removed, or modified in SiteConfig.
5. Click **Save**.

   Settings are saved to the selected GV STRATUS servers.

Next, configure rules.

Proxy Streaming Server set up process

Only systems with the Proxy Streaming Server require this process. Use SiteConfig for network setup and software install.

GV STRATUS supports the Proxy Streaming Server, which will allow the GV STRATUS Web Client to offer frame accurate playback of proxy material, within an HTML5 standard browser. This is essential for GV STRATUS Web Client users to edit clips, apply logging, create subclips, and generate STRATUS EDLs within a web client environment.

Important: The Proxy Streaming Server must be configured in order to use the Simple Editor tool in* GV STRATUS *Web Clients.

If you received your Proxy Streaming Server already set up from Grass Valley, skip set up tasks and do the test task only.

1. *SiteConfig Proxy Streaming Server network set up* on page 907. Only systems with a Proxy Streaming Server require this process.
2. *SiteConfig Proxy Streaming Server software install* on page 909. Only systems with a Proxy Streaming Server require this process.
3. *SabreTooth Proxy Streaming Server license process* on page 910. Only systems with a Proxy Streaming Server require this process.
4. *Configuring settings: Proxy Streaming Server* on page 910. Only systems with a Proxy Streaming Server require this process.

SiteConfig Proxy Streaming Server network set up

Only systems with a Proxy Streaming Server require this process.

If you received your system already set up from Grass Valley, your Proxy Streaming Server or servers are already included in the SiteConfig system description and set up on the network, so you can skip these tasks. Otherwise, work through the topics in this section.

SiteConfig Proxy Streaming Server network set up

Only systems with a Proxy Streaming Server require this process.

If you received your system already set up from Grass Valley, your Proxy Streaming Server or servers are already included in the SiteConfig system description and set up on the network, so you can skip these tasks. Otherwise, work through the topics in this section.

Adding a Proxy Streaming Server to the SiteConfig system description

- Proxy Streaming Server(s) are racked, cabled, and powered on.

- The system description must contain a group.

This topic applies to a GV STRATUS server that is a Proxy Streaming Server.

1. In the **Network Configuration | Devices** tree view, right-click a group and select **Add Device**.
2. Configure settings for the device you are adding as follows:
   - Family: GV STRATUS
   - Device Type: GV STRATUS Server
   - Model: GV STRATUS Proxy Streaming Server
   - Name – This is the device name, as displayed in the SiteConfig device tree view and device list view. This name can be different than the host name (network name). You can accept the default name or enter a name of your choice. Devices in the tree view are sorted alphabetically.
   - Amount — Select the number of Proxy Streaming Servers, according to your system design.
   - Platform — Select **x64**.
   - Control network– Select the control network.
   - Starting Address – Select from the list of available addresses on the selected control network. If adding multiple devices, this is the starting address, with addresses assigned sequentially to each device added.
3. Click **OK** to save settings and close.

   SiteConfig adds the Proxy Streaming Server to the system description as a placeholder device.
4. Verify that unmanaged control network interface is configured correctly and modify if necessary.

Next, add the Proxy Streaming Server to the control network.

Adding a GV STRATUS server to the control network with SiteConfig

Use SiteConfig to configure network settings on a separate GV STRATUS server.

Before doing this task, make sure the GV STRATUS server is added as a placeholder device to the SiteConfig system description.

The following steps are the standard tasks for adding a device to the control network using SiteConfig. Use these steps for the GV STRATUS server you are adding.

1. Discover the device using SiteConfig device discovery.
2. Assign the discovered device to the placeholder device in the SiteConfig system description.
3. Modify the control network interface to ensure communication on the control network.
4. Modify the host name and/or device name as desired.
5. Ping the device to verify network communication.
6. Verify credentials to ensure SiteConfig can install software on the device.
7. Generate and/or add to host tables as appropriate for your network.

Related Topics

Adding a device to a network with SiteConfig on page 490
Adding a device to a network with SiteConfig on page 490

SiteConfig Proxy Streaming Server software install

Only systems with a Proxy Streaming Server require this process.

If you received your system pre-configured from Grass Valley, software is already installed, so you can skip these tasks. Otherwise, work through the tasks in this section as follows:

Add software role for the Proxy Streaming Server

Before doing this task, make sure devices are added to the SiteConfig system description with the correct family and device type. Refer to *Complete listing of device types, roles, and software packages for GV STRATUS devices* on page 194.

1. As appropriate for your system design and licensing, in your SiteConfig system description, configure role as follows:
   - For your Core Server, or a separate Proxy Streaming Server, these roles are automatically added in SiteConfig when the GV STRATUS Proxy Streaming Server device is added. If not, add the new role as follows:
     - GV STRATUS Proxy Streaming Service
     - GV Embedded Security Manager
     - GV Log Manager
2. Save SiteConfig and verify in `C:\ProgramData\Grass Valley\ConfigurationDataFiles\SiteConfig` that .scsd and .config files are saved to the server.

If you want to verify all your currently configured SiteConfig roles, refer to the complete list of roles and software packages.

Installing software for the Proxy Streaming Server

Use SiteConfig to install software for the Proxy Streaming Server.

- The server on which you are installing software is in the SiteConfig system description and communicating on the control network.
- The server on which you are installing software has its credentials set in SiteConfig to allow access.

1. Verify the SiteConfig roles currently assigned to the server. If the roles are not correct for your system design, add or remove roles accordingly. The role should be as follows:
   - GV STRATUS Proxy Streaming Service
2. Add the server to a deployment group, such as the GV STRATUS deployment group.

3. Add the following file to the deployment group:
   - *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab file that apply to this device:
     - *GrassValley_STRATUS_Proxy StreamingService_x.x.x.cab*

   Refer to release notes for version numbers.
4. Do the SiteConfig **Check Software** operation on the server.
5. Verify that deployment tasks are set to **Install** for the files listed above.
6. Deploy software to the server.
7. Restart as prompted.
8. After deployment is complete, start the GV STRATUS Proxy Streaming Service.

Next, license the Proxy Streaming Server.

SabreTooth Proxy Streaming Server license process

The Proxy Streaming Server license should be installed on the GV STRATUS server with role of Common Services.

One STRATUS-PROXYSTREAMING license is required for each GV STRATUS server running the Proxy Streaming software component in your GV STRATUS system. This is a SabreTooth floating license. It is possible to deploy more than one Proxy Streaming Server per system. Each server must have its own license. This license enables web streamings, with the maximum number of 40 streams per server.

If you received your system pre-configured from Grass Valley, licenses are already installed, so you can skip these tasks. Otherwise, do the following:

1. Refer to the license sheet that you received with your GV STRATUS license. The license sheet has the Sales Order number that you need.
2. On the GV STRATUS server with role of Common Services, run the SabreTooth License Manager, generate a unique ID, and send the email to Grass Valley requesting your license or licenses.

   Refer to this Topic Library for detailed licensing procedures.
3. When you receive your license file, use SabreTooth License Manager and install it on the server.

Configuring settings: Proxy Streaming Server

If you received your system pre-configured from Grass Valley, your proxy streaming settings are already configured so you can skip these tasks. Otherwise, work through this section to configure your proxy streaming settings.

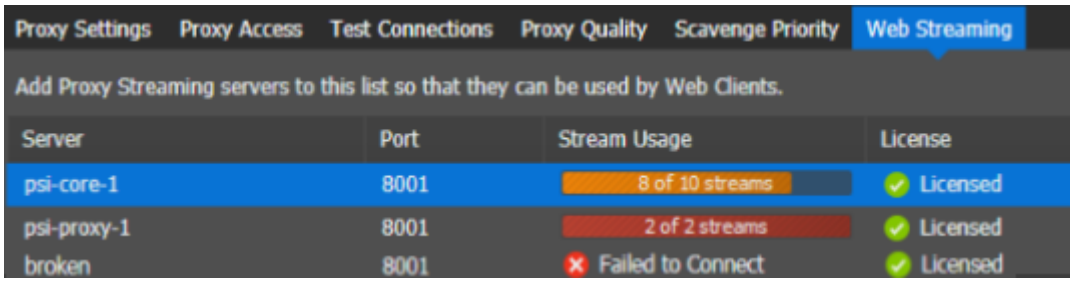
Important: The Proxy Streaming Server must be configured in order to use the Simple Editor tool in* GV STRATUS *Web Clients.

- This SiteConfig role must be assigned in the Express/Core server:
  - GV STRATUS Proxy Streaming Service

    — To enable frame accurate playback and the ability to seek, cue and mark proxy files in GV STRATUS Web Clients within an HTML5 standard browser.

- This license must be installed in the Express/Core server via SabreTooth:
  - STRATUS-PROXYSTREAMING
    — This license enables web streamings, with the maximum number of 40 streams per server.

1. In the Control Panel application, click **Core | Proxy Config | Web Streaming**.

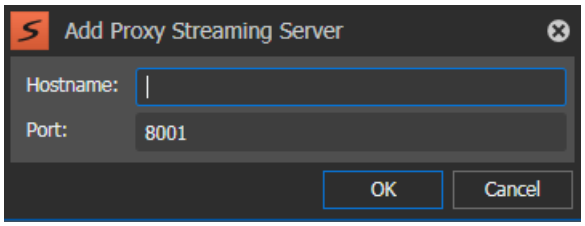


2. Configure settings as follows:

Setting or button	Description
Add	Opens the Add Proxy Streaming Server dialog box.
Modify	Opens the Modify Proxy Streaming Server dialog box for the selected server.
Configure	Allows you to configure the maximum number of stream usage and set the SSL certificate for secure connection of web streams.
Remove	Removes the selected server.
Save	Saves the current settings.
Cancel	Discards any new settings and reverts to the last saved settings.

3. Click **Add** to add the Proxy Streaming Server in your operation.

   The Add Proxy Streaming Server dialog box opens.



4. Configure settings as follows:

Setting or button	Description
Hostname	The name of the proxy streaming server to be used by GV STRATUS Web Clients in your system.
Port	Specifies the port number for the proxy streaming server. These ports are supported as below: • **8001** — This port is used for a specialized service for the transport of proxy streaming requests by the Proxy Streaming Gateway Service. By default, the service opens port 8001 for HTTP traffic. If the base port number is configured, this will be used as the HTTP port number. • **8002** — This port is used for a secure service for the transport of proxy streaming requests. The service must be configured with valid SSL certificates for browsers to successfully make use of WSS. By default, the service opens the port number incrementally after the HTTP port (e.g. if the HTTP port is 8001, the HTTPS port will be 8002). Except if the HTTP port is set to 80, the standard HTTPS will use port 443. • **8003** — This port is used by a web browser to assist with the setup of peer-peer WebRTC connections in complex network scenarios. By default, the service opens the port number incrementally after the HTTPS port (e.g. typically 8003). Except if the HTTP port is configured as 80, the standard STUN port of 3478 will be used.

5. Click **OK**.
6. Click **Configure** to set the maximum number of streams allowed for each Proxy Streaming Server or to set the SSL certificate for secure connection of web streams in your operation.

   NOTE: Each STRATUS-PROXYSTREAMING license enables web streaming in* GV STRATUS *Web Clients with up to 40 streams per server.

   When the core services are initially installed they automatically generate a type of certificate called a "self-signed" certificate. This certificate offers basic encryption capabilities, but cannot be used to verify the server. By default browsers do no trust self-signed certificates as they can be created by anyone and offer no protection against imposters and middle-man attacks.

   In order for the browser to trust the server and begin an HTTPS connection, it needs to validate a certificate. These certificates must come from a known organization called a certificate authority – one that the browser trusts to verify the server is who it says it is.
7. Click **Save** to save your Proxy Streaming Server settings.
8. Repeat steps 3-7 to add more Proxy Streaming Server(s), if applicable.

Fully qualified domain configuration

Only systems that must be integrated with a fully qualified domain require this process.

Use the topics in this section as appropriate for the site's domain requirements.

Prerequisites for Grass Valley domain configuration topics

Only qualified Grass Valley personnel should use these topics.

The topics in this section provide high-level configuration and reference information. The topics are intended for Grass Valley personnel that are certified for domain configuration. Conceptual explanations and detailed steps are not included, as these are assumed to be known by the certified individual. Do not attempt to use these topics if you are not qualified.

In the task flow for configuring a standard GV STRATUS system in customer documentation, instructions are not provided for a fully qualified domain. Those specialized instructions are provided in this section, but other standard system configuration instructions are not. Grass Valley personnel certified for domain configuration must combine the standard instructions with the specialized instructions as appropriate.

Active Directory integration checklist

These questions must be answered at the customer site before configuring the domain.

	Requirement	Question	Answer
☐	There must be a domain at the customer site.	What is the name of the current domain?	
☐	Grass Valley personnel must have access to DNS servers to view/verify DNS entries.	What are the names and IP addresses of DNS servers?	
☐	A dedicated domain is recommended but not required.	What is the name of the domain dedicated for Grass Valley systems?	
☐	A dedicated Organizational Unit (OU) is required.	What is the name of the OU dedicated for Grass Valley systems?	
☐	Local administrator rights are required.	What is the name of the Group Policy and OU to which local administrator rights are applied?	
☐	GV devices must be integrated into DNS.	Are you prepared to integrate GV devices into your DNS?	
☐	Non-complex passwords are required.	What is the name of the OU and/or Group that enables non-complex passwords?	

	Requirement	Question	Answer
☐	Domains must have trust relationships to allow GV services to run.	Are there multiple domains? If so, what are the trust relationships between domains?	
☐	Domain/DNS servers must be co-located with GV equipment.	Where are the Domain/DNS servers located?	

Users in a group in the domain

These users accounts and credentials are required.

Place the users in the table below into a Grass Valley Administrators group. Name the group with a name such "Grass Valley Administrators". Requirements for this group are as follows:

- Read and write permissions are given by default.
- Complex passwords must be disabled or not required.

Table 17: Grass Valley domain accounts

User name	Password	Permissions	Note
GVAdmin	Administrator password	Local admin	This account is required. It is the default internal system account.
movie	M0vieK2M0vie	Local admin	This account is required.
<an account to run Grass Valley services>	Administrator password	Local admin	This account is a recommended best practice. This account is dedicated to run Grass Valley services, so that problems with other accounts do not cause service access errors. It is named with a unique account name.

Internal system/domain account considerations

By default, the internal system account that the GV STRATUS system uses to access assets and some internal system functions is the GVAdmin account. If your site policies require a fully qualified domain account or a different account, that account must be configured throughout the GV STRATUS system.

You configure the internal system account settings in GV STRATUS Control Panel. To locate these settings, click **Core | STRATUS Core Services | Primary Site**. This account is used by the K2 Summit system and by the GV STRATUS system to write proxy files to the SMB proxy share on the server hosting the GV STRATUS system HTTP server.

Take the following into consideration if your system does not use the default internal system/domain account.

- All GV STRATUS, K2 Summit, High resolution media storage, and Proxy media storage servers must allow the internal system account to have administrator privileges. This includes the following:
  - The proxy share on the server hosting the GV STRATUS system HTTP server. Depending on system configuration, this could be one of the following types of servers:
    - GV STRATUS Express server
    - GV STRATUS Proxy server
    - GV STRATUS Proxy Storage file system server
  - Grass Valley Media Server MDI
  - The Xcode Engine working directory
  - K2 Summit system
  - The EDIUS project folder on the K2 media file system
  - An export share to which K2 media or GV STRATUS assets are exported
  - For consistency, a server that runs the FileZilla FTP service and the associated Generic FTP MDI settings can also use the internal system account for FTP access.

- GV STRATUS software components that are installed with the following installation packages require the internal system account. You configure this account in deployment options when you install the software.

  GrassValley_STRATUS_CommonServices

  GrassValley_STRATUS_ControlPanelService

  GrassValley_STRATUS_CoreServices

  GrassValley_STRATUS_CRArchive_MDI

  GrassValley_STRATUS_Databases

  GrassValley_STRATUS_DataMover

  GrassValley_STRATUS_DIVA_MDI

  GrassValley_STRATUS_ExternalMedia

  GrassValley_STRATUS_FlashNet_MDI

  GrassValley_STRATUS_GFTP_MDI

  GrassValley_STRATUS_HttpProxyServer

  GrassValley_STRATUS_IngestServices

  GrassValley_STRATUS_Masstech_MDI

  GrassValley_STRATUS_MediaFlow

  GrassValley_STRATUS_MEWS

  GrassValley_STRATUS_Proxy_MDI

  GrassValley_STRATUS_ProxyStreamingService

  GrassValley_STRATUS_RenderEngine

  GrassValley_STRATUS_Rules

  GrassValley_STRATUS_ScheduledTransferEngine

  GrassValley_STRATUS_SocialMedia

  GrassValley_STRATUS_Summit_MDI

  GrassValley_STRATUS_TrafficGateway

  GrassValley_STRATUS_Transcode

  GrassValley_STRATUS_WebApps

  GrassValley_STRATUS_WebClient

  GrassValley_DeviceKeyService

  GrassValley_LogManager

  GrassValley_LogViewer

- SQL Security logins must be configured for the internal system/domain account.

Related Topics

About the GV STRATUS system user on page 483

Configure domain on all Grass Valley products

Once the domain is set up, configure the domain on Grass Valley products.

Before doing this task, the Grass Valley personnel must have authority, or be working with on-site IT personnel who have authority, to configure GV computers and groups in the domain.

1. Add all Grass Valley devices to the domain.

   If you are using DNS that is available on the domain server make sure you update your DNS entry accordingly.

2. On GV STRATUS servers, configure GV STRATUS services to logon with your internal system/domain account.
   a) Open the Windows operating system Services Control Panel.
   b) From the following list, identify the services running on the server, and configure each of those services to logon with your internal system/domain account.

      - GV Device Key Service
      - GV Log Manager
      - GV Proxy Streaming Gateway Service
      - GV STRATUS ASK
      - GV STRATUS Control Panel Services
      - GV STRATUS Data Mover Engine
      - GV STRATUS External Media Engine
      - GV STRATUS Ingest Config
      - GV STRATUS Ingest Core
      - GV STRATUS Ingest DB
      - GV STRATUS MDI DIVA.
      - GV STRATUS MDI Flashnet.
      - GV STRATUS MDI Masstech.
      - GV STRATUS MDI GFTP. (Optional)
      - GV STRATUS MDI Proxy
      - GV STRATUS MDI Summit
      - GV STRATUS MediaFlow Workflow Engine
      - GV STRATUS Resolver
      - GV STRATUS Rules Engine
      - GV STRATUS Rules Wizard
      - GV STRATUS Scheduled Transfer Engine
      - GV STRATUS Social Media Engine
      - GV STRATUS Traffic Gateway
      - GV STRATUS Xcode Control Engine

   The following is an example of a script for automation from the command line. In this example the domain name is GVDOMAIN and the internal system account is GVAdmin:

   ```
   sc config "StorageUtilityHost" obj= "GVDOMAIN\GVAdmin" password=
   "yourpassword"
   ```

3. Identify the user groups that must be configured in GV STRATUS Authorization Manager to support the site's workflow, then do the following:
   a) If a group does not already exist in the domain, create the group in the domain.

      Make sure the group name corresponds to the group name required by the GV STRATUS workflow.

   b) Add users to groups to support the site's GV STRATUS workflow.

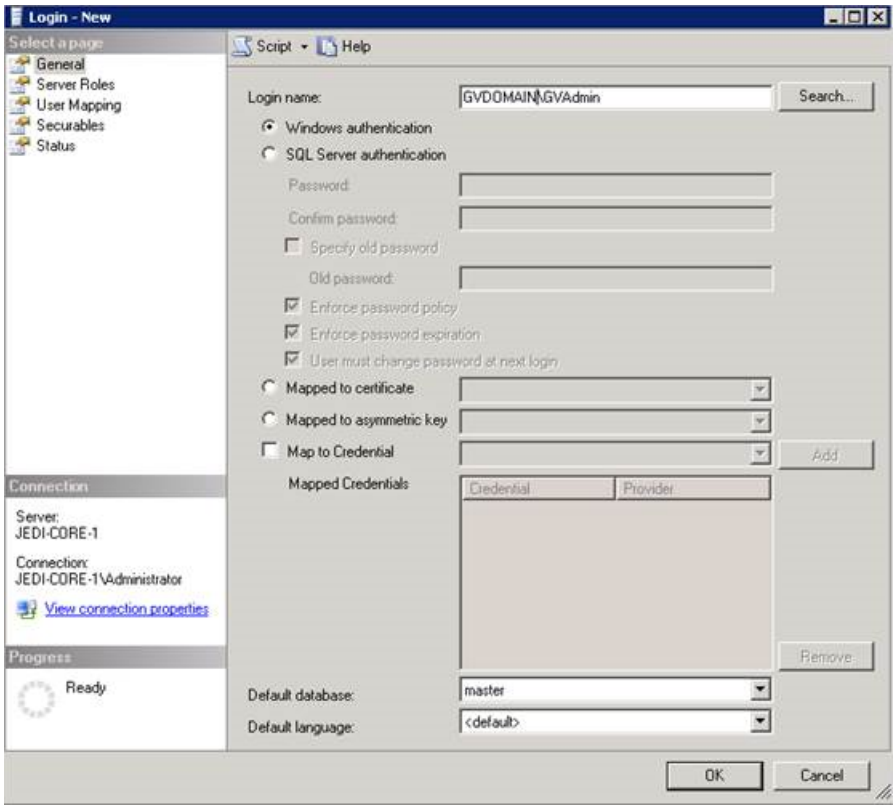
Configure SQL Security logins

On the GV STRATUS Core server, SQL Security logins must be configured for the internal system/domain account.

1. Open SQL as Administrator to log on.
2. Open SQL Server Management Studio and browse to **Security | Logins**.
3. Right-click on the Logins and add a new Login.
4. On the General page:

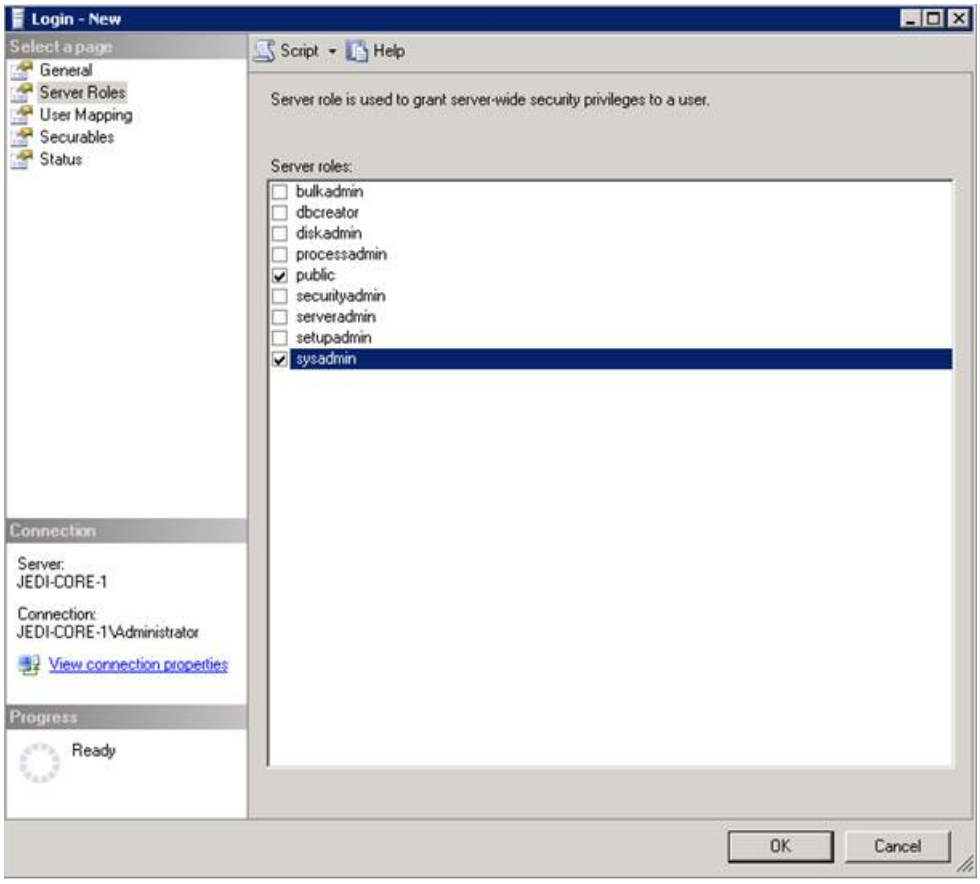
   In the **Login name** field, enter the internal system/domain account.

   For a domain GVDOMAIN, enter `GVDOMAIN\GVAdmin`.



5. On the Server Roles page:

   Check the box for **public** and **sysadmin** Server Roles.



6. Click **OK** to save settings and close.

Domain SiteConfig setup for software installation and upgrades

Before deploying software, you must ensure that the internal system/domain account is configured in deployment options. Failure to do so can result in the software installation process changing the internal system/domain account back to the default account. Once deployment options are configured, they are retained for future deployment sessions.

1. Follow steps for a normal GV STRATUS/Summit system, but with the following steps to ensure that the internal system/domain account is configured in deployment options.
2. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.
3. In the Tasks list view, view tasks and determine if you must set deployment options.

   Tasks that need to have deployment options set display in the Details column a message stating "Deployment options required."

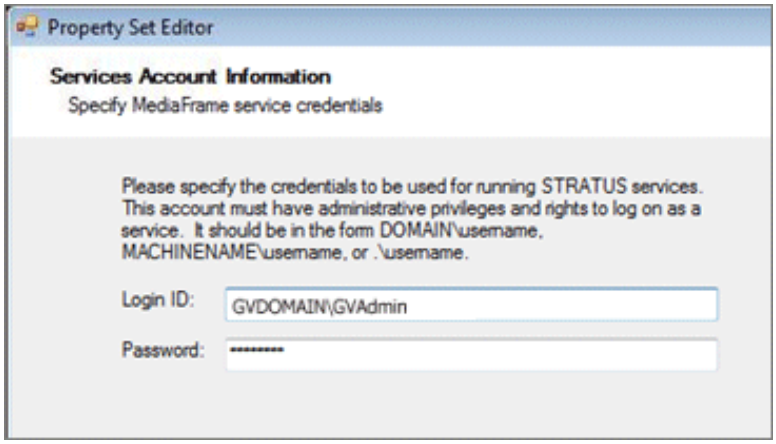
   If you select a task that needs to have its deployment options set, the Start Deployment button is disabled and the message is displayed next to the button.

4. Do one of the following to set deployment options:

   - Double-click the task.
   - Select the task and click the **Options** button.

   A wizard opens.

5. For the following install packages that require a services account, work through wizards and use the internal system/domain account.

Software	Deployment options
GrassValley_STRATUS_CommonServices GrassValley_STRATUS_ControlPanelService GrassValley_STRATUS_CoreServices GrassValley_STRATUS_CRArchive_MDI GrassValley_STRATUS_Databases GrassValley_STRATUS_DataMover GrassValley_STRATUS_DIVA_MDI GrassValley_STRATUS_ExternalMedia GrassValley_STRATUS_FlashNet_MDI GrassValley_STRATUS_GFTP_MDI GrassValley_STRATUS_HttpProxyServer GrassValley_STRATUS_IngestServices GrassValley_STRATUS_Masstech_MDI GrassValley_STRATUS_MediaFlow GrassValley_STRATUS_MEWS GrassValley_STRATUS_Proxy_MDI GrassValley_STRATUS_ProxyStreamingService GrassValley_STRATUS_RenderEngine GrassValley_STRATUS_Rules GrassValley_STRATUS_ScheduledTransferEngine GrassValley_STRATUS_SocialMedia GrassValley_STRATUS_Summit_MDI GrassValley_STRATUS_TrafficGateway GrassValley_STRATUS_Transcode GrassValley_STRATUS_WebApps GrassValley_STRATUS_WebClient GrassValley_DeviceKeyService GrassValley_LogManager GrassValley_LogViewer	

6. If you have multiple devices of the same type, you can enter deployment options for one of them using the wizard. Then, when you bring up the same wizard on every device, you can choose the **Use options from** radio button and select the first device for which you set options.

   SiteConfig copies the options you set for the first device and fills in the blanks on the wizard.

7. Install software via SiteConfig as you would for a standard GV STRATUS/Summit system.

Domain GV STRATUS Control Panel configuration

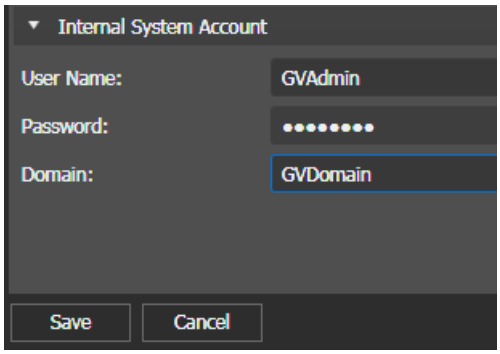
Before configuring GV STRATUS Control Panel:

- The entire system must be restarted in the following order so that the registry settings take effect:
  - K2 systems
  - All other servers
- GV STRATUS servers and K2 Summit systems must be licensed.
- K2 Summit system channels must be configured.
- Grass Valley recommends the GV STRATUS Control Panel is only configured on the Core server.

1. Configure Control Panel as you would a normal GV STRATUS system, except for the following steps.

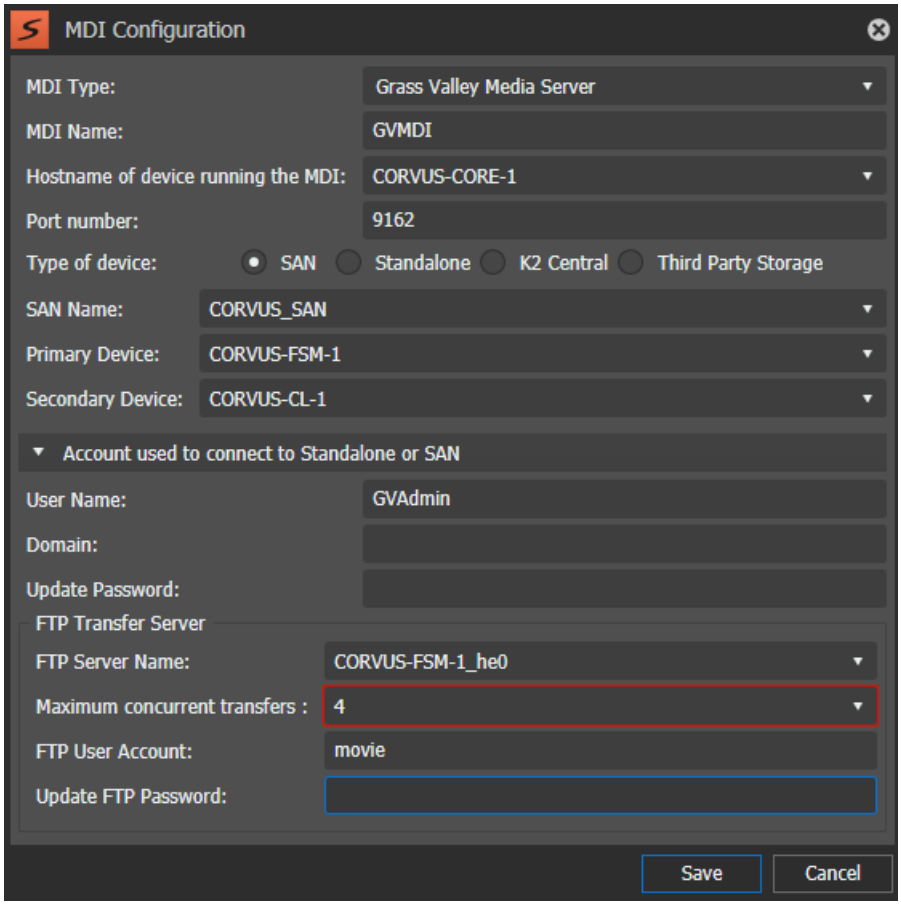
   In some fields you must manually enter text rather than selecting from a list.

2. Select **Core | STRATUS Core Service | Primary Site** and do the following:
   a) Set the Database Server to the core name and choose a site name.
   b) Under **Internal System Account**, enter the domain.



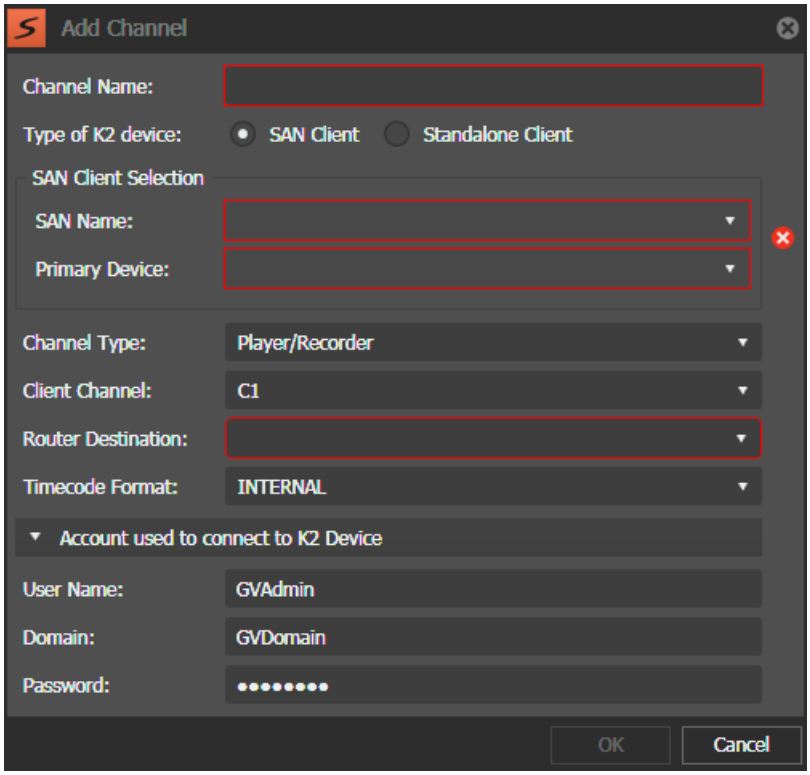
3. Select **Core | MDI** and configure a Grass Valley Media Server MDI to your SAN.

   The SAN name is arbitrary. Choose the name that you want to appear in the Navigator of GV STRATUS. Be sure to set the credentials to use the GVAdmin account on the fully qualified domain, such as GVDOMAIN.

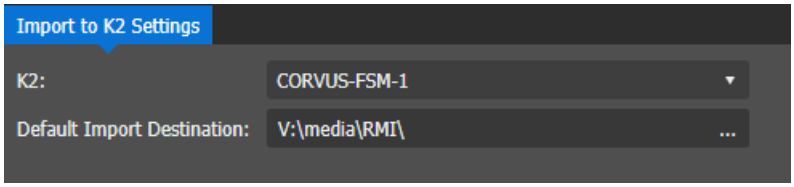


4. Select **Core | MDI** and set up Generic FTP MDI, if applicable.

5. Select **Applications | Ingest | Channel Setup** and set the credentials to use the internal system/domain account.



6. Select **Applications | RMI** and select the K2 system to import clips into.



   The K2 setting is the name you used for your Grass Valley Media Server MDI. After entering this you should be able to browse to the desired Default Import Destination.

7. Shut down the entire system.
8. Power up in the following order:
   - FSM/K2 Manager (Log in before powering up K2 Summit clients.)
   - K2 Summit systems (Verify AppCenter is functioning on each client before powering up other servers.)
   - All other servers.
9. Finish configuration of other devices (such as EDIUS, XRE/Render Engine, NCS/GV STRATUS Rundown, Archive servers etc.) as needed.

   Some reboots may be required.

Verify domain and internal system account

Make sure the correct accounts are configured throughout the system.

1. On GV STRATUS servers, verify that services are using the correct accounts.
   a) Open the Windows operating system Services Control Panel.
   b) From the following list, identify the services running on the server, and verify that the correct domain and internal system account is listed in the **Log On As** column.

      For example, verify that **GVDOMAIN\GVAdmin** is listed in the **Log On As** column.

      - GV Device Key Service
      - GV Log Manager
      - GV Proxy Streaming Gateway Service
      - GV STRATUS ASK
      - GV STRATUS Control Panel Services
      - GV STRATUS Data Mover Engine
      - GV STRATUS External Media Engine
      - GV STRATUS Ingest Config
      - GV STRATUS Ingest Core
      - GV STRATUS Ingest DB
      - GV STRATUS MDI DIVA.
      - GV STRATUS MDI Flashnet.
      - GV STRATUS MDI Masstech.
      - GV STRATUS MDI GFTP. (Optional)
      - GV STRATUS MDI Proxy
      - GV STRATUS MDI Summit
      - GV STRATUS MediaFlow Workflow Engine
      - GV STRATUS Resolver
      - GV STRATUS Rules Engine
      - GV STRATUS Rules Wizard
      - GV STRATUS Scheduled Transfer Engine
      - GV STRATUS Social Media Engine
      - GV STRATUS Traffic Gateway
      - GV STRATUS Xcode Control Engine

2. On the GV STRATUS Core Server, verify that AppPool is using the correct accounts as follows:
   a) Open the Windows operating system Server Manager.
   b) In the tree-view navigate to **Roles | Web Server (IIS) | Internet Information Services (IIS) Manager | Connections | <server_name> | Application Pools**.
   c) For the following Application Pool, verify that the correct domain and internal system accounts are listed in the **Identity** column.

      For example, verify that **GVDOMAIN\GVAdmin** is listed in the **Identity** column.

      - STRATUSAppPool

3. On the server hosting the GV STRATUS system HTTP server, such as GV STRATUS Express server, GV STRATUS Proxy server, or GV STRATUS Proxy Storage file system server, repeat steps and verify the following:

   AppPool:

   - HttpProxyAppPool

4. On the GV STRATUS Conform Server, repeat steps and verify the following:

   Windows Service:

   - GV STRATUS Conform Engine

   AppPool:

   - STRATUSAppPool

5. On the GV STRATUS Proxy Encoder, repeat steps and verify the following:

   Windows Service:

   - GV STRATUS MDI Encoder

   AppPool:

   - STRATUSAppPool

Grass Valley SMB Storage configuration

Prerequisites for SMB storage configuration topics

Only qualified Grass Valley personnel should use these topics.

The topics in this section provide high-level configuration and reference information about Grass Valley's support of Server Message Block (SMB) storage. The topics are intended for Grass Valley personnel that are certified for storage configuration. Conceptual explanations and detailed steps are not included, as these are assumed to be known by the certified individual. Do not attempt to use these topics if you are not qualified.

In the primary task flow for configuring a standard K2 or GV STRATUS system in customer documentation, instructions are not provided for SMB storage. Those specialized instructions are provided in this section, but the complete standard system configuration instructions are not. Grass Valley personnel certified for storage configuration must combine the standard instructions with the specialized instructions as appropriate.

Storage and domain requirements for SMB storage

The K2 Summit system on SMB storage must be created with the following requirements for hi-res and lo-res locations and domain.

- One private share:
  - Private Media Share: This is a high-resolution realtime network. This network must be segmented, non-routable, and private. For example purposes in these topics, this share is represented by the following:

    `\\gvstorage-private\mediashare`

- Two public shares:
  - Public Media Share: This is a high-resolution non-realtime network. For example purposes in these topics, this share is represented by the following:

    `\\gvstorage-public\mediashare`
  - Public Proxy Share: This is a low-resolution network. For example purposes in these topics, this share is represented by the following:

    `\\gvstorage-public\proxy`

    There should only be one proxy location used throughout the system.

- Besides configuring the Control Network, the following servers might require a special network adapter to connect to the SMB storage:
  - HTTP Proxy Server
  - Conform, Encoder, Render Engine, and XRE server(s)
  - FSM/K2 Manager
  - K2 Summit Clients systems

- The system must be on a fully qualified domain.

For details about configuring a specific brand of SMB storage to support K2 Summit systems, refer to the *Grass Valley Knowledge Base*.

SiteConfig software installation and upgrade on SMB storage systems

Before deploying software, you must ensure that roles are configured to support SMB storage. Failure to do so can result in the software installation process changing back to default roles. Once roles are configured, they are retained for future deployment sessions.

1. Follow steps for a normal GV STRATUS/Summit system, but with the following steps to ensure that roles are configured and software is installed.
2. Identify the software that corresponds to the following SiteConfig roles. This software must be uninstalled before these roles are removed.
   - All SNFS (StorNext File System) roles on K2 Summit clients, K2 Manager, XRE, Render Engine, Conform, Proxy Encoder, and HTTP Proxy server.
   - The iSCSI bridge role on the K2 Manager.

3. Using SiteConfig, uninstall the identified software.
   a) In the **Software Deployment | Deployment Groups** tree view, select the device or the group of devices to which you are deploying software.

      The corresponding software deployment tasks are displayed in the Tasks list view.

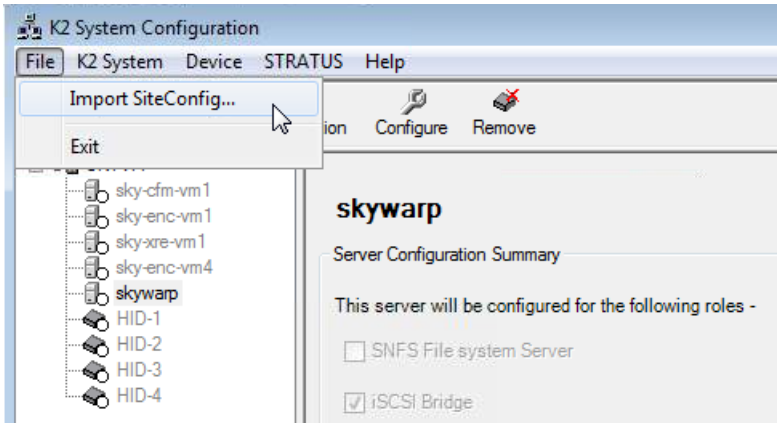
   b) For the software you are deploying, select the **Deploy** check box in the row for the uninstall task.
   c) Unselect the **Deploy** check box for all other deployment tasks for all other software.
   d) Click the **Start Deployment** button.

      Deployment tasks run and software is uninstalled. Progress is reported and next steps are indicated in both the Status and Details columns.

   e) Perform manual steps if indicated, such as dismissing a dialog box on the device and/or restarting the device.
   f) Monitor progress as indicated by both the Status and Details column. When finished, the Status column indicates complete.
4. Remove SiteConfig roles as follows.
   - All SNFS (StorNext File System) roles on K2 Summit clients, K2 Manager, XRE, Render Engine, Conform, Proxy Encoder, and HTTP Proxy server.
   - The iSCSI bridge role on the K2 Manager.
5. Add the GV STRATUS Summit Services role to the K2 Manager.
6. Sync to the core as follows:
   a) Select **Tools | Options | Network Configuration**, and enter the core server name.
   b) Select **File | Save**.
7. Install software via SiteConfig as you would for a normal GV STRATUS/Summit system.

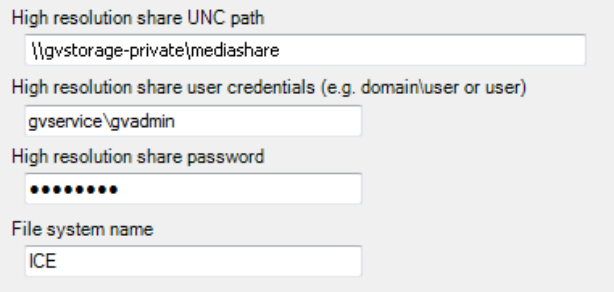
K2Config setup for SMB storage

1. After deploying software, note the location of the saved SCSD in the SiteConfig title bar.
2. Open K2Config ("K2 System Configuration" on the desktop).
3. Select **File | Import SiteConfig** to import the SCSD file into K2Config.



4. Switch from **Online Production** to **ThirdPartyNAS**.

5. Configure the K2 Manager with the UNC path, the high res domain credentials and a chosen File system name.



   If using FT Server (NEC) for K2 Manager or NH (FTP) roles, connections are the same for all roles. There is one connection to the Private Media Share and one connection to the control (not SMB storage) network. Both control and FTP traffic use the control network. There is no separate connection for FTP traffic.

6. If you have GV Render Engine without the Advanced Encoder role in your operation, remove the GV Render Engine from K2Config.
7. After the K2 Manager reboots, configure the Summit clients. The K2 Manager settings are used by default.
8. Configure the proxy server, and encoder to use SMB Attached storage access.
9. Under **STRATUS | Network Configuration**, make sure that the core server name is entered.
10. Under **STRATUS | Sync to Control Panel**, select "Overwrite… " and Sync now.
11. Verify that the SiteConfig and K2Config files are up-to-date in the following directories on the core:
    - *C\ProgramData\Grass Valley\ConfigurationDataFiles\K2Config*
    - *C\ProgramData\Grass Valley\ConfigurationDataFiles\SiteConfig*

Reapply K2 services to the domain after upgrade

When upgrading K2 system software on a system with SMB storage, you must do the following:

- Re-apply the K2Config **ThirdPartyNAS** settings after each K2 Summit system upgrade.

GV STRATUS Control Panel configuration for SMB storage

Before configuring GV STRATUS Control Panel:

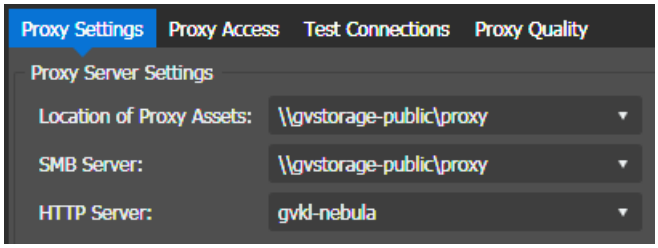
- The entire system must be restarted in the following order so that the registry settings take effect:
  - K2 systems
  - All other servers
- GV STRATUS servers and K2 Summit systems must be licensed. License K2-NASCONNECT is required.

- K2 Summit system channels must be configured.

1. Configure Control Panel as you would a normal GV STRATUS system, except for the following steps.

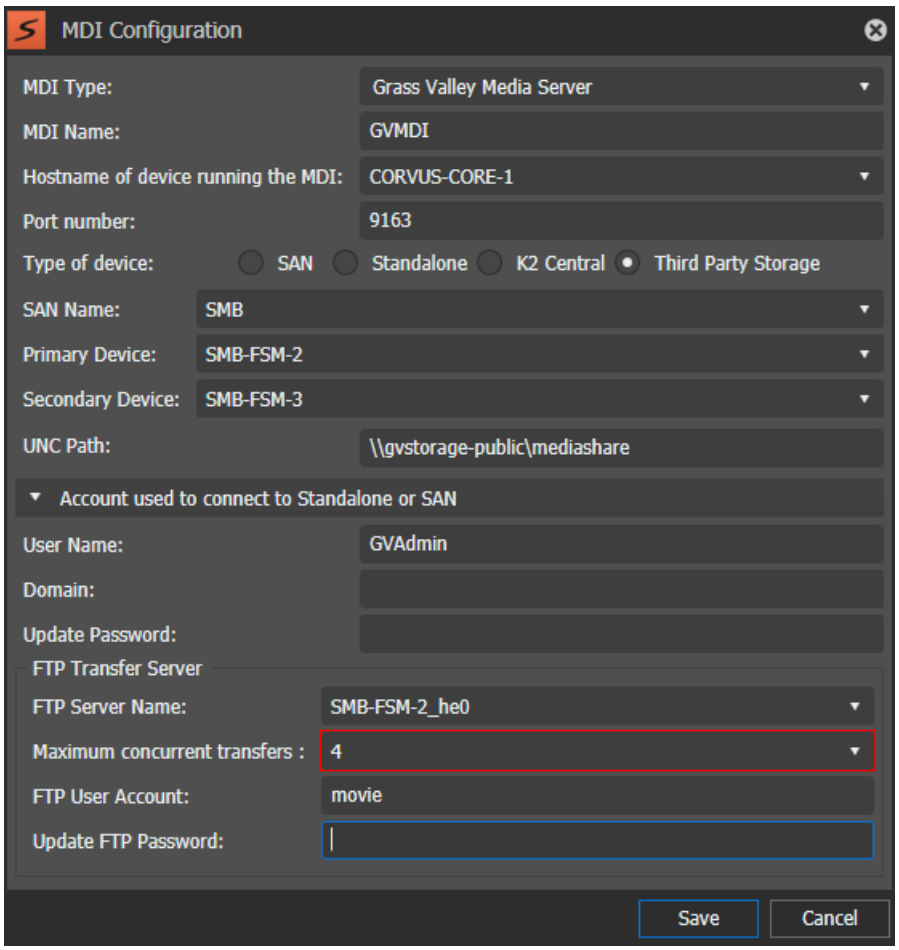
   In some fields you must manually enter text rather than selecting from a list.

2. Select **Core | Proxy Config | Proxy Settings** and do the following:
   a) Set the Location of Proxy Assets and SMB Server to the Public Proxy share, such as `\\gvstorage-public\proxy`.



   b) Enable proxy Creation to set the proxy registry keys on the Summit clients.
   c) Enable Proxy Encoders for auto-scavenging.
   d) Save and Test Connections.

3. Click **Core | MDI Configuration | Add | Grass Valley Media Server**, select **Third Party Storage** option for the Type of Device, and enter the **UNC Path** to the Public Media share, such as `\\gvstorage-public\mediashare` .



   The MDI service will map to this location.

4. For the SAN name, enter the name of the SMB storage system.
5. To set the primary and secondary device, select as follows:
   - If there is only one client, use the client as the primary device and the FSM/Storage Manager as the secondary device.
   - If a shared storage, configure the primary FSM or Storage Manager as the primary device and the secondary FSM (if exists) or FTP Server as the secondary device.
6. Mount the SMB storage Public Media Share, such as `\\gvstorage-public\mediashare`, as the V: drive on the hi-res PC.

   You can also mount the removable media to the PC.
7. Shut down the entire system.

8. Power up in the following order:
   - FSM/K2 Manager (Log in before powering up K2 Summit clients.)
   - K2 Summit systems (Verify AppCenter is functioning on each client before powering up other servers.)
   - All other servers.

High resolution GV STRATUS client with SMB storage setup

- The client PC must meet GV STRATUS client PC system requirements.
- The client PC must not have a special network adapter to connect to the SMB Storage.

1. Do the following steps to setup a standard GV STRATUS high resolution client PC.
   a) Install GV STRATUS software on the client PC.
   b) In GV STRATUS Control Panel, configure the client PC as a high resolution client.
   c) In GV STRATUS Control Panel, assign licenses and roles as appropriate for user accounts and customer site workflows.
2. On the client PC, map the `V:` drive to the Public Media Share.

EDIUS/XRE Setup for SMB storage

1. Install/upgrade EDIUS and GV Render Engine software as directed by standard instructions in GV STRATUS customer documentation.

   Make sure you follow the proper sequence for installation and running applications.
2. Mount the `V:` drive to your GV Render Engine server and any high resolution STRATUS/EDIUS clients.
   - For SMB storage, mount the Public Media Share, such as the following:

     `\\gvstorage-public\mediashare`
3. Add an EDIUS project folder at the root of the `V:` drive, as directed by standard instructions in GV STRATUS customer documentation.
4. In GV STRATUS Control Panel, click **Applications | EDIUS | EDIUS Project** and set **Default project location** to the UNC path of the above EDIUS folder, as follows:
   - For SMB storage, use a path to the Public Media Share, such as the following:

     `\\gvstorage-public\mediashare\EDIUS`

GV STRATUS Rundown setup for SMB storage

If the system with SMB storage uses GV STRATUS ActiveX for the GV STRATUS Rundown drag-and-drop workflow, implement the workaround for the following Known Problem.

DE7006	Description:	After dragging a clip from GV STRATUS ActiveX to the playlist in GV STRATUS Rundown on an SMB (Isilon) system, the clip status never changes to Ready.

	Workaround:	On the K2 Media Server with role of file system server (FSM), add a domain key to the config file found at *C:\Program Files (x86)\Grass Valley\ STRATUS Summit Service\Atlas.Service.Summit.ServiceHost.exe.config*. The following example illustrates a domain key with value gvservice.com.
		`<appSettings>`
		`  <add key="Hostname" value="localhost"/>`
		`  <add key="Username" value="GVAdmin"/>`
		`  <add key="Password" value="yourpassword"/>`
		`  <add key="Domain" value="gvservice.com"/>`
		`</appSettings>`
		Restart the K2 Media Server to put the change into effect. This requires a restart of the entire system. Make sure you use the correct sequence for shutdown and power up of devices.

You must implement this manual workaround after every upgrade.

K2 Central Storage configuration

Use the topics in this section as appropriate for the K2 Central Storage configuration.

Prerequisites for K2 Central storage configuration topics

Only qualified Grass Valley personnel should use these topics.

The topics in this section provide high-level configuration and reference information about K2 Central storage. The topics are intended for Grass Valley personnel that are certified for storage configuration. Conceptual explanations and detailed steps are not included, as these are assumed to be known by the certified individual. Do not attempt to use these topics if you are not qualified.

Storage and domain requirements for K2 Central

- K2 Central TX Shared Storage supports up to five K2 Summit clients, with 16 channels of 100 Mb/s video streams or up to 20 channels of 50 Mb/s video streams simultaneously.
- Both the Control and FTP networks must be configured for the K2 Central.
- Only the Control network needs to be configured for K2 Summit clients.
- Discovery agents must be installed on K2 Central and K2 Summit clients.
- K2 Central cannot be configured as a proxy server/storage.

- For an Express GV STRATUS system, the K2 Central proxy must be configured to the Express core storage.
- For a medium A1 GV STRATUS system, the K2 Central proxy must be configured to a separate K2 Summit SAN if a SAN is also part of the system. The proxy server must be a K2 SAN client to the SAN system.
- For a large B1/C1 GV STRATUS system, the K2 Central proxy must be configured to the Proxy Storage system server.
- Administrator/GVAdmin passwords could be changed, if necessary.
- Hosts files must be updated and added to domain.

K2 Central Storage setup and installation

Configure as follows:

1. Disconnect network cables and unplug direct connections from K2 Central server to the K2 Summit clients.
2. Switch off the power to K2 Central and take out the front drives.
3. Power on the K2 Central, insert the USB thumb drive, load Acronis, and use the `K2central_v1-11.tib image` to image the K2 Central.

   The K2 Central will reboot automatically after the imaging process.
4. Power off the K2 Central to reinsert the front drives, and switch on the power again for the K2 Central server.
5. Configure the Control and FTP networks on the K2 Central server.
6. Update hosts files and add to domain.
7. Install Discovery Agent, and select K2 Central Server as the server type.
8. Procure the *GrassValley_K2system_ x.x.x.x.cab*, and install via SiteConfig. Then, reboot the K2 Central server.
9. On the K2 Central desktop, run Storage Initializer to create a new file system. Then, reboot the K2 Central server.
10. After initializing storage, run the K2 Central Config to set the number of FTP streams for K2 Central server to **10**.
11. Share the V: drive of the K2 Central.
12. If you have EDIUS configured in your system, create an EDIUS folder on the V: drive.
13. If the GVAdmin password was changed, update the following file on the K2 Central server:

    `C:\Program Files (x86)\Grass Valley\STRATUS Summit Service\Atlas.Service.Summit.ServiceHost.exe.config`

NOTE: K2 Config does not support the K2 Central system. K2 Central will be corrupted if configured to K2 Config. For GV STRATUS versions 4.8 and higher, K2 Centrals are configured entirely in GV STRATUS Control Panel, once they have been deployed via SiteConfig as K2 Central devices. If you configured a K2 Central in GV STRATUS version 4.5, please refer to the 4.8 upgrade procedures to undo the manual steps that were required to configure K2 Central with GV STRATUS 4.5 application.

SiteConfig software installation on K2 Central

The K2 Summit clients must be disconnected from the K2 Central while software is installed.

1. Follow steps for a normal GV STRATUS/Summit system SiteConfig software installation, but with the following steps to ensure that correct roles are configured and software is installed.
2. In the **Network Configuration | Devices** tree view, right-click a group and select **Add Device**.
3. Configure these settings for the K2 Central server as follows:
   - Family – Select **K2**.
   - Type – Select **K2 Central Server**.
   - Model – Select **K2 Central TX Server**.
   - Name – This is the device name, as displayed in the SiteConfig device tree view and device list view. This name can be different than the host name (network name). You can accept the default name or enter a name of your choice. Devices in the tree view are sorted alphabetically.
   - Amount — Select **1**.
   - Platform — Select **x64**.
   - Control network– Select the control network.
   - Starting Address – Select from the list of available addresses on the selected control network.
4. Then add K2 Summit clients as follows:
   - Family – Select **K2**.
   - Type – Select **K2 Central Client**.
   - Model – Select **K2 Central Client**.
   - Name – This is the device name, as displayed in the SiteConfig device tree view and device list view. This name can be different than the host name (network name). You can accept the default name or enter a name of your choice. Devices in the tree view are sorted alphabetically.
   - Amount — Select **1**.
   - Platform — Select **x64**.
   - Control network– Select the control network.
   - Starting Address – Select from the list of available addresses on the selected control network. If adding multiple devices, this is the starting address, with addresses assigned sequentially to each device added.
5. Click **OK** to save settings and close.

   SiteConfig adds the K2 Central server and K2 Central clients to the system description.
6. Add the K2 Central Server and K2 Central clients to the control network.
7. Then, add the K2 Central Server and K2 Central clients to the desired software deployment group.
8. Add the **GV STRATUS Summit Service** role to the K2 Central server.
9. Add the appropriate system cabs and deploy software.
10. Sync to the core server as follows:
    a) Select **Tools | Options | Network Configuration**, and enter the core server name.
    b) Select **File | Save**.
11. Configure and install other GV STRATUS/Summit devices as you normally would.

12. Connect K2 Central clients to the K2 Central server once software is installed.

    The K2 Central clients should be automatically configured to the K2 Central storage.

13. Reboot K2 Central clients after connecting them to the K2 Central server.

K2 Summit clients setup for K2 Central

Configure settings as follows:

- Re-image the K2 Summit clients, by selecting K2 Central when imaging.
- Configure only the Control networks on the K2 Summit clients.
- Update hosts files and/or add to domain.
- Install the Discovery agent, and select **K2 Central client** as the server type when installing via SiteConfig.
- Reboot, and reconnect the direct connections to the K2 Central server.
- Configure K2 Summit clients, by applying K2 Central settings to each Summit.
- License the K2 Summit clients and configure K2 channels as desired.

GV STRATUS Control Panel configuration for K2 Central

Before configuring GV STRATUS Control Panel:

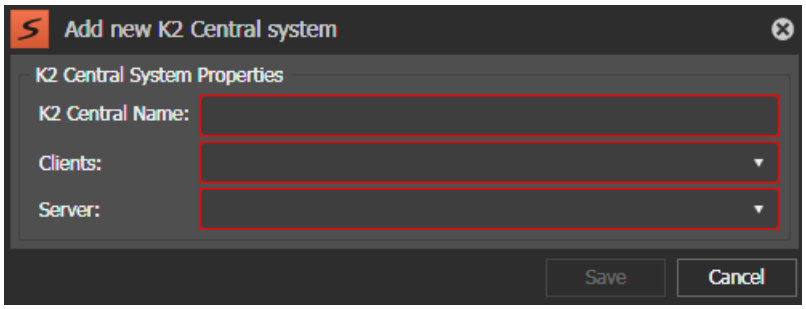
- The entire system must be restarted in the following order so that the registry settings take effect:
  - K2 systems
  - All other servers
- GV STRATUS servers and K2 Summit systems must be licensed.
- K2 Summit system channels must be configured.

1. Configure Control Panel as you would a normal GV STRATUS system, except for the following steps.

   In some fields you must manually enter text rather than selecting from a list.

2. Select **Core | K2 Storage | K2 Central | Add**.

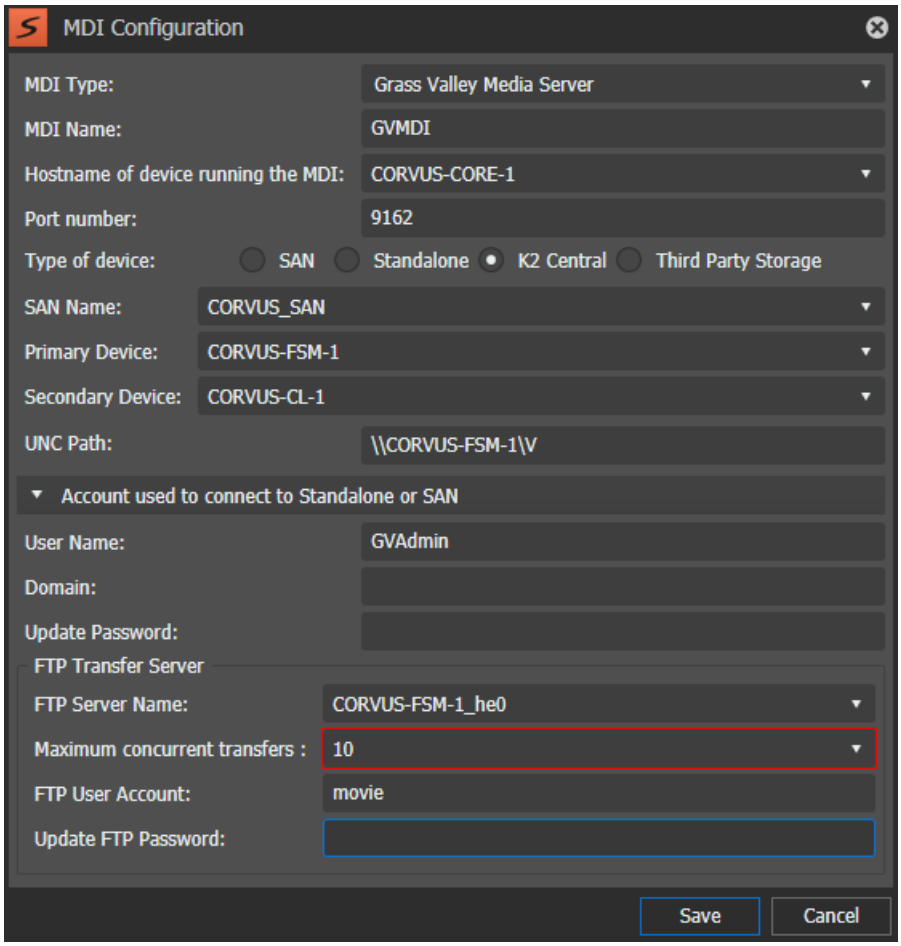
   The **Add new K2 Central system** dialog box appears.



3. Enter the name of the K2 Central system, select the K2 Central server and K2 clients for the system, and click **Save**.

   To add multiple K2 Central systems, you can use the **Add** button repeatedly on the K2 Central tab.

4. Select **Core | MDI** and configure a Grass Valley Media Server MDI for the K2 Central system.



5. Select **K2 Central** for the Type of device.

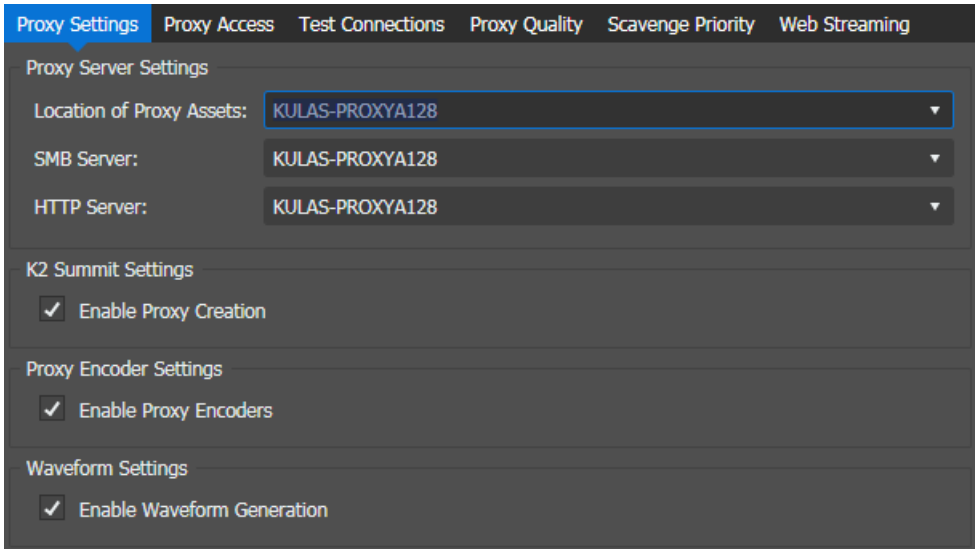
   For the SAN name, enter the name of the K2 Central system. Then, enter the UNC path to the K2 Central system.

   Select the Summit client or server designated to be the primary and secondary device, if applicable.

   NOTE: For optimum system performance, it is recommended that if there are K2 Summit Clients use them for the primary and secondary device. If there is only one client, use the client as the primary device and the FSM/Storage Manager as the secondary device.

   Be sure to set the credentials to use the GVAdmin account on the fully qualified domain, such as GVDOMAIN. Then, click **Save**.

6. Select **Core | Proxy Config | Proxy Settings** and do the following:
   a) Set the Location of Proxy Assets, SMB Server, and HTTP Server.



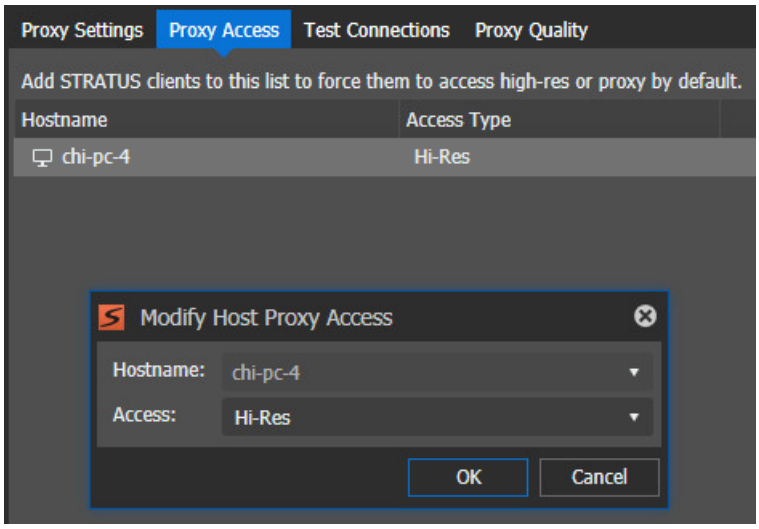
   b) Enable proxy Creation to set the proxy registry keys on the Summit clients.
   c) Enable Proxy Encoders for auto-scavenging.
   d) Enable Waveform Generation for proxy files if you need it for EDIUS systems in your operation.
   e) Save and Test Connections.
7. Shut down the entire system.
8. Power up in the following order:
   - FSM/K2 Manager (Log in before powering up K2 Summit clients.)
   - K2 Summit systems (Verify AppCenter is functioning on each client before powering up other servers.)
   - All other servers.
9. Finish configuration of other devices (such as EDIUS, XRE/Render Engine, NCS/GV STRATUS Rundown, Archive servers etc.) as needed.

   Some reboots may be required.

High resolution GV STRATUS client with K2 Central setup

- The client PC must meet GV STRATUS client PC system requirements.

1. Do the following steps to setup a standard GV STRATUS high resolution client PC.
   a) Install GV STRATUS software on the client PC.
   b) In GV STRATUS Control Panel, click **Core | Proxy Config | Proxy Access** to configure the client PC as a high resolution client.



   c) For Hostname, select the name of the GV STRATUS PC that you are setting as high-resolution client.
   d) For Access, select **Hi-Res**.
   e) Click **OK** to save settings and close.
2. On the client PC, map the `V:` drive to the K2 Central server.

EDIUS/GV Render Engine Setup for K2 Central

1. Install/upgrade EDIUS and GV Render Engine software as directed by standard instructions in GV STRATUS customer documentation.

   Make sure you follow the proper sequence for installation and running applications.
2. On the K2 Central server, share the V: drive.
3. To configure the EDIUS share folder, contact Grass Valley Support for the qualified setup and configuration with all GV STRATUS system types.
4. Mount the `V:` drive to your GV Render Engine server and any high resolution GV STRATUS/EDIUS clients.

5. In GV STRATUS Control Panel, click **Applications | EDIUS | EDIUS Project** and set **Default project location** to the UNC path of the above EDIUS folder, as follows:

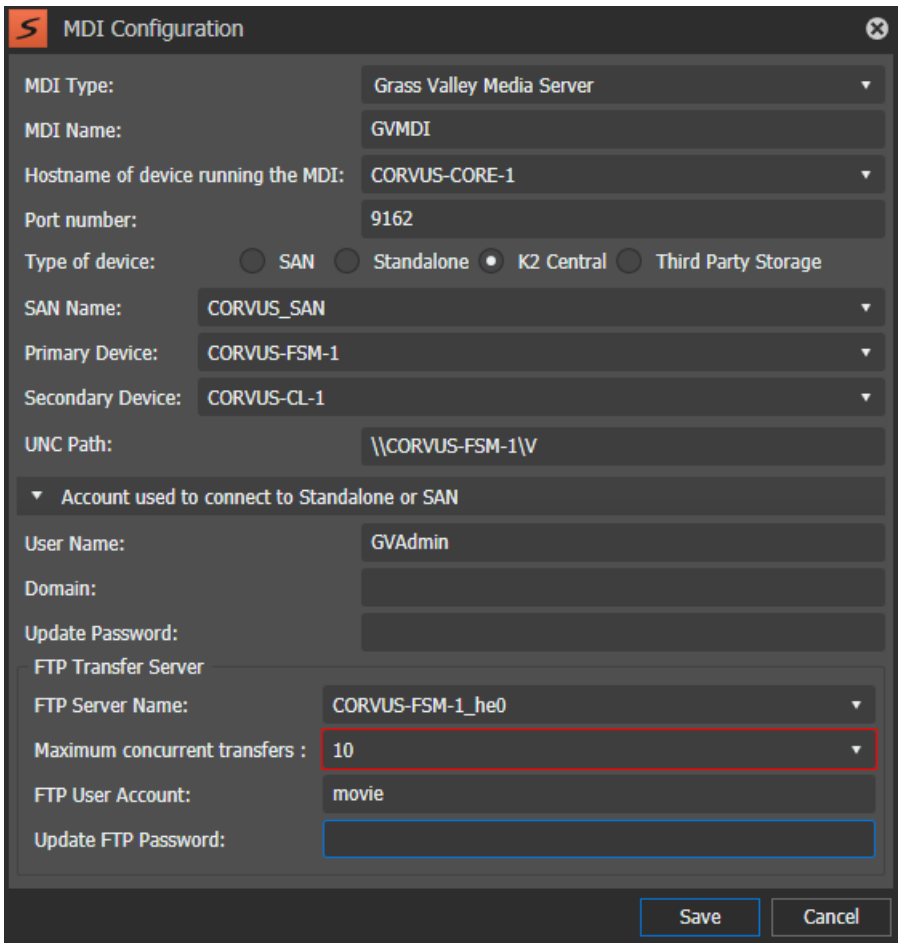
   - For K2 Central, use a path to the EDIUS folder on the K2 Central server, such as the following:

     `\\[K2CentralServerName]\V\[EdiusFolderName]`

   NOTE: If there are multiple K2s on the* GV STRATUS *system besides the K2Central, then the EDIUS project folder may be located on a different K2.

6. Click **Core | MDI Configuration | Add | Grass Valley Media Server** and set **K2 Central** for the type of K2 device. Select the K2 Central system as the SAN Name, Primary Device, Secondary Device, and set the UNC path to the K2 Central system.

   NOTE: For system performance, is it recommended that if there are K2 Summit Clients use them for the primary and secondary device. If there is only one client, use the client as the primary device and the FSM/Storage Manager as the secondary device.



   Complete the MDI configuration and click **Save**.

7. In the **Core | Engines** settings, verify that each GV Render Engine is displayed, desired streams configured, and the engine status is running.

8. If you have EDIUS Workgroup or EDIUS XS workstations; on EDIUS Server Settings, configure as follows:

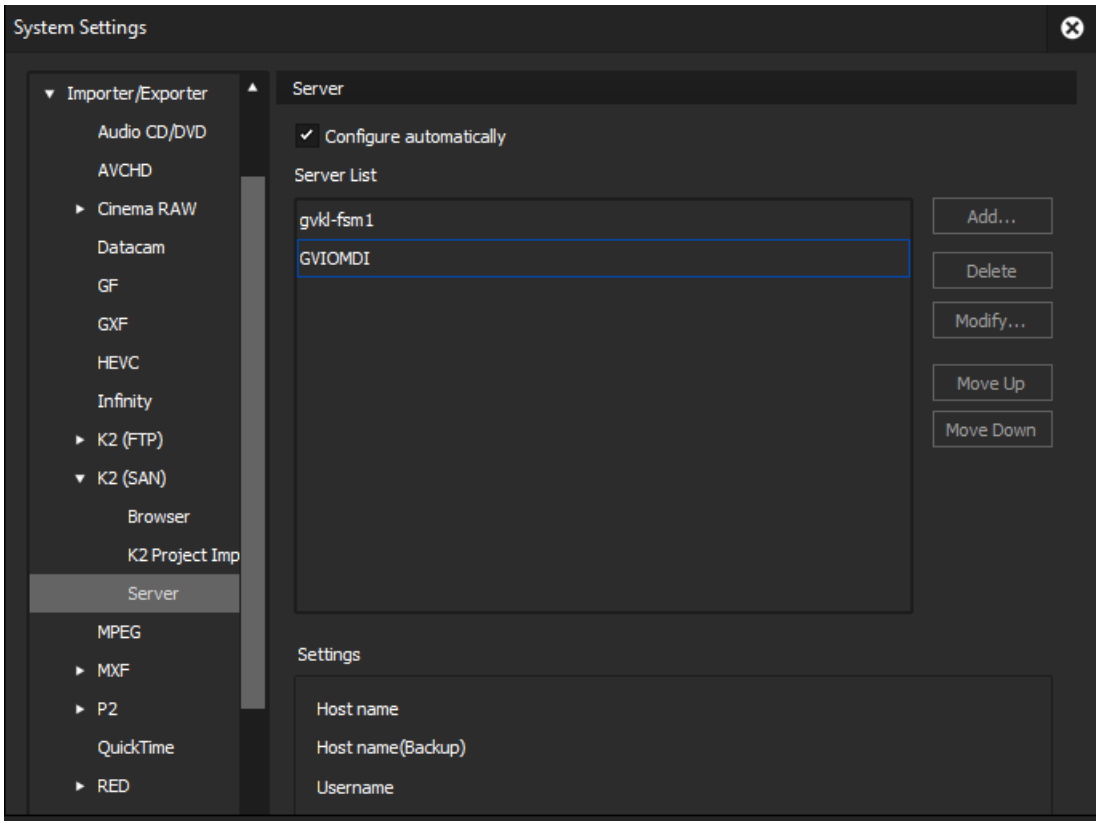
   These settings must be the same as your UNC path already configured on the GV STRATUS Control Panel. The settings identify the storage locations EDIUS accesses. A K2 storage location can be a K2 Summit standalone system or for a K2 SAN, the K2 Media Server with role of file system server (FSM).

   a) From the EDIUS application, click **Settings | System Settings**.

      EDIUS System Settings window opens.

   b) In the Importer/Exporter tree-view, click **K2 (SAN)**.

      Server settings open.



   c) Users are recommended to select the **Configure automatically** check-box.

      For the **Configure automatically** setting, take note of the following:

      - If the **Configure automatically** check-box is selected, the K2(SAN) drives will be automatically populated after each installation or software upgrade.

        NOTE: If the Grass Valley Media Server MDI has UNC path settings configured for third party storage, K2 central, or K2 Summit standalone; each server will be mapped according to its UNC path and not to a drive letter.

      - If the **Configure automatically** check-box is not selected, configure the K2 storage location following these steps below.

   d) In **Server** section, click **Add**.

The **Server Settings** dialog box opens.

e) Verify or make settings as follows.

Table 18: Server Settings

Setting	Value
Name	Enter a name that identifies the K2 storage location to display in the folder view.
Address	Enter the IP address or DNS name of the server that is the K2 storage location.
Address(Backup)	If the K2 storage location is a redundant K2 SAN, the IP address or DNS name of the redundant K2 Media Server with role of file system server (FSM).
Username	Enter the user name required when making the connection to the server configured above. For example, GVAdmin.
Password	Enter the password required for the user name configured above.
Domain	Enter the domain for the user credentials configured above. If not a domain account, leave this setting blank.
Storage Drive	Select the K2 storage location. It must be a drive available on the local system. For a K2 SAN this is typically the `v:` drive. For a K2 Summit standalone system this is typically a mapped network drive.
Show only SNFS drives	For a K2 SAN, select this setting. For a K2 Summit standalone system, clear this setting.
Connection Test	Click this button to test the connection to the server with the settings entered in the **Server settings** dialog box.

f) Click **OK** to save settings and close.

9. Restart the entire GV STRATUS system in the following order:

   - B1 proxy server (if applicable)
   - K2 Central servers, Stand-alones, primary FSMs
   - Secondary FSMs (if applicable)
   - All K2 Summits, iSCSI clients, GVREs, PCs
   - Core/Workflow/DME servers

10. Open Embedded Security Managers on the K2 Central and K2 Summit clients, and put them in Enabled mode.

Troubleshooting the GV STRATUS system

Troubleshooting tools

You can use the following to troubleshoot your GV STRATUS system:

- The GV STRATUS application Status Viewer panel.
- The GV Log Viewer application, on GV STRATUS servers.
- Windows Event Viewer

Also refer to K2 system documentation for K2 troubleshooting information.

Related Topics

Working with GV Log Viewer on page 472

If you have trouble launching EDIUS XS

Confusion about EDIUS for GV STRATUS licensing can cause problems.

The following is required in order to launch the EDIUS for GV STRATUS as a low-resolution editor (EDIUS XS) correctly:

- Your GV STRATUS system must have a Flex, Pro, or Elite license.
- You must be logged on with the EDIUS XS role assigned.
- The client PC on which you are launching EDIUS must not be licensed for EDIUS Workgroup. This is an EDIUS license, intstalled on the client PC and managed by EDIUS license management. It is not a Sabretooth license.

The EDIUS for GV STRATUS application can launch and operate as follows:

- A high resolution editor, identified as EDIUS Workgroup, which can operate in STRATUS mode or in standalone mode. In STRATUS mode, the EDIUS for GV STRATUS application can access GV STRATUS high resolution assets. In standalone mode, the EDIUS for GV STRATUS application cannot access GV STRATUS high resolution assets.
- A low resolution proxy editor, identified as EDIUS XS, which operates in a single mode that must access GV STRATUS proxy assets.

Both of these applications can launch from the **EDIUS** icon .

The same EDIUS software installation package is used to install both types of EDIUS for GV STRATUS applications, so there can be confusion about which application is being launched. This is especially true if licenses for both applications apply to the same client PC, which is not supported. When you launch an EDIUS for GV STRATUS application, it detects the licensing on the client PC. If licensed for EDIUS Workgroup, you are prompted to logon and the EDIUS Workgroup application always launches. You cannot launch EDIUS XS. If not licensed for EDIUS Workgroup you are prompted to logon. Based on your logon, the application checks licensing and roles on the GV STRATUS Core server. If the license includes EDIUS XS and your logon account is assigned the EDIUS XS role, EDIUS XS launches. Therefore, if you have ever licensed the client PC for EDIUS Workgroup, do not use that PC for EDIUS XS.

Troubleshooting tips

Symptom	Solution
Problem accessing the GV STRATUS system.	Check the Status window. Check that the Core Services server is running. Check that the server is connected to the client network. Check that connections are secure.
Problem opening proxy assets	1. Verify that proxy can be created by K2 Summit record channels and the GV STRATUS server that creates proxy assets. 2. Verify the internal system account has read/write access to the proxy share and the user playing the asset has read access. 3. Verify that you can access the proxy via the Proxy HTTP server.
Core Services server is accessible using IP address but not server name	Host tables or DNS entries must be set to map name to IP address. This should be coordinated with facility IT personnel.
Problem accessing the GV STRATUS application or its features	Check that the account used to log into the GV STRATUS workstation has licenses and roles assigned.
GV STRATUS Control Panel application does not provide correct information in drop-down lists.	Check the SiteConfig log and make sure a "saved system description to control panel service host" appears every few minutes. If not, make sure the correct control panel service host is configured in SiteConfig.
No video appears when you click the Live Streaming Video button.	Check networking and connection to the K2 Summit/SAN system V:\ drive. To test, navigate on the K2 Summit/SAN system to the V:\live streaming directory. Open the corresponding *.sdp file in Quicktime and verify that video is available.
Problem with Live Streaming when the K2 Summit system's IP address is changed.	On the K2 Summit system navigate to `V:\live streaming` and use Notepad or a similar text editor to open a `*.sdp` file. Check the first IP address listed in the file, on the `o=` line. If it is not the K2 Summit system's Control Connection IP address, delete the `*.sdp` files in the directory and restart the K2 Summit system.
A device running code that communicates with the GV STRATUS SDK cannot access the GV STRATUS Core server. This occurs if the device has a network proxy server that disallows local connections.	Disable the network proxy server.

Symptom	Solution
The GV STRATUS application takes a long time to open or does not open.	This can happen when the application attempts to load the last used workspace when it opens and there is a problem with that workspace. To open with the default workspace, hold down the left-hand **Alt** key while the application opens. To open with all user settings disabled, open the application from the command prompt using the failsafe switch, as in `STRATUS /failsafe`.
A "Windows could not start the GV STRATUS ... service" Error 1069 message appears.	This can happen when a password is changed using an improper procedure. Refer to related topics in this Topic Library.

Related Topics

Changing passwords on page 710

Test proxy media generation

This test is valid for standalone K2 Summit systems. You can check the proxy media that the K2 Summit system generates. This can be helpful in troubleshooting situations where you need to verify that the proxy is available to other applications, such as the GV STRATUS application.

Use this procedure for test purposes only. Accessing proxy media as explained in this procedure is not supported for operational use.

1. Verify that in K2 AppCenter Configuration Manager, a K2 Summit system channel is enabled for live network streaming and for recording proxy files.
2. Verify that there is video available at the channel's SDI input.
3. Verify proxy live network streaming as follows:
   a) On the K2 Summit system, navigate to *C:\live stream*.
   b) Identify the file that corresponds to the channel enabled for live network streaming.
      The file name is *hostname_Cx,sdp*, where *x* is the channel number.
   c) Double-click the file that corresponds to the channel enabled for live network streaming.
      QuickTime Player opens.
   d) View and verify the proxy video stream.

4. Verify recording proxy files as follows:
   a) Navigate to the proxy location.

      On a K2 Summit system that has not been configured to write proxy elsewhere, the location is `V:\proxy`. If configured by applications such as GV STRATUS to write proxy elsewhere, navigate to the configured location.

   b) While viewing the proxy location, start recording a new clip on the K2 Summit channel enabled for recording proxy files.

      The K2 Summit system creates a new folder at the proxy location. The folder is named with a long GUID.

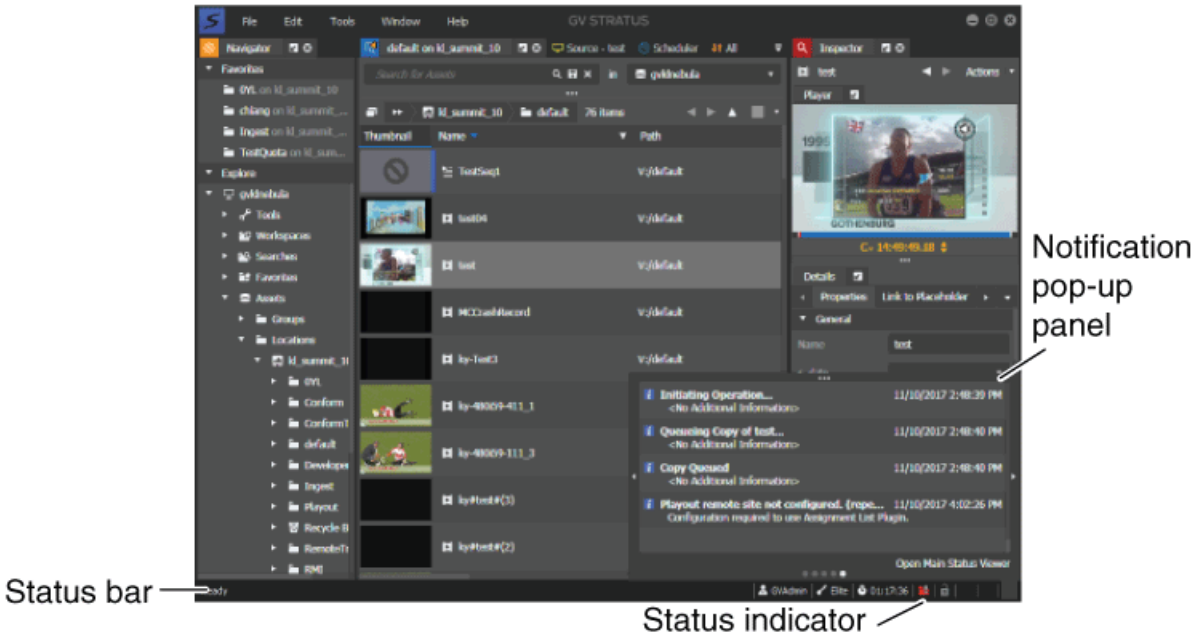
   c) Stop the recording on the K2 Summit channel.
   d) In the new folder, double-click the `proxy.mp4` file.

      QuickTime Player opens.

   e) View and verify the proxy file.

About application status

You can view the status of the application as follows:



Status Bar

Indicates whether the application is ready or not, the user account currently logged on, and license information.

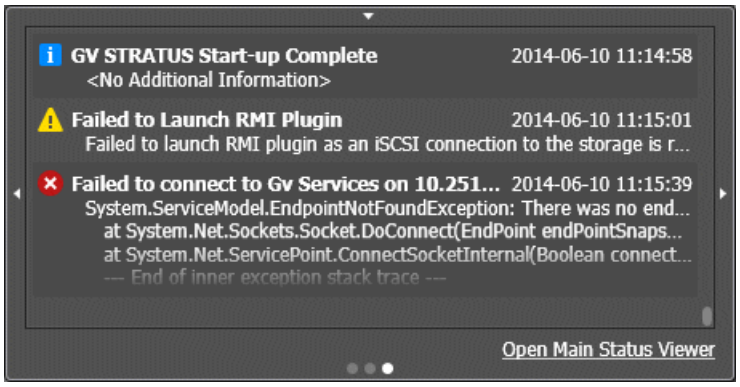
Status Indicator

Displays an alert when a problem occurs that requires your attention.

Notification pop-up panel

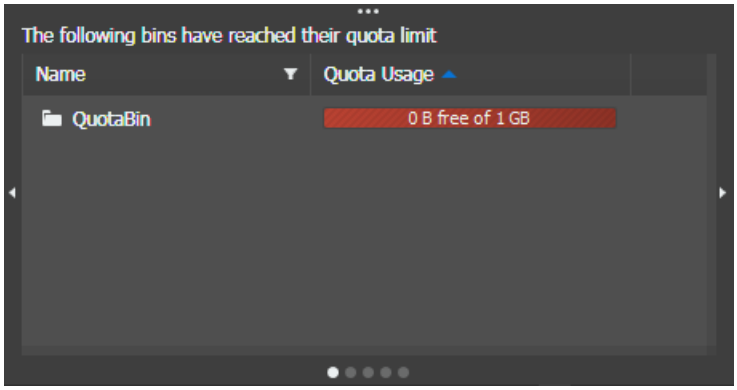
Provides a condensed view of status.

To open the Notification pop-up panel to the Status page, in the lower-right GV STRATUS application Status bar, click the Status indicator. The Status indicator can display the **Error** message icon.



To open the Status Viewer panel for an expanded view, click **Open Main Status Viewer**.

To view other notifications, click the arrow on the right of the pane. You can view security notification, background tasks, job status, system status, and bin quota limit, if reached.



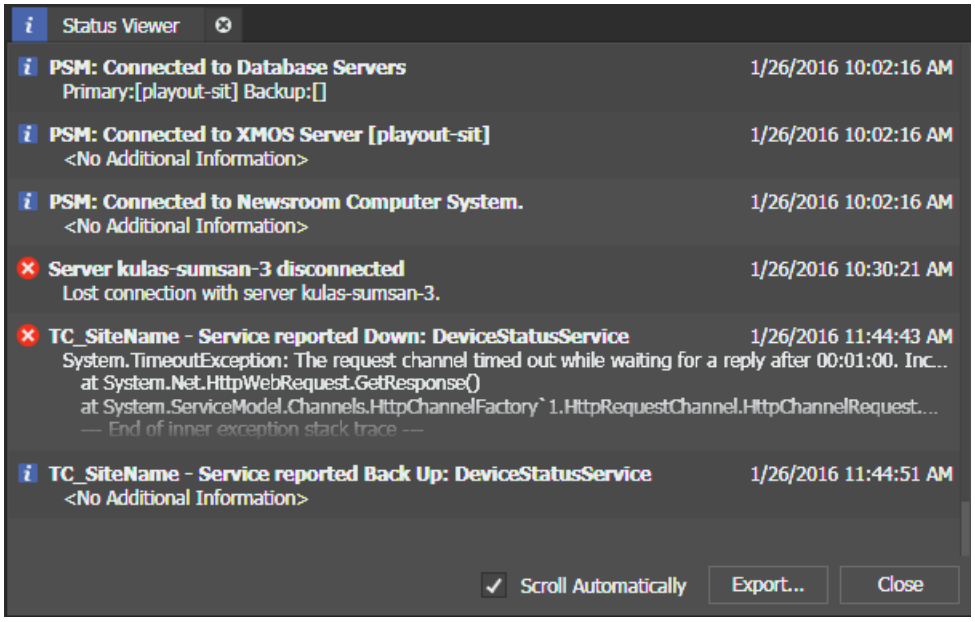
To close the Notification pop-up panel, click the down-arrow on the top edge of the panel or click the Status indicator again.

Status Viewer panel

Allows you to view the status of the application, its components, workspace layout, and any services associated with the application.

To open the main Status Viewer panel, do one of the following:

- Click the Status indicator then click **Open Main Status Viewer**.
- Click **Help | Status**.



The Status Viewer panel gives a complete view of information. You can quickly evaluate the system status information by scanning the display icons:

- **Information**: Indicates an information message.
- **Warning**: Indicates a warning message.
- **Error**: Indicates an error message.

By default, the **Scroll Automatically** box is checked.

Viewing and copying version and status information

You can view version information and status information. If necessary, you can also copy the information and send it to Grass Valley support.

- To access version information do the following:
  a) Click **Help | About**.
     The About dialog box opens.
  b) To copy the detailed system information, click the **Copy Details** button.
  c) When finished viewing or copying the information, click **Close**.
     The dialog box closes.
  d) Paste the copied information into a text file or email, and send it to Grass Valley support.

- To access status information do the following:
  a) Click **Help | Status**.
     The Status Viewer panel opens.
  b) To copy status information, double-click a status message.
     A message box opens.
  c) Highlight the message information and press **Ctrl + C**.
  d) Paste the copied information into a text file or email, and send it to Grass Valley support.

Commissioning checklist

Commissioning checklist

Commissioning checklist

Use the following lists to guide the overall task flow of commissioning the system. This commissioning process assumes you received your system completely set up and configured from Grass Valley.

Test Grass Valley commissioning

1. Rack, cable, and power on, using the *K2 and GV STRATUS System Cabling Guide* that shipped with the system.
2. On a K2 Summit system, open K2 AppCenter and test basic record and play operations.
3. From the control point PC, ping all K2 and GV STRATUS devices to test network connectivity.
   If the system has no control point PC, do this test from the GV STRATUS server.
4. In the GV STRATUS application, do the following:
   a) In the Navigator, verify access to K2 Summit system bins.
   b) Create a Channel Panel and test record/play operations.
   c) In the Navigator, select assets on the K2 Summit system.
      The assets appear in the Asset List.
   d) Double-click an asset in the Asset List.
      The asset opens in the Inspector.
   e) In the Inspector, verify that the asset has a proxy association.
5. In the Asset List, right-click the high-resolution asset and select **Regenerate Proxy**.
6. Verify the following behavior:
   a) In the **Associations** tab of the Inspector, the proxy association is momentarily not visible.
      This occurs as the GV STRATUS system deletes the proxy asset.
   b) In the **Associations** tab of the Inspector, the proxy association shows as recording.
      This occurs due to the GV Render Engine is in the process of regenerating the proxy asset.
   c) In the **Associations** tab of the Inspector, the proxy association is visible again.
      This occurs as a result of the GV Render Engine has finished regenerating the proxy asset.

If tests succeed, the system is operating correctly, as it did when it left Grass Valley.

Commission customer site

1. Configure the GV STRATUS server on the corporate LAN.
2. Assign GV STRATUS licenses/operations to groups/users.
3. Verify system requirements on GV STRATUS client PCs
4. If any high-resolution GV STRATUS client PCs, make cable connections to control and media (iSCSI) networks.
5. Install/configure SiteConfig support on GV STRATUS client PCs
6. On the control point PC, open SiteConfig and do the following:
   a) Add corporate LAN.
   b) Add GV STRATUS client PCs.
   c) Install GV STRATUS software on GV STRATUS client PCs.
7. If any high-resolution GV STRATUS client PCs, open K2Config and configure the PCs as iSCSI clients on the K2 SAN.
8. On one of the customer-supplied GV STRATUS client PCs, open the GV STRATUS application and do the following:
   a) In the Navigator, verify access to K2 Summit system bins.
   b) Create a Channel Panel and test record/play operations.
   c) In the Navigator, select assets on the K2 Summit system.
      The assets appear in the Asset List.
   d) Double-click an asset in the Asset List.
      The asset opens in the Inspector.
   e) In the Inspector, verify that the asset has a proxy association.
9. In the Asset List, right-click the high-resolution asset and select **Regenerate Proxy**.
10. Verify the following behavior:
    a) In the **Associations** tab of the Inspector, the proxy association is momentarily not visible.
       This occurs as the GV STRATUS system deletes the proxy asset.
    b) In the **Associations** tab of the Inspector, the proxy association shows as recording.
       This occurs due to the GV Render Engine is in the process of regenerating the proxy asset.
    c) In the **Associations** tab of the Inspector, the proxy association is visible again.
       This occurs as a result of the GV Render Engine has finished regenerating the proxy asset.

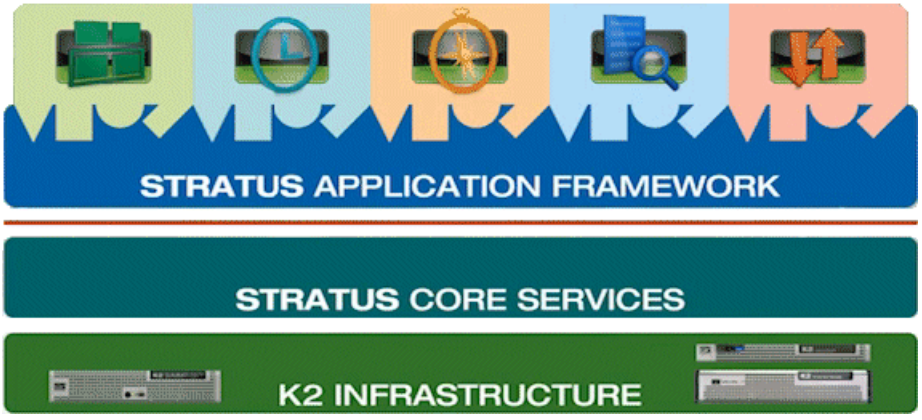
GV STRATUS Operation

Overview of the GV STRATUS application

About the GV STRATUS product

The GV STRATUS® Video Production and Content Management System is the next generation of Grass Valley application software, designed for the entertainment, on-air operations, and news markets. GV STRATUS includes a powerful asset management solution and all the tools to help you produce your content from all ingests needs, preparation, editing, review and approval, playout and of course, archiving. GV STRATUS uses a common Service Oriented Architecture, to provide a modular, high performance, and highly configurable user experience and does away with the old concept of separate, individual tools which can be hard to configure, and even harder to use. GV STRATUS is built with modules that are added as services to assemble your workspace into an environment tailored specifically to your needs, in an almost infinite number of combinations. This means you have a virtually unlimited and fully integrated tool-set at your command. GV STRATUS is format and resolution independent. Proxies are generated on the fly for any video coming into the system and are fully available to all the users within seconds.

The GV STRATUS product includes the GV STRATUS Application Framework and the GV STRATUS Core Services. These layers provide you with access to the K2 Infrastructure to support your workflow requirements.



The GV STRATUS Application Framework includes the following:

- The GV STRATUS application — This is the primary application for using GV STRATUS tools for your media workflow. It is documented in this Topic Library.
- The GV STRATUS Control Panel application — The GV STRATUS application that provides central configuration of the software components of the GV STRATUS system. It is documented in this Topic Library.
- The GV Event Viewer — This is the application that displays detailed information about significant events on your GV STRATUS server, which is very useful when troubleshooting problems and errors. It is documented in this Topic Library.

These applications run on standard networked PCs.

The GV STRATUS Core Services include software components that run as services on one or more GV STRATUS Core servers. They are documented in this Topic Library.

The K2 Infrastructure includes the devices and software that make up a K2 Summit system at version 8.0 and higher. Depending on the system necessary to support your workflow requirements, this can include K2 clients, servers, RAID storage devices, and network switches. They are documented in this Topic Library and the "Installing and Servicing the K2 SAN" section of the K2 Topic Library.

Logging on

When you log on to the GV STRATUS system, the GV STRATUS application assigns GV STRATUS licenses and roles based on your user account credentials, as set by the system administrator in the GV STRATUS Control Panel application. If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins and assets that are part of your workflow. If GV STRATUS metadata access control is enforced, your credentials must give you adequate permissions on metadata fields that are part of your workflow. Your credentials must also give you access to all your K2 systems.

1. From the Windows desktop, do one of the following:
   - Open the **GV STRATUS** icon shortcut.
   - Click **Start | All Programs | Grass Valley** and click the **STRATUS** icon.

   A Log On dialog box opens.
2. Enter your user name.

   If you use domain credentials, enter in format `<domain>\<username>`. For example, if your domain is "gv" and your username is "GVuser", enter `gv\GVuser`.

   If you have successfully logged on before, select your user name from the drop-down list.
3. Enter your password.
4. Verify that the application is correctly referencing the Control Panel Services Host as follows:
   a) If not already showing, click the **Options** button to show settings.
   b) Verify or enter the hostname (do not enter the IP address) of the GV STRATUS server with the SiteConfig role of GV STRATUS Control Panel Service. This is the Control Panel Services Host. In most systems this is the main GV STRATUS Core server.

      If you have successfully logged on before, your hostname is automatically populated. You can select a hostname from the drop-down list if you have previously logged on to multiple hosts in your operation.
5. Click **Log On**.

The application opens.

GV STRATUS features are enabled according to the roles associated with your log on credentials.

When you log on to the application, the settings you make on one PC are available on other PCs when using the same user credentials, including the following:

- Settings from the User Preferences dialog box
- Workspaces

- Channel Panel configurations and Salvos
- Searches

About the GV STRATUS application

The GV STRATUS application allows you to manage digital video production workflows. The GV STRATUS application runs on a networked Windows operating system computer.

The GV STRATUS application provides the following panels for use in most workflows:

Navigator: The panel that contains the tree-view.

Asset List: The panel that displays the list for the item currently selected in the Navigator panel or the search results.

Inspector: The panel that displays details of the asset currently loaded.

The Status bar reports application status and displays status indicators.

In addition, the GV STRATUS application provides tools designed for specific workflows. You can arrange the panels and tools of the GV STRATUS application to create a customized workspace.

Tools and devices within the GV STRATUS application are available according to assigned roles and licensing. If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets, and metadata that do not have read permissions are not visible. Markers and segments permissions must be set to **Allow** in order to create, update, or delete markers and segments.

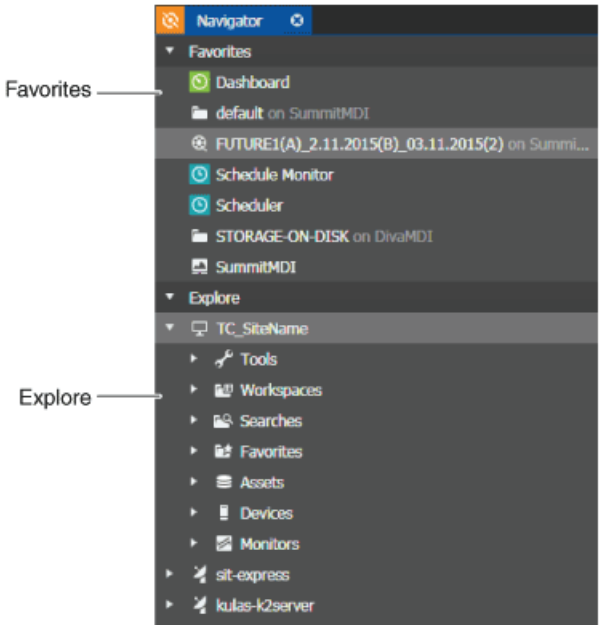
Related Topics

About application status on page 947

Customizing the application workspace on page 1392
Arranging control tray buttons on page 971
About Newsroom Basic on page 466

The Navigator panel

The Navigator panel functions as the starting point for workflows using the GV STRATUS application. For most of the items in the Navigator, if you select the item it is displayed in the active Asset List panel.



The Navigator panel contains the following sections:

- **Favorites** — A list of shortcuts to GV STRATUS items.
- **Explore** — A tree-based hierarchy with which you can browse your system.

From the Explore section, you can access the following:

Tools: Expands to display the tools that support the various workflows available in the STRATUS application.

Workspaces: Expands to display default and saved workspaces.

Searches: Expands to display searches that can be reused and shared.

Favorites: Expands to display a list of favorites.

Assets: Expands to display a view of groups and assets based on the information available in the STRATUS database. Any assets can be grouped together, regardless of their actual location in K2 system storage.

Devices: Expands to display the devices that the STRATUS application accesses or controls.

Monitors: Expands to display tools for monitoring transfers and web pages. The **Jobs** icon and the **Dashboard** icon appear here.

Access Restricted: Indicates the asset or bin has restricted access.

Offline: Indicates the K2 Summit system is offline. The red "X" overlay disappears automatically if the K2 Summit is back online.

The Navigator panel displays all items under the node for your local site.

If you have remote sites configured in your system, the Navigator panel displays nodes for those sites. Only the **Assets** node is displayed under remote sites. Asset indicators identify assets on remote sites.

If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets, and metadata that do not have read permissions are not visible. Markers and segments permissions must be set to **Allow** in order to create, update, or delete markers and segments.

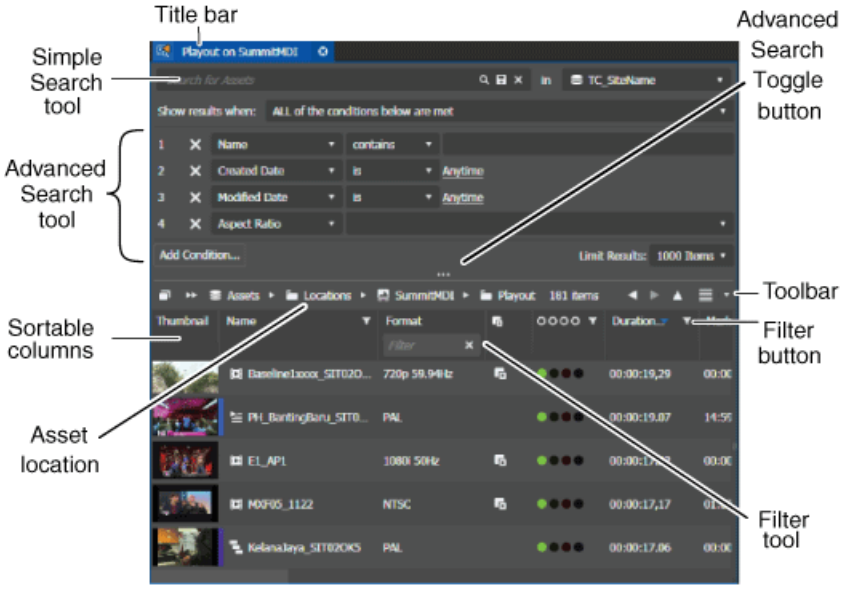
Related Topics

About the GV STRATUS Assets view on page 417

Asset indicators on page 977

The Asset List panel

The Asset List panel displays the contents of the item selected in the Navigator panel, such as a tool, bin, or search. Each time you select an item in the Navigator panel, an updated view of its contents is displayed. The Asset List panel typically appears on the middle of the GV STRATUS application window.



The Asset List panel features are as follows:

- Title bar — Displays the name of the item that has its contents displayed in the Asset List panel. The name is displayed in both the title bar and the toolbar.
- Simple Search tool — Searches on asset Names, asset Descriptions, asset Tags, asset Comments, and custom Text fields.
- Advanced Search tool — Searches on asset metadata and other properties. The Advanced Search tool opens when you click the **Advanced Search Toggle** button.
- Sortable columns — Sorts the list when you click the column head.
- Asset location — Displays the location of the asset, relative to the Navigator hierarchy, when you hover over the asset name in the toolbar.
- Toolbar — Provides buttons for navigating and displaying asset lists.
- Filter tool — Filters the list based on criteria you enter. The Filter tool opens when you click the **Enable Filter** button.

You can open multiple Asset List panels and compare them side by side. Only one Asset List panel is active at a time. The active panel dynamically updates when you select an item in the Navigator panel. You can click on a panel to make it the active Asset List panel.

If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets, and metadata that do not have read permissions are not visible. Markers and segments permissions must be set to **Allow** in order to create, update, or delete markers and segments.

Related Topics

About searches on page 988

Customizing the display of list items on page 981

Asset List panel buttons

These buttons located on the Asset List panel toolbar let you perform various functions:

Start Search: Initiates a search for the specified items.

Save Search: Saves this search for future use.

Remove Condition: Removes condition from the search tool.

Advanced Search Toggle: Toggles display of the advanced search parameters for the current provider

Navigate Asset Lists: Goes to previous, to next, and up.

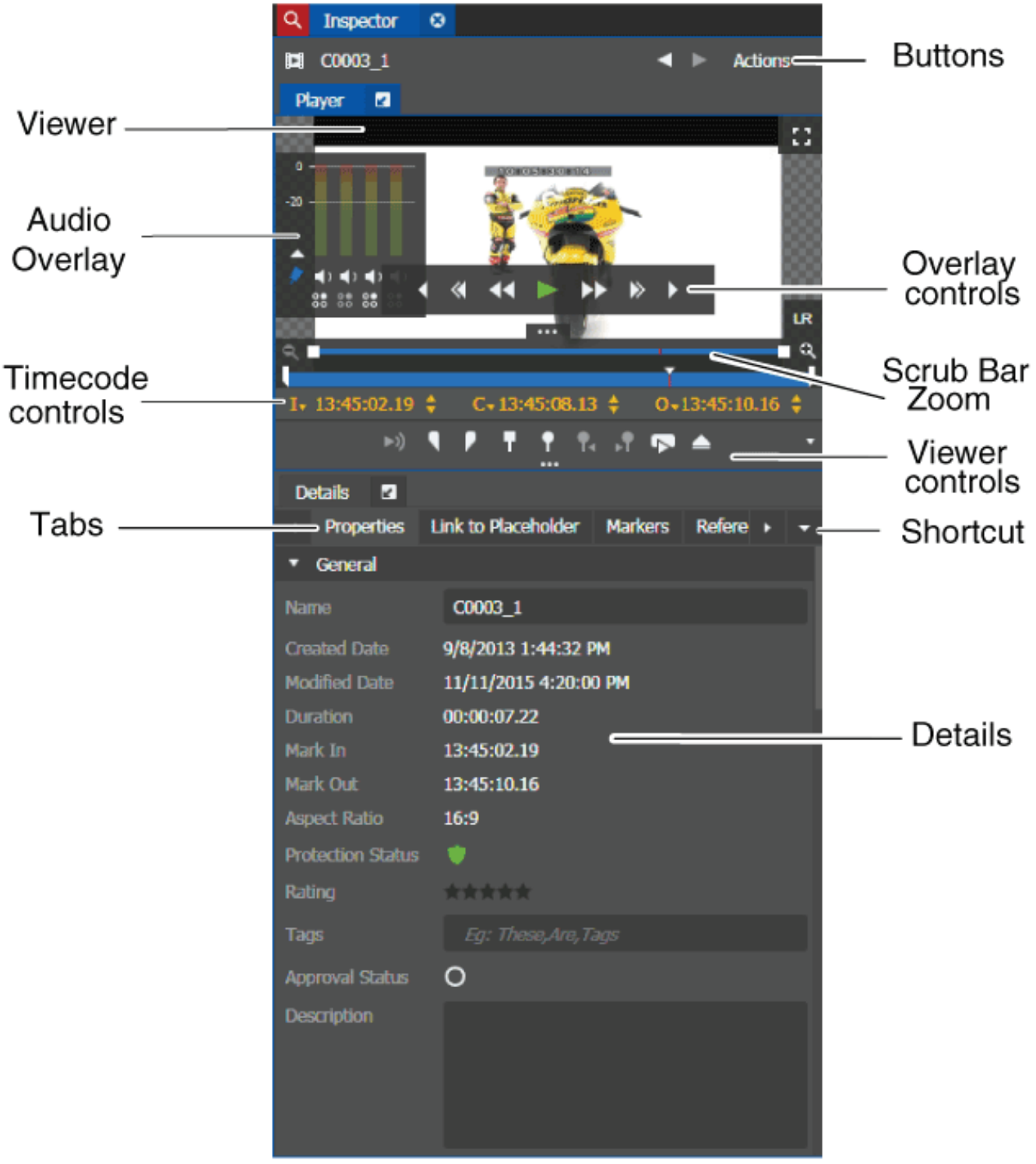
Open New Panel: Opens a new panel.

View Mode: Controls the display and size of the items in a list or panel.

Enable Filter: Enables the list to be filtered by the values in the column.

The Inspector panel

The Inspector panel allows you to mark up, manage, and view detailed information for an asset. The Inspector panel typically appears on the right side of the GV STRATUS application window.


Inspector
C0003_1
Actions
Buttons
Player
Viewer
Audio
Overlay
Overlay
controls
LR
Timecode
controls
I 13:45:02.19
C 13:45:08.13
O 13:45:10.16
Scrub Bar
Zoom
Viewer
controls
Details
Tabs
Properties
Link to Placeholder
Markers
Refere
Shortcut
General
Name
C0003_1
Created Date
9/8/2013 1:44:32 PM
Modified Date
11/11/2015 4:20:00 PM
Duration
00:00:07.22
Mark In
13:45:02.19
Mark Out
13:45:10.16
Aspect Ratio
16:9
Protection Status
Rating
Tags
Eg: These,Are,Tags
Approval Status
Description
Details

The Inspector panel features are as follows:

- Viewer — Allows you to view and mark up an asset. You can show and hide viewer controls to accommodate resizing the Inspector panel.
- Audio Overlay — Allows you to manage audio of the asset. You can mute or isolate specific audio channels on the audio overlay.
- Buttons — Provides a menu of actions for managing the asset and navigation buttons to view previous/next objects.
- Overlay Controls — Transport controls navigate through the asset. Visible when you hover the mouse pointer over the asset. Movable with drag-and-drop. Not all controls are displayed when the panel is not fully expanded.
- Viewer controls — Allows you to mark up the asset.
- Scrub Bar Zoom — Allows you to zoom on the scrub bar.
- Timecode Controls — Allows you to select the mark in/out and other timecode types to display. Also lets you navigate through the clip to a specific timecode. If desired, the timecode controls can also be resized in the panel.
- Details — Provides tabs with sections for viewing properties, metadata, placeholders, markers, and relationships. You can create custom metadata sections in GV STRATUS Control Panel to organize settings on tabs.
- Tabs — Allows you to view asset details in separate sections. On some tabs you can make changes, such as modifying metadata, linking assets to placeholders, and setting recurring events. Standard Asset List features, such as sortable columns, are available on tabs with a list display. You can click the shortcut to display a drop-down list of tabs, and quickly select a tab display.

The features in the Inspector panel can change dynamically, depending on the tool that launches the Inspector panel, the roles assigned, and the type of asset that is displayed. The Viewer controls are the same as those in the Source Viewer.

If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets, and metadata that do not have read permissions are not visible. Markers and segments permissions must be set to **Allow** in order to create, update, or delete markers and segments.

Related Topics

Viewer buttons on page 1139
Identify high and low resolution while viewing on page 997
Using the scrub bar zoom to navigate on page 997
Using the Audio Overlay on page 1002
Identifying and selecting the timecode type on page 1095
Toggling between camera angles in Inspector and Channel Panel on page 1002

About GV STRATUS tools

The GV STRATUS application contains the following tools. You can find the tools in the Navigator panel under the **Tools** node.

Advanced Logging: The tool that creates and customizes logging of assets.

Assignment List: The tool that creates placeholders for clips and coordinates with rundown stories on the Newsroom Computer System and with GV STRATUS Rundown.

Channel Panel : The tool that includes channels and channel gangs for controlling one or more K2 channels.

House Number: The panel that populates the house number list and links assets to house numbers from the traffic system.

Playlist Editor: The tool that creates and modifies playlists. This tool uses a K2 channel.

RMI: RMI is the acronym for Removable Media Interface. It is the tool that populates and ingests files from multiple removable media devices such as P2 and XDCAM. The RMI tool requires a GV STRATUS client with access to high-resolution assets.

Scheduled Transfer: The tool that schedules events to be transferred into a repository.

Scheduler: The tool that schedules events to be recorded.

Segmentation Tool: The tool that creates segments from assets.

Send Message: The tool that sends and receives messages and attachments between users logged on to GV STRATUS applications.

Source Viewer: The tool that plays assets and provides controls for adding markers, keywords, and other features.

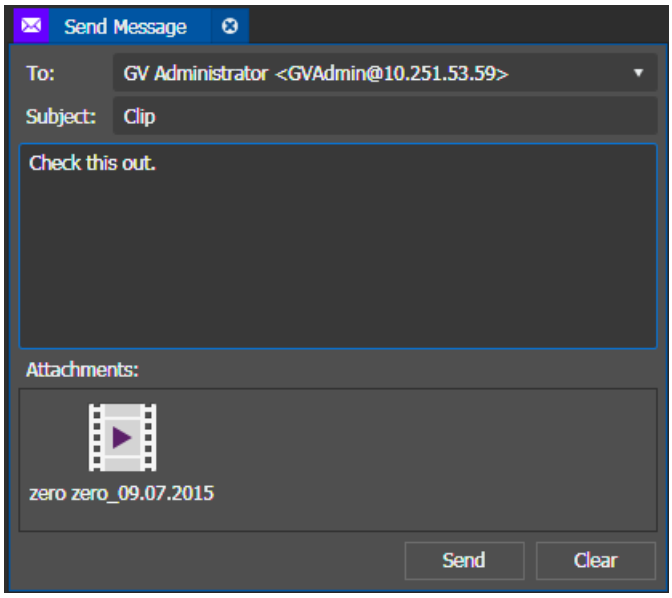
Storyboard Editor: The tool that creates and modifies sequences. This tool does not use a K2 channel.

Related Topics

The Advanced Logging tool on page 1284
The Assignment List tool on page 1316
The Channel Panel tool on page 1070
The House Number panel on page 1384
The RMI tool on page 1058
The Playlist Editor tool on page 1098
The Scheduler tool on page 1022
The Segmentation tool on page 1371
The Source Viewer on page 1138
The Storyboard Editor tool on page 1137
The Send Message tool on page 409
The Director tool

The Send Message tool

The Send Message tool allows you to send and receive messages with attachments. If you are logged on to a GV STRATUS application you can send a message to another person that is currently logged on to a GV STRATUS application and on the same network subnet. The Send Message tool appears in the GV STRATUS application and in the GV STRATUS Control Panel application when you launch it from the Navigator panel.



Send Message tool features are as follows:

- To field — Specifies the GV STRATUS user to whom the message is sent. Select a user from the drop-down list.
- Subject field — Contains the title of the message.
- Message field — Contains the message.
- Attachments field — Provides a field to which you drag attachments.
- Send button — Sends the message.
- Clear button — Clears all fields in the Send Message panel.

You can attach the following:

- Clips
- Playlists
- Saved searches
- Workspaces
- Bins
- Logging buttons
- Button Panels
- Advanced Logging Tool composite panel
- Tools
- Devices
- Locations
- Monitors
- Channel Panels
- Drives

When you send an attachment, you are actually sending a link to the attachment, rather than the attachment itself.

When you receive a message, a Message dialog box opens and displays the message. If the message has an attachment, you can do the following:

- Open the attachment by double-clicking it.
- Create a copy of the attachment in the Navigator panel or drag it to other panels in the GV STRATUS application. Consider the size of the attachment before creating a copy.

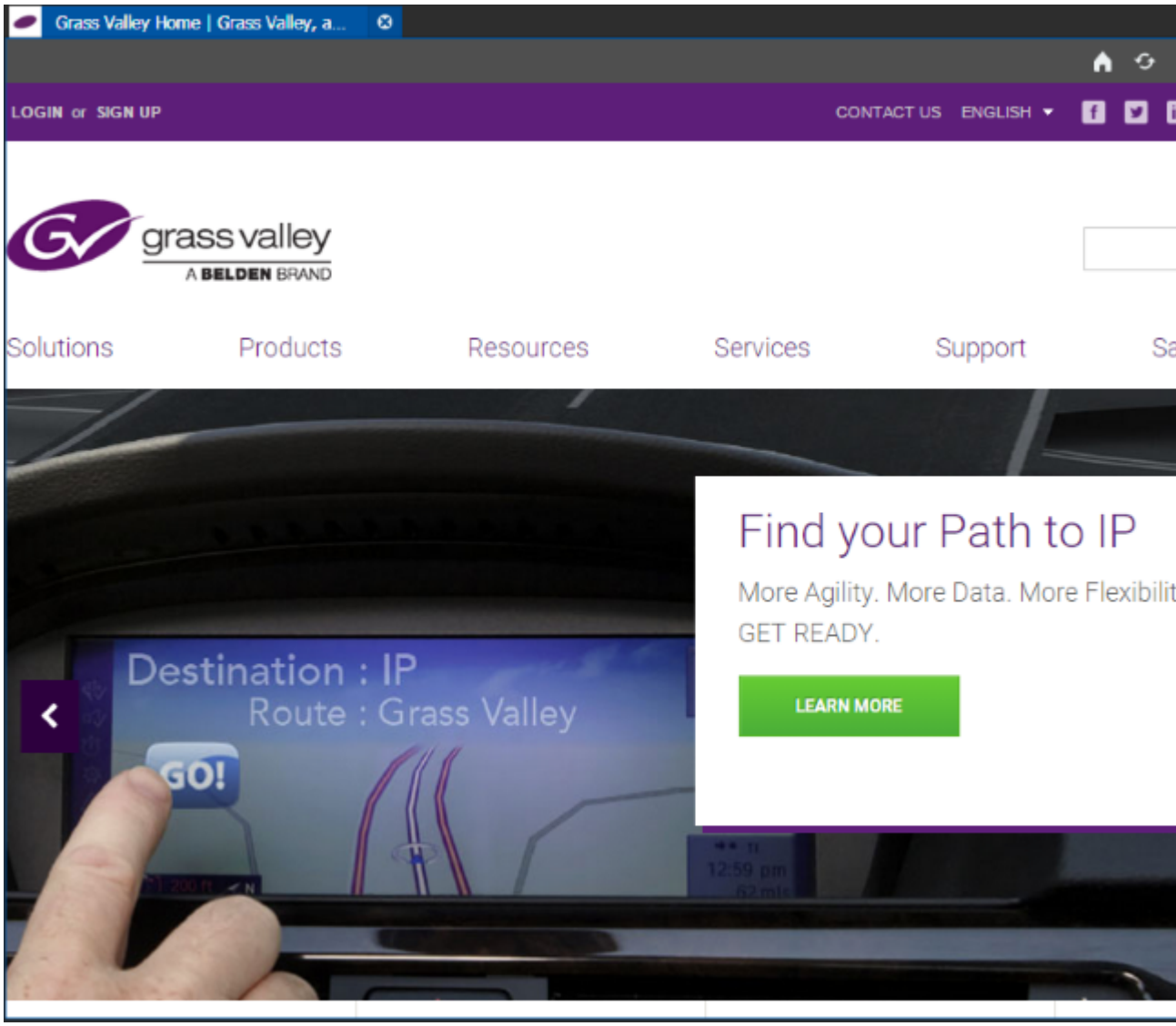
The Send Message tool is more similar to Instant Messaging than it is to E-mail, as there is no Outbox or Inbox functionality to store messages. If a person is not logged on to a GV STRATUS application you can not send them a message. Likewise, if you are not logged on to a GV STRATUS application you can not receive a message.

The Web Monitor

The Web Monitor allows you to view a web page in a GV STRATUS application panel. You configure the web page address in GV STRATUS Control Panel. You can configure multiple web pages.

The Web Monitor displays the name of each configured web page in the GV STRATUS application Navigator panel, from which you can launch each web page as a separate Web Monitor panel. When you hover your cursor near the side borders of the Web Monitor panel, forward and back browse buttons appear.

You can also drag and drop any web page under the Web Monitor node into the **Favorites** panel to easily access a frequently used web page in your operation.

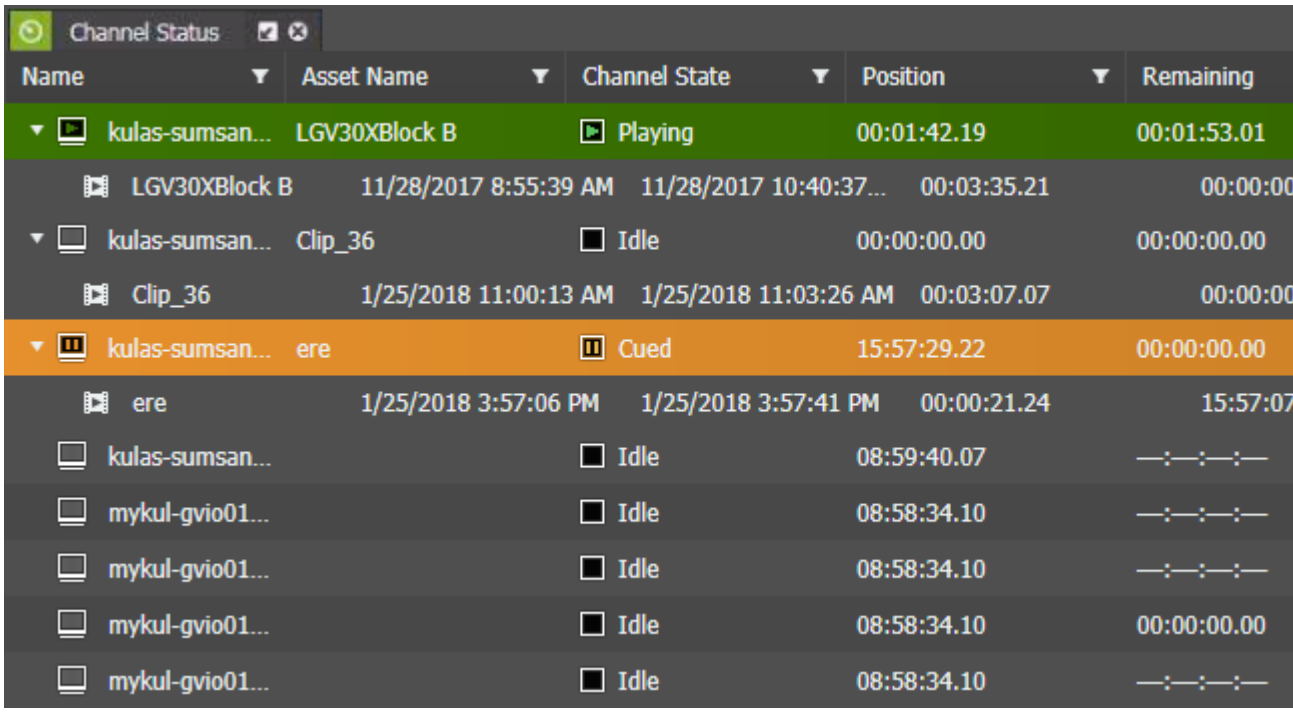


The Dashboard tool

The Dashboard tool allows you to view information about the current activity on the GV STRATUS system.

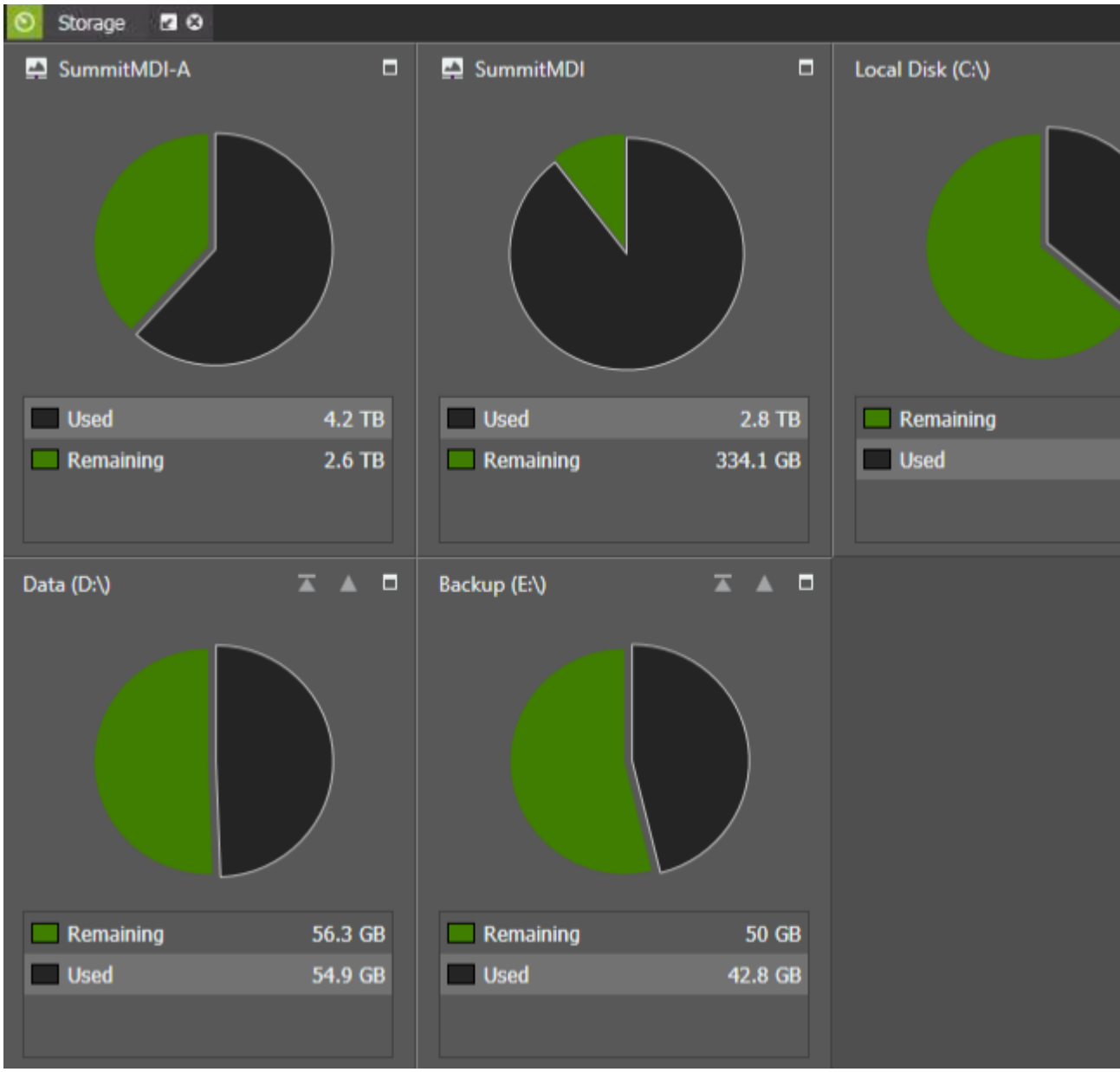
You can view the Dashboard tool either in the GV STRATUS application or the GV STRATUS Control Panel. You can also drag and drop any Dashboard panel into the **Favorites** section in the Navigator to easily access your Dashboard status. If you are assigned with appropriate roles in the GV STRATUS Control Panel, these options are available for the Dashboard tool under the Monitors node.

The Channel Status displays channel state and usage information when selected. You must be assigned with the **Dashboard** and **Dashboard - Channel Status** roles in order to view the panel. You can customize the display of list items, similar to Asset List items, with features such as sort, filter, and add/remove columns.

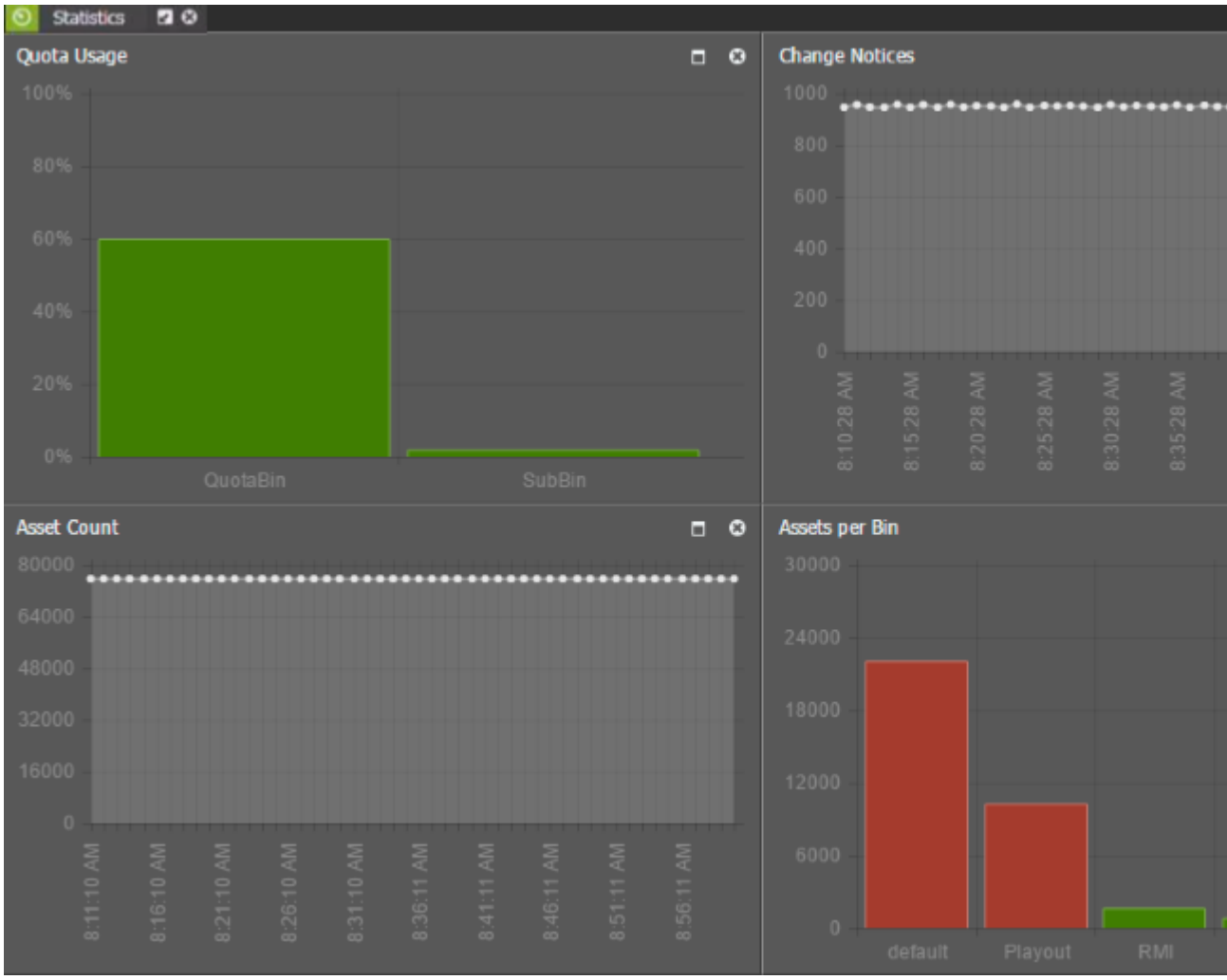


When a channel has an asset loaded, the asset details display in an expandable, separate line below the channel. You can also view the status of each channel whether it's idle, recording, or cueing assets.

The Storage panel reports storage capacity available on K2 devices and the local GV STRATUS PC. K2 storage displayed in the Storage dashboard panel now reflects 100% of its volume instead of the previous value of approximately 95%. You must be assigned with the **Dashboard** and **Dashboard - Storage** roles in order to view the panel. You can right-click on the **Used** report to explore storage levels further. Those storage reports can also be viewed via an internet browser at:
http://<coreservername>/webapps/statistics/?mode=storage

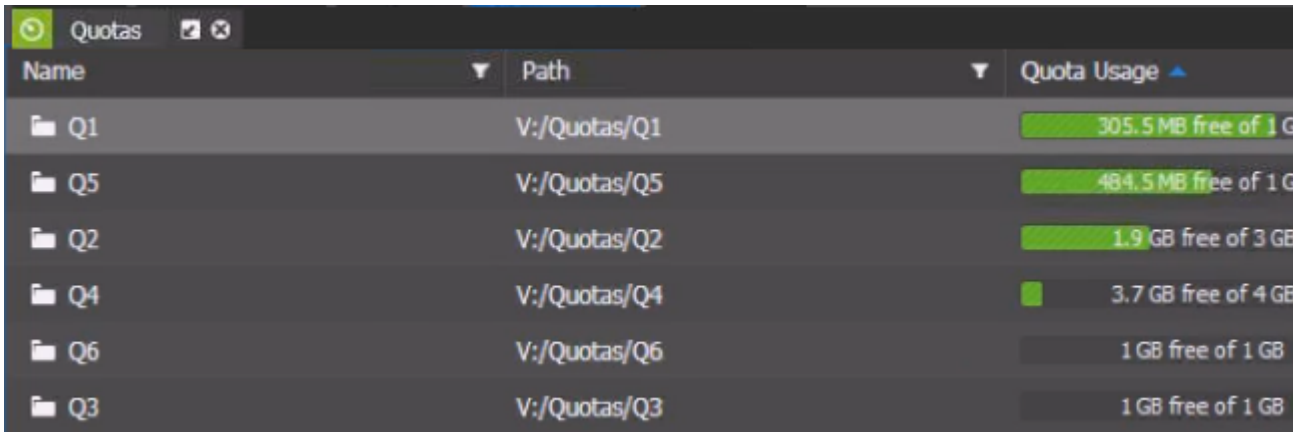


The Statistics panel displays data in graphical form for change notices, asset count, user sessions, system sessions, quota usage, and top 5 of assets per bin in the GV STRATUS system. In order for the Statistics panel to display via the Dashboard, the **GV STRATUS Web Apps** SiteConfig role must be installed on the GV STRATUS Core server. You must also be assigned with the **Dashboard** and **Dashboard - Statistics** roles in order to view the panel. Alternatively, those statistics can be viewed via an internet browser at: `http://<coreservername>/webapps/statistics/`

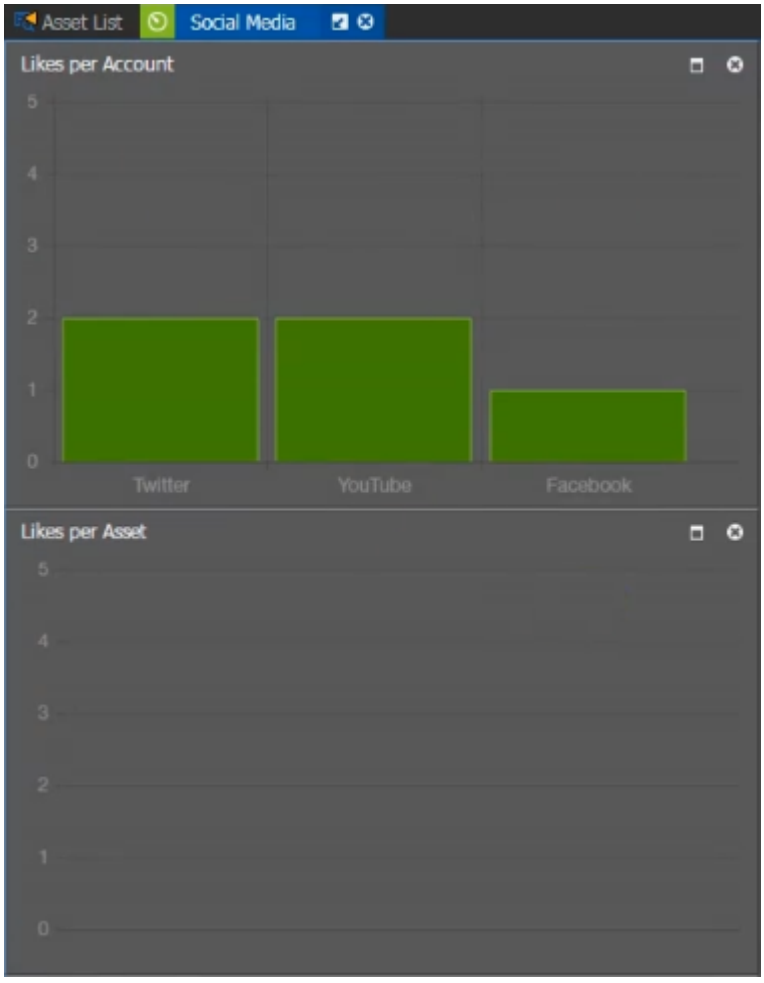


The Quotas panel displays the amount of disk space that the GV STRATUS system reserved for specific bins and the current quota usage. You must be assigned with the **Dashboard** and **Dashboard - Quotas** roles in order to view the panel. The quota of each bin is configurable via the StorNext Administration application on K2 Summits. The quota display turns orange when the disk space is less than 100MB of the limit, and turns red when it reaches the limit. The Quota Status icon displays on the status bar when the quota limit is reached. You can click the icon to launch the status viewer panel and view the quota limit.

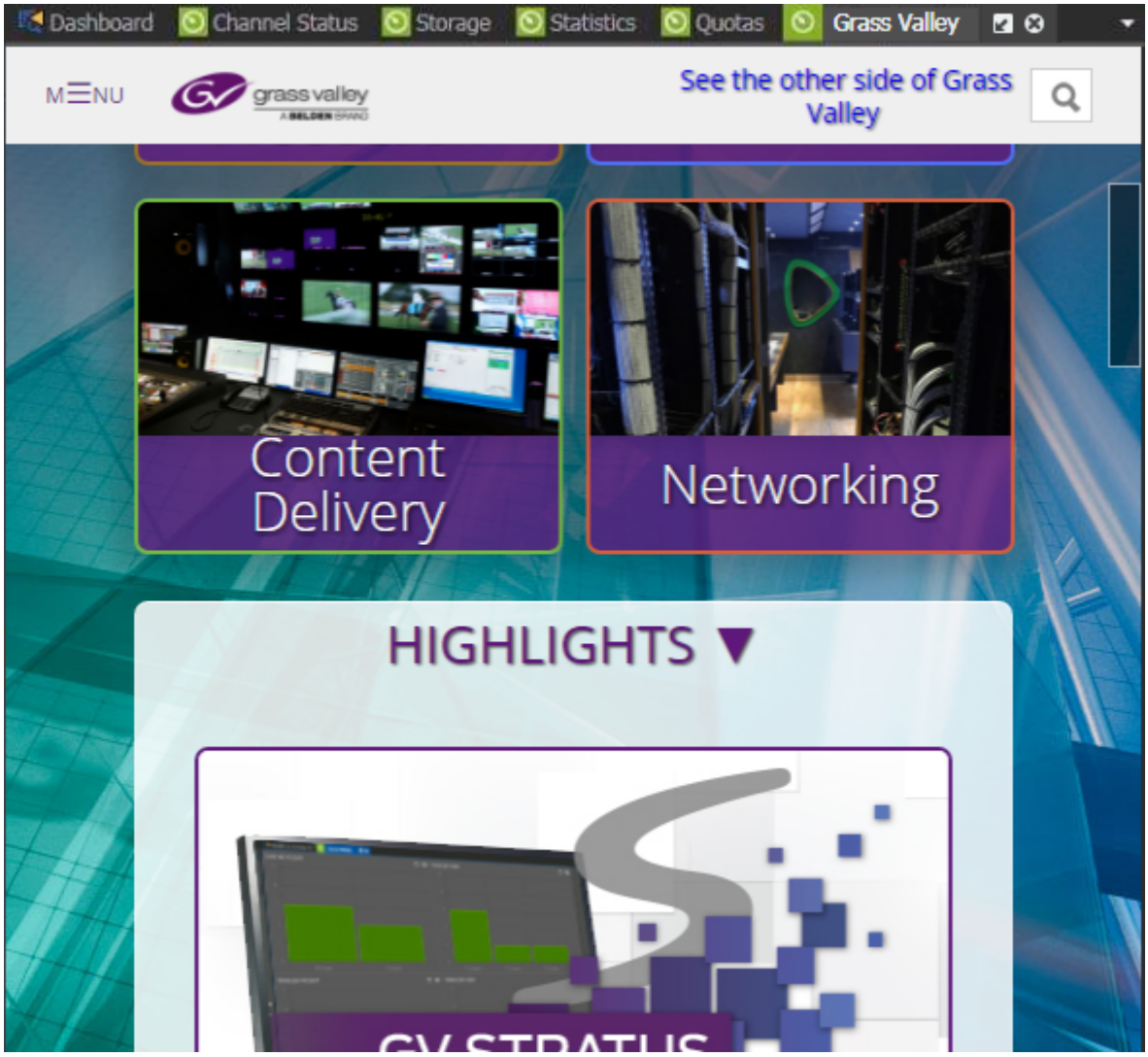
NOTE: The quota limit on K2 Summit system is only supported for K2 SAN media folders.



The Social Media panel displays data in graphical form for statistical information of all Social Media platforms. You must be assigned with the **Dashboard** and **Dashboard - Social Media** roles in order to view the panel. Once an asset is published via the configured social media account, it is possible to gather statistical data such as (View-, Like- and Share-) counts from the social media platform. In addition to the display via the Dashboard tool, those statistics can also be viewed via an internet browser at: *`http://<coreservername>/webapps/statistics/?mode=social-media`*



If a webpage is configured in GV STRATUS Control Panel for display in the Dashboard tool, you can select the webpage under Dashboard options and view the display on a separate panel.

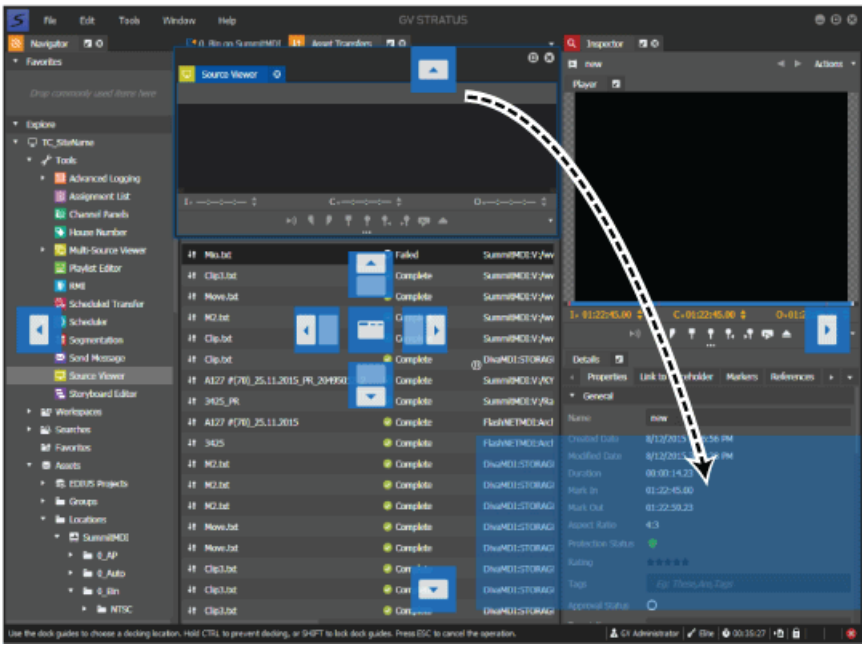


Related Topics

Web Monitor Add/Modify settings on page 377

About customizing the application workspace

You can rearrange the panels of the application to best suit your workflow needs.



Features for customizing the workspace are as follows:

- Undock panels and move them to another location within the application window, within another panel, or to their own location on the Windows desktop.
- Hide panels so that they show only as a tab.
- Close panels.
- Resize panels.
- Save an arrangement of docked and undocked panels as a uniquely named workspace.
- Load a workspace to automatically arrange panels.

Related Topics

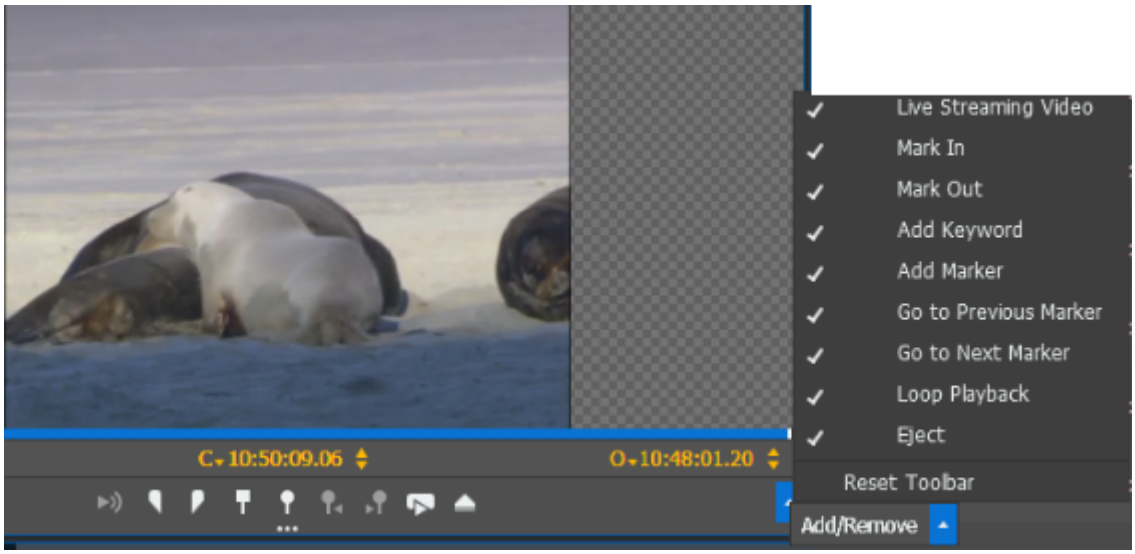
Customizing the application workspace on page 1392

Arranging control tray buttons

Viewers and players have a control tray that provides access to buttons. As you resize a panel smaller and the buttons do not all fit in the control tray, the buttons overflow onto a drop-down menu. You can configure buttons to show and to overflow as the panel is resized.

1. To show/hide the control tray, click the **Show/Hide Control Tray** button. ...

2. Click the drop-down arrow on the far right of the control tray.



The overflow menu displays hidden buttons.

3. Click **Add/Remove**.

   A menu of buttons opens.

4. Select the buttons to display.
5. If desired, select **Reset Toolbar** to return the buttons to their default display.

Your button configuration is saved with your GV STRATUS user preferences and propagated as follows:

- When you select buttons to display in a Channel Panel, all channels of the same type (player/recorder or recorder-only) and view mode size in that Channel Panel display your selection of buttons. Similarly, all gangs of the same type (containing at least one player/recorder or all recorder-only) display your selection of buttons.
- When you select buttons to display in a Playlist Editor, any channel in the Playlist Editor displays your selection of buttons.

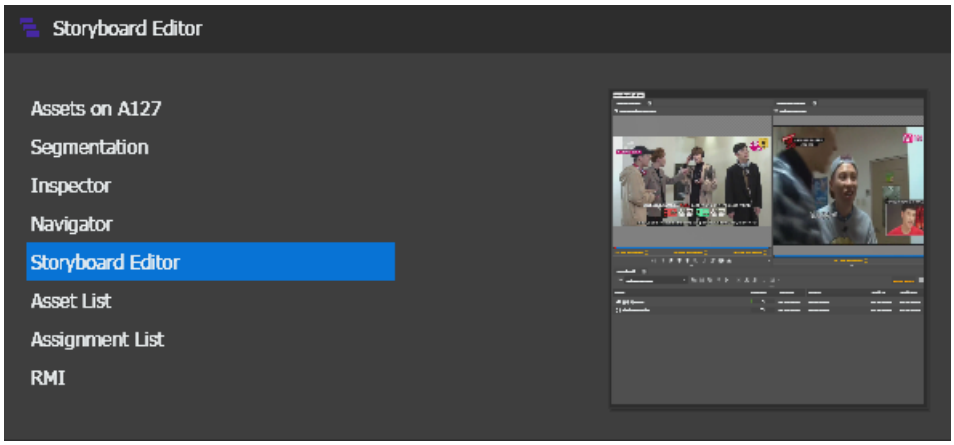
Focusing on a tool

You can easily select and focus on a specific tool in the GV STRATUS application.

1. To select a tool from the list of opened tools, use keyboard shortcuts as follows:

   - **Ctrl + Tab**, or
   - **Alt + F7**

   The pop-up dialog appears with a list of opened tools with thumbnails.



2. Press **Tab** or **F7** key repeatedly to move down the list, and release the hold on **Ctrl** or **Alt** key to select a tool.

   In addition, you can also press **Shift** together with **Ctrl + Tab** or **Alt + F7** keys to move up the list. Then, release the hold on all shortcut keys to select a tool from the list.

When selected, the tool is given focus. If the tool includes a player or viewer such as the Inspector, Advanced Logging Suite, Segmentation, or Storyboard Editor, then the primary viewer in the tool is automatically in focus.

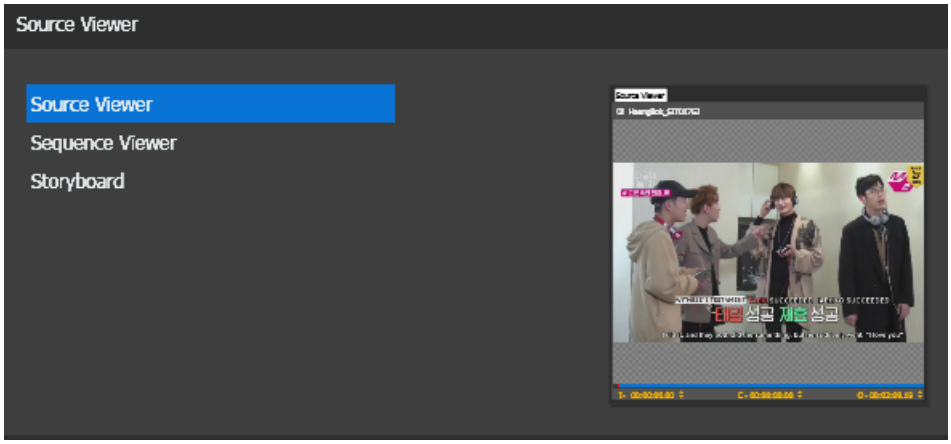
Focusing on a viewer in a tool

This is only applicable to GV STRATUS tools with multiple embedded views such as Inspector, Advanced Logging Suite, Segmentation, or Storyboard Editor.

You can easily select an embedded view to move focus to that part of the tool.

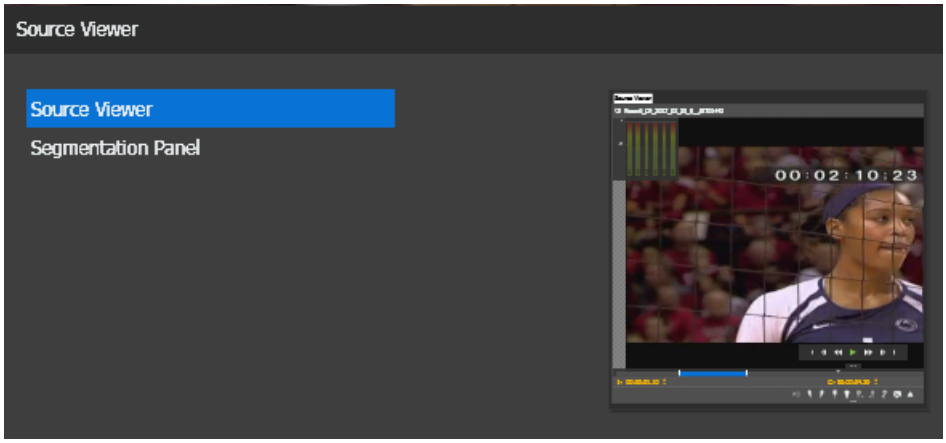
1. To select a specific panel in a tool, use keyboard shortcuts **Shift + Tab** to view and select from the list.

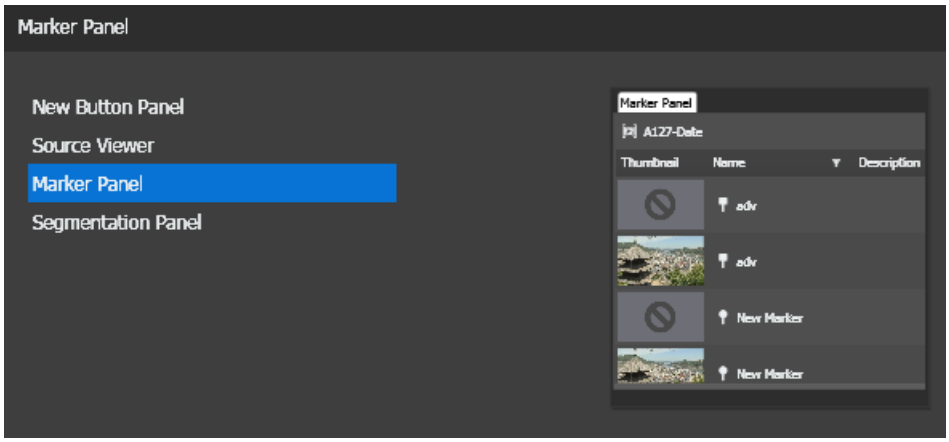
   The pop-up dialog appears with a list of panels in the tool with thumbnails.



In case of multiple viewers such as in the Storyboard Editor, you can select to focus either on the Source Viewer or Sequence Viewer.

Examples below are for the Segmentation and Advanced Logging tools.





2. Press the **Tab** key repeatedly to move down the list, and release your hold of the **Shift** key to select a panel or viewer.

   The selected panel or viewer is now in focus.

Previewing a live streaming video

You can preview live video input of K2 Summit channels.

1. Click the **Live Streaming Video** button on a Channel Panel, Playlist Editor, Source Viewer, or Scheduler tool.

   The live streaming video is displayed as follows:

   - If a Playlist Editor or Channel Panel, the video is displayed in the K2 channel.
   - If a Source Viewer or Scheduler tool, the video is displayed in Source Viewer.

2. Click the **Live Streaming Audio** button to isolate the selected audio for a live video stream.

   When enabled, audio from all other live video streams is automatically muted.

   The **Live Streaming Audio** button is disabled by default when the channel first opens.

   The audio can only be enabled one channel at a time.

Related Topics

Using the Audio Overlay on page 1002

Managing assets

Using the Explore section

The Explore section of the Navigator panel lets you browse the various items in the application.

1. In the Navigator panel, expand the Explore section by clicking on the **Show/Hide** button.
   The Explore section expands.
2. Select the node that you want to explore.
   The Asset List panel displays the contents of the selected node.

About the GV STRATUS Assets view

In the Navigator panel, the Assets node provides a view that is based on the information available in the GV STRATUS Database. This allows the GV STRATUS application to provide you with flexibility for viewing and organizing your assets. You can configure bins and folders based on users, projects, events, or other parameters to suit your particular workflows.

Under the Assets node are the following nodes:

- Groups — Provides a view of folders that can contain assets from any location in the GV STRATUS system. This allows you to create folders and group assets without being constrained by the locations of the assets. The folders you create are visible and accessible by everyone on the GV STRATUS system. The folders exist in the GV STRATUS Database but not in K2 Summit/SAN storage. In previous Grass Valley products, Groups were known as "Collections".
- Locations — Provides a view of bins in K2 Summit/SAN storage. When you create a bin, it is created in K2 Summit/SAN storage.
- EDIUS Projects — Provides a view of bins in the EDIUS Projects folder. The EDIUS Projects node appears under the Assets node only if logged-in users have the EDIUS Project Management role assigned to them. While an EDIUS project is being edited, the project and its included sequences and clips are locked in the GV STRATUS application.

The Navigator panel also provides a Devices node. Under the Devices node you find the local computer on which the GV STRATUS application is installed. Archive servers configured in GV STRATUS Control Panel are also shown under the Devices node if you have the Archive Rights or Restore Rights roles.

If you have the role of Media Manager, as configured in GV STRATUS Control Panel, the Navigator panel also provides the following:

- The Groups view includes the Lost and Found folder, which you can check for assets that do not have a location or that might not be otherwise accessible in the Assets view.
- Permission is granted to move assets from an archive system to the GV STRATUS system. Without this permission, assets may be copied but not moved.

The GV STRATUS Database controls both the Assets view and the Devices view. The database keeps the operations you perform in synchronization with the GV STRATUS/K2 system overall. The GV STRATUS Database also associates extended metadata with each of your assets, as well as keeps track of relationships between assets. You can use this metadata as search criteria with the advanced search tool.

Related Topics

About the Lost and Found folder on page 469

Browsing assets

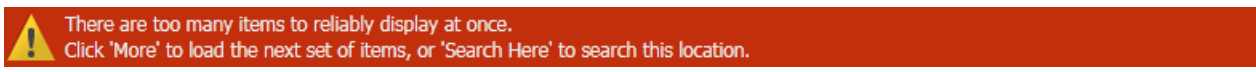
From the Navigator panel, you can access bins and sub-bins of assets.

1. In the Navigator panel, select the bin, group or location you want to browse.

   The list of sub-bins and top-level assets or files displays in the Asset List panel.

   Asset enumeration is limited to 2500 per page in the GV STRATUS 32-bit application, and 10,000 per page in the 64-bit application.

   If the limit is reached, a warning displays in the Asset List panel. You can click **More** to load the next batch of assets, or click **Search Here** to decrease the number of assets displayed.



2. To expand a bin, click the arrow next to the bin name in the Navigator panel. To minimize the bin, click the arrow next to the bin name a second time.
3. Use the scroll bar to move up and down the list of bins and sub-bins.

***NOTE: Offline K2 Summits are indicated by a red "X" overlay on K2 Summit icons and bins in the* Navigator.**

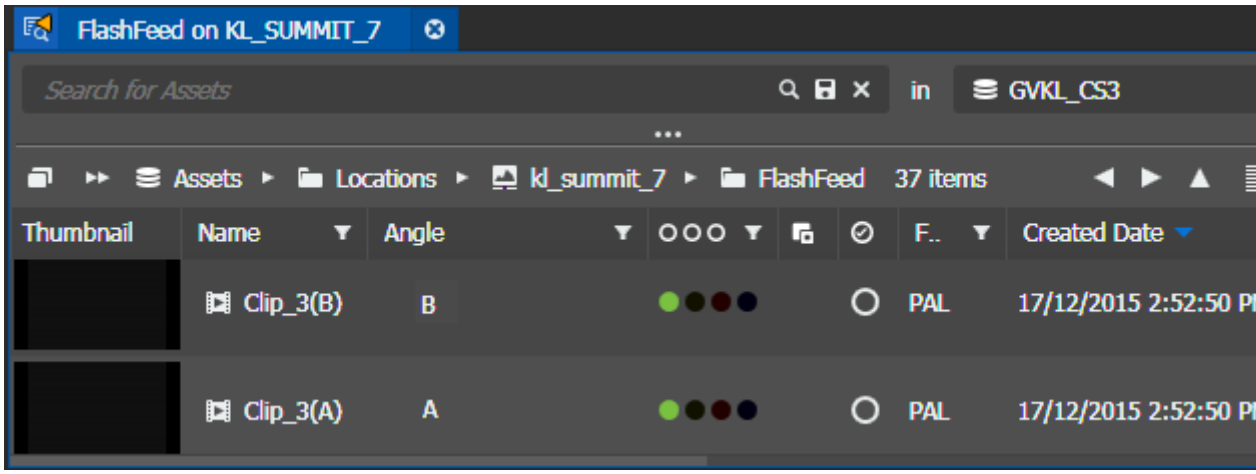
Browsing camera angles

From the Asset List panel, you can view an asset's associated camera angles. If a clip is recorded with gang record, each clip recorded in the gang is considered an angle.

This feature is typically used to integrate with a K2 Dyno Replay Controller workflow.

In the Asset List panel, right-click a gang-recorded clip and select **View Related | Camera Angles**.

The list displays all of the clips in the gang record as camera angles.



Asset indicators

These icons indicate the type of asset.

3D Clip: Identifies the asset as a 3D clip.
Clip: Identifies the asset as a clip.
Clip Transfer: Identifies the asset status as in progress for import or transfer.
Key and Fill: Identifies the asset as a key and fill.
Multimedia: Identifies the asset as multimedia.
Placeholder: Identifies the asset as a placeholder.
Playlist: Identifies the asset as a playlist.
Recording Clip: Identifies the asset as a recording clip.
Sequence: Identifies the asset as a sequence.
Subclip: Identifies the asset as a subclip or any single clip that references a parent clip.
Archived Clip: Identifies the asset as type archived clip.

Archived Multimedia: Identifies the asset as type archived multimedia.

Proxy: Indicates that the high-resolution asset has proxy.

Remote asset: Identifies the asset as type remote clip.

These colors provide additional indicators.

Asset with no content: Identifies the asset as type with no content.

Clip: Identifies the asset as type clip.

Playlist: Identifies the asset as a playlist.

Subclip: Identifies the asset as a subclip or any single clip that references a parent clip.

Sequence: Identifies the asset as a sequence.

These indicators report the status of the high resolution asset.

Online	**Archived**	**Unavailable**	**Remote**
Identifies that the asset has high-resolution material on the K2 Summit/SAN system.	Identifies that the high-resolution material of the asset is archived.	Identifies that the high-resolution material of the asset is unavailable.	Identifies that the high-resolution material of the asset is on a remote GV STRATUS system.

Status not indicated: Identifies that the indicator is not reporting the relevant status. For example, if a particular colored indicator reports that an asset is "Remote", this dark indicator reports that the asset is "Not Remote".

This icon indicates that GV STRATUS security settings are applied to the asset or bin.

Access Restricted: Indicates the asset or bin has restricted access.

These buttons provide the ability to toggle the Protection Status of assets in the Asset List and Inspector.

Unprotected: Indicates that the asset's Protection Status is Unprotected and available for public use.

Protected: Indicates that the asset's Protection Status is Protected.

These buttons allow the change of an asset's approval status in the Inspector.

None: Identifies the approval status of the clip as none.

Approved: Identifies the approval status of the clip as approved.

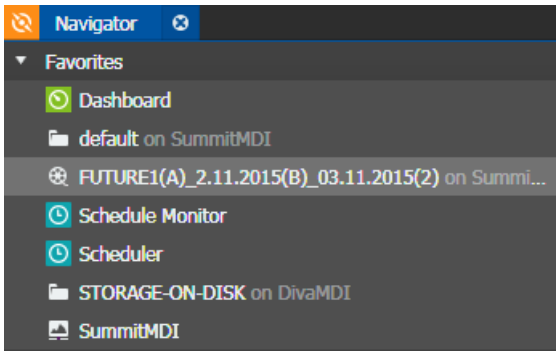
Rejected: Identifies the approval status of the clip as rejected.

Adding a favorite

You can drag and drop any type of GV STRATUS item to the Navigator panel and save it there as a shortcut.

1. In the Navigator panel, expand the Favorites section by clicking on the **Favorites** Show/Hide control.

   The Favorites section expands.



2. Identify the item that you want to make a favorite.
3. Drag and drop the item to the Favorites section.

A shortcut to the item is displayed in the Favorites section.

Removing or deleting a favorite

1. To remove a favorite from the Favorites section, right-click on the favorite and select **Delete**.
2. Depending on the type of favorite selected, either a **Confirm Remove** or a **Delete or Remove** dialog box opens. Select **Remove** or **Remove from Favorites**.

   The favorite is removed from the Favorites section. The item itself is not deleted from its original location.
3. To delete the item itself, select **Delete** in the **Delete or Remove** dialog box.

   The item is deleted from its original location.

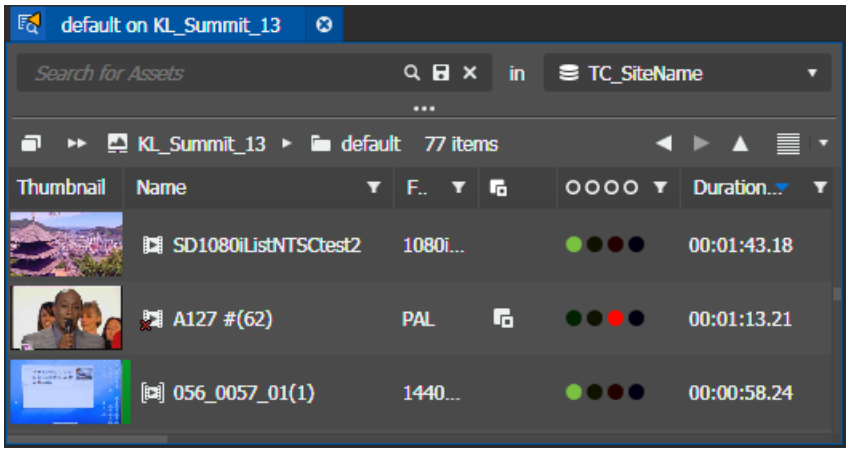
Managing Asset Lists

The topics in this section describe features for managing Asset Lists.

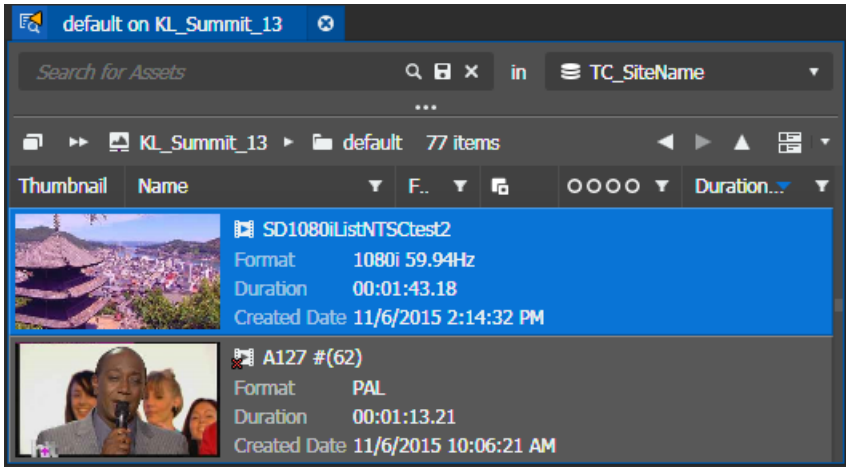
About view modes

You can customize the arrangement of items in a list in the Asset List panel. View modes can be selected as follows:

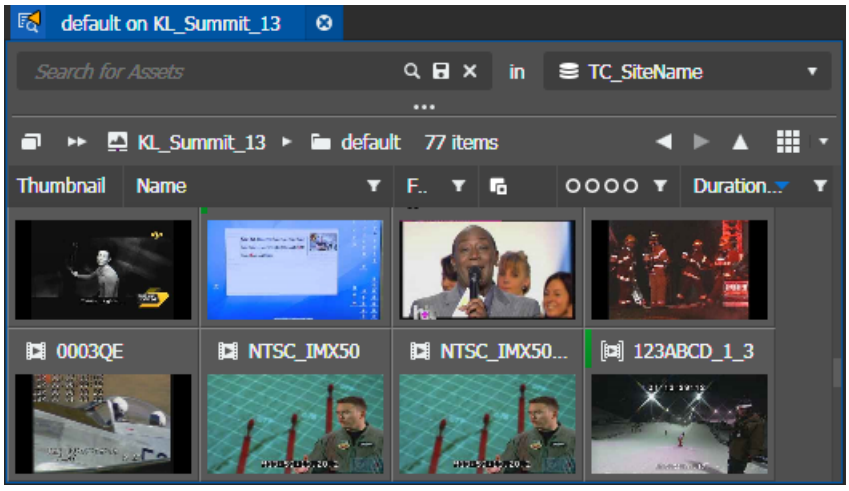
Details view



Tiles view



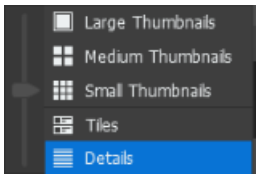
Thumbnails view



Customizing the display of list items

To customize the arrangement of items in a list, do one of the following:

- Either right-click in the list and click **View Mode** or click the **View Mode** down-arrow and select your preferred view.
- Click the **View Mode** button multiple times to toggle between sizes.
- You can shrink or enlarge the Thumbnails view mode as follows:
  a) Right-click in the list and select **View Mode**, or click the **View Mode** button down-arrow.



  b) To adjust the size, use the Slider bar.
- You can select the order of properties displayed in the Tiles view mode as follows:
  a) Right-click in the list and select **View Mode** and **Tiles**.
  b) Right-click in the list and select **Tile Properties**

  The Property Order dialog box displays the top three properties.
  c) Highlight a property and use the up/down arrows to move the property up or down in the display.
  d) Click **OK**.

  The property is displayed in the desired order.
- In Details mode, you can add or remove columns as follows:
  a) Right-click a column head.
  b) Select **Columns**.
  c) Select or de-select the columns to display.
- In Details mode, you can change the size of thumbnail display by resizing the thumbnail column.

Once the changes have been made, the customized display is saved into your Workspace.

Related Topics

The Asset List panel on page 956

Sorting a list view

1. You can do the following:
   a) Click a column head.

   Items are sorted based on the entries in that column.
   b) To reverse the sort order, click the column head again.

2. To sort items in a list, do the following:
   a) Right-click an item.
   b) Select **Arrange By**.
      A list of categories is displayed.
   c) Select the category on which to sort.
      The items are sorted based on the selected category.
   d) To reverse the sort order, select the category again.

Adding and removing columns in a list

You can configure the columns displayed in an Asset List to support your specific workflow.

1. Right-click a column head and select **Columns**.
   A menu of columns opens.
2. Select or clear check marks to arrange the columns displayed in your list.
   Custom metadata fields, as configured in GV STRATUS Control Panel, are displayed at the bottom of the menu.

Related Topics

Using custom metadata in Inspector on page 1018

Opening multiple Asset List panels

When you open a new Asset List panel, it displays as a tab in the original Asset List panel. The new panel can be undocked or moved to another location within the application window or to its own location on the Windows desktop. For example, if you are ingesting files on two different servers, you could compare the contents of their bins by viewing two adjacent Asset List panels.

To open a new Asset List panel, click the **Open New Panel** button.

The new Asset List panel has the same view mode as the original Asset List panel and is automatically set as active; when you click on a bin in the Navigator panel, or create a new search, the results are displayed in this active panel even if it is hidden beneath other panels.

To compare multiple Asset List panels

You can easily compare searches or the contents of different bins by creating multiple Asset List panels.

1. Open a new Asset List panel.
   The newly created Asset List panel is automatically made active.
2. Dock the newly created Asset List panel next to the original Asset List panel.
3. To populate the active Asset List panel, click on the desired item in the Navigator panel or perform a search.
4. To populate the other Asset List panel, first make it active.
5. Populate the other Asset List panel by clicking on the desired item in the Navigator panel or performing another search.

Managing multiple tabs in a panel

If you have more tabs than the application can display at one time, you can use the following:

- Left/right arrows at the top left and right corners of the panel let you scroll the displayedtabs in a panel.
- Hovering the mouse over a tab allows you to preview the contents of that tab.
- A drop-down arrow lets you select from a list of all the tabs open in the panel.
- Pressing **CTRL + Tab** allows you to switch between all open tabs in every panel.

Protecting an asset using Inspector

1. In the Asset List, double-click on the asset.

   The asset is loaded into the Inspector panel.

2. On the General tab, for the **Protection Status** property, click the **Unprotected** button.

   The button toggles between protected and unprotected to set the status.

   The asset is now protected. To verify this, you can hover over the the **Protected** button and view the property.

3. To unprotect the asset, click the **Protected** button.

NOTE: Protected assets cannot be renamed, deleted, or modified in any way.

Protecting multiple assets in Asset List

1. In the Asset List, if it is not already displayed, display the Protection Status column.
2. In the row for each asset you are locking, click the **Unprotected** button.

Assets toggle from unprotected to protected.

Filtering assets

You can filter a list of assets in the Asset List panel.

1. In the Navigator panel, select the bin or group that you want to filter. You can also filter search results.

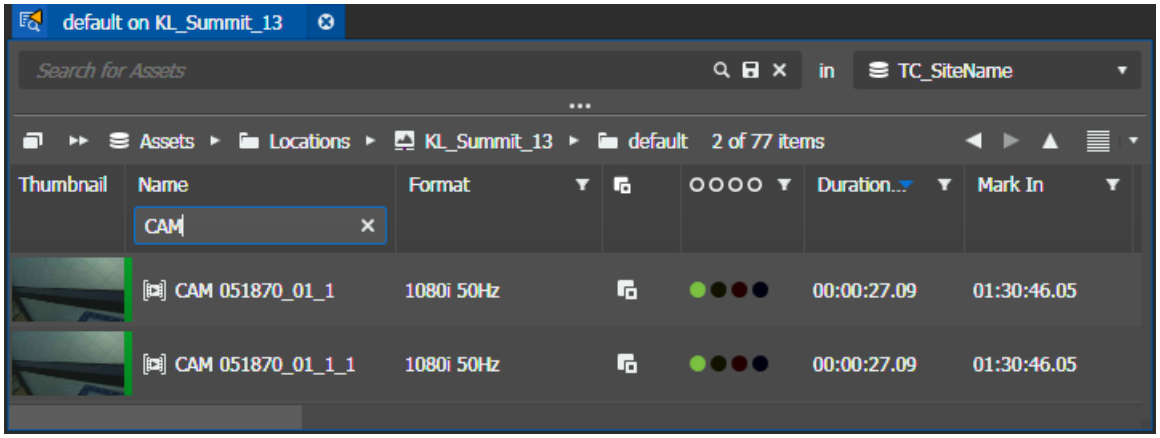
   The assets are displayed in the Asset List panel.

2. Identify the column by which to filter assets. Next to the column heading, click the **Enable Filter** button.

   A text field opens in the column heading cell.

3. Enter the filter criteria. As you enter each character, the list displays results accordingly.

4. To filter by multiple criteria, click the **Enable Filter** button in multiple columns and enter filter criteria. The list displays only results that match all criteria.



   You can also filter as follows:

   - Filter asset rating by entering the rating number from 0 to 5.
   - Filter boolean custom metadata by entering letters in the words 'true' and 'false'. However, filtering by the letter 'e' returns results with both true and false items.
   - Filter color by entering the RGB hexadecimal value without the alpha symbol. For example the hexadecimal value of pure red is #FF0000, so searching for red would be entering **FF0000**.

5. To remove a filter, click the **X** button in the field.

Renaming assets

- If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, and metadata.
- In order to change the name of an asset, you must be assigned with the **Rename Asset Rights** role and write permission for the **Name** property in Metadata | Permissions settings of GV STRATUS Control Panel.

1. Select an asset that you want to rename on the Asset List.
2. Do one of the following:

   - Press the **F2** key
   - Right-click and select **Rename**.

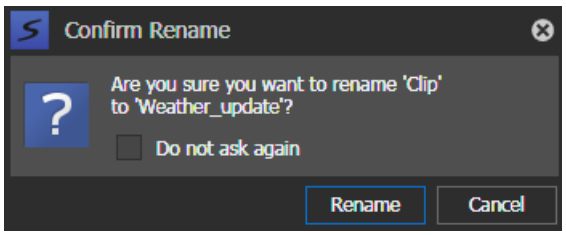
3. Enter the new name for the asset.

   The name must conform to asset and bin name limitations.

   The name change must not be a change in capitalization only.

4. Press **Enter**.

   The Confirm Rename dialog appears.



5. Click **Rename** to confirm the change.

The asset name changes to the new name.

⚠ ***CAUTION: Renaming an asset directly via K2 AppCenter on the K2 Summit renames the physical association, and also the GV STRATUS asset.***

Related Topics

Limitations for creating and naming assets and bins on page 1428

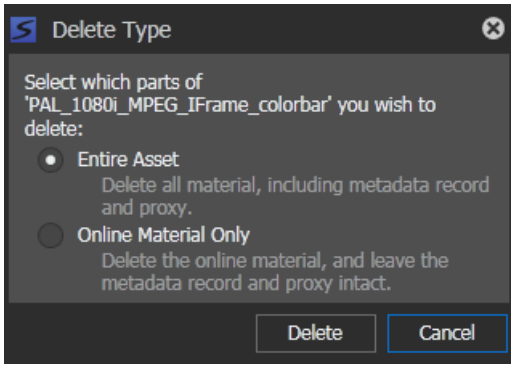
Deleting assets

Your delete operations depend on how your user account is configured in GV STRATUS Control Panel. Delete buttons, menu items, and keyboard shortcuts are disabled if delete rights are denied. An asset with a child association (shallow copy) cannot be deleted. Deleting an asset with multiple high-resolution associations (deep copy) deletes the entire asset from multiple locations. A Media Manager has additional options to delete parts of an asset. If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins and assets that do not allow read permissions are not visible.

1. In an Asset List panel, right-click the asset you are deleting and select **Delete**.

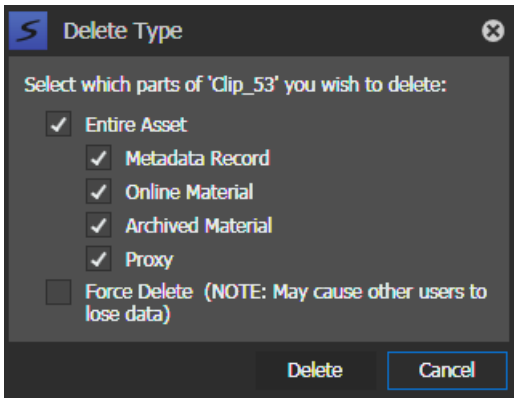
   A Delete Type dialog box opens. The dialog box for Media Managers offers additional options.

2. If you are not a Media Manager, select your options as follows:



- Entire Asset — Select this to delete the entire asset including online material and proxy. Archived material is not deleted.
- Online Material Only— Select this to only delete online material. Metadata, proxy, and archived material is not deleted.

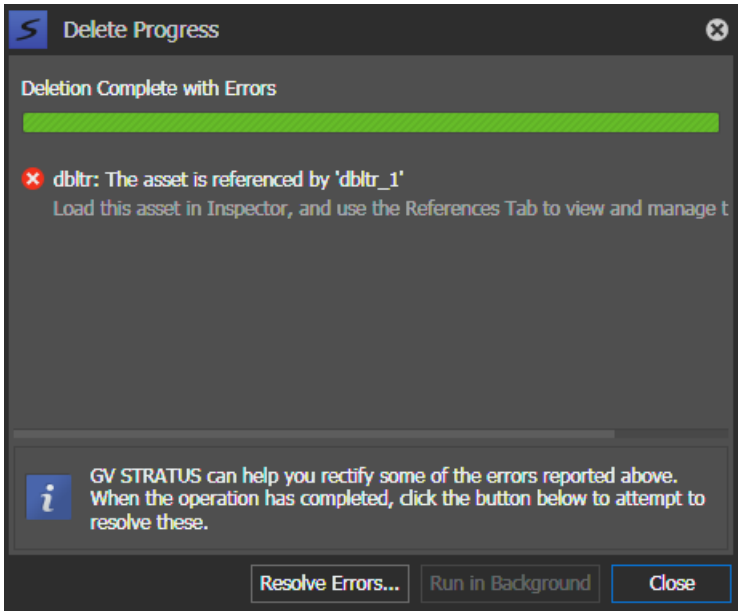
3. If you are a Media Manager, select your options as follows:



- Entire Asset — Select this to delete the entire asset including online material, archived material, metadata, and proxy. If one part of the asset is in use or blocked from deletion, no part of the asset will be deleted.
- Metadata Record — Select this to only delete the metadata of the asset.
- Online Material — Select this to only delete online material of the asset on the K2 Summit/SAN system.
- Archived Material — Select this to only delete archived material of the asset on the archived system.
- Proxy — Select this to only delete the proxy of the asset.
- Force Delete — Select this to delete the entire asset even if one part of the asset is in used by other users.

4. Click **Delete**.

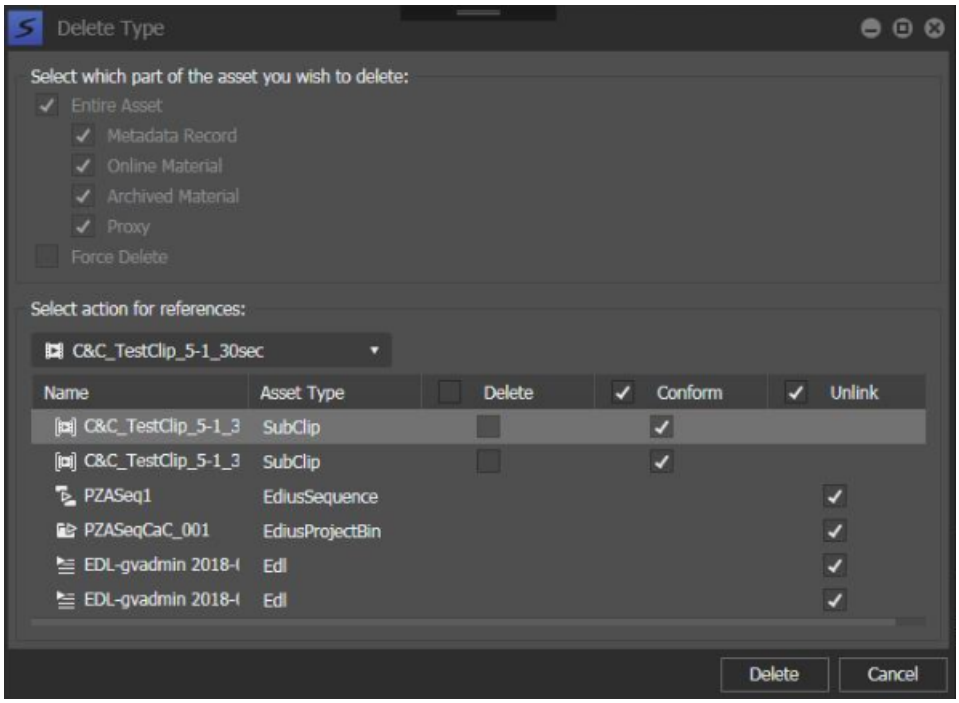
5. If one or more of the assets you are deleting have child associations, the **Delete Progress** dialog box displays "`...The asset is referenced...`".



Proceed as follows to continue with the delete operation:

a) Click **Resolve Errors**.

The **Delete Type** dialog box opens.



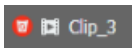
b) Select the asset you are deleting in the **References** drop-down list.

c) For each item that references the asset, select either **Delete**, **Conform**, or **Unlink** check box as follows:

- **Delete**: Deletes the subclip or sequence that references the asset.
- **Conform**: Conforms and saves the subclip or sequence that references the asset. Original subclips and sequences are deleted after the conform is complete.
- **Unlink**: Unlinks the reference to EDIUS sequence, EDIUS Project bin, or STRATUS EDL. For EDIUS, the asset will no longer be part of the EDIUS sequence and removed from the EDIUS Project bin. For STRATUS EDL, the asset will no longer be included as an event in the STRATUS EDL when you view it in the Simple Editor tool.

NOTE: You cannot delete an asset referenced to EDIUS or STRATUS EDL if it is still linked to the sequence, project bin, or EDL. The Delete button is disabled if the Unlink check-box is not selected.

6. Click **Delete**.

A red icon displays on the Asset List to indicate that the asset is being deleted. 

If the asset is dragged into the Inspector while being deleted, the viewer displays the message: **This Item is Being Deleted**

The asset is deleted according to your selection. However, online material can only be deleted if the asset is not in use (for example, if the asset is loaded in a K2 Summit channel).

Related Topics

Asset copies and deletions on page 443
Asset copies and deletions on page 443

Searching assets

The topics in this section describe search features.

About searches

You can search assets using the Simple Search tool at the top of the Asset List panel. When you type in text, specify the remote or local GV STRATUS system to search (the search provider), and press Enter. Results are displayed in a search results asset list.

For a simple search you can enter text with advanced query syntax. Assets with names, tags, descriptions, comments, marker text, or custom text data that match the search are returned.

Use the the **Advanced Search Toggle** button ... next to the Search text field to use additional criteria and conditions.

You can save a search and re-use it later on. Searches are saved in the Navigator panel. When you click on a search, the search runs and results are displayed.

These search features apply to searching the GV STRATUS system. If you search outside the GV STRATUS system, GV STRATUS search features do not apply.

Related Topics

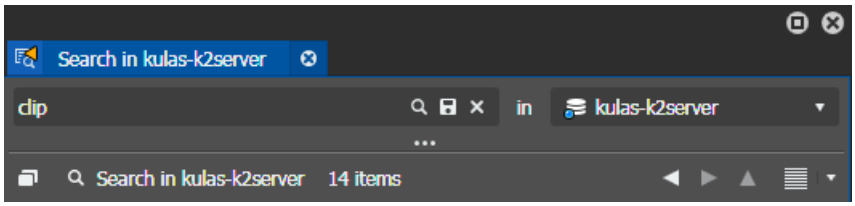
The Asset List panel on page 956

About advanced query syntax, advanced searches and custom expressions on page 423

Searching assets with the Simple Search tool

1. In an Asset List panel Location drop-down list, select the GV STRATUS system you want to search.
2. In the Simple Search tool, enter your search.

   For a simple search you can enter text with advanced query syntax. Assets with names, tags, descriptions, comments, marker text, or custom text data that match the search are returned.
3. To start the search, press **Enter**.



Assets matching the search criteria are displayed in a search results asset list.

If it is not apparent why some assets were returned for your search, add columns to the search results asset list or view assets in Inspector.

Related Topics

About searches on page 988

Search constraints and considerations on page 992

About advanced query syntax, advanced searches and custom expressions on page 423

About advanced query syntax, advanced searches and custom expressions

A combination of search features provide flexibility in creating GV STRATUS searches. Entering text with advanced query syntax is available in both the Simple Search tool and the Advanced Search tool. The Advanced Search tool provides additional capabilities.

The advanced query syntax available when you enter text is as follows:

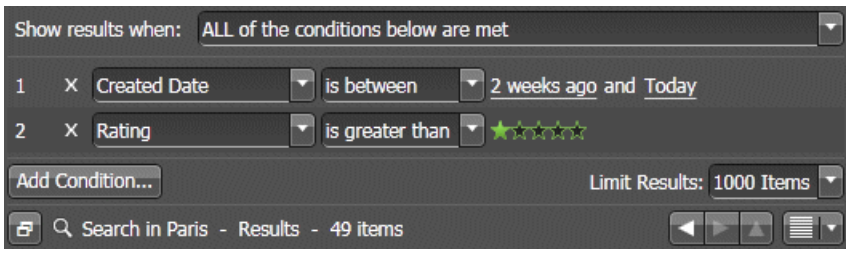
- If you search on one or more words (with no search syntax), the search returns assets that match all the words in any order. This is the Boolean "AND" operator. This is a change from previous versions, where this was a phrase search.

- Search syntax is as follows:
  - If you enter words surrounded by quotation marks, the search returns assets that match that exact phrase, with the words in the exact order.
  - Text surrounded by quotation marks is searched literally. Any search syntax or operators within the quotation marks are interpreted as plain text instead.
  - Simple boolean operators AND, OR and NOT are supported. Enter these operators in all capital letters.
  - Parenthesis control the precedence of the boolean operations.

The following are advanced query syntax examples. Each example is followed by the steps the GV STRATUS system goes through as it processes the search:

- “the quick brown” (fox OR dog) jumped over the NOT lazy cat
  1. Contains the phrase “the quick brown” AND
  2. Contains ‘fox’ or ‘dog’ AND
  3. Contains ‘jumped’ AND
  4. Contains ‘over’ AND
  5. Contains ‘the’ AND
  6. Does not contain ‘lazy’ AND
  7. Contains ‘cat’
- abc AND (def OR ghi)
  1. Contains ‘abc’ AND
  2. Contains ‘def’ OR ‘ghi’
- abc AND def OR ghi
  1. Contains ‘abc’ AND ‘def’ OR
  2. Contains ‘ghi'

The **Advanced Search Toggle** button ... next to the Simple Search tool provides additional capabilities to the search tool.



You can search using multiple conditions. You define the type of search as follows:

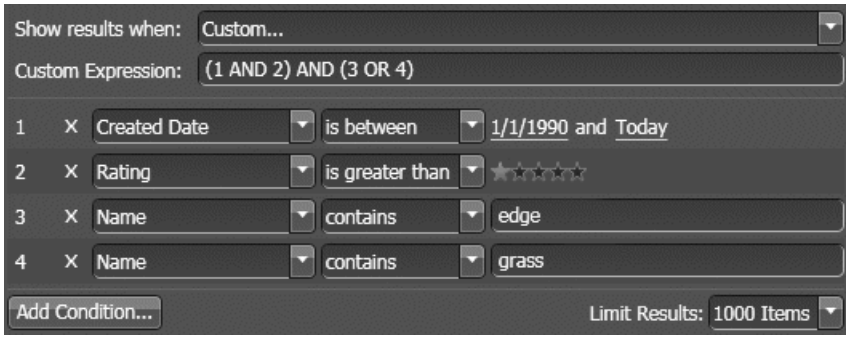
- ALL of the conditions below are met — This is the Boolean "AND" operator. The search returns assets that match all conditions. Only conditions with values (conditions that are not blank) are included in the search.

- ANY of the conditions below are met — This is the Boolean "OR" operator. The search returns assets that match any of the conditions. Only conditions with values (conditions that are not blank) are included in the search.
- Custom — You can enter text to create a custom expression using Boolean operators.

  In your custom expression, you use the condition numbers (1, 2, 3, 4, etc) to represent the condition on which you are searching. For example, if you have configured condition 1 as "Asset Name is basketball" and condition 2 as "Asset Created is Today", then entering custom expression "1 AND 2" finds assets named basketball created today.

  The "OR" and "AND" operators are at the same precedence, so for complex expression you use parentheses to group relationships. The following are examples of complex expressions:

  - (1 AND 2) OR (1 AND 3)
  - ((1 AND 4) OR 3) AND ((2 OR 4) AND 3)



You can use advanced query syntax in the Advanced Search tool. When you create a "contains" condition that searches a text field, you can enter text with advanced query syntax to search that field. The following is an example of this type of condition:

- Name | contains | guitar NOT rock

In this way a search in the Simple Search tool is equivalent to a "contains" search that searches multiple text fields by default. For a simple search you can enter text with advanced query syntax. Assets with names, tags, descriptions, comments, marker text, or custom text data that match the search are returned.

You can also search for custom metadata in the Advanced Search tool. In addition, the custom metadata search allows you to search for an empty field.

For an extended application of boolean logic in the Advanced Search tool, you can create multiple conditions that search text fields, each of which use advanced query syntax. Then you can combine those conditions as a custom expression.

Related Topics

Searching assets with the advanced search tool on page 992

Search constraints and considerations

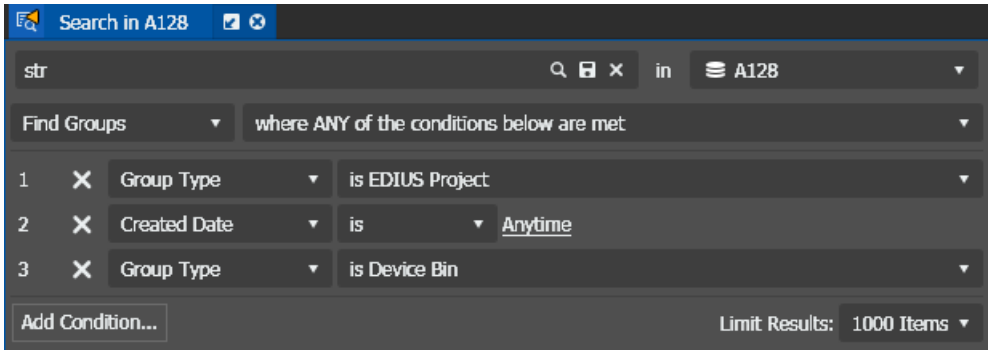
By default, search results are limited to 2000 items in the 32-bit application, and 5000 items in the 64-bit application. In the advanced search section, you can define the limit, from 50 to 5000 items.

To increase the success of your search, do the following:

- With the exceptions explained below, non-alphanumeric characters, such as !, -, _, @, #, %, etc., are interpreted as breaks and are searched the same as a space between words in the search string. Do not form a search using these characters alone. The exception is the asterisk character (*), which is not interpreted as a break.
- Non-alphanumeric characters that are a part of common conventions such as dates, times, decimals, fractions, timecode, email addresses, IP addresses, etc., are not interpreted as a break in the convention. If a word has an @ character in the middle, it is interpreted as an email address and the @ character is not searched as a space between words.
- To include non-alphanumeric characters in your search, surrounded your search word or words with quotation marks.

Searching assets with the advanced search tool

1. Enter the text that you want to search in the Simple Search field.
2. Click the **Advanced Search Toggle** button ... at the bottom of the Simple Search tool.
   The advanced search options open.



3. In the Location drop-down list, select the location (search provider) you want to search in.
4. Select either **Find Assets** or **Find Groups** on the left drop-down list.
   - **Find Assets** — The search returns assets only such as clip, sub-clip, list, sequence, edl, and EDIUS sequence.
   - **Find Groups** — The search returns groups such as STRATUS Group, EDIUS Group, EDIUS Project, EDIUS Template, and Device Bin.

5. For the drop-down list on the right, select the type of search you are doing:
   - **where ALL of the conditions below are met** — The search returns results that match all conditions.
   - **where ANY of the conditions below are met** — The search returns results that match any condition.
   - **where a Custom expression is satisfied..** — A Custom Expression field opens in which you can enter a custom search expression.
6. Click the **Add Condition** button and configure search conditions as follows:
   - For each condition (1, 2, 3, 4, etc) select from lists or enter text to define the condition.

     A **Marker** search includes marker name, marker description, and marker tags. While a custom metadata field search also allows you to search for an empty field.
   - Click the **Add Condition** button again to add or the **X** button to remove conditions from the list.
   - When you create a "contains" condition that searches a text field, you can enter text with advanced query syntax to search that field.
   - When you create an "is between" condition, you can enter dates and times to specify a time range for the search.
   - When you create the "is Empty" condition, you can search for empty fields including rating, tags, and Boolean custom metadata.
7. In the **Limit Results** drop-down list, select the maximum number of assets in your search results.
8. To start the search, press **Enter**.

   Results matching the search criteria are displayed in the Asset List.

If it is not apparent why some assets were returned for your search, add columns to the search results asset list or view assets in Inspector.

If you need to reset columns later, you can right-click on the Asset List and select **Columns | Reset Columns to Default**.

Related Topics

Search constraints and considerations on page 992

About advanced query syntax, advanced searches and custom expressions on page 423

Determining the location of a search result asset

If a location of an asset is not displayed in the search result asset list **Path** column, you can find all of the asset's locations in the **Associations** tab of the Inspector panel.

1. From the search result list, select the asset that needs its location path determined.
2. Open the asset in the Inspector panel.

   The asset displays in the Inspector. The location of the asset displays under the **Path** column in the **Associations** tab.

Related Topics

Adding and removing columns in a list on page 982

Stopping a search or stopping refreshing a bin

To stop a search or a refresh in progress, click the red X in the Progress indicator

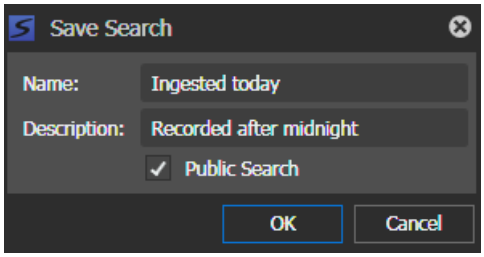
The application stops the search or refresh, and the Progress indicator disappears.

Saving searches

Searches that you create can be saved in the Navigator panel and reused later.

1. To save a search, click the the **Save** button next to the **Search** text field.

   The Save Search dialog box displays.



2. Enter the name of the search and, if desired, a description.
3. If you have the role of Media Manager, you can make the search available to all GV STRATUS system users by selecting **Public Search**.
4. Click **OK**.

Using a saved search

1. In the Navigator panel, expand the **Searches** node.
2. Find saved searches, organized as follows:
   - Public Searches: Searches saved as public by GV STRATUS system users with the role of Media Manager.
   - Saved Searches: Searches saved by you.
3. Select a saved search.

   The search is re-run. The Asset List panel displays the latest results.

Creating and modifying bins and groups

- To create bins, you must be logged on to the GV STRATUS application user account with the assigned role of **Bin Creation Rights**.

Use this procedure to create or modify a bin in your K2 Summit/SAN system storage.

Creating or modifying a bin under the Locations node in Navigator affects a corresponding bin in K2 storage. Groups created under the Groups node in Navigator create shortcut folders in the STRATUS database, which do not correspond directly to K2 bins.

1. Do one of the following to create a bin:
   - In the Navigator panel, right-click a K2 Summit/SAN system or a bin.
   - Right-click in an Asset List panel for a K2 Summit/SAN system bin.

   NOTE: To prevent corrupting the K2 database, do not exceed 8 nested bins levels when creating bins.
2. Select **New | Bin**.

   A New Bin dialog box opens.
3. Enter a name for your bin and click **OK**.
4. If GV STRATUS security settings are enforced, load the bin into Inspector and verify bin ownership.

   If the parent bin has Owner Hint security settings configured, the created bin automatically inherits the configured owner or owners, regardless of the user account creating the bin.
5. To change a bin name, right-click a bin and select **Rename**.

   You must be assigned **Rename Bin Rights** in GV STRATUS Control Panel. If GV STRATUS security settings are enforced, you must have adequate permissions. If not, menu selections are disabled.

   Rename bins with care. A bin containing a large number of assets can consume system resources for an extended period of time while the rename operation is applied.

   NOTE: Renaming a bin removes it from the Favorites node. You must add the bin to the Favorites node again after renaming it.

Related Topics

Limitations for creating and naming assets and bins on page 1428

Asset copies and deletions

When you copy an asset, different types of associations are created, depending on the K2 storage location and the type of asset copy, as follows:

- Shallow copy — When you copy assets and both copies are in the same K2 storage location, shallow copies are created. With a shallow copy, the high-resolution media files are not copied. Rather, the K2 media database and the GV STRATUS database contain a record for each shallow copy, and each record references the same media files. In the GV STRATUS system, this results in an asset with multiple references, similar to a subclip.
- Deep copy — When you copy assets and the copies are in different K2 storage locations, deep copies are created. With a deep copy, the high-resolution media files are copied. The K2 media database on each K2 system references its own media files. The GV STRATUS database references all the media files on all the different K2 storage locations and archive locations. In the GV STRATUS system, this results in an asset with multiple high-resolution associations.

When deleting assets, the following occurs:

- Assets with shallow copies — When the GV STRATUS system attempts to delete the shallow copy, the asset is not deleted. You must delete the referenced copy before you can delete the asset.
- Assets with deep copies — When you delete any one of the associated high-resolution assets, in any K2 storage or archive location, by default the GV STRATUS system deletes all the high-resolutions assets in all locations. Since it is one asset with multiple high-resolutions associations, the entire asset with all its associations is deleted. If you only want to delete a high-resolution association, you can do so on the **Associations** tab in the Inspector.

Take care when creating copies, considering your workflow in which copied assets are deleted. The GV STRATUS roles of **Delete Rights** and **Media Manager** can be assigned to user accounts to implement the desired workflow. As part of the delete operation, Media Managers can specify online/archive deletion and choose whether to delete or conform referenced copy of assets.

Related Topics

Deleting assets on page 985

Deleting assets on page 985

Viewing a video asset

1. Do one of the following:
   - Double-click an asset in the Asset List.
   - Drag an asset from the Asset List and drop it on the Inspector video player area.
   - Right-click on an asset in the Asset List, select **Open With | Inspector**.

   The asset displays in the Inspector.
2. View the video displayed in the upper area of the Inspector.

3. If desired, expand the video to full-screen view.

Related Topics

Using the Audio Overlay on page 1002

Identify high and low resolution while viewing

The following applies to viewing a video asset in the Source Viewer, Sequence Viewer, and viewers in Inspector, Advanced Logging, and Segmentation tools.

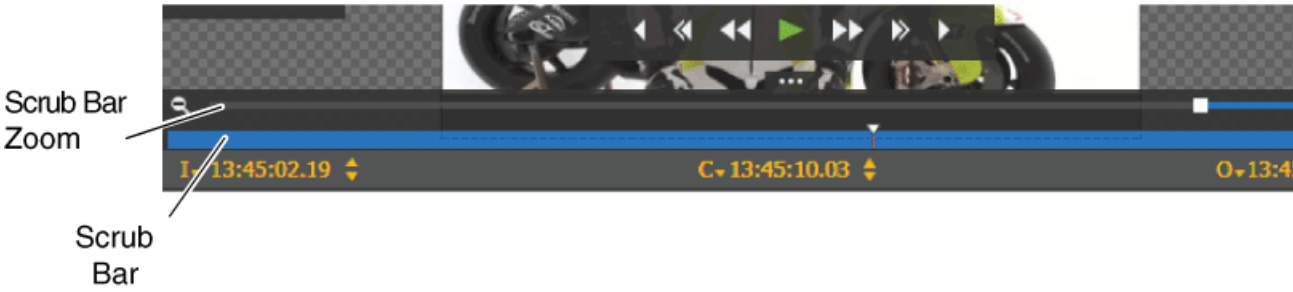
1. Load a video asset into the viewer.
2. Hover the cursor over the player as necessary so that overlay controls appear.
3. Identify the indicator in the lower right of the viewer as follows:

   LR **Proxy Playback**: Identifies currently loaded asset as low-resolution proxy.

   HR **High-Res Playback**: Identifies currently loaded asset as high-resolution.

Using the scrub bar zoom to navigate

You can use the scrub bar zoom on specific part of the asset by zooming on the scrub bar itself. This is particularly useful for assets with long duration. You can easily zoom on the scrub bar to get to a segment on the timeline.



- Drag the scrub bar slider to navigate through the clip.
- Click at any point along the scrub bar to jump the slider to that location in the clip.
- Select the **Toggle Zoom Controls** button, and do as follows:
  - Click the **Zoom In** button to zoom in the scrub bar display. The scrub bar zooms in for users to navigate.
  - Click the **Zoom Out** button to zoom out the scrub bar display. The scrub bar zooms out for users to navigate.
- In zoomed in position, you can also drag the **Scrub Bar Zoom** to a different position on the timeline. The Scrub Bar moves synchronously with the **Scrub Bar Zoom** so you can zoom at a different position on the timeline.

- By default, the **Scrub Bar Zoom** collapses automatically if the viewer is left idle. For the **Scrub Bar Zoom** to remain fixed on the viewer, you need to set the **Scrub bar Size** setting to **Fixed Size** in the Player tab of User Preferences setting.

Related Topics

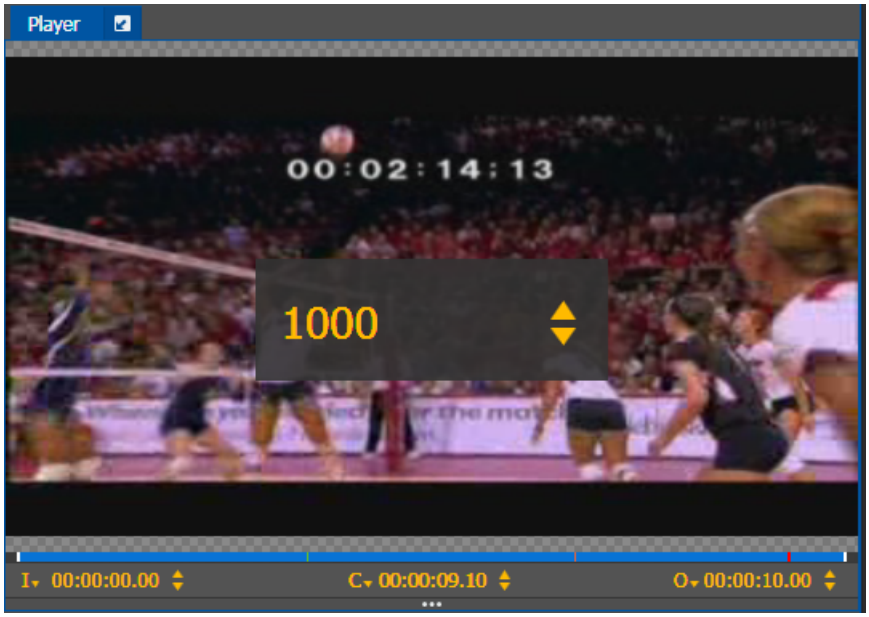
Configuring Source User Preference

Modifying timecode to navigate asset playback

You can enter any number to move the current timecode on the player or viewer to navigate an asset.

1. Ensure the player or viewer is in focus, and enter any numeric key.

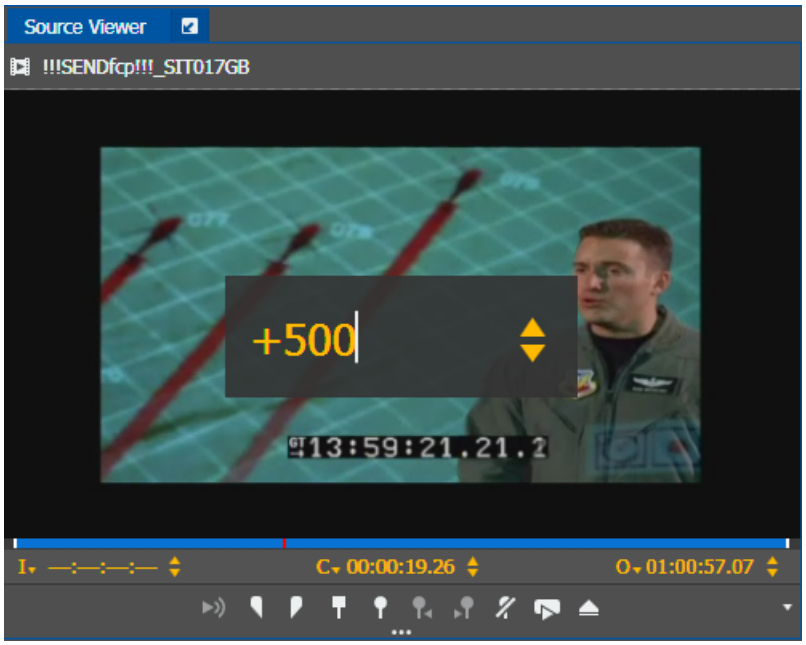
   The timecode editor appears with the numeric values you entered.



2. Press **Enter**.

   The playback point advances to the specified timecode, as indicated on the scrub bar.

3. You can also key in the **+** or **-** keys to enter a relative value to the current timecode.



The playback point advances if you entered the **+** key with a numerical value, and goes back relative to the current timecode if you entered the **-** key with a numerical value.

4. Press the **Esc** key to cancel the operation, if needed.

Viewing a video asset in full screen

The following applies to viewing video asset in the Source Viewer, Sequence Viewer, and viewers in Inspector, Advanced Logging, and Segmentation tools.

Click the **Full Screen** button on the upper right of the viewer.

The viewer expands and displays in full screen.

The overlay transport controls, timecode controls, scrub bar, and keyboard shortcuts can still be used to navigate through the asset in full screen mode.

If desired, the timecode controls can also be expanded and resized in full screen view.

Restoring viewer to normal size

Click the **Restore** button on the upper right of the viewer.

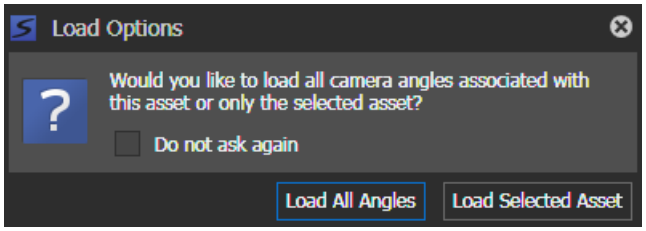
The viewer restores to its normal size.

Viewing asset with multiple angles

The following only applies to viewing video asset with multiple angles.

1. Load the asset into the Inspector panel.

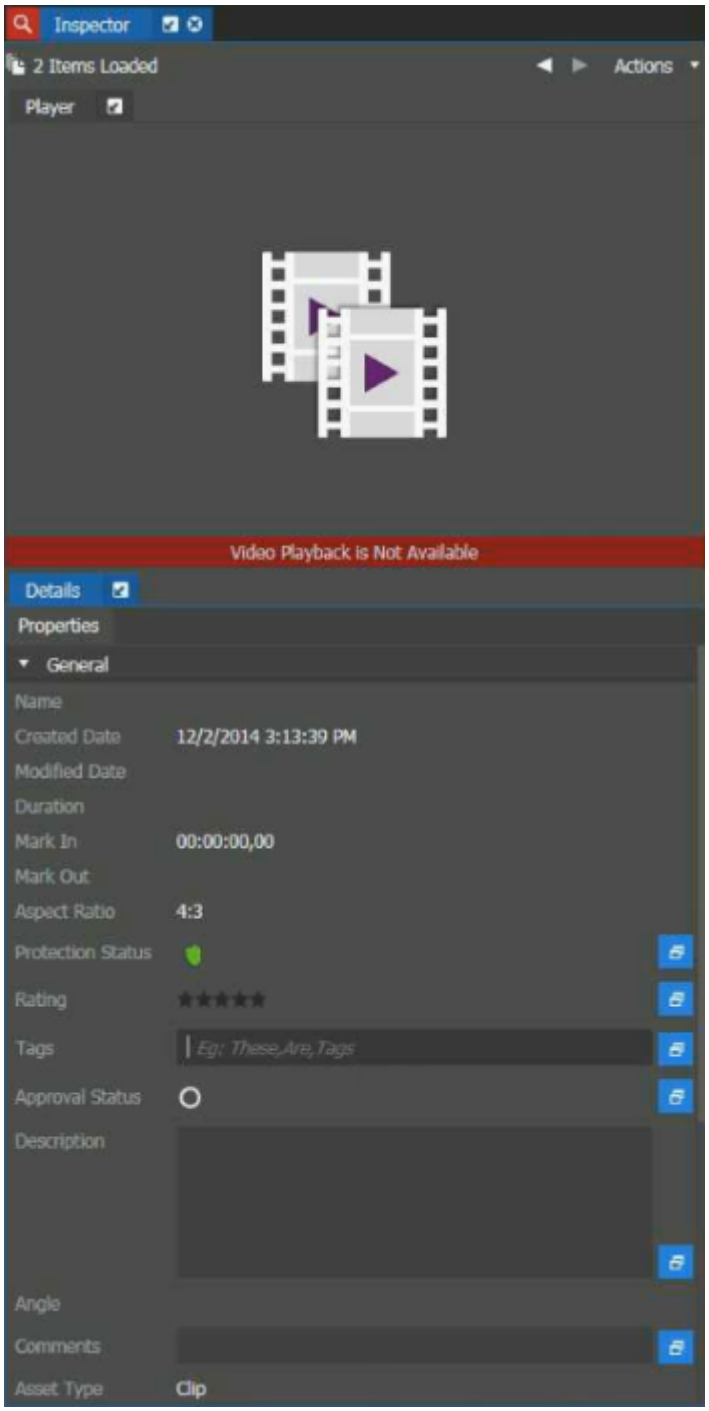
   The **Load Options** dialog appears.



2. Select **Load all angles** to view assets with multiple angles.
3. Select the **Do not ask again** checkbox to load all angles each time you view an asset with multiple angles, if desired.

   If the checkbox is not selected, the **Load Options** dialog displays each time you load an asset with multiple angles.

The asset displays in the Inspector panel.


Inspector
2 Items Loaded
Actions
Player
Video Playback is Not Available
Details
Properties
General
Name
Created Date
12/2/2014 3:13:39 PM
Modified Date
Duration
Mark In
00:00:00,00
Mark Out
Aspect Ratio
4:3
Protection Status
Rating
Tags
Eg: These,Are,Tags
Approval Status
Description
Angle
Comments
Asset Type
Clip

Toggling between camera angles in Inspector and Channel Panel

If a clip is a part of a K2 Dyno camera angle set or a GV STRATUS gang record set, in Inspector player and in Channel Panel player you can toggle between the associated clips in the set.

1. On the player, hover your mouse pointer on the top right of the asset.

   The **Camera Angle** selector overlay displays.

   NOTE: You can only toggle between angles for playback of ganged recorded assets or K2 Dyno camera angle assets.

2. Select the desired angle on the overlay display.

   The clip of the selected angle displays.

   You can also toggle camera angles of audio only assets. The player displays thumbnail of the audio only asset, and the **Camera Angle** selector overlay displays available angles that you can select.

Related Topics

Browsing camera angles on page 977

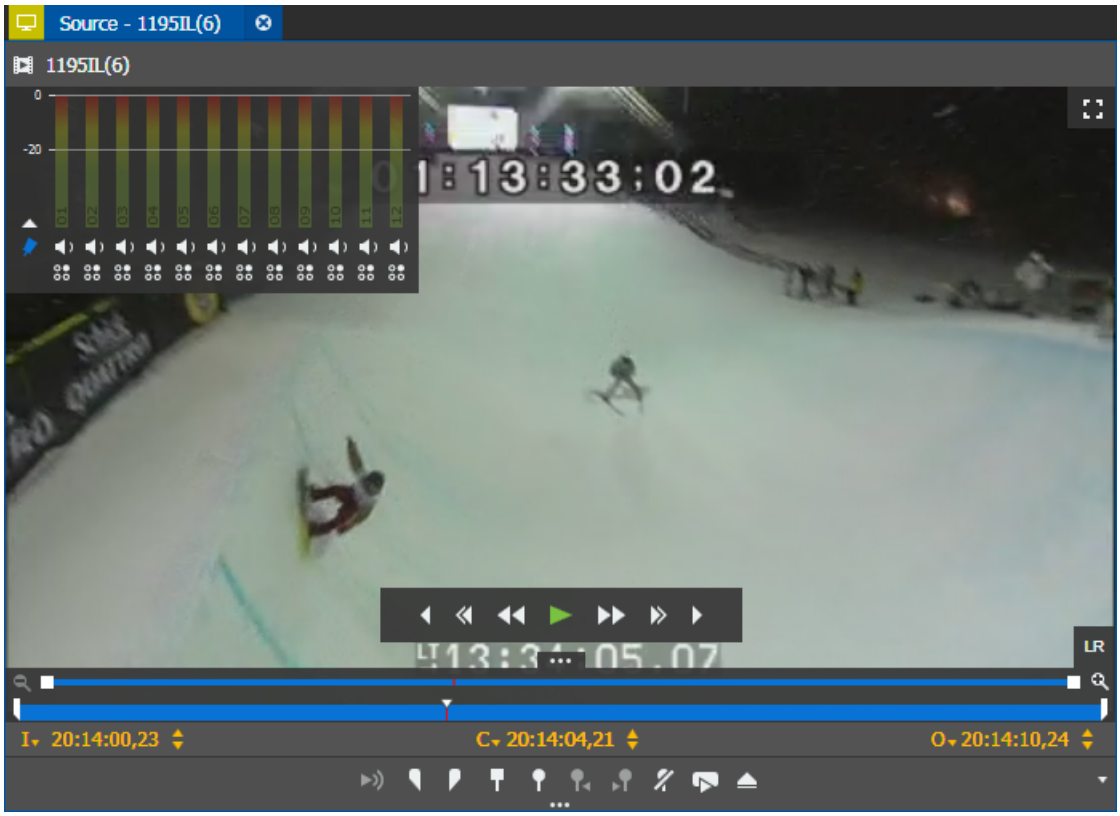
Using the Audio Overlay

The audio overlay is available on the Source Viewer, the Sequence Viewer, and the Inspector. The number of audio meter display depends on the number of audio tracks associated with the asset.

You can load and play assets up to 64 audio tracks if viewing a high-resolution clip, but only up to 32 audio tracks if viewing a low-resolution clip.

1. On the Source Viewer, the Sequence Viewer, or the Inspector player, hover your mouse pointer on the top left of the asset.

   The audio overlay of the asset displays. Each audio meter bar is labeled with the audio track number for easy reference.

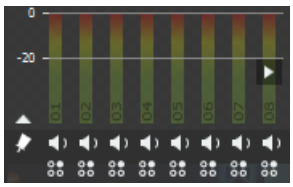


2. You can manage audio for the asset by clicking the appropriate button:

   - To mute specific audio channels, click the **Mute** button.
   - To isolate the selected audio channel while muting others, click the **Solo** button.

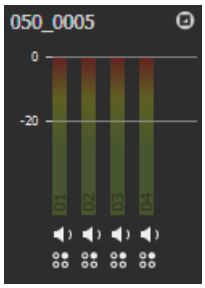
   Meters on muted channels will continue to display audio levels.

3. Click the **Pin Audio** button to pin the audio overlay and fix it in place.
4. Click the **Collapse Audio** button to show or hide meter bar display of audio channels.
5. Click the arrow button to go to the next page if there are multiple pages in the audio overlay.



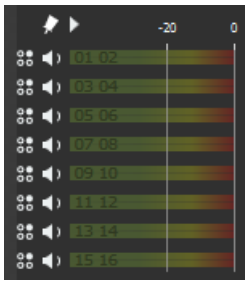
6. Drag the audio overlay off the viewer panel, if desired.

   The audio overlay is re-sizable and can be undocked. The clip name displays on the audio overlay if it is off the viewer panel.



7. To return the audio overlay to its original position on the viewer, click the **Redock** button.

The audio meter settings can be configured by selecting **Edit | User Preferences | Player**.



You can set the audio meter grouping to **Stereo** as shown above with 2 audio labels in combined channels. To toggle the audio meter display between **Mono** and **Stereo**, use these shortcut keys: **Shift + Alt + G**

You can also set the audio meter orientation to be stacked horizontally or vertically in User Preferences settings. The default is set to be stacked horizontally.

GV STRATUS supports the display of audio tags if already configured in the User Preferences settings. Audio tags can be selected from drop-down lists on the **Audio Tags** tab of the Inspector and automatically displayed on the audio meter.

Related Topics

Configuring Player User Preferences on page 1008

Adding or modifying audio tags of an asset

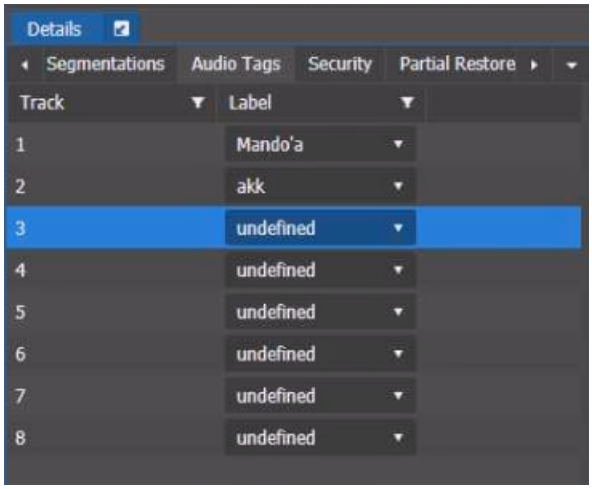
- The asset type is not a List.
- The asset status is not set as **Protected**.
- The asset is not associated to an archived asset.
- You must be assigned with either one of the following:
  - Media Manager role, or
  - Write permission for Audio Tags in **Core | Metadata | Permissions** in GV STRATUS Control Panel
- Ensure the **Meter Display** setting is configured to **Audio Tags (if present)** option in **Edit | User Preferences | Player** of the GV STRATUS application.

1. In the Asset List, double-click the asset.

   The asset loads in the Inspector panel.

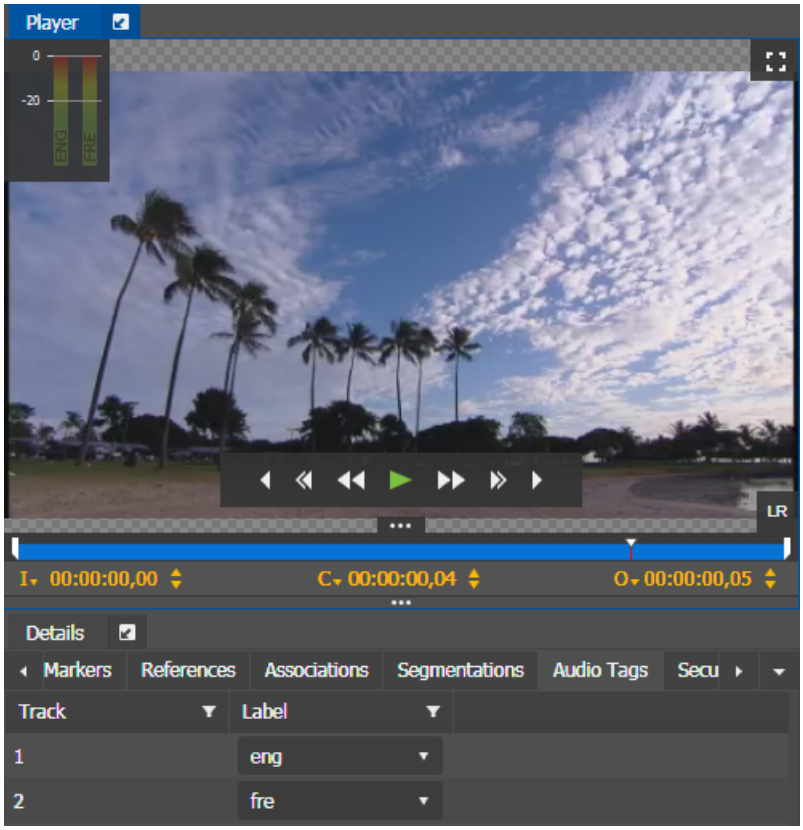
2. Select the **Audio Tags** tab.

   The Audio Tags tab displays.

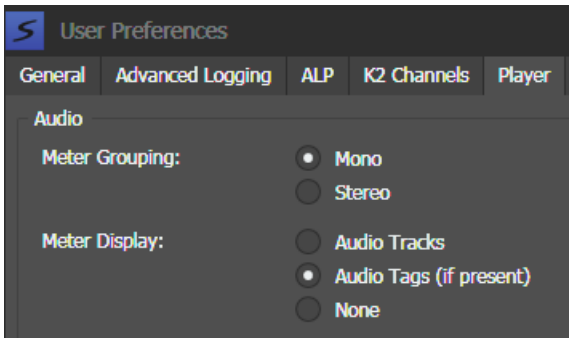


3. Select an audio track from the list.
4. Click the drop-down list under the **Label** column and select a tag for the audio track.
5. Repeat steps 3-4 to add or modify audio tags of other tracks in the asset.

Labels of audio tags display on audio meters of the Player as set in the **Audio Tags** tab.



If your Audio Tag labels are not displayed on the Player, go to **Edit | User Preferences | Player | Meter Display** and select **Audio Tags (if present)** option as shown below:



Related Topics

Audio Tag Management settings on page 354
Audio Tag Add/Modify settings on page 357

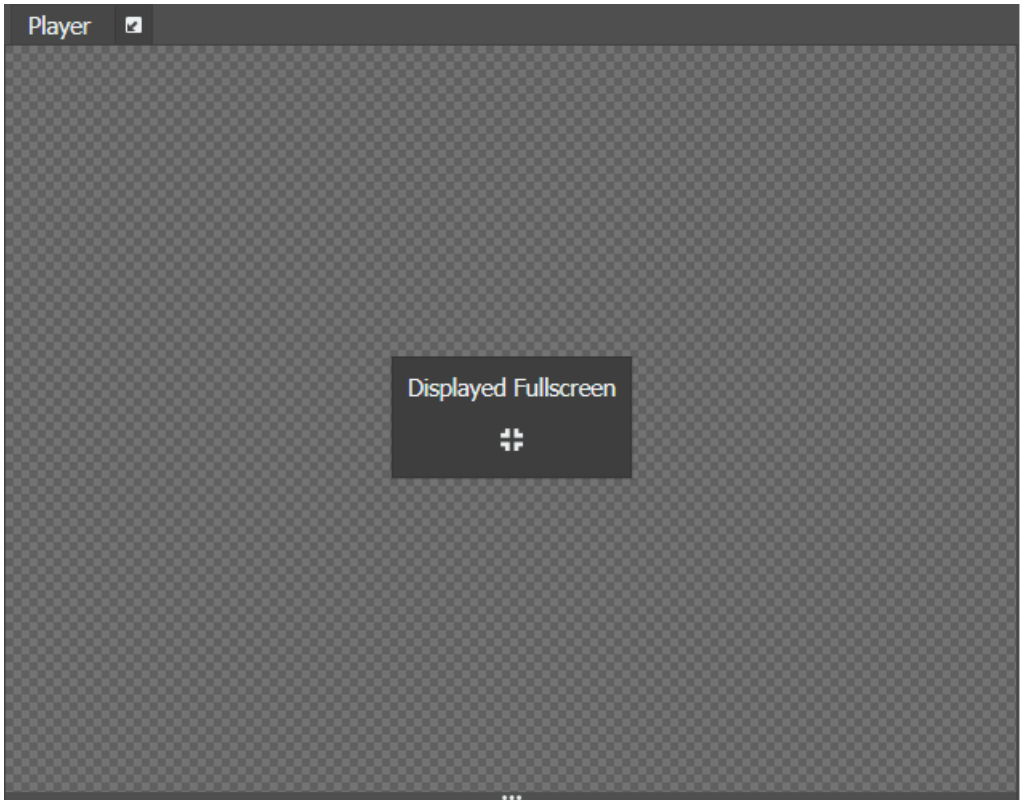
Sending video asset to the next display monitor

The video asset needs to be in full screen mode before you can enable the next display control.

1. Click the **Next Display** button on the upper right of the viewer.

   The video asset displays on the next display monitor.

   The viewer in GV STRATUS application shows the **Displayed Fullscreen** dialog.



2. To view the asset in both next display monitor and GV STRATUS viewer, load the same asset in the Inspector panel and click the **Full Screen** button.
3. To restore the playback from the next display monitor to the GV STRATUS viewer, click the **Restore** button.

Access to multiple GV STRATUS sites

You can access assets on remote GV STRATUS sites.

If you have remote sites configured in your system, the Navigator panel displays nodes for those sites. Only the **Assets** node is displayed under remote sites. Asset indicators identify assets on remote sites.

When you access multiple GV STRATUS sites, you do so from the context of your local site. Both local and remote GV STRATUS client PCs must be able to resolve the hostnames of local GV system servers, such as Core Server, Proxy Server, and K2 system. This local site is your primary site, where you do your normal workflow tasks, such as ingesting, editing, and playing out on channels. When you access a remote site, you can search and browse the remote assets, but you cannot edit or do other operations on remote assets. You must transfer the remote asset to your local site in order to apply the full range of GV STRATUS operations to the asset. Asset transfers are allowed both ways between your local and remote sites.

The GV STRATUS system uses progressive download to display low-resolution proxy video of assets from remote sites. This minimizes the effect of a slower load time when you load an asset into Inspector or some other GV STRATUS viewer. Progressive download selectively downloads and caches the portion of the low-resolution proxy video asset just before and after the current scrub bar position in the video player, until finally the entire proxy file asset is downloaded. As long as the GV STRATUS application remains open, the downloaded proxy asset remains locally available. If you load the proxy asset into the video player again, the GV STRATUS application uses the locally cached proxy file asset. In the GV STRATUS viewer, a spinning progress indicator displays caching and shaded indicators on the scrub bar display the portion of the proxy asset cached. You can also edit Player User Preferences to control when progressive download occurs.

Related Topics

Asset indicators on page 977

Configuring Player User Preferences

You can configure the audio meter display in the Player User Preferences setting.

When remote assets are slow to open in a GV STRATUS video player, you can configure how the GV STRATUS application handles the download to the video player.

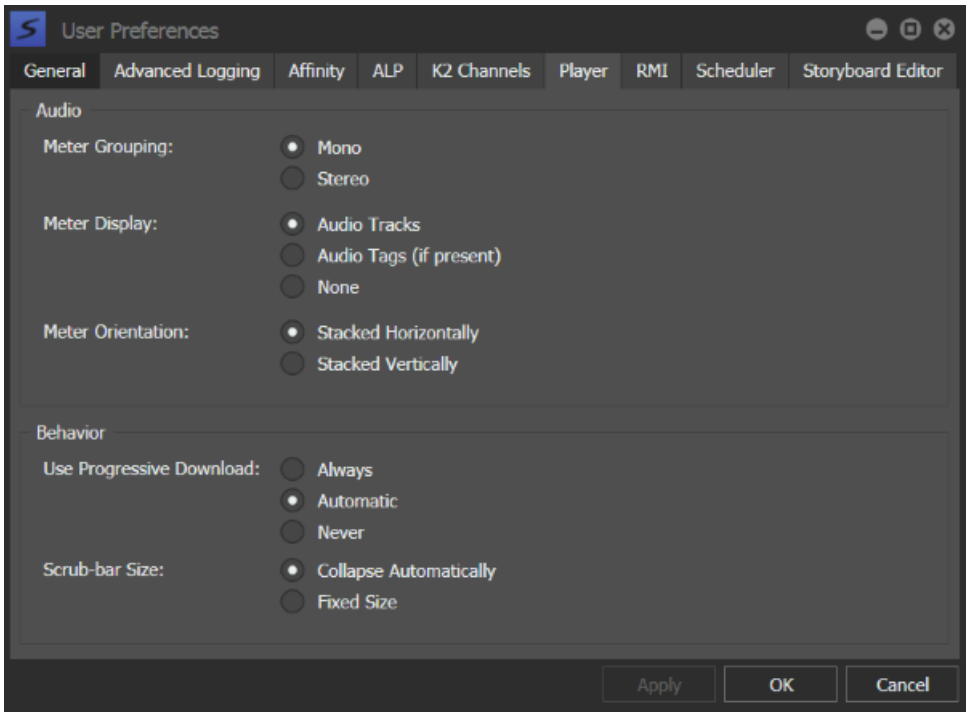
Scrub bar and scrub bar zoom position in the Inspector and other viewers can also be configured on this tab.

1. Select **Edit | User Preferences**.

   The User Preferences dialog box opens.

   The GV STRATUS application shows or hides sections based on the roles assigned to your GV STRATUS log on credentials.

2. Select the **Player** tab.



3. Select from the following Audio options:

- **Meter Grouping**: For audio meter grouping setting, select one from below.
  - **Mono**: Audio Overlay displays Mono audio tracks, with 1 channel per audio bar. This is the default setting.
  - **Stereo**: Audio Overlay displays Stereo audio tracks, with 2 channels combined per audio bar.
- **Meter Display**: For the audio meter label display, select one from below.
  - **Audio Tracks**: Displays track number on the audio bar, which is the default setting.
  - **Audio Tags**: Displays audio tags on the audio bar. You can configure audio tags for audio channels on the K2 AppCenter configuration manager, as per asset basis.
  - **None**: No audio label display if this option is selected.
- **Meter Orientation**: For the audio meter orientation display, select one from below.
  - **Stacked Horizontally**: Audio Overlay displays audio meter stacked horizontally, which is the default setting.
  - **Stacked Vertically**: Audio Overlay displays audio meter stacked vertically.

4. Select one of the following progressive download options:

   - **Always**: If you only access remote GV STRATUS sites, select this option. The GV STRATUS application uses progressive download for all assets on all sites.
   - **Automatic**: If you access both local and remote sites, or if your network access is sometimes slow, select this option. If a remote site, the GV STRATUS application uses progressive download. If a local site, the GV STRATUS application tests each asset's download speed and if slow, the application tries to download it three times. If the speed is still slow, the GV STRATUS application switches to progressive download for all assets from all sites. The GV STRATUS application continues to use progressive download until it is restarted.
   - **Never**: If you never access remote sites and you do not want to use progressive download, select this option. The GV STRATUS application does not test an asset's download speed. If an asset's download speed is too slow, performance of other GV STRATUS operations can be affected.

   Progressive download selectively downloads and caches the portion of the low-resolution proxy video asset just before and after the current scrub bar position in the video player, until finally the entire proxy file asset is downloaded. As long as the GV STRATUS application remains open, the downloaded proxy asset remains locally available. If you load the proxy asset into the video player again, the GV STRATUS application uses the locally cached proxy file asset.

5. Select one of the following scrub-bar size options:

   - **Collapse Automatically**: The scrub bar and scrub bar zoom collapse automatically when the viewer is left idle, which is the default setting.
   - **Fixed Size**: If selected, the scrub bar and scrub bar zoom remain fixed on the viewer always.

6. To apply a change and continue editing user preferences settings, click **Apply**.
7. To accept any changes and close the dialog box, click **OK**.

   The dialog box closes.

Changing the thumbnail of an asset

If you are assigned with the **Change Thumbnail Rights** role, you can change the thumbnail of an asset.

1. Load the asset into the Inspector to view the asset.
2. In the asset, identify the image to use as the new thumbnail.
3. Then do one of the following:

   - Click the **Actions** menu on the Inspector, and select **Set Asset Thumbnail**.
   - Right-click on the asset and select **Set Asset Thumbnail**.
   - Press these shortcut keys: **Ctrl + B**

The new thumbnail replaces the previous thumbnail on the Asset List.

Importing image file as thumbnail of an asset

- You must be assigned with **Change Thumbnail Rights** role to change the thumbnail of an asset.
- The image file must not exceed 128KB in size.

- Image file formats such as JPG, PNG, TIF, and GIF are supported.

You can import an external image and set it as the thumbnail of an asset.

1. Select an asset in the Asset List.
2. Right-click on the asset and select **Upload Thumbnail**.

   The **Select Thumbnail File** dialog opens.
3. Browse and select an image to import as the new thumbnail.
4. Click **Open**.

The new thumbnail replaces the previous thumbnail of the asset.

Adding or modifying metadata

1. To add or modify metadata in the Inspector panel, do the following:
   a) Open an asset in the Inspector panel.

b) On the Properties tab, click the **Show/Hide** button of the **General** or **Other** (if displayed) section to display metadata.
c) Add star ratings, tags, descriptions, comments and other information.

Tags are comma delimited, so you can enter multiple tags.

d) To add a keyword, click the **Add Keyword** button. ( )
e) To add a marker, click the **Add Marker** button. (**Insert**)

2. To add or modify metadata in an Asset List, do the following:
a) Display assets in an Asset List.
b) View the Asset List in the Details view.
c) Display the desired columns.
d) Use **ALT + Click** to modify text.

Related Topics

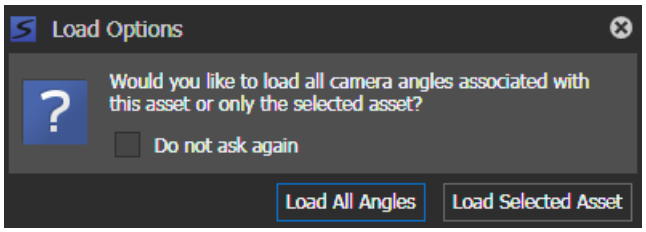
Limitations for creating and naming assets and bins on page 1428

Adding metadata to assets with angles

The following only applies to assets associated with multiple angles.

1. Drag the asset from the Asset List into the Inspector panel.

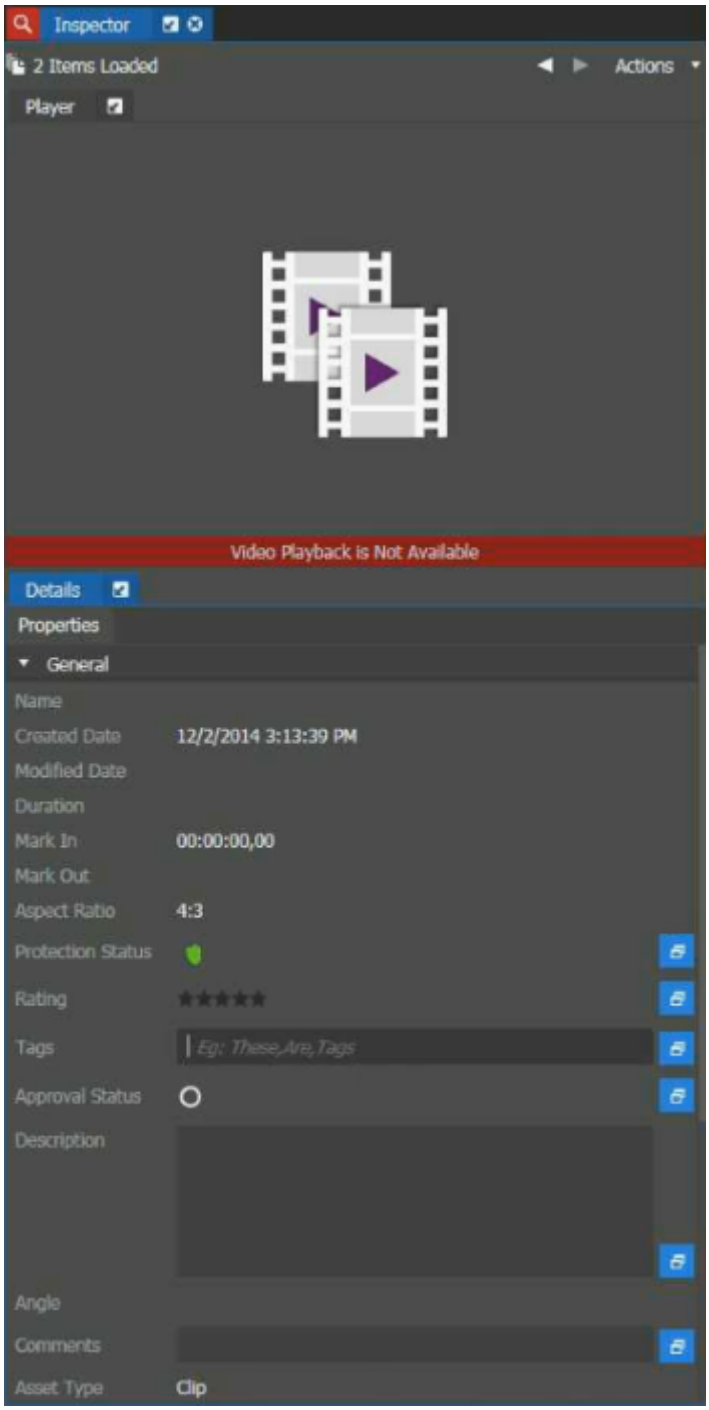
The **Load Options** dialog appears.



2. Select **Load all angles** to load all assets with associated angles.

   Select the **Do not ask again** checkbox to load all angles each time you view an asset with multiple angles, if desired.

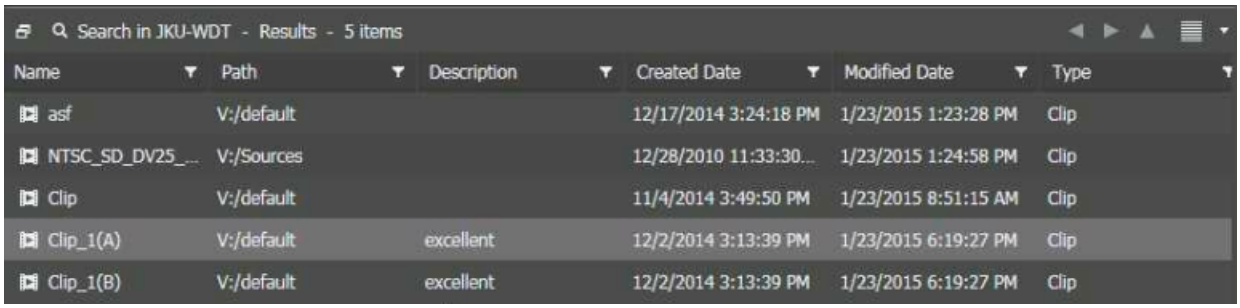
   Assets load into the Inspector panel.



3. Add or modify asset metadata such as tags, description, or comments in the **General** section of the Inspector panel.

   The metadata is applicable to all loaded assets with multiple angles.

   If you added a description in the Inspector panel, the same description appears for all associated assets in the Asset List.



4. To only add metadata to a specific asset, click the **Property Options** button next to a specific field in the Inspector panel.

   The **Property Options** button is deselected, and the button color changes from blue to gray.

   The newly added metadata is not applicable to all associated assets.

5. Click the **Property Options** button again if you want the metadata to be applicable to those assets with multiple angles.

Copying asset metadata

- If GV STRATUS security is enforced, your credentials must give you full permissions on bins, assets, and metadata.
- You must be assigned with the **Copy Metadata** role in GV STRATUS Control Panel.

1. Select an asset that you want to copy on the Asset List.
2. Do one of the following:
   - Press **Ctrl + C** keys
   - Right-click and select **Copy**
3. Select another asset on the Asset List to paste the metadata into.
4. Right-click on the asset and select **Paste Metadata**.

Metadata, markers, segments, and segmentations from the copied asset now display in the destination asset.

NOTE: Markers, segments, and segmentations are copied only if their marks are contained within the Mark In/Out values of the destination asset(s).

Copied metadata includes:

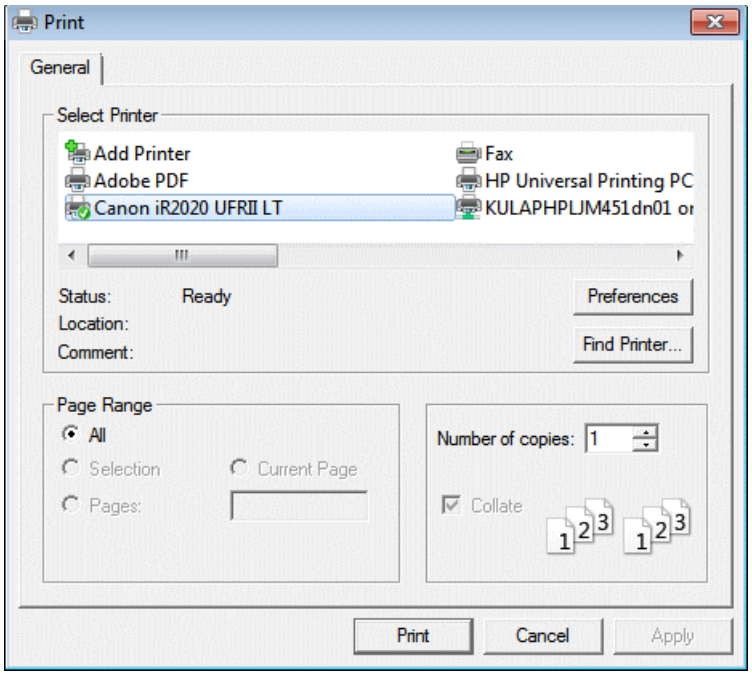
- Rating

- Description
- Extended Comments
- Linked House Number
- Keywords
- Locked status
- Metadata Expiry Date
- Custom Metadata

Printing asset metadata

1. Right-click on an asset in the Asset List and select **Print**. (**Ctrl + P**)

   The Print dialog appears.



2. Select your printer and click **Print**.

   Asset metadata prints on the selected printer in the same order of appearance as in the Inspector.

   NOTE: Custom metadata with Text-Unlimited fields are not included in the printout.

Using custom metadata in Inspector

You can use custom metadata fields, as configured in GV STRATUS Control Panel, to support your workflow.

1. From the Inspector panel, do the following to use custom metadata:
   a) Open an asset in the Inspector panel.
   b) On the Properties tab, click the **Show/Hide** button of the **General** section.
   c) View or modify your custom metadata as desired.

When the selected custom metadata type is unlimited text, the large metadata is not loaded with the asset in Inspector panel. Click the **Click to View** link to display metadata. You can also right-click on the metadata display and select **Expand for Editing** to edit the metadata in a larger window.

NOTE: For Number field types, the example value displays in gray to easily distinguish numbers only metadata in the* Inspector *panel.

2. From an Asset list, do the following to use custom metadata:
   a) Right-click to select **Columns** and add the column or columns to the Asset List that correspond to your custom metadata.
   b) Use **ALT + Click** to modify text, numbers and dates.

Related Topics

Adding and removing columns in a list on page 982
Custom Metadata Add/Modify Field settings on page 319

Viewing relationships

You can view lists of related assets, based on the type of relationship.

In the Asset List identify the asset whose relationships you want to view and do one of the following:

- Open the asset in the Inspector panel and select a tab from several relationship tabs.
- Right-click the asset and select **View Related**. A menu of relationship types is displayed. Select a relationship type. Relationships are displayed in the Asset List.

Viewing the properties of an item

You can view the properties of an item in several locations in the application.

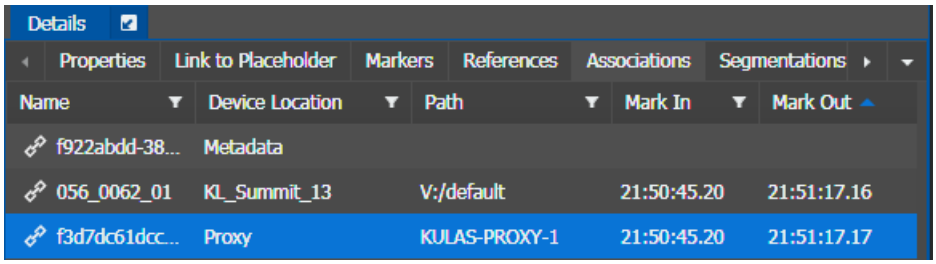
- To view basic asset properties as a tooltip, hover the mouse pointer over an item in the Asset List panel.
- To view more asset properties, open the asset in the Inspector panel and view the General section.
- To view properties of a playlist or sequence event, right-click on the event in the Editor Panel and select **Properties**, or drag the event to the Inspector panel.

  The event's properties display in the Inspector panel.
- To modify the display of properties in Tiles view, right-click on the Asset List panel, select **Tile Properties**, and reorder the top three items as desired.
- To view the properties associated with a keyword or marker, hover the mouse pointer over the symbol associated with that keyword or marker.

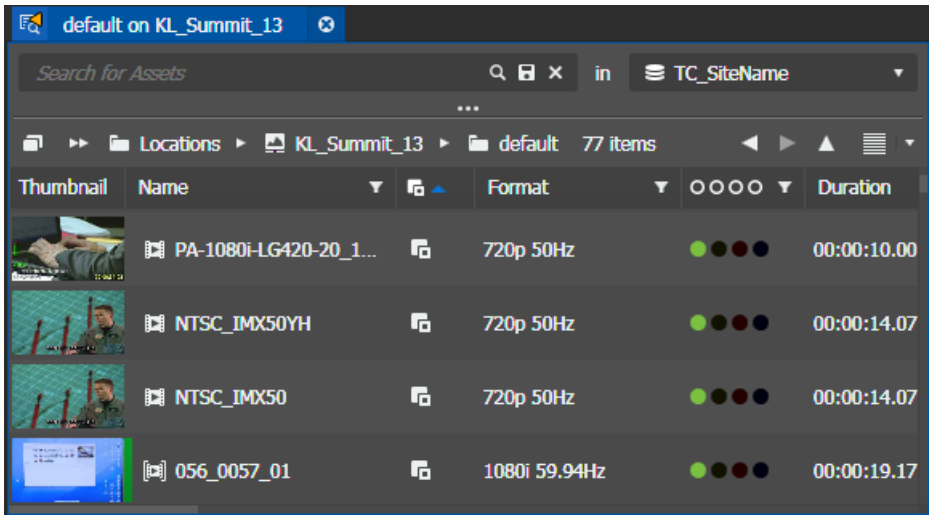
  The thumbnail and properties associated with the keyword or marker appear as an overlay tooltip.

Verifying proxy association

1. To verify the proxy association of a single asset using the Inspector panel, do the following:
   a) In the GV STRATUS application Asset List, double-click an asset.
      The asset is displayed in the Inspector.
   b) In the Details panel of the Inspector, click the **Associations** tab.
   c) Verify that there is a row that reports **Proxy** in the **Device Location** column.



2. To verify the proxy association of multiple assets in an Asset List, do the following:
   a) Add the **Has Proxy** column to the Asset List, if it is not already added.
   b) Identify assets with the the **Proxy** asset type icon in the column.
   c) Sort the list on the **Has Proxy** column.



Related Topics

Regenerating proxy on page 1022
Adding and removing columns in a list on page 982
Sorting a list view on page 981

Regenerating proxy

If configured in GV STRATUS Control Panel Proxy Config settings, a Render Engine automatically generates low-resolution proxy for a high-resolution asset. You can also manually regenerate the proxy for an asset.

You cannot generate proxy for a growing clip. You must allow the recording of the high-resolution asset to complete before generating proxy.

1. If the asset is currently loaded in the Inspector panel, eject it before generating proxy for it.
2. In the GV STRATUS application Asset List, right-click the asset and select **Regenerate Proxy**.

The Render Engine creates the proxy asset.

In the **Associations** tab of the Inspector, the proxy association shows as recording until the proxy has been successfully regenerated.

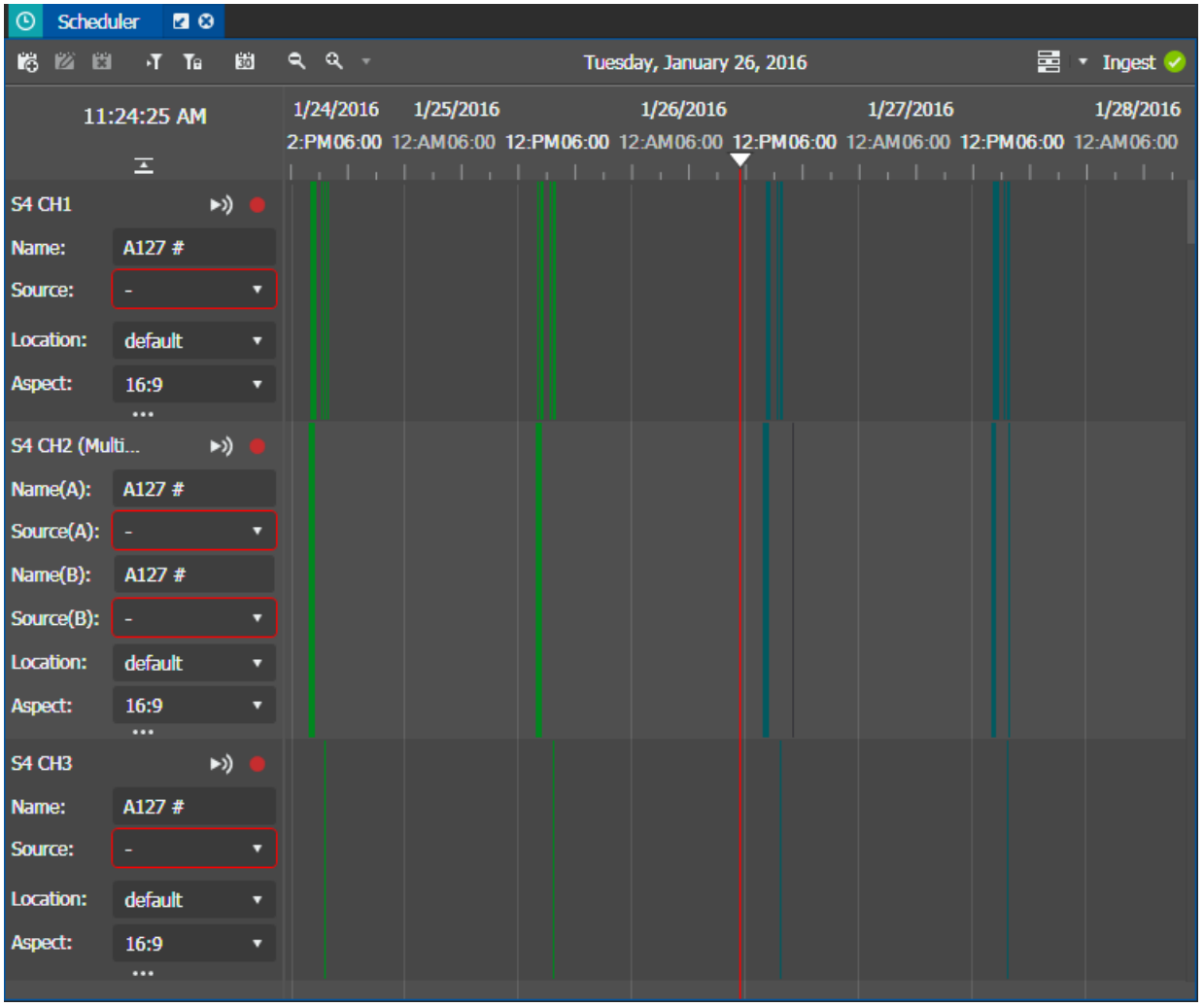
Related Topics

Verifying proxy association on page 1021

Ingesting assets

The Scheduler tool

The Scheduler tool allows you to view configured channels and schedule events to be recorded for later use. The Scheduler tool appears in the application as a panel that can be accessed from the Window menu or the tools section of the Navigator panel. In the Navigator panel, the parent Scheduler tool contains all displayed channels. Channel groups under the parent Scheduler tool contain a sub-set of channels, as configured in GV STRATUS Control Panel.



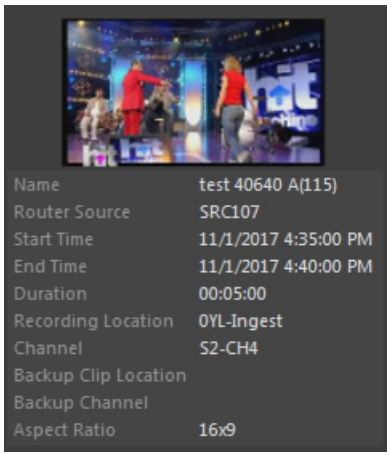
The Scheduler tool features are as follows:

- Clock — Shows current time according to the system time of the Ingest Service server. If the client PC time is in a different timezone than the server, the server time is converted to the client PC timezone.
- Timeline — Shows dates and hours to guide event scheduling.
- Available channels — Shows channels that are configured to record events.
- Scheduler toolbar — Consists of buttons for scheduling and viewing events.
- Current time indicator — Moves along the timeline according to the current time.
- Scheduled events — Shows events that have been added to the Scheduler tool.
- Ingest Service status indicator — Shows the connection status between Ingest core service and the Scheduler tool.
    - — Connected
    - — Disconnected

With the tool, you can schedule events to record in advance, by specifying the date, time, and duration of the recording. You can also choose whether to schedule a single event, main and backup events, recurring events, open ended events, or crash record an event.

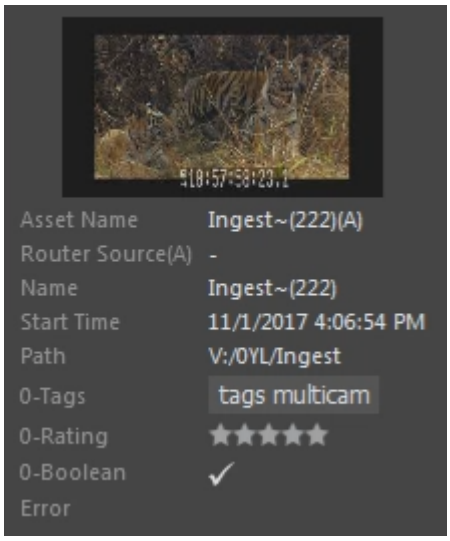
By default, the Scheduler tool opens to the current day, date, and time according to your system time.

If you hover on an event on the Scheduler tool, a tooltip appears to show the event name, video thumbnail, router source, recording location, channel, time information, duration of the event, and error description if available.



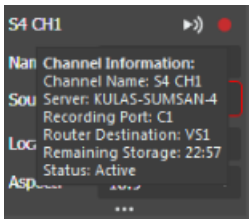
You can also configure specific properties to display on the tooltip via the Timeline Information settings in GV STRATUS Control Panel. However, this is only supported for the Track View mode of the Scheduler. The order of property display on the tooltip is according to the order of configured properties in the Timeline Information settings. If configured with full permissions, you can include custom metadata display on the tooltip.

NOTE: It may take several seconds for the tooltip to load asset information as configured in Timeline Information settings. The tooltip loads event properties initially, and loads asset properties automatically after.



NOTE: Scheduler supports the display up to 8 fields of properties for single camera recordings, and 6 fields of properties for Multicam recordings.

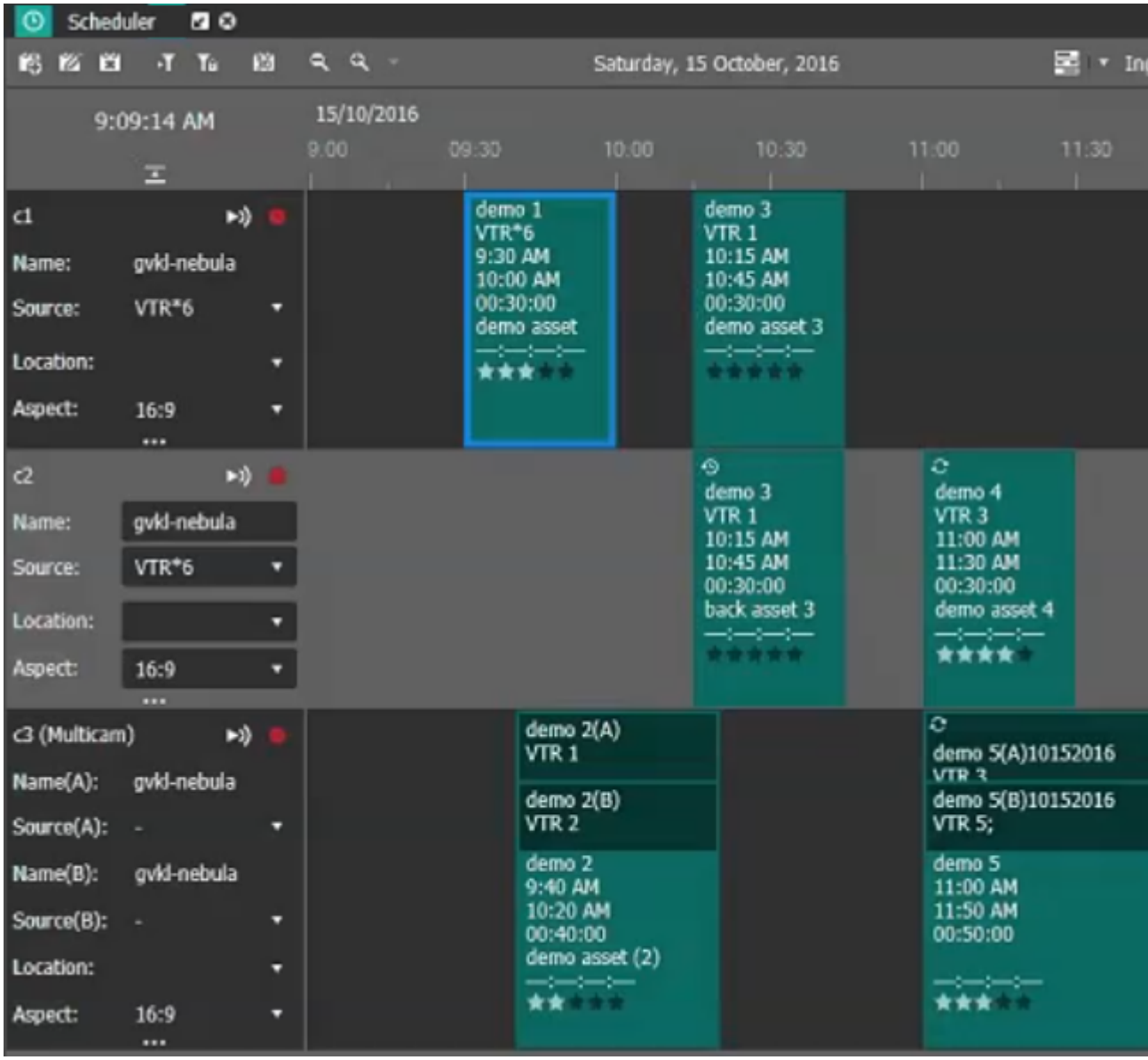
If you hover on a channel, a tooltip appears to show the channel name, server name, recording port, router destination, remaining storage and status of the channel. When the channel is down, the font color of the channel name changes from white to orange.



You can also configure a Multicam channel that can record two incoming video feeds in the Scheduler tool. An event recorded via the Multicam channel creates two assets, nominally referred to as _(A) and _(B). Since those assets are created together, the record and stop commands to the channel affect both assets simultaneously.

NOTE: Recording will not proceed if there is insufficient storage on the* K2 system*. The recording button is disabled when remaining storage is less than the default crash duration as set in the GV STRATUS Control Panel application.

If desired, you can configure specific properties on event display for the Track View timeline of Scheduler tool. The configuration can be done on the Timeline Information tab of Ingest settings in GV STRATUS Control Panel



If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets, and metadata that do not have read permissions are not visible. Markers and segments permissions must be set to **Allow** in order to create, update, or delete markers and segments.

Related Topics

Timeline Information settings on page 388

Setting up control for Scheduler channels in the K2 AppCenter on page 385

Scheduler buttons

These buttons located on the Scheduler toolbar let you perform various functions.

Add Event: Adds a scheduled event.

Modify Event: Modifies the selected event.

Delete Event: Deletes the selected event.

Go to Current: Goes to the current time of day in the timeline.

Toggle Timelock: Goes to the current time of the day in the timeline and turns on the timelock mode.

Go to Date: Goes to the current day in a calendar.

Zoom In: Zooms in the view of the timeline. The slider between **Zoom In** and **Zoom Out** also zooms the view of the timeline.

Zoom Out: Zooms out the view of the timeline. The slider between **Zoom In** and **Zoom Out** also zooms the view of the timeline.

Record details toggle: Toggles display of the record details for all channels.

View Mode: Controls the display and size of the items in a list or panel.

These buttons located on each channel window in the Scheduler let you record an event immediately.

Record: Starts recording. Toggles with Stop button.

Stop: Stops recording. Toggles with Record button.

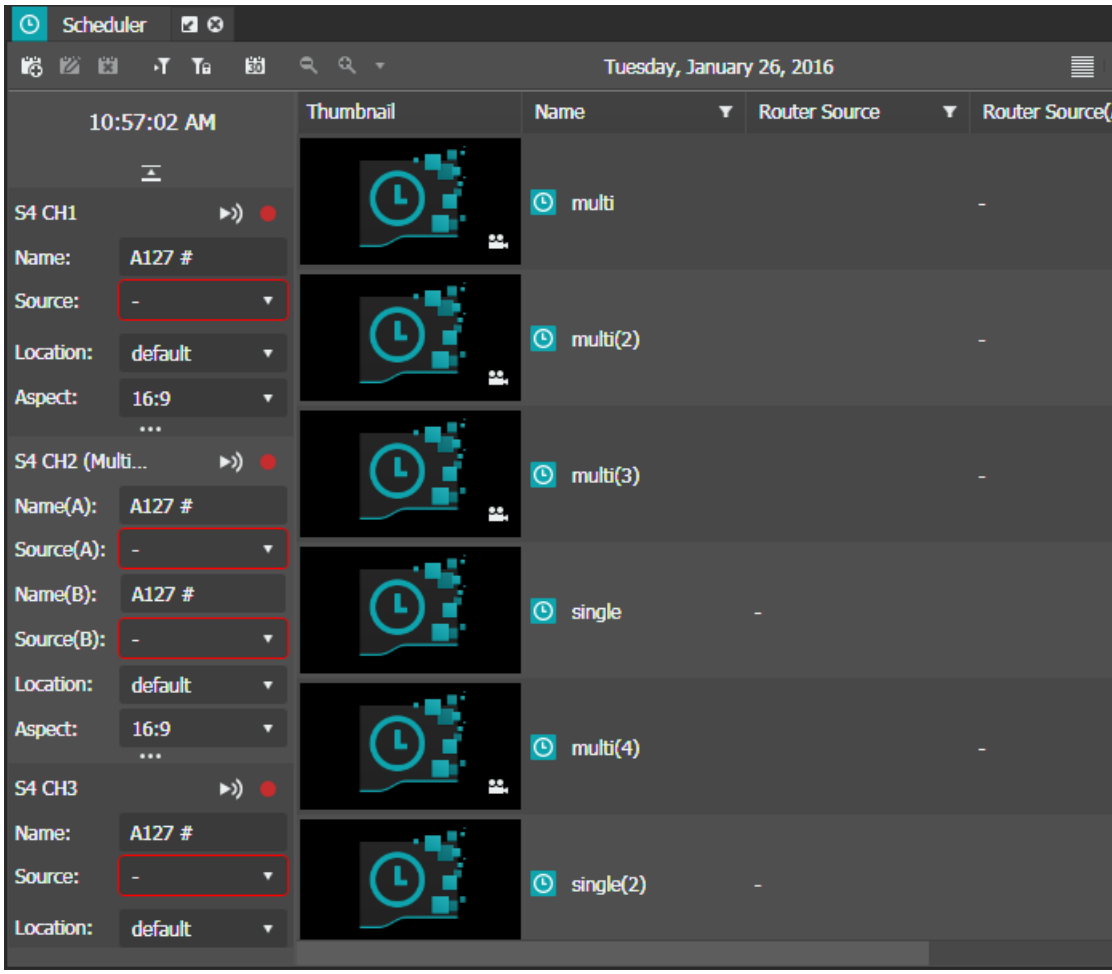
Expand: Shows/hides settings and lists.

Live Streaming Video: Enables/disables the display of the live video stream.

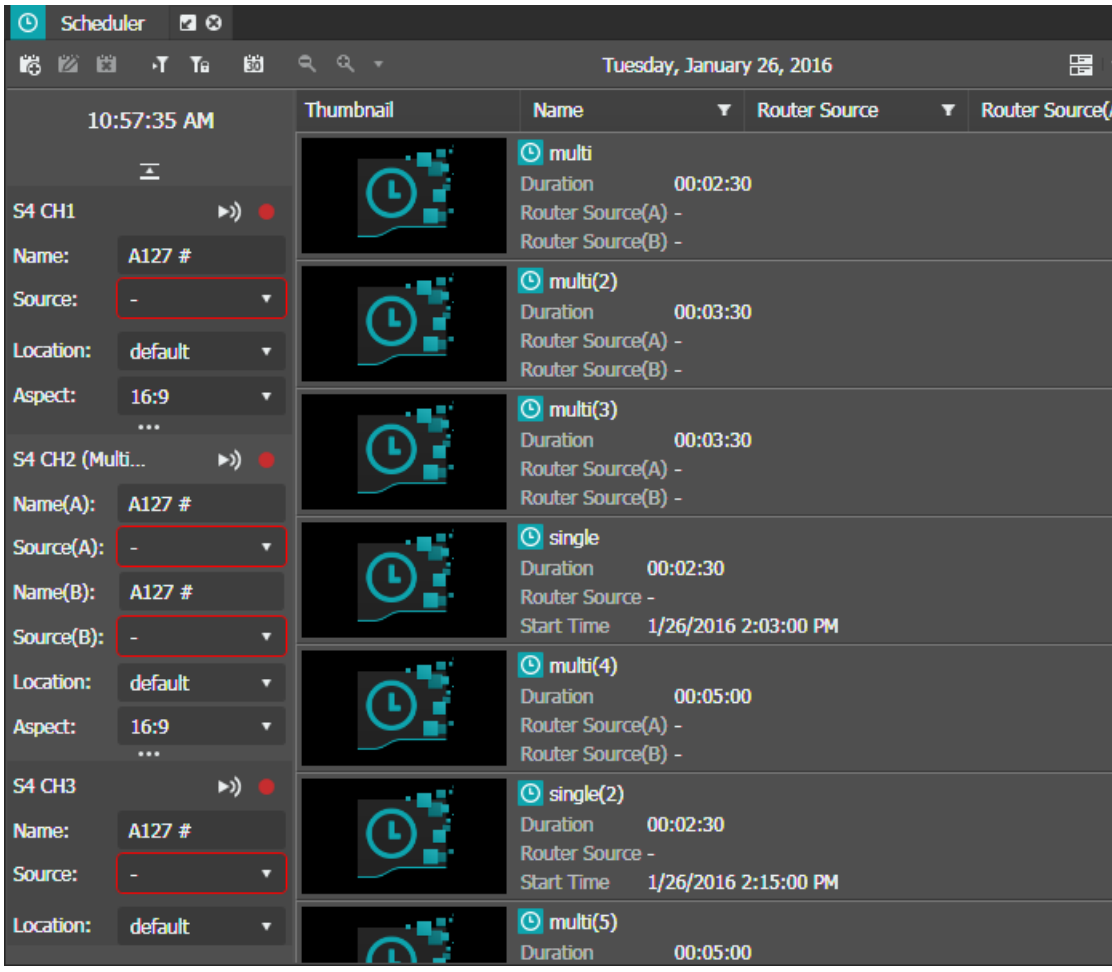
About view modes

You can customize event display in the Scheduler tool. There are 6 types of view modes that can be selected as follows:

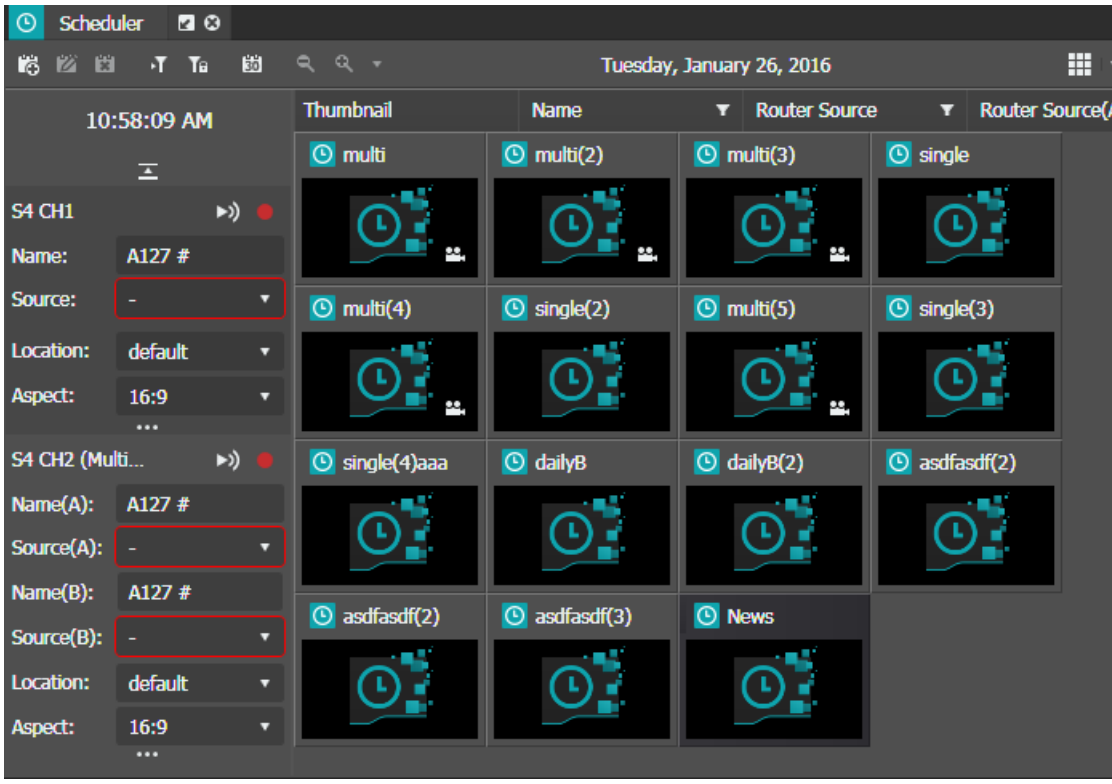
Details view



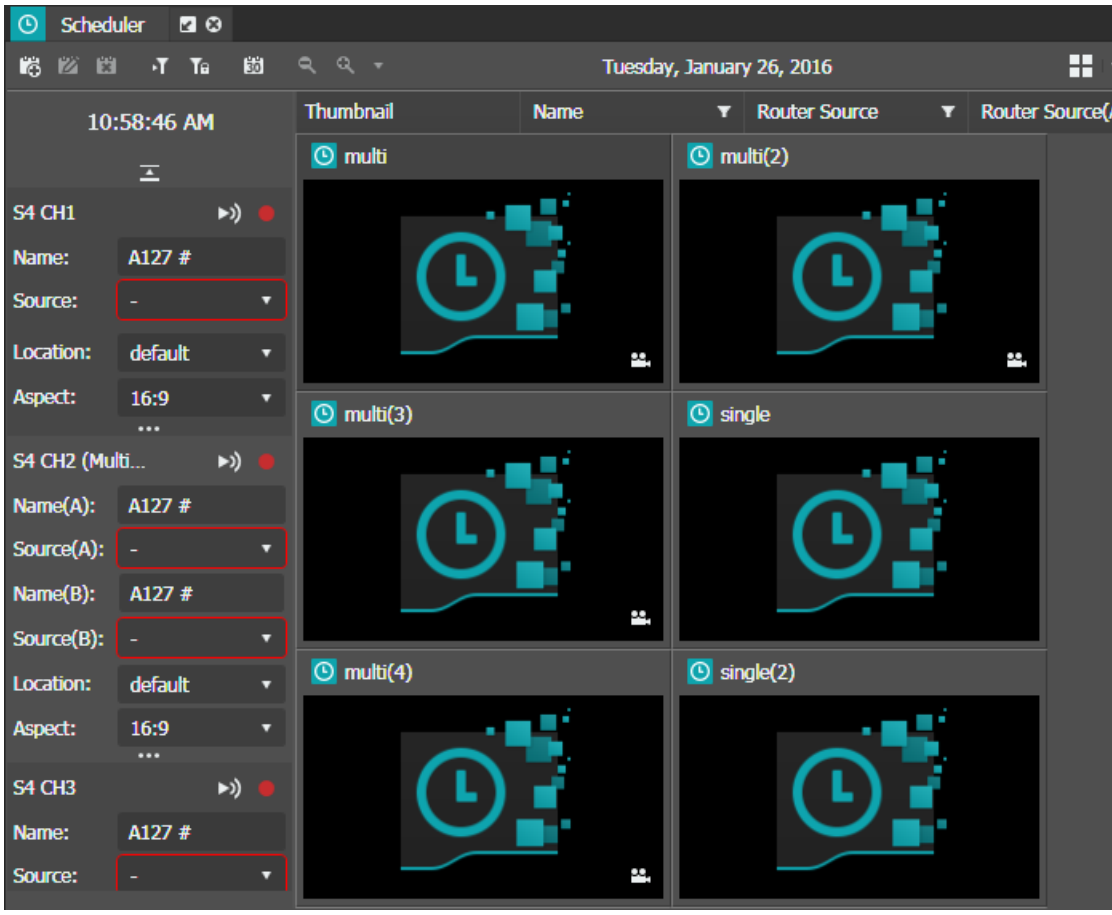
Tiles view


Scheduler
Tuesday, January 26, 2016
10:57:35 AM
S4 CH1
Name: A127 #
Source: -
Location: default
Aspect: 16:9
S4 CH2 (Multi...
Name(A): A127 #
Source(A): -
Name(B): A127 #
Source(B): -
Location: default
Aspect: 16:9
S4 CH3
Name: A127 #
Source: -
Location: default
Thumbnail
Name
Router Source
multi
Duration 00:02:30
Router Source(A) -
Router Source(B) -
multi(2)
Duration 00:03:30
Router Source(A) -
Router Source(B) -
multi(3)
Duration 00:03:30
Router Source(A) -
Router Source(B) -
single
Duration 00:02:30
Router Source -
Start Time 1/26/2016 2:03:00 PM
multi(4)
Duration 00:05:00
Router Source(A) -
Router Source(B) -
single(2)
Duration 00:02:30
Router Source -
Start Time 1/26/2016 2:15:00 PM
multi(5)
Duration 00:05:00

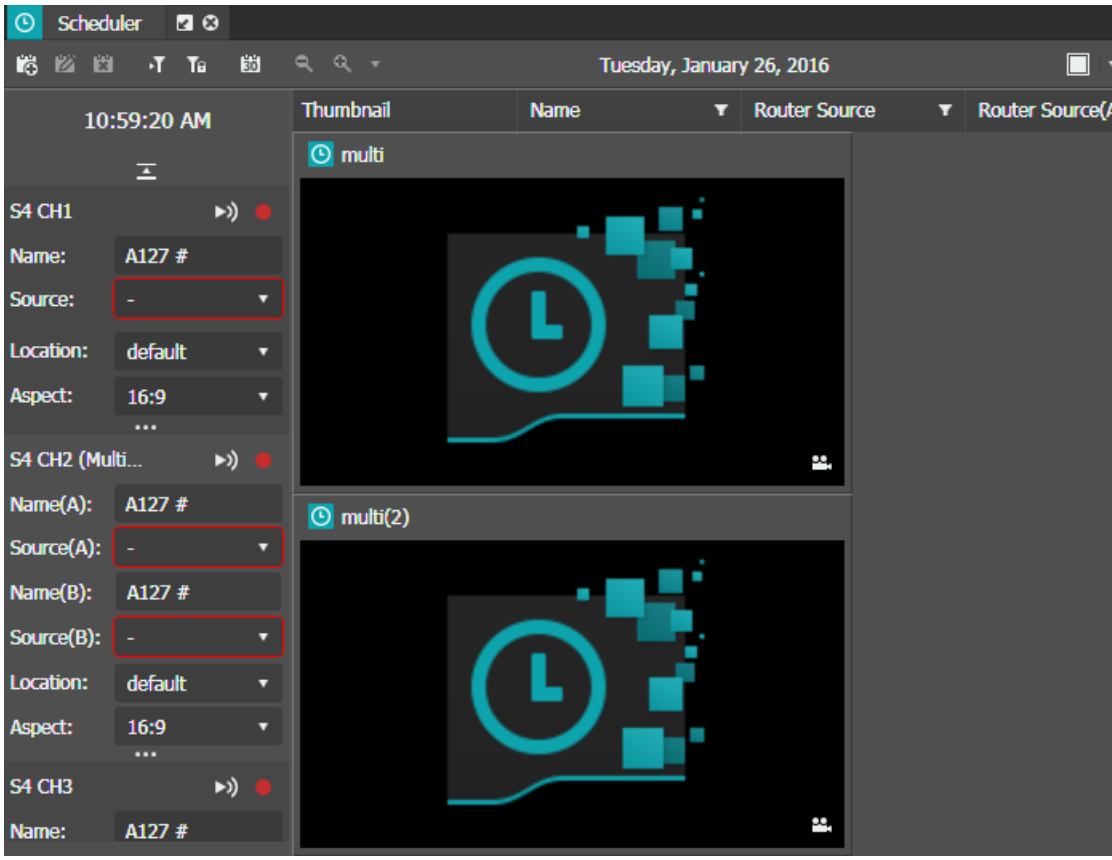
Small Thumbnails view



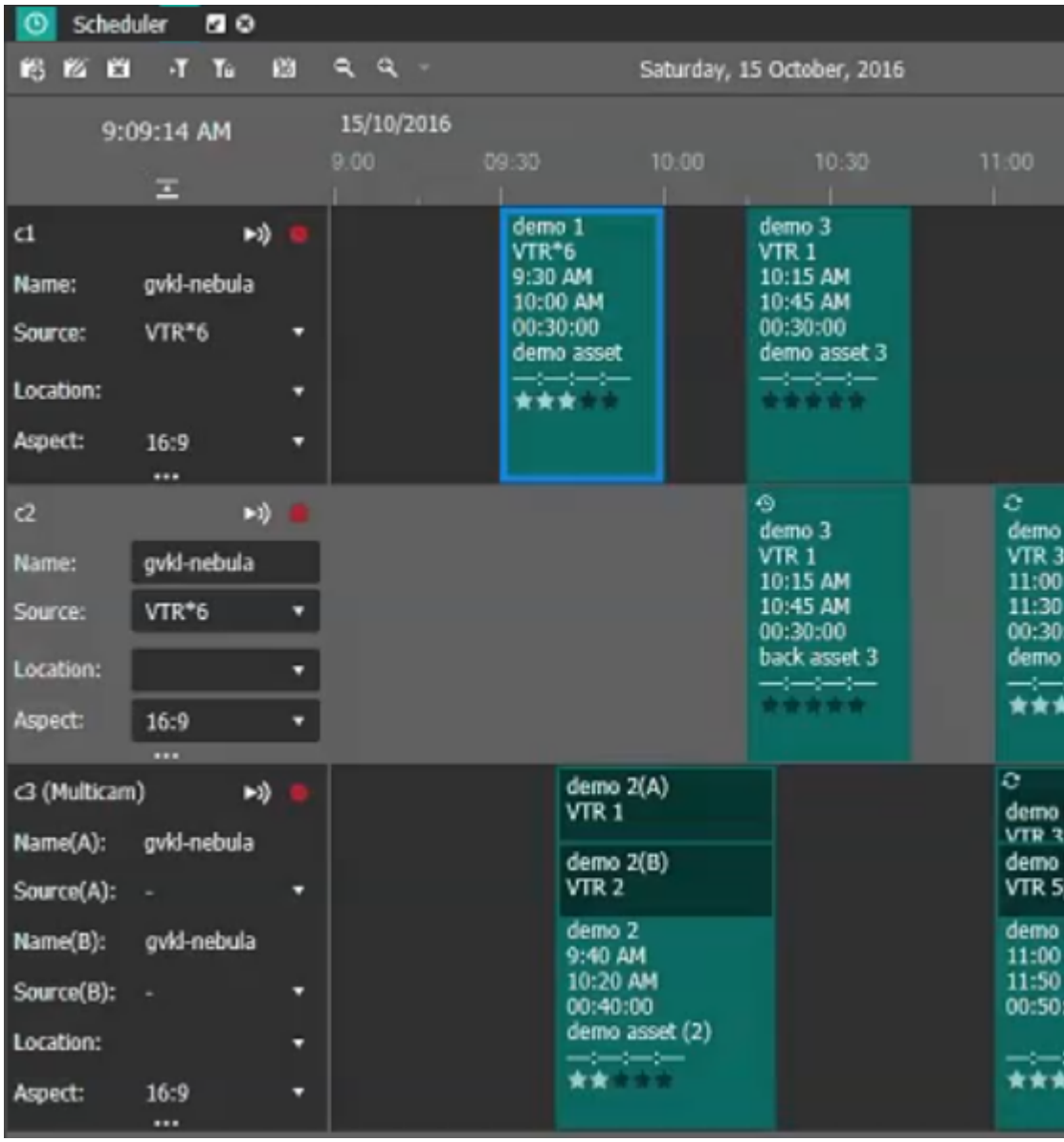
Medium Thumbnails view



Large Thumbnails view



Track view



You can configure event properties to be displayed on the Track View timeline. The configuration can be done on the Timeline Information tab of Ingest settings in GV STRATUS Control Panel

Related Topics

Customizing the display of list items on page 981

Event status colors

Each event displays in a color that identifies its status in the Scheduler.

Event Color	Event Status
Blue	READY

Event Color	Event Status
Black	RESERVED CHANNEL FOR SPECIFIC RECORDING
Yellow	CUEING
Orange	CUED
Red	RECORDING
Green	RECORDED SUCCESSFULLY
Purple	ERROR IN RECORDING

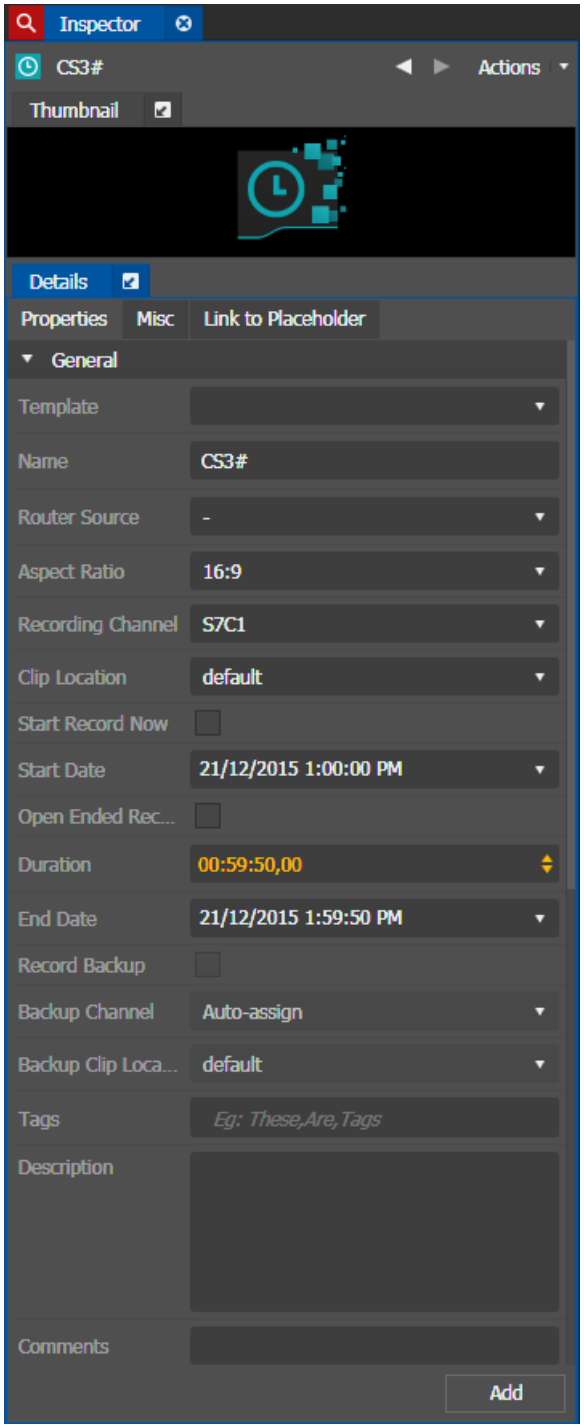
Adding an event

- If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, and metadata.
- In order to link to a placeholder, you must be assigned with write permission for the **Name** property in Metadata section of GV STRATUS Control Panel.
- If quota is configured on the K2 system bin, ensure you have enough disk space before recording assets.

- It is recommended to set the quota on a destination bin to at least 2GB. Records will not begin if there is less than 1GB of free space remaining in the destination bin.

To ingest feeds, add an event in the Scheduler tool for each feed that you want to record.

1. Click the **Add Event** button. (A)
   The Inspector panel loads event properties.



Tip:** You can also right-click anywhere on the* **Scheduler's track view and select* ***Add Event*** *from the context menu. The Inspector panel automatically shows the channel and start time based on the location of your mouse on the* **Scheduler** *interface.*

2. Fill in properties of your event according to the following:
   a) Template — Select a template from the drop-down list, if it's already configured.
   b) Name — Enter a name for the scheduled event.

      NOTE: If you reached the character limit, the Name field will be disabled and a red cross indicator displayed. Shorten the event name to enable the field again.

   c) Router Source — If a router is configured as part of the system, select router source for the event from the drop-down list. If configured as a Multicam channel in GV STRATUS Control Panel, two router sources are available.If configured in the **Router | Connection** settings of the GV STRATUS Control Panel, router sources are displayed in alphabetical order.
   d) Recording Channel — Channel availability depends on the configuration in your system. You can only see and select channels that have been configured for the Scheduler tool. Make sure that the channel is not in Continuous Record mode.
   e) Clip Location — Select a record location bin for the event from the drop-down list.

      If the bin has security access permissions configured, the recorded clip inherits those permissions.

      If the option to **Only show location according to recording device** is selected in the Ingest Location Setup in GV STRATUS Control Panel, you can only view and select clip locations in the same K2 system as the configured recording channel.

      NOTE: If the recording channel is set to Auto-assign, all clip locations are available in the drop-down list.

   f) Start Record Now — Check this box to start recording immediately after you click the **Add** button. If you don't enter the end time of the event, the default is set to1 hour. You can also set the default duration in the Ingest panel of the GV STRATUS Control Panel application.
   g) Start Date — Enter the date and time you want the recording to start. The default date is the current date. You can also select your start date from the calendar when you click the drop-down arrow. Enter the time using the format **hour:minutes:seconds**.

      NOTE: When scheduling two events back to back, a space of 10 seconds is required from the stop of the first record to the start of the second record. In order to compensate this, it is recommended that the default record duration reflect a stop time 10 seconds prior to the rounded duration (e.g., 00:59:50 for a 1 hour record).

   h) Open Ended Record — Check this box if you want the recording to continue until you manually stop it. With this record, you only need to provide the start time.
   i) Duration — Enter the duration of the event. The default duration can be set in the Ingest panel of the GV STRATUS Control Panel application. The maximum duration that can be set for an event is 23:59:59.
   j) End Date — Enter the date and time you want the recording to end. You can also select your end date from the calendar when you click the drop-down arrow.
   k) Record Backup — Check this box if you want to record a backup of the feed.
   l) Backup Channel — Select a backup channel from the drop-down list.

      ***NOTE: You cannot select the same channel for both main and backup recordings. Backup channel is disabled when only one channel is configured for the* Scheduler.**

   m) Backup Clip Location — Select a record location for the backup clip.

If the option to **Only show location according to recording device** is selected in the Ingest Location Setup in GV STRATUS Control Panel, you can only view and select clip locations in the same K2 system as the configured recording channel.

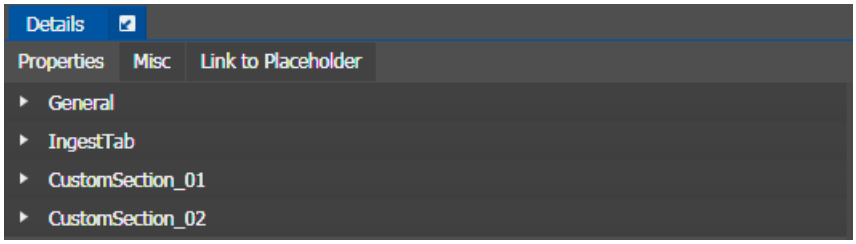
n) Tags — Enter a tag, or tags for the event.
o) Description — Enter the description of the event.
p) Comments — Enter any comments that you have on the event.

By default, the Scheduler tool opens to the current day, date, and time according to your system time. The time of day format within the Scheduler is directly from the current time of day format of your machine.

To set the 24 hour format to your Scheduler, change the time format of your Windows client by selecting **Start | Control Panel | Clock, Language and Region**, and change the time format accordingly.

NOTE: Changes to the* Scheduler*'s time format can only be seen after a restart of the GV STRATUS application.

3. Enter more event information under the **Custom** section, if desired.



You can create custom metadata and assign metadata fields to specific tabs in **Core | Metadata | Inspector Sections** settings within the GV STRATUS Control Panel application.

4. In the **Misc** tab of the Inspector, you can select the **Recurring Event** check box if you want the scheduled event to occur more than once.
5. In the **Link to Placeholder** tab of the Inspector, you can select a placeholder if you want to link it to your event, and click the **Link** button.

   The placeholder name and ID fill in to replace the name of the event, and the placeholder row color changes to light blue to signify it as Being Edited in the Assignment List tool. You can also configure the **Being Edited** status color in the **ALP** tab of user preferences settings.

   NOTE: For playout via* GV STRATUS Rundown*, ensure the clip record location is the same as the configured send destination in* GV STRATUS Control Panel*.

6. Click the **Add** button in the Inspector panel.

   The event is added to the Scheduler tool with a **Ready** status.

   While recording, if the bin in which a growing asset exists reaches its quota, the clip will be forced to stop recording but will remain in the bin.

7. To add another event, in the Inspector panel, fill in properties and other information as in the steps earlier in this procedure, then click the **Add** button.

   It is not necessary to click the **Add Event** button.

Related Topics

Limitations for creating and naming assets and bins on page 1428
Inspector Sections settings on page 327
Setting up control for Scheduler channels in the K2 AppCenter on page 385

Adding an event using Quick Schedule

- If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, and metadata.
- In order to link to a placeholder, you must be assigned with write permission for the **Name** property in Metadata section of GV STRATUS Control Panel.
- If quota is configured on the K2 system bin, ensure you have enough disk space before recording assets.
- It is recommended to set the quota on a destination bin to at least 2GB. Records will not begin if there is less than 1GB of free space remaining in the destination bin.

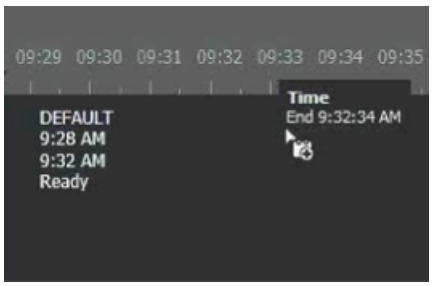
With Quick Schedule, you can add events directly on the scheduling interface.

NOTE: Quick Schedule is only supported on the Track view mode of the Scheduler tool.

1. Right-click on a channel timeline and select **Quick Schedule**. (**Q**)

   Once you are in the Quick Schedule mode, your mouse pointer turns into the **Add Event** icon with time tooltip for your reference.

2. Click to select the start time, and drag your mouse to the right to select the end time.



3. Release the mouse after the end time is selected.

   The event displays on the timeline of the Scheduler tool.

4. Right-click on the event, and select **Modify Event** to add other properties to the event.

   The Inspector loads the event properties.

   If the event is created on a Multicam channel, two router sources appear for the event in the Inspector.

5. Edit properties of the event.

6. Click the **Modify** button to commit your changes.

The event adds to the Scheduler tool with a **Ready** status.

Adding a recurring event

If you want to schedule an event to record on more than one occasion, such as every day, every week, or once a month, you can create a recurring event.

Recurring events can be scheduled on single or multi-cam channels.

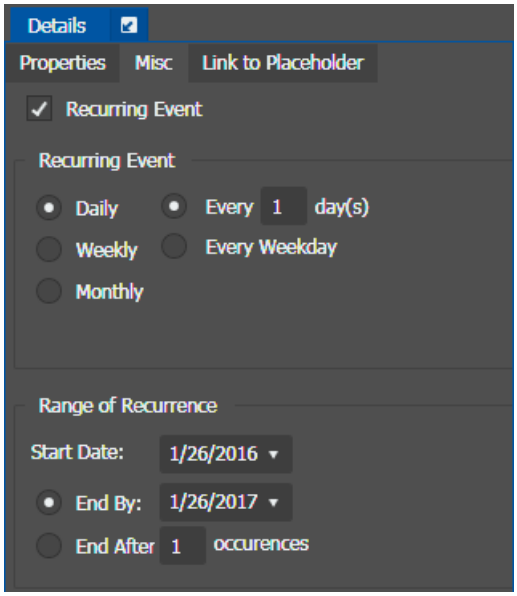
Scheduling a recurring event is the same as scheduling a one-time recording except that you enter information about how the event recurs throughout time. You can schedule the event to recur up to three years in advance.

1. Add a new event.

   The Inspector panel loads new event properties that need to be filled in.

2. Click on the **Misc** tab.
3. Select the **Recurring Event** check box.

   The Recurring Event section opens.



4. Select how you want the event to recur:

   - Daily - Enter the number of days for the event to recur or select **Every Weekday**.
   - Weekly - Enter the number of weeks for the event to recur and check the boxes for the day or days you want the event to record.
   - Monthly - Select a specific date of the month or a specific day of the month to record.

5. Select the range of recurrence, by selecting a Start date, and either an End by date or an End after a certain number of occurrences.

   NOTE: If your range of recurrence includes the start or end time of the Daylight Saving Time, a dialog pops up to warn the possibility of time change in your scheduled recording.

   Click **OK** to close the dialog.

6. Click **Add**.

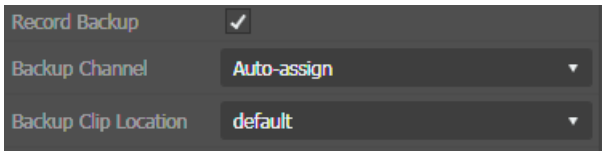
   Recurring events appear on the Scheduler tool.

Adding a backup event

- If quota is configured on the K2 system bin, ensure you have enough disk space before recording assets.
- It is recommended to set the quota on a destination bin to at least 2GB. Records will not begin if there is less than 1GB of free space remaining in the destination bin.

You can create a backup event simultaneously with the main event, to avoid unexpected loss of a recording. You can also set a backup event if you want to record multiple volumes with different front end K2 systems.

1. Add a new event.
2. Select the **Record Backup** checkbox.



3. Select the **Backup Channel** from the drop-down list.

   Available channels are listed depending on channel setup within Ingest setting in the Control Panel application.

4. Select the **Backup Clip Location** from the drop-down list.

   It is highly recommended that you select a separate bin or server for the location of the backup.

   NOTE: If the clip location for main and backup events are the same, the title of the backup event will be appended with '_b' to differentiate it from the main event.

   If the option to **Only show location according to recording device** is selected in the Ingest Location Setup in GV STRATUS Control Panel, only recording locations in the same K2 system as the configured Ingest channel are available for selection.

   NOTE: If the recording channel is set to Auto-assign, all clip locations are available in the drop-down list.

5. Click **Add**.

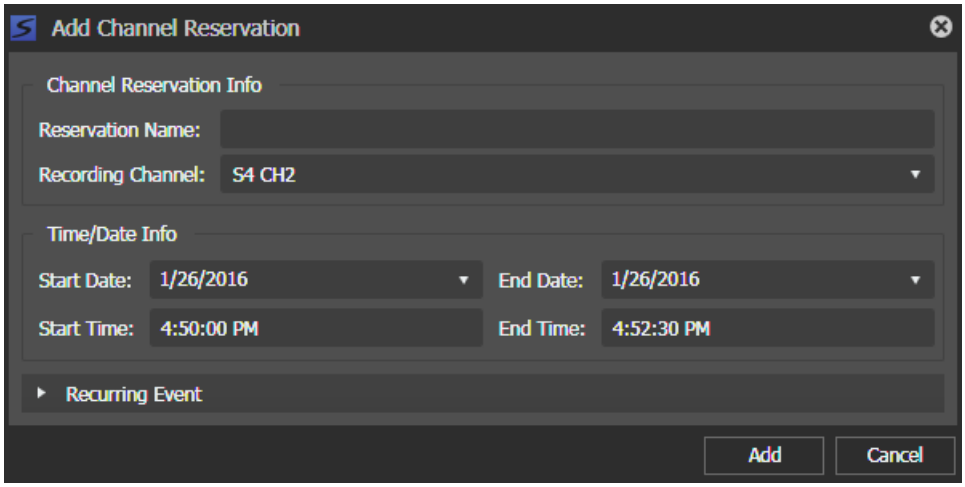
   Both main and backup events appear on the Scheduler tool.

Adding a channel reservation

Channel reservation allows you to reserve a channel for future events and crash records. This ensures that the channel is reserved for a specific recording and cannot be used to schedule any other events.

1. Right-click and select **Add Channel Reservation**.

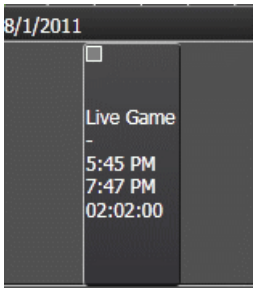
   The Add Channel Reservation dialog opens.



2. Specify the name of the reservation.
3. Select the recording channel from the drop-down list.
4. Select the start date, start time, end date, and end time in the Time/Date Info section.
5. Click the **Recurring Event** Show/Hide control if you want to reserve the channel for a recurring event.

   Select how you want the event to recur by filling up the Recurring Event section.
6. Click **Add**.

   The channel reservation appears as a black event on the Scheduler tool.



You cannot quick-schedule other events or extend other events to overlap with a channel reservation, but you are allowed to crash record.

Starting a crash record event

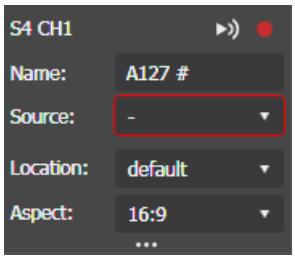
- If quota is configured on the K2 system bin, ensure you have enough disk space before recording assets.
- It is recommended to set the quota on a destination bin to at least 2GB. Records will not begin if there is less than 1GB of free space remaining in the destination bin.

You can crash record when you want to record an event immediately. You can also configure a default duration for all crash record events in the GV STRATUS Control Panel application.

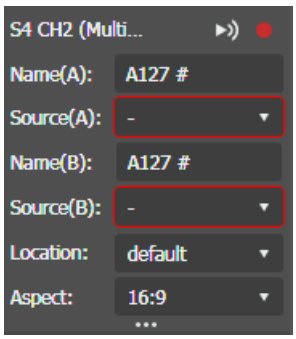
NOTE: Ensure that you have sufficient storage before proceeding with crash record. If the remaining storage on the* K2 system *is less than the default crash duration that was set in the GV STRATUS Control Panel, the Record button is disabled.

1. Enter name and source as follows:

   - If configured as a Player/Recorder channel in GV STRATUS Control Panel, enter the name of the clip in the **Name** field and select the router source for the recording from the **Source** drop-down list, if available.



   - If configured as a Multicam channel in GV STRATUS Control Panel, enter a name in both **Name** fields and select two router sources for the recording from the **Source** drop-down list, if available.



   If configured in the **Router | Connection** settings of the GV STRATUS Control Panel, router sources are displayed in alphabetical order.

   NOTE: If you do not enter a name prior to the crash record, the application sets a default feed name according to your Ingest settings in the* GV STRATUS Control Panel *with a default suffix. If a clip already exists with the same name, the application uses the next available default suffix. Once the event name is entered in the panel, the default feed name will not be used.

2. Select the bin for the clip to be recorded into from the **Location** drop-down list. If you do not enter a location prior to the crash record, the clip is recorded into the channel's default bin.

   If the option to **Only show location according to recording device** is selected in the Ingest Location Setup in GV STRATUS Control Panel, only recording locations in the same K2 system as the configured Ingest channel are available for selection.

3. Select the **Aspect ratio** if recording to an SD channel.

4. Click the **Record** button.

   The event cues and begins recording. While recording, the channel and event display red.

5. If you want to change the event duration while recording, right-click on the event and select **Modify Event**, or click the **Modify Event** button. (**M**)

   Event properties display in the Inspector panel.

   You can also double-click the recording event to launch event properties in the Inspector.

6. Enter the new **End Time** for the event and click **Modify**.

   The crash record event updates to the new end time.

   While recording, if the bin in which a growing asset exists reaches its quota, the clip will be forced to stop recording but will remain in the bin.

7. If you want to stop the recording at any time, click the **Stop** button. (**S**)

   Recording stops and the event status changes to Done.

Locating an event

To locate an event in the Scheduler tool, you can scroll along the timeline and use navigation buttons on the toolbar.

1. Scroll to the date and time of the event on the timeline if you know the starting date and time of the recording.
2. Click the **Zoom In** button. (**Up Arrow**)

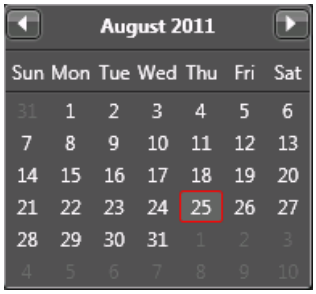
   The Scheduler window zooms in to show the timeline in detail. You can keep zooming in until it shows one-minute increments on the timeline.

3. Scroll along the timeline to find your event.
4. To zoom out the Scheduler window, click the **Zoom Out** button. (**Down Arrow**)

   You can keep zooming out until it shows six-hour increments on the timeline.

5. You can go to the previous day (**G**) or the next day (**H**) by scrolling the timeline or pressing those shortcut keys.
6. To find other events on different dates, click the **Go to Date** button. (**D**)

   A calendar opens for you to select a specific date to view on the Scheduler. You can select a day of any month from the calendar and go to that date in the Scheduler.



7. To automatically get to the current time of the day in the Scheduler's track view mode, choose one of these steps below:
   - Click the **Go to Current** button.
   - Click the **Toggle Timelock** button. The timelock turns on and the current time indicator is locked to the center of the Scheduler tool. The timeline moves accordingly but the Scheduler locks the current time display at the center of the scheduling track all the time.

   This is useful if you want to check the event that is currently recording.

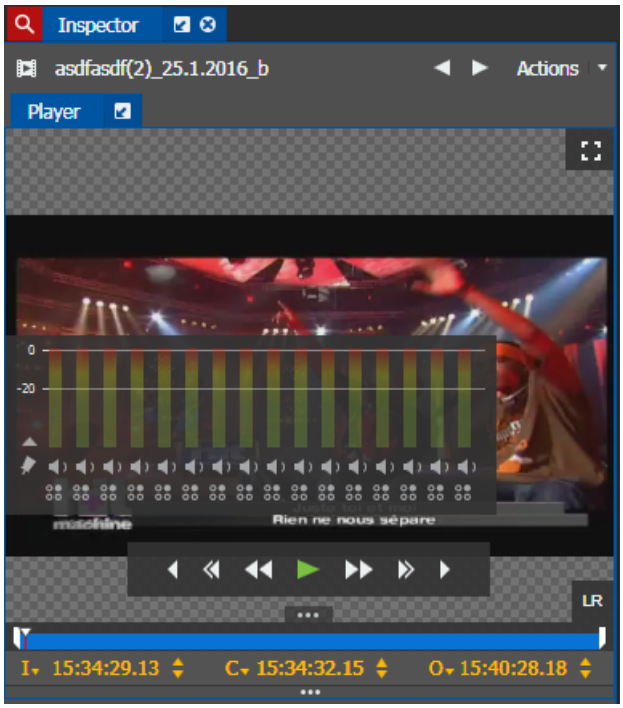
   The timelock turns off if you scroll along the track again.

Previewing an event

You can preview a currently recording event or a recorded event of the Scheduler tool. The event can be previewed either on the Inspector or Source Viewer panel.

1. Select a currently recording event or a recorded event.
2. Load the event for preview as follows:
   - If a Multicam channel, double-click either of the two available clips to load it into the Inspector panel.
   - If not a Multicam channel:
     - Double-click the event to load it into the Inspector panel.
     - Drag the event and drop it into the Inspector or the Source Viewer panel.

   The clip loads.



3. You can use transport control buttons within the panel to view the clip.

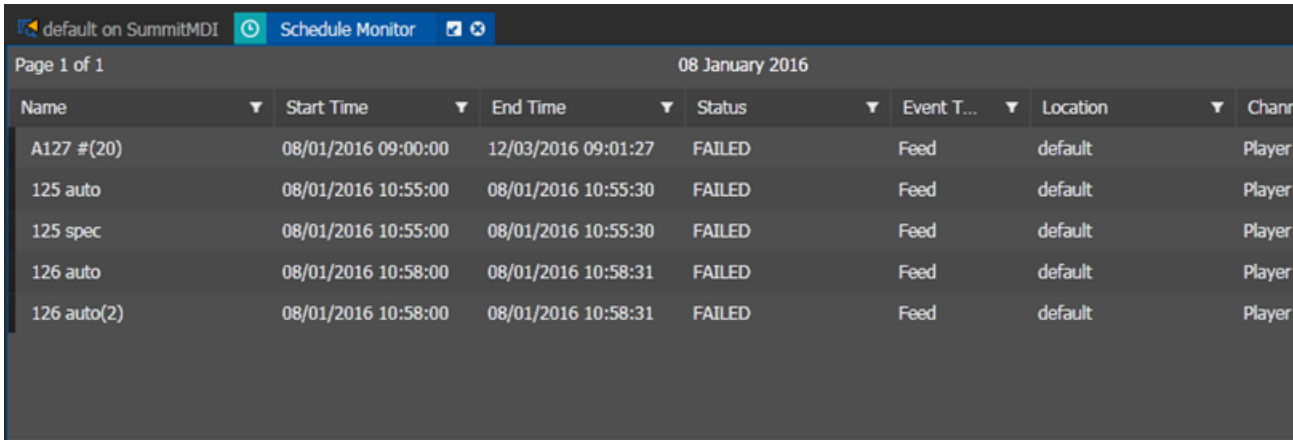
Related Topics

Previewing a live streaming video on page 975

Monitoring Ingest Schedule on a large screen

The Schedule Monitor allows you to view Ingest Schedule on a separate panel than the Scheduler. You can configure the panel to be displayed on a large screen so ingest events can easily be monitored.

To launch the Schedule Monitor panel, click the **Monitors** node in the Navigator panel and select **Schedule Monitor**.



Events display in multiple pages according to the size of **Schedule Monitor** panel. Each page advances automatically and the page number displays on the upper-left of the panel.

The text field and slider at the bottom of the **Schedule Monitor** panel adjusts font size.

You can configure the Schedule Monitor settings in Scheduler User Preferences.

Related Topics

Event status colors on page 1033
Configuring Scheduler User Preferences on page 1055

Renaming an event

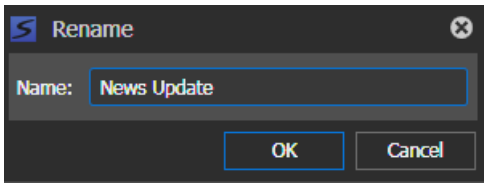
- If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, and metadata.
- In order to change the name of an event, you must be assigned with write permission for the **Name** property in Metadata section of GV STRATUS Control Panel.

1. Select the event that you want to rename.

2. Do one of the following:

   - Press the **F2** key
   - Right-click and select **Rename Event**.

   The Rename dialog appears.



3. Enter the new name for the event.

   The name must conform to asset and bin name limitations.

   The name change must not be a change in capitalization only.

   NOTE: If you reached the character limit, the Name field will be disabled and a red cross indicator displayed. Shorten the event name to enable the field again.

4. Click **OK**.

The event name changes to the new name.

Renaming an event via double-click is also supported subject to these conditions below:

- Double-click to rename event from Inspector is different from the right-click to modify event.
- Double-click to rename event from Inspector is only supported for single event, recurring event is not supported.
- Double-click to rename event from Inspector will only take effect on the selected event, regardless of main or backup event.

Related Topics

Limitations for creating and naming assets and bins on page 1428

Modifying an event

- If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, and metadata.
- In order to link to a placeholder, you must be assigned with the **Rename Asset Rights** role and write permission for the **Name** property in Metadata section of GV STRATUS Control Panel.

You can modify an event by changing the event name, date, recording channel, clip location, router source, duration, timing information, adding a backup for the existing event, or linking the event to a placeholder.

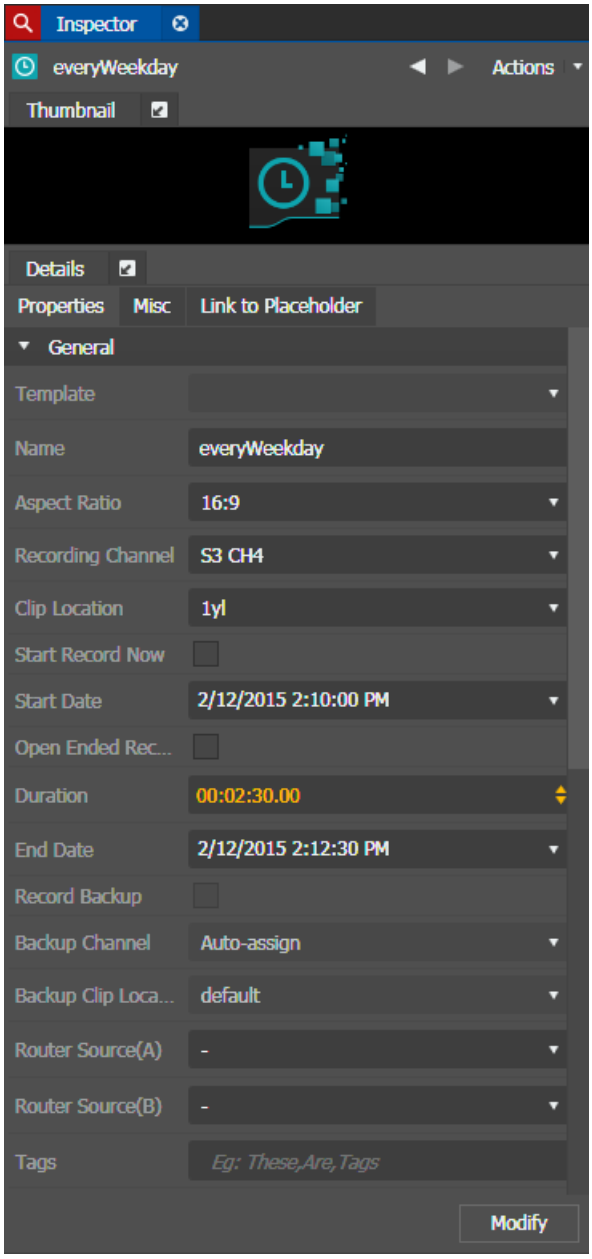
1. Select the event you want to modify on the Scheduler tool.

2. Do one of the following:

   - Click the **Modify Event** button. (**M**)
   - Right-click and select **Modify Event**

   The event opens in the Inspector panel.

   ***NOTE: Double-clicking an event is not supported when you want to modify a scheduled event. Make sure you follow exact steps in this topic to modify event in the* Inspector.**



3. If the event is part of a series, a dialog box pops up asking if you want to modify this occurrence or the entire series. Select the one you want to modify and click **OK**.

   Event properties display in the **Properties** tab of the Inspector.

   If the event is created on a Multicam channel, two router sources appear for the event in the Inspector.

4. Modify the event properties.

   NOTE: If you reached the character limit, the Name field will be disabled and a red cross indicator displayed. Shorten the event name to enable the field again.

   If the option to **Only show location according to recording device** is selected in the Ingest Location Setup in GV STRATUS Control Panel, only recording locations in the same K2 system as the configured Ingest channel are available in the **Clip Location** drop-down list.

   NOTE: If the recording channel is set to Auto-assign, all clip locations are available in the drop-down list.

5. To set as a recurring event, click on the **Misc** tab and edit event properties.
6. To link the event to a placeholder, select a placeholder on the **Link to Placeholder** tab and click the **Link** button.

   NOTE: If an event is double-clicked then linked to a placeholder, the clip will not be renamed according to the placeholder's title. Make sure that you follow exact steps in this topic to modify event in the* Inspector *and link to a placeholder. In addition, linking to a placeholder is not supported for recurring events.

7. Click the **Modify** button on the **Properties** tab.

The event updates with those changes on the Scheduler tool.

Viewing and modifying metadata of events

You can view and modify metadata of an event in the Inspector panel. The inserted metadata can then be used as the search criteria to easily search assets in the Asset List panel.

1. To view or modify metadata of an event, do one of the following below:

   - Drag and drop the event into the Inspector panel.
   - Double-click the event.

   The event metadata loads into the Inspector panel.

2. On the **Properties** tab, you can view or modify metadata of the event.

   If GV STRATUS metadata access control is enforced, your credentials must give you adequate permissions. You can only view metadata with read permissions, and modify metadata with write permissions. If read or write permissions are denied, your metadata fields will be disabled.

   You can also change the order of metadata display via **Metadata | Inspector Sections** in the GV STRATUS Control Panel. However, it is only applicable to **Tag, Comment, Description** and custom metadata.

3. To lock the status of the event, click the **Unprotected** button.

   The event is now protected. To unprotect, click the **Protected** button.

4. To add a star rating, click the star or stars next to Rating.

   When you add a star, it retains the color fill even when the mouse is no longer hovering over it.

5. To view list of placeholders and related assets, see other tabs of the Inspector panel.

Related Topics

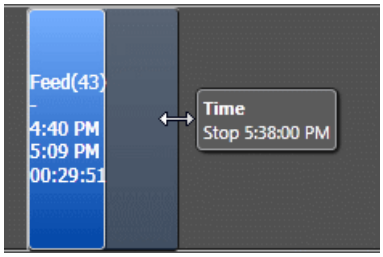
Viewing relationships on page 1020
Verifying proxy association on page 1021

Extending an event

You can extend the start and end time of an event on the scheduling interface itself.

NOTE: This feature is only supported in the* Scheduler*'s track view mode.

1. Select the event that you want to extend within the Scheduler tool.
2. Point your mouse at the edge of the event so that the mouse pointer turns into a double-sided arrow.
3. Click and drag to extend the start or end time of the event.



   You can see the time tooltip and event shadow indicating the time change.

4. Release your mouse at the new time.

   A dialog box opens for you to confirm the change.

5. Click **Yes**.

   The Scheduler tool updates the event to a new start time or end time.

Moving an event

You can move a scheduled event within the same channel or to a different channel. This is useful when the current channel is not available or another event needs to be scheduled into the channel at the same time.

NOTE: This feature is only supported in the* Scheduler*'s track view mode.

1. Select the event you want to move on the Scheduler tool.
2. Press the **Ctrl** button and drag the event to another time or another channel.

   Once you drag the event, a tooltip appears to help you decide the start time of the event.

3. Drop the event to the new location and release the **Ctrl** button.

   A dialog box opens for you to confirm the move of the event.

4. Click **Yes**.

   The Scheduler tool updates the event change.

Deleting an event

You can delete events that have been scheduled if you need to.

1. Select an event or multiple events that you want to delete.

   To select multiple events, hold the **Shift** key down and select all events between two selected events; or hold the **Ctrl** key down and select events randomly.

2. Do one of the following:

   - Click the **Delete Event** button. (**Delete**)
   - Press the **Delete** key on your keyboard.
   - Right-click on the event and select **Delete** from the context menu.

3. When prompted **Delete this event?**, click **Yes**.

Events are deleted from the tool.

Deleting a recurring event

When you want to delete a recurring event, you can choose either to delete a single occurrence of the recurring event or the whole series.

1. Select the recurring event that you want to delete.
2. Click the **Delete Event** button. (**Delete**)
3. When prompted **Do you want to delete this occurrence or the entire series?**, select the option that you want.
4. Click **OK**.

The recurring event is deleted from the Scheduler tool.

Creating a template

A template saves time by storing information that can be used for future events.

A template can be created in two ways:

- Create a template from an existing event
- Create a template from the user preferences setting

Saving event as a template

To enable the Custom Metadata Feature on Scheduler Event Templates after a new install, refer to *Setting Custom Metadata in the Ingest Database* on page 688.

You can save an existing event as a template in the Scheduler tool.

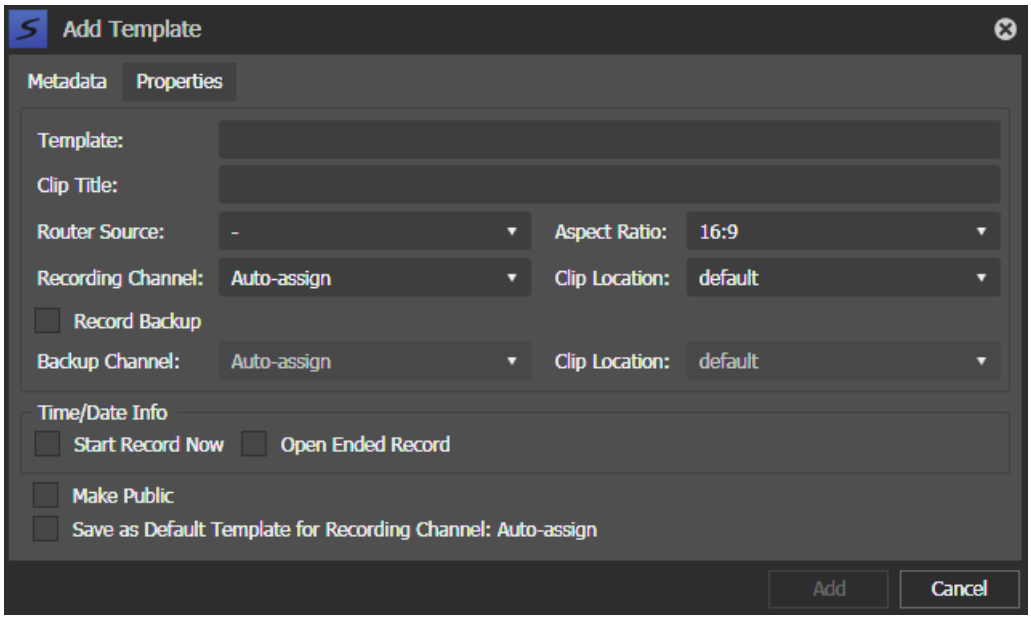
1. Select the event you want to use as a template.

2. Right-click and select **Save As Template**.

   NOTE: The Save As Template option on the context menu is not supported for events scheduled on the multicam channel.

   The Add Template dialog opens.

3. Fill in the information on the **Metadata** tab to be included in the template.



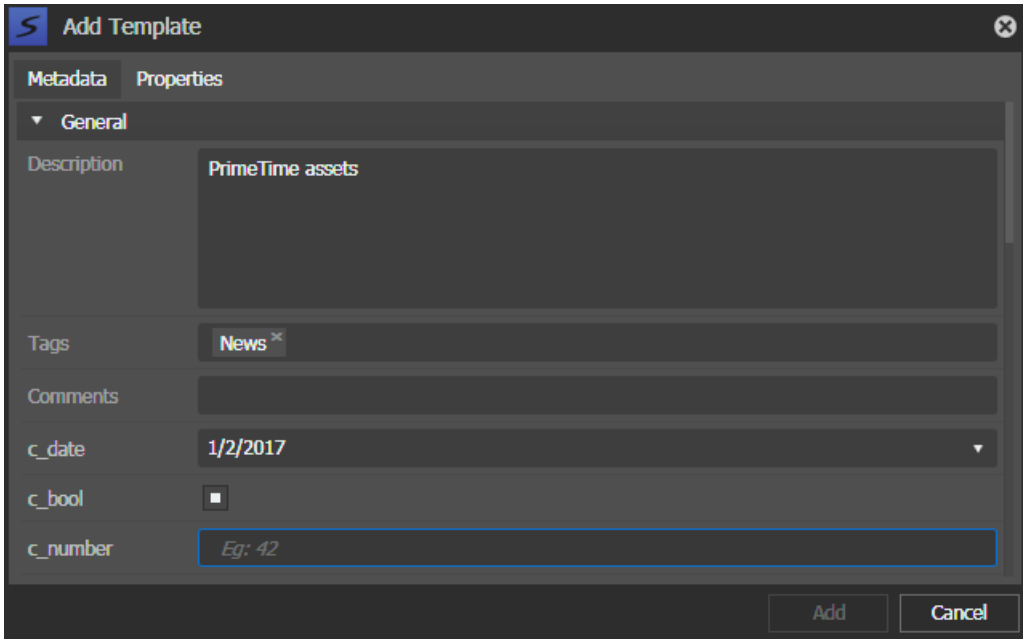
a) Template — Enter the name of the template.
b) Clip Title — Enter a different clip title if needed. By default, the clip title of the selected event is automatically entered in this field.
c) Router Source — Select a different router source to record from in the drop-down list if needed. By default, the router source of the selected event is automatically entered in this field.
d) Aspect ratio — Select the aspect ratio if recording to an SD channel.
e) Recording Channel — Select a different channel than the one automatically entered from the selected event if needed.
f) Clip Location — Select a different record location than the one automatically entered from the selected event if needed.

   If the option to **Only show location according to recording device** is selected in the Ingest Location Setup in GV STRATUS Control Panel, only recording locations in the same K2 system as the configured Ingest channel are available for selection.

   NOTE: If the recording channel is set to Auto-assign, all clip locations are available in the drop-down list.

g) Record Backup — Check the box if you want to record backup of an event as part of the event template. Select the backup channel and clip location from the drop-down lists.
h) Start Record Now — Check this box to save the crash record attribute in the template.
i) Open Ended Record — Check this box to save the open ended record attribute in the template.
j) Make Public — Check this box if you want the template to be available to everyone.
k) Save as Default Template for Recording Channel: — Check this box if you want to assign the template as a default template for the particular channel. This allows users to crash record easily and saves time by not having to fill up details of the event.

4. Click on the **Properties** tab, then enter the Description, Tags, Comments, and custom metadata if configured, into the template.



   Custom metadata must be configured in the GV STRATUS Control Panel before they can be displayed on the Properties tab. Read and write permissions must also be assigned to each custom metadata. If write permission is denied, the custom metadata is not editable on the Properties tab.

5. Click **Add** to save the template.

   NOTE: You cannot create a template from a channel reservation, but only from feed events on the* Scheduler *tool.

The template is available for you, and other users within your broadcast operation if you set it as a public template. You can select it within the Template drop-down list when you add or modify an event.

Configuring Scheduler User Preferences

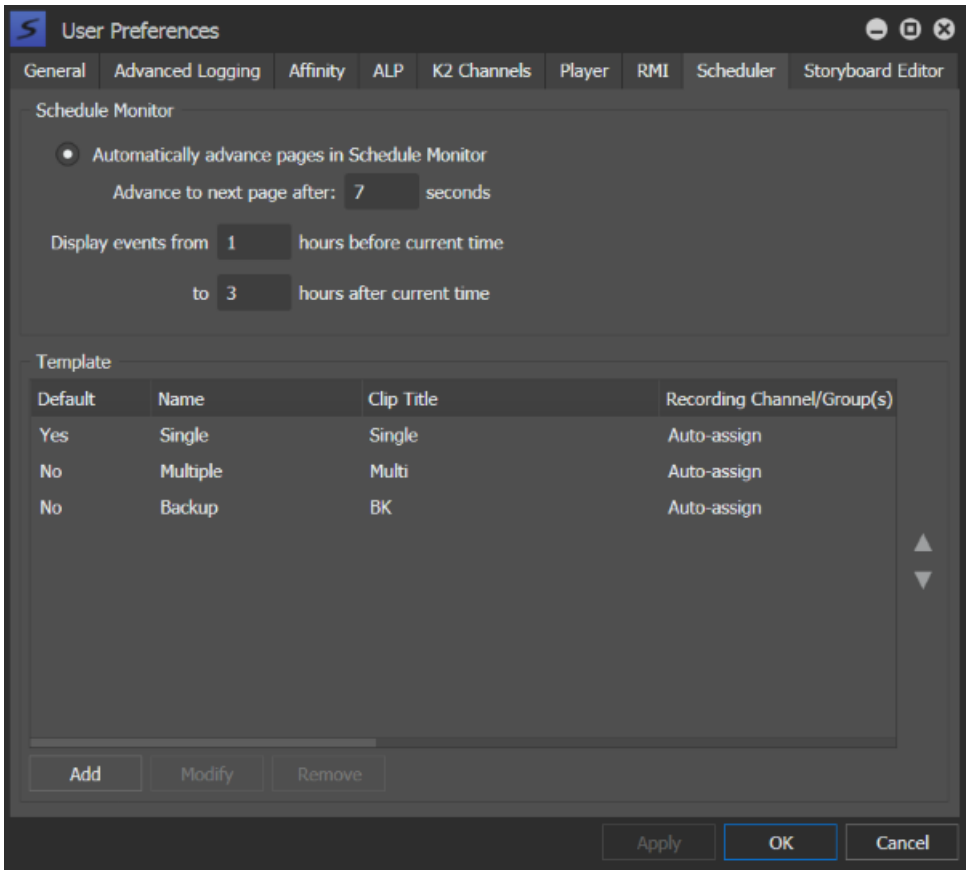
You can configure Schedule Monitor settings and create an event template within the user preferences window.

1. Select **Edit | User Preferences**.

   The User Preferences dialog box opens.

   The GV STRATUS application shows or hides sections based on the roles assigned to your GV STRATUS log on credentials.

2. To configure Scheduler user preferences, select the **Scheduler** tab.



3. To configure Schedule Monitor settings, do the following:
   a) If you want Schedule Monitor pages to change automatically, select **Automatically advance pages in Schedule Monitor**.
   b) Enter the number of seconds before advancing to the next page.
   c) Enter the desired number of hours before and after the current time for event display in the Schedule Monitor.

      NOTE: When setting the number of hours before and after the current time, do note that all the events will be kept in memory. Set the hours to the minimum viable value for your system environment.

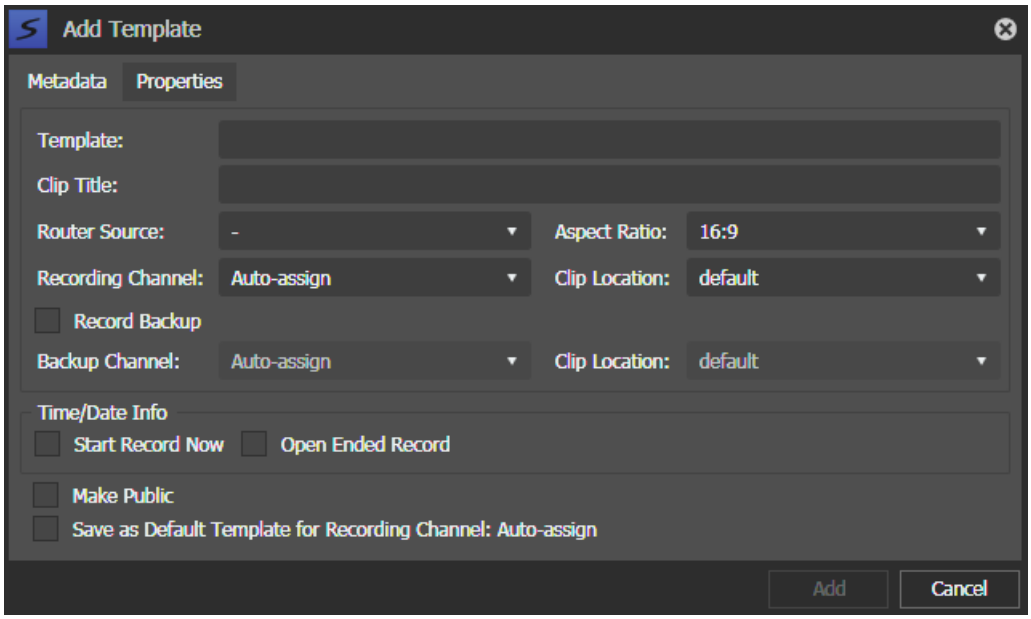
   Ingest events display in the Schedule Monitor according to selected settings.

4. To create a template, click **Add**.

   The Add Template dialog opens.

   NOTE: To enable the Custom Metadata Feature on Scheduler Event Templates after a new install, refer to Setting Custom Metadata in the Ingest Database on page 688.

5. Fill in the template information on the **Metadata** tab of Add Template dialog.

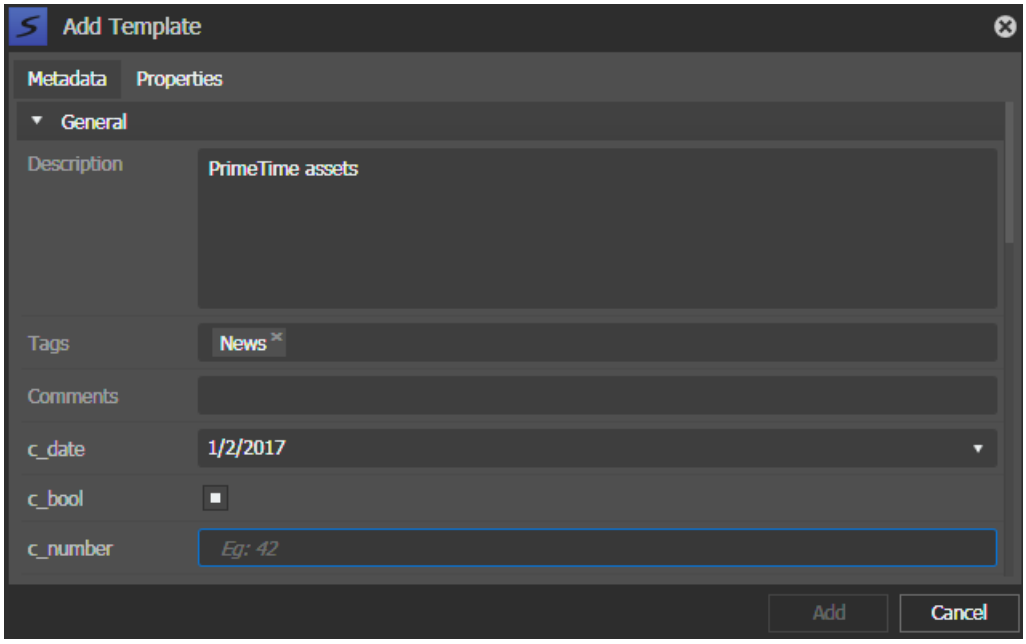


If the option to **Only show location according to recording device** is selected in the Ingest Location Setup in GV STRATUS Control Panel, only Clip Locations in the same K2 system as the configured Ingest channel are available for selection.

NOTE: If the recording channel is set to Auto-assign, all clip locations are available in the drop-down list.

You can also select the check box to make the template public and set a default template for the selected recording channel.

6. Click on the **Properties** tab, then enter the Description, Tags, Comments, and custom metadata if configured, into the template.



Custom metadata must be configured in the GV STRATUS Control Panel before they can be displayed on the Properties tab. Read and write permissions must also be assigned to each custom metadata. If write permission is denied, the custom metadata is not editable on the Properties tab.

7. Click **Add** to save the template.

   The newly added template appears on the template list in the Scheduler user preferences.

   You can select the template when adding or modifying events in the Scheduler tool.

8. To apply a change and continue editing user preferences settings, click **Apply**.
9. To accept any changes and close the dialog box, click **OK**.

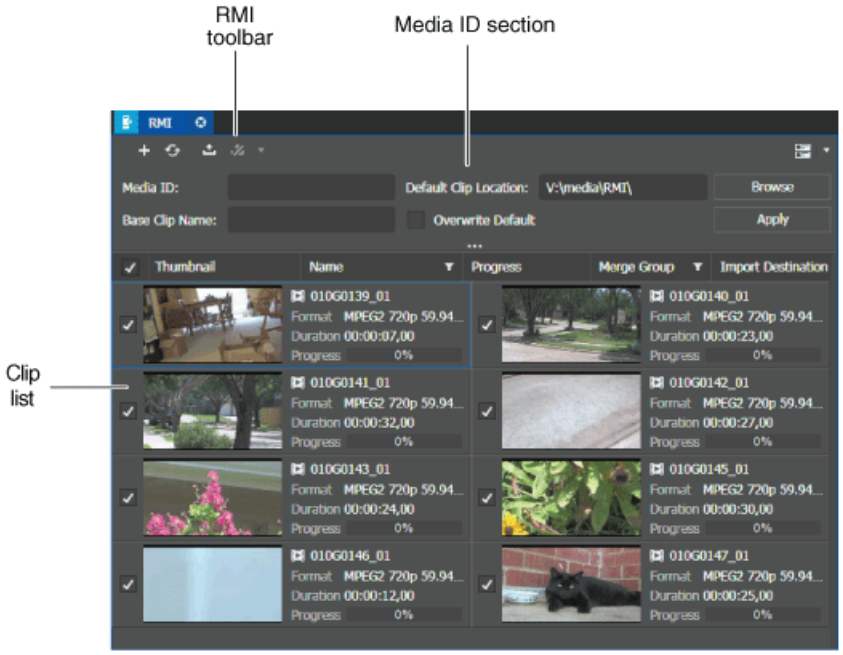
   The dialog box closes.

Related Topics

Monitoring Ingest Schedule on a large screen on page 1047

The RMI tool

RMI is the acronym for Removable Media Interface. It is the tool that populates and ingests files from multiple removable media devices such as P2 and XDCAM. The RMI tool requires a GV STRATUS client with access to high-resolution assets. The Removable Media Interface (RMI) allows you to populate and ingest files from multiple removable media devices. In the GV STRATUS application, RMI appears as a tool in the Navigator panel. The RMI tool allows you to populate files from the Panasonic P2, Sony XDCAM, Sony XDCAM EX, and JVC removable media devices.



RMI panel features are as follows:

- RMI toolbar — Consists of buttons for adding removable media, populating clip list, and importing clips.
- Clip list — Populates the clip list once removable drive is detected.
- Media ID section — Allows you to add Media ID, base clip name, overwrite default clip name, and change the default import location.

Standard Asset List features such as filter list, sort list, asset tooltip, and customization of **View Mode** are available in the RMI tool.

You can also drag and drop clips within the list to change the order of the clip list.

If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, metadata, markers, and keywords.

RMI format specifications

The following clip format specifications apply to the RMI.

Removable Media	Clip Format
Panasonic	DV25, DV50, DV100, AVC-I 50, AVC-I 100
Sony	XDCAM SD, XDCAM HD, XDCAM EX SD, XDCAM EX HD, XDCAM MXF on SxS, XAVC
JVC	XDCAM EX

Related Topics

Formats supported for import and export on page 1429

RMI buttons

These buttons located on the RMI panel let you perform various functions.

- **Select All**: Selects or deselects all items in the RMI list.
- **Media ID**: Opens or closes the Media ID section.
- **Add Media**: Adds media to the RMI tool.
- **Refresh**: Refreshes all clips in the RMI list.
- **Import**: Imports selected media to the assigned bin.
- **Cancel Import**: Cancels the import media process.

Configuring RMI User Preferences

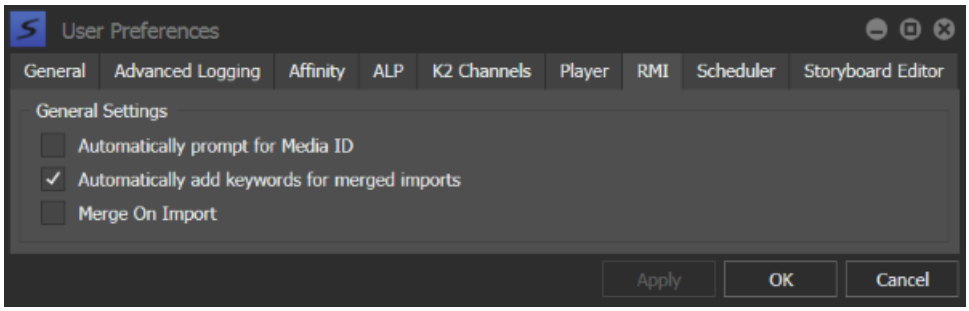
You can configure RMI settings within the user settings preferences window.

1. Select **Edit | User Preferences**.

   The User Preferences dialog box opens.

   The GV STRATUS application shows or hides sections based on the roles assigned to your GV STRATUS log on credentials.

2. To configure RMI user preferences, select the **RMI** tab.



3. Do the following:

   - To launch the Media ID section automatically when a new removable device is detected, select the **Automatically prompt for Media ID** checkbox.
   - To insert keywords automatically during merged imports, select the **Automatically add keywords for merged imports** checkbox.
   - To always merge clips during import, select the **Merge On Import** checkbox. This makes RMI merges multiple clips into a single clip during every import.

4. To apply a change and continue editing user preferences settings, click **Apply**.
5. To accept any changes and close the dialog box, click **OK**.

   The dialog box closes.

Accessing media

Removable media devices are automatically detected when attached to the system or mapped to a network drive. The RMI tool requires one of the following types of GV STRATUS clients:

- Low-resolution (proxy) client PC with SMB access to K2 storage.
- High-resolution client PC on K2 media (iSCSI) network, which requires the GV STRATUS high resolution license.

Once the RMI tool detects specific clip formats, it populates the list in the RMI panel.

Media detection modes are as follows:

- Active clip detection mode — When you launch the RMI panel, the application checks the folder structure on all the windows mapped drives from A to Z that it detects. Once the application detects a removable media folder structure, the application locates all clips in that drive and populates the clip list to be shown on the panel.
- Passive clip detection mode — When you introduce a new drive to the system, the application checks whether the new drive has a removable media folder structure. If it does, the application locates all clips contained in the new drive and populates the clip list.

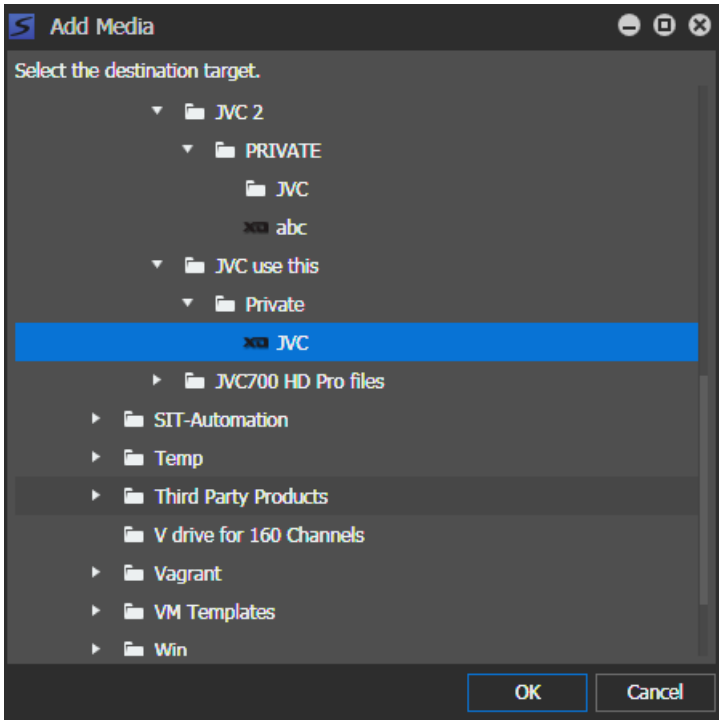
The application also monitors the drive for media removal. Once the removable media is ejected, the clip list is cleared from the RMI panel.

Adding media

You can browse folders to locate media from removable media devices and load those media into the RMI tool.

1. Click the **Add Media** button. +

   The Add Media dialog box opens.



2. Browse folders to locate media from removable media devices.

   Supported folder structures such as P2, XDCAM, and XDCAM EX can be identified from their folder logo as shown above.

   When GV STRATUS security is enforced, you must have write permissions to the destination.

3. Select the removable media folder.
4. Click **OK**.

   Clips from the removable media folder appear in the RMI tool.

Related Topics

Limitations for creating and naming assets and bins on page 1428

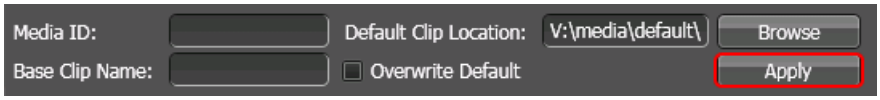
Adding a media ID

You can add a media ID to clips on the RMI to identify clips for your broadcast easily.

1. Click the **Media ID** button. ...

   The Media ID section opens.

   NOTE: The Media ID section also opens automatically when a new removable device is detected, if the Automatically prompt for Media ID checkbox is selected in the user preferences window.



2. Enter the Media ID to identify clips from each removable device.
3. Enter a default clip name in the **Base Clip Name** field. The application sets the base clip name with a default suffix for every clip populated in the RMI panel. If you don't enter a base clip name, the application uses original clip names from the removable device.

   NOTE: The base clip name will only overwrite names that have not been previously altered. For instance, if a photographer overrides the default clip name on the camera itself, RMI will not overwrite that name. However, selecting Overwrite Default overrides all default clip names.

4. Change the **Default Clip Location**, if you want to import clips to a different location.

   You can click **Browse** to search for other locations in your K2 Summit system.

   When GV STRATUS security is enforced, you must have write permissions to the destination.

5. Check the **Overwrite Default** box if you want the base clip name to overwrite original clip names.
6. Click the **Apply** button.

   The Media ID section closes.

The RMI updates according to details entered in the Media ID section.

Previewing a clip

- If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, metadata, markers, keywords, and segments.

Clip previews allow you to easily select, deselect and decide what to import from the RMI tool. You can preview clips using the Inspector and Source Viewer panel.

1. Select a clip that you want to preview from the RMI list.

2. Do one of the following below:

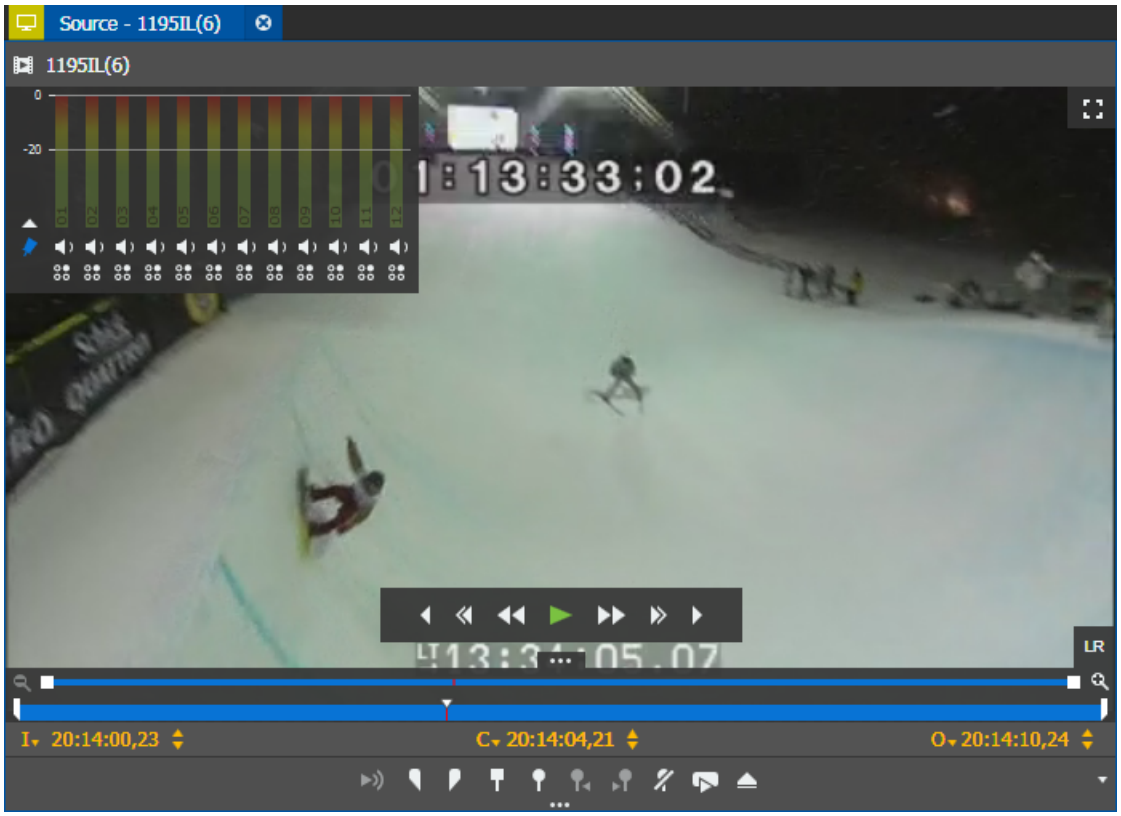
   - Double-click on the clip.

     The clip loads into the Inspector panel.

     If you have previously launched the Source Viewer, you can see the clip loads into both Source Viewer and the Inspector panel.

   - Right-click and select **Preview Highlighted Clips**.

     The clip loads into the Source Viewer panel.



NOTE: You can also select multiple clips and preview them, but only if they are of the same video and compression format.

3. Click the **Play** button.

   You can navigate through the preview using transport control buttons on the Inspector and Source Viewer panels. If you are previewing multiple RMI clips, each clip is indicated by a symbol above the scrub bar.

   You can also view markers and keywords on the clip. Marker permissions must be set to Allow on the **Security** tab of the Inspector to create, update, or delete markers and keywords.

Editing clip properties

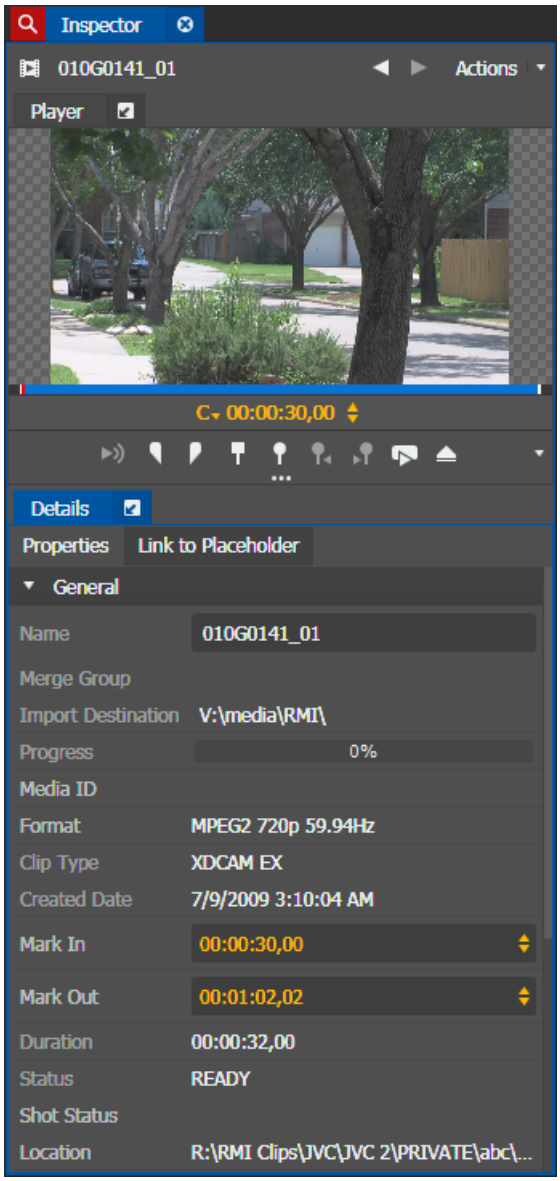
If GV STRATUS metadata access control is enforced, your credentials must give you adequate permissions. You can only view metadata with read permissions, and modify metadata with write permissions. If read or write permissions are denied, your metadata fields will be disabled.

You can edit clip properties within the RMI tool.

1. Double-click on a clip in the RMI list.

   The clip loads and its properties display in the Inspector panel.

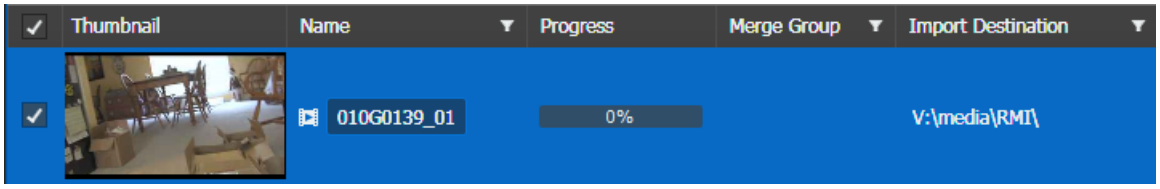
2. You can edit the clip name in the **General** section.



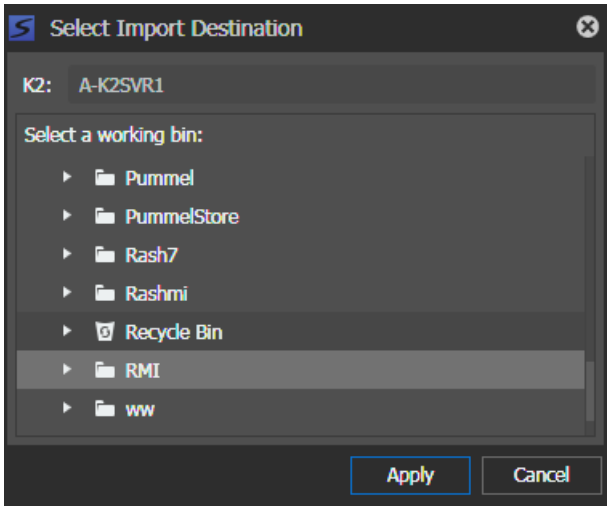
3. You can edit mark in and mark out points in the Inspector.

4. In the **Other** section, you can only view properties of the clip.
5. To just rename the clip title on the RMI panel; right-click on the clip, and select **Rename**.

   The name of the clip becomes editable and you can rename the clip on the panel itself.



6. To change the import destination of a clip; right-click on the clip, select **Modify Location**, and choose a new import destination.



When GV STRATUS security is enforced, you must have write permissions to the destination.

Related Topics

Limitations for creating and naming assets and bins on page 1428
Metadata Mapping Add/Modify Field settings on page 324
Permissions settings on page 321

Linking clip to a placeholder

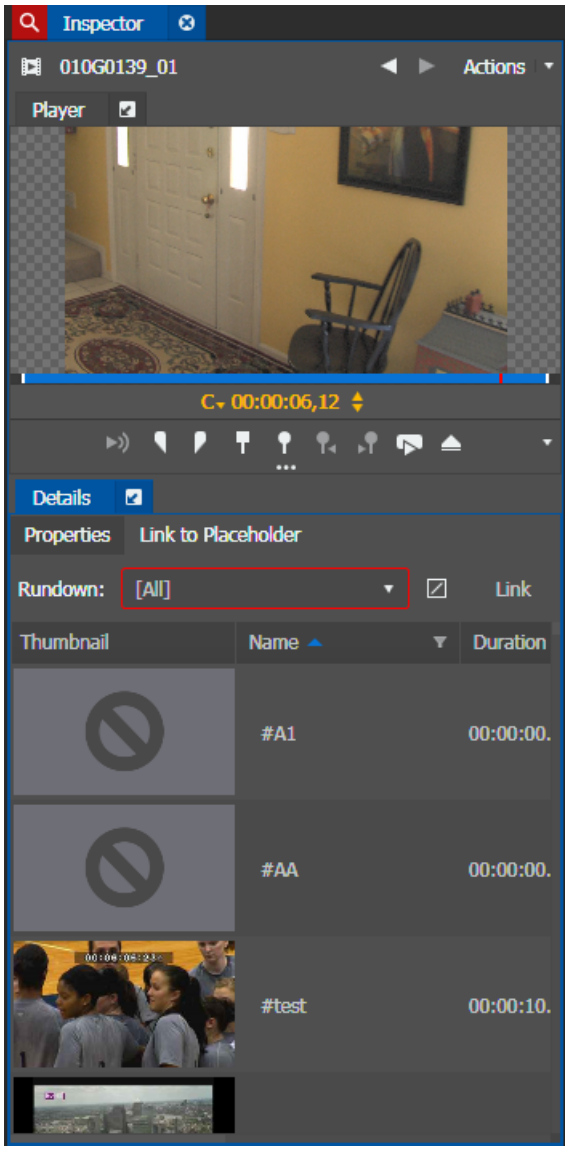
- If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, and metadata.
- In order to link to a placeholder, you must be assigned with the **Rename Asset Rights** role and write permission for the **Name** property in Metadata section of GV STRATUS Control Panel.

You can link a clip to a placeholder prior to import.

NOTE: For playout, make sure the clip import destination is the same as the playout location.

1. Double-click on a clip.

   The clip properties display in the Inspector.



2. In the **Link To Placeholder** tab, click the **Missing Placeholders Only** button to only display placeholders with missing clips.
3. Select a placeholder to link the clip to.
4. Click the **Link** button.

   The placeholder name and ID filled in to replace the previous name of the clip. The clip is now associated with the placeholder, and the placeholder is categorized as being edited in the Assignment List.

After the clip is imported, the placeholder status in the Assignment List changes to **READY** and the duration is updated.

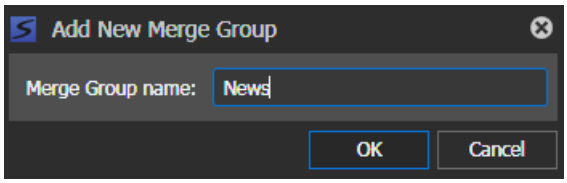
Merging clips into group

You can create groups and merge clips into a group before importing. This allows operators to create groups of clips, name them, and then import them without having to repeat multiple imports separately.

1. Highlight clips that you want to merge into a group.
2. Right-click and select **Add to Merge Group**.

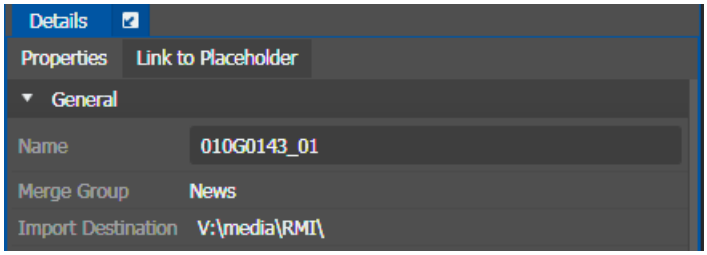
   You can choose to create a new group or use existing group names from the context menu.

   If the **Merge On Import** option is selected in the RMI User Preferences settings, all clips will be merged into a single clip on every import.
3. If you want to create a new group, select **Add New Merge Group** and enter the group name.



   If the **Automatically add keywords for merged imports** option is selected in the RMI User Preferences settings, keywords will be added automatically to merged imports. Marker permissions must be set to Allow for keywords to be added successfully. Without full permissions, no keywords will be added to merged assets.
4. Click **OK**.

The merge group name that you selected appears in the Merge Group property of each clip. You can view the property in the Inspector panel.



The merge group name will become the name of the imported clip once the import process is completed.

If you wish to remove clips from the group, right-click on those clips and select **Remove from Merge Group**.

Related Topics

Configuring RMI User Preferences on page 1060

Trimming a clip

With the RMI tool, you can trim a clip prior to import. To use the Trim operation, you must be logged on with a user account to which the Trim Rights role is assigned. If the role is not assigned, the Trim operation is not available.

NOTE: Trimming is only supported with individual clips.

1. On the RMI list, select the clip that you want to trim.
2. Drag the clip from the RMI tool and drop it into the Inspector.
3. Navigate to the desired starting point using the scrub bar, and click the **Mark In** button. (**I**)
4. Navigate to the desired end-point using the scrub bar, and click the **Mark Out** button. (**O**)

   Trim Asset is enabled when the asset has a mark-in or mark-out point. It is disabled if the asset does not have a mark-in or mark-out point.

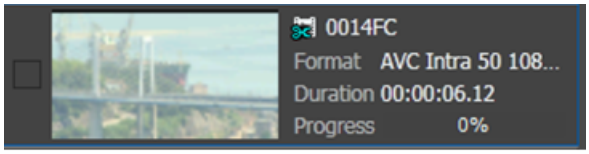
   NOTE: If a clip is a part of Dyno record train sequence, Mark In and Mark Out points should not be set beyond the limit of the guard band, as configured for the record train sequence.

5. Click the **Actions** drop-down arrow and select **Trim Asset**.

   The **Confirm Trim** dialog opens.

6. Click **Trim** to trim the clip.

   You can see the new duration and the scissor icon within the RMI list to signify that it is a trimmed clip.



If you eject or reinsert the disk, mark points are lost.

Importing clips

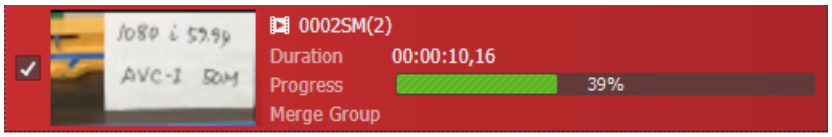
- RMI settings must be configured in the GV STRATUS Control Panel.
- If GV STRATUS security is enforced, you must have full read and write permissions to the destination.
- For RMI import with metadata mapping, you must have full read and write permissions to the mapped custom metadata.
- If quota is configured on the destination bin, ensure you have enough disk space before importing clips.

1. Check the box next to each clip that you want to import.

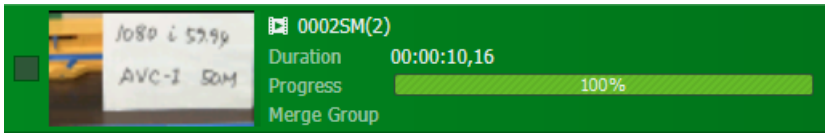
   You can also check the **Select All** button on the RMI toolbar to select all clips in the list.

2. Click the **Import** button.

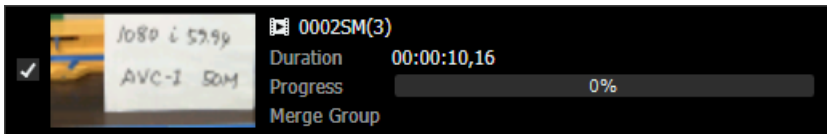
   If GV STRATUS security is enforced, the button is disabled if you do not have write permissions to the destination.



   While the import proceeds, you can see the clip row turns red, the progress bar grows, and the percentage number increases. Once the import is complete, the clip row turns green and the clip status changes from **Importing** to **Done**.



If the color of the clip row turns black, the clip fails to import.



You can view the **Error Message** column to check the cause of the failure.

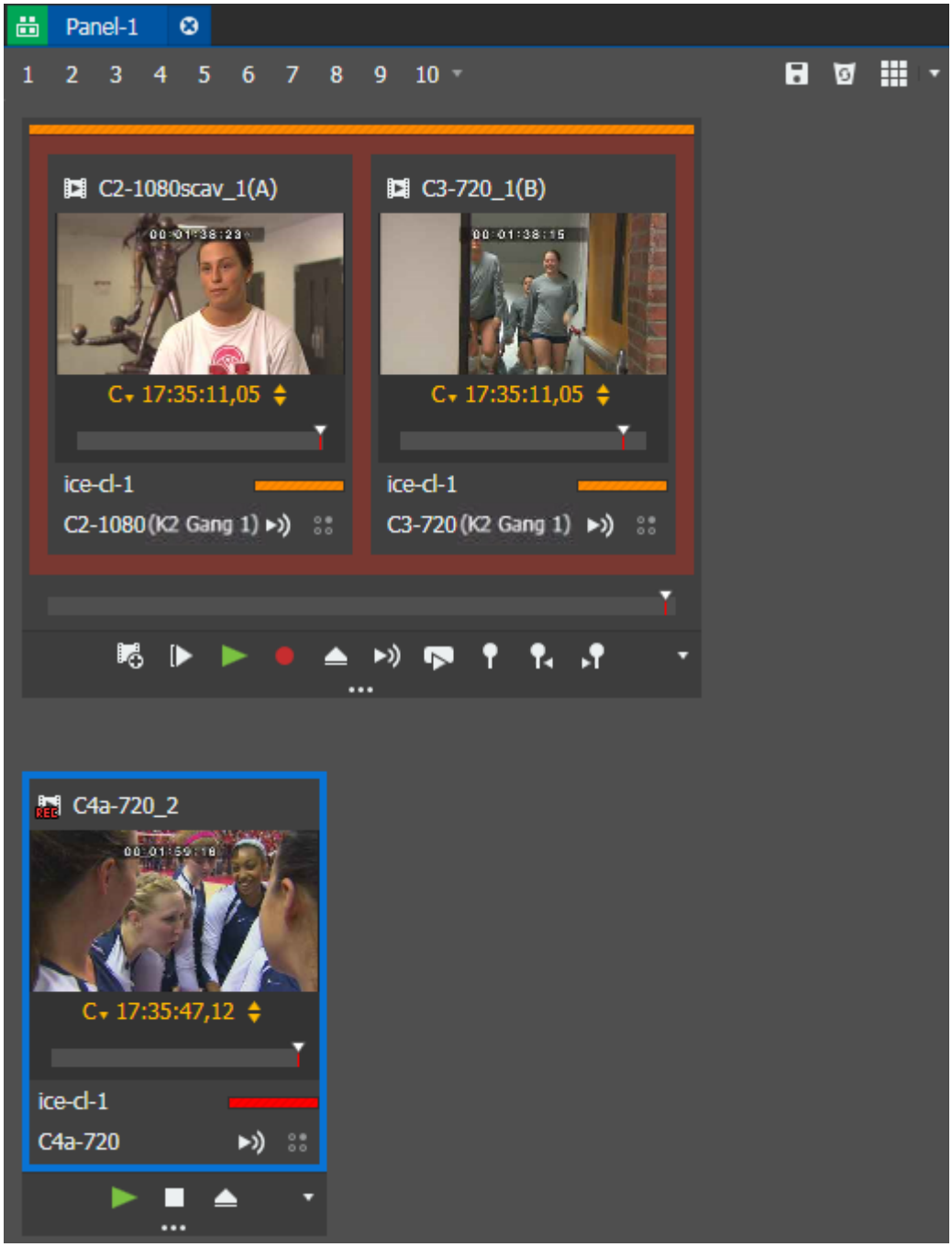
Related Topics

Troubleshooting tips on page 1403
RMI settings on page 396
Set up RMI PC access to high-resolution assets on page 557
Metadata Mapping Add/Modify Field settings on page 324
Permissions settings on page 321

Working with GV STRATUS Channels

The Channel Panel tool

A Channel Panel allows you to control one or more K2 system and GV I/O appliance channels. A Channel Panel appears in the GV STRATUS application as a tool when you launch it from the Navigator panel.



Channel Panel features are as follows:

- Ganged channels — Operate multiple channels simultaneously. The background color of the gang group identifies the gang. The channel name includes channel gang info, when the channel is a part of a K2 or GV I/O appliance gang.

- Transport controls — Controls a channel or a channel gang and adds markers to the loaded clip. A gang's transport controls affect the operations of all the channels in the gang simultaneously. Individual channels in a gang have overlay transport controls that can control the channel independent of the gang.
- Tally indicator — Indicates current operational status by colors, as follows:
  - **Red**: Recording
  - **Green**: Playing
  - **Orange**: Cued. Media is loaded and ready to play.
  - **Gray**: Idle. No media loaded.
- Toolbar — Provides buttons for access to panel functions.
- Asset type icon — Appears when an asset is loaded and indicates the type of asset.
- Single channel — Operates one channel.
- Scrub bar slider — Finds scenes quickly within a clip or playlist.
- Show/Hide transport controls — Shows or hides transport controls on a channel or a gang.

You can open multiple Channel Panels and use them simultaneously to suit your workflow needs.

If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets, and metadata that do not have read permissions are not visible. Markers and segments permissions must be set to **Allow** in order to create, update, or delete markers and segments.

Related Topics

Toggling between camera angles in Inspector and Channel Panel on page 1002

Channel Panel buttons

These buttons located on the Channel Panel toolbar let you perform various functions:

Salvo: Loads, creates, or removes a salvo.

Save: Saves the current settings. The settings are saved to the Channel Panel configuration.

Trash: Removes an item, such as a channel or production element, from the panel when you drag and drop the item on the icon.

View Mode: Controls the display and size of the items in a list or panel.

These transport control buttons let you control channels:

New Clip: Creates a new clip and allows you to name the clip before recording.

Cue Start: Cues to the beginning of the asset.

Record: Starts recording. Toggles with Stop button.

Stop: Stops recording. Toggles with Record button.

Play: Plays the clip. Toggles with the Pause button.

Pause: Pauses the play operation. Toggles with Play button.

Eject: Ejects the current asset.

These buttons located on the channels and gangs in the Channel Panel extend the functionality of controls:

Add Marker: Logs an item for the current position.

Go to Previous Marker: Goes to previous keyword/marker.

Go to Next Marker: Goes to next keyword/marker.

Hide Markers and Keywords: Hides marker and keyword indicators on the scrub bar.

Loop Playback: Loops the current asset between mark in to mark out.

Show/Hide Control Tray: Shows or hides the control tray.

Live Streaming Video: Enables/disables the display of the live video stream.

Live Streaming Audio: Enables/disables the audio of the live video stream.

Related Topics

Using mouse wheel for transport control on page 1144
Arranging control tray buttons on page 971

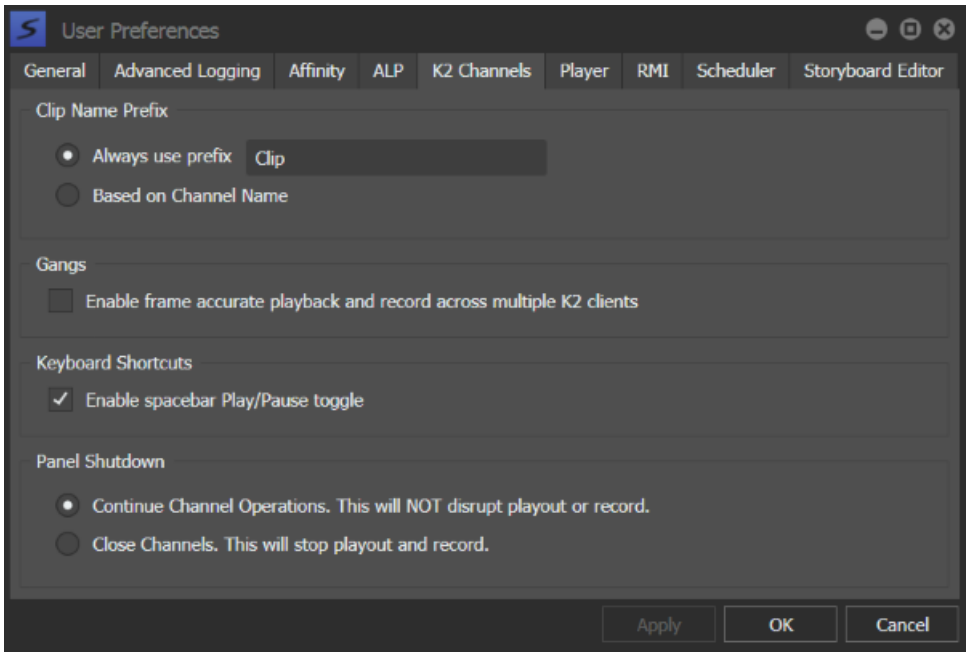
Configuring K2 Channels User Preferences

1. Select **Edit | User Preferences**.

   The User Preferences dialog box opens.

   The GV STRATUS application shows or hides sections based on the roles assigned to your GV STRATUS log on credentials.

2. To configure Channel Panel user preferences, select the **K2 Channels** tab.



3. To configure the default clip name prefix for new assets, do the following:

   - To add or modify the default clip name prefix for new assets, select **Always use prefix** and then enter your desired prefix.

     If you enter illegal characters, the **OK** and **Apply** buttons are grayed out.

     Tip: Use a short prefix if an asset's total pathname could be too long. You must limit the pathname to 150 characters or less. Asset and bin name limitations are described in a separate topic.

   - To use the channel name in the clip name prefix, select **Based on Channel name**.

   When the application applies a default clip name, if a clip already exists with the same name, the application appends a number to the end of the clip name prefix to ensure it is a unique name. This is done regardless of naming preference used.

4. To enable or disable frame accurate setting for ganged channels, configure the **Enable frame accurate playback and record across multiple K2 clients** check box. This setting applies only for gangs with channels from multiple K2 Summit systems. When enabled, there is a very slight pause when starting play/record operations as the GV STRATUS application synchronizes channels.

   Do not enable this frame accurate gang setting unless all K2 Summit systems have their time of day clocks set to a house LTC feed. This setting is in K2 AppCenter. If the frame accurate gang setting is enabled and K2 Summit systems are left at the default time of day setting of the Windows operating system clock, synchronization problems are likely, even if using a synchronization tool.

5. To enable or disable the play and pause function using the spacebar while playing an asset, configure the **Enable spacebar Play/Pause toggle** box.

   These settings apply to Channel Panel and Playlist Editor.

6. To configure the behavior of channel operations when you close a panel or the application, do the following:

   - To allow any record or play operations currently underway to continue, select **Continue Channel Operations**.
   - To stop any record or play operations currently underway, select **Close Channels**.

   These settings apply to Channel Panel and Playlist Editor panels.

7. To apply a change and continue editing user preferences settings, click **Apply**.
8. To accept any changes and close the dialog box, click **OK**.

   The dialog box closes.

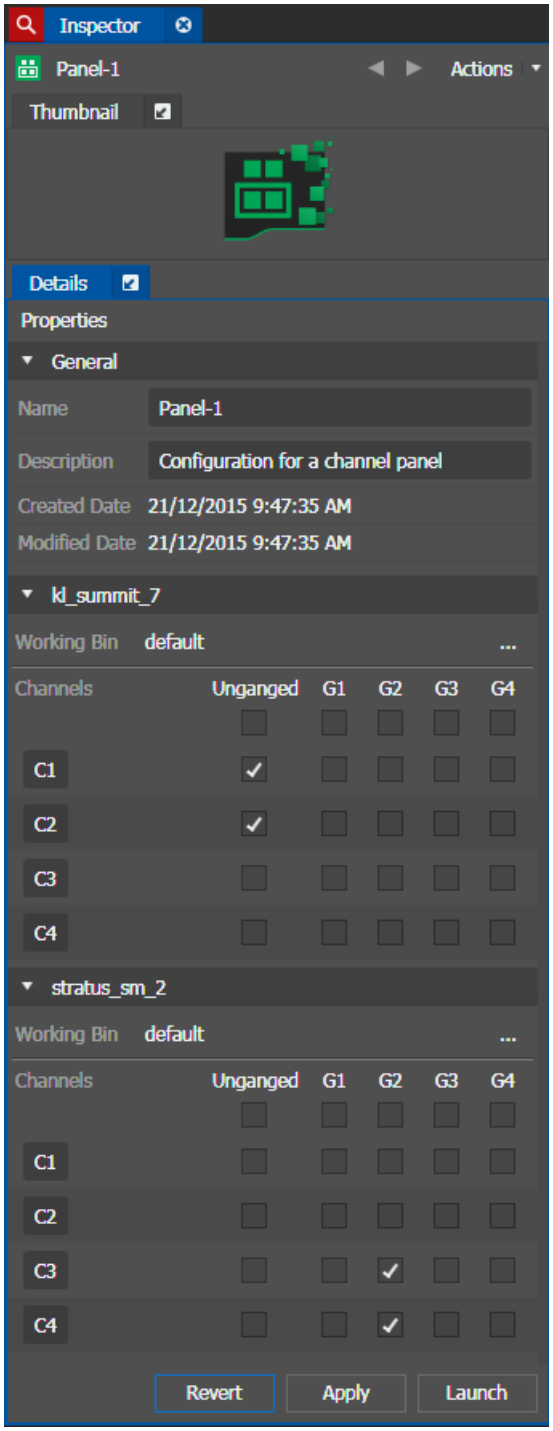
Related Topics

Limitations for creating and naming assets and bins on page 1428
Channel Panel ganging limitations on page 1097

Creating a Channel Panel

1. In the Navigator panel expand the **Tools** node, right-click **Channel Panels** and select **New Channel Panel**.

   The Channel Panel configuration is displayed in the Asset List and settings open in the Inspector panel.



2. On the **Properties** tab, enter a name and description for the Channel Panel you are creating.
3. Click the **Show/Hide** button to display each K2 system's or GV I/O appliance's channels as desired.
4. Select the working bin for the system as follows:
   a) Click the **Browse** button.
      A tree view section opens.
   b) Navigate the tree view and create or select the bin.
   c) Click **Apply**.
      The tree view section closes.

   The working bin applies to all the channels on the K2 Summit or GV I/O appliance system.

   NOTE: The working bin is set for all the channels from the same K2 Summit/SAN system or GV I/O appliance used in the Channel Panel.
5. Configure channels as follows:

   - To add channels to a gang, select channel checkboxes in the gang's column.
   - To add a channel as a single channel, select the channel checkbox in the **Unganged** column.
   - To add all channels to gang or as unganged, select the appropriate checkbox in the top row.
   - If desired, enter names for channels.

     These names are for display in the GV STRATUS application only.

     If a channel is configured on the K2 Summit system as a ChannelFlex channel, you can enter multiple names to identify the different ChannelFlex inputs and/or outputs.

   Settings are automatically saved as you configure.
6. To launch the Channel Panel from the Inspector panel, click **Launch**.

Related Topics

Limitations for creating and naming assets and bins on page 1428

Launching and closing a Channel Panel

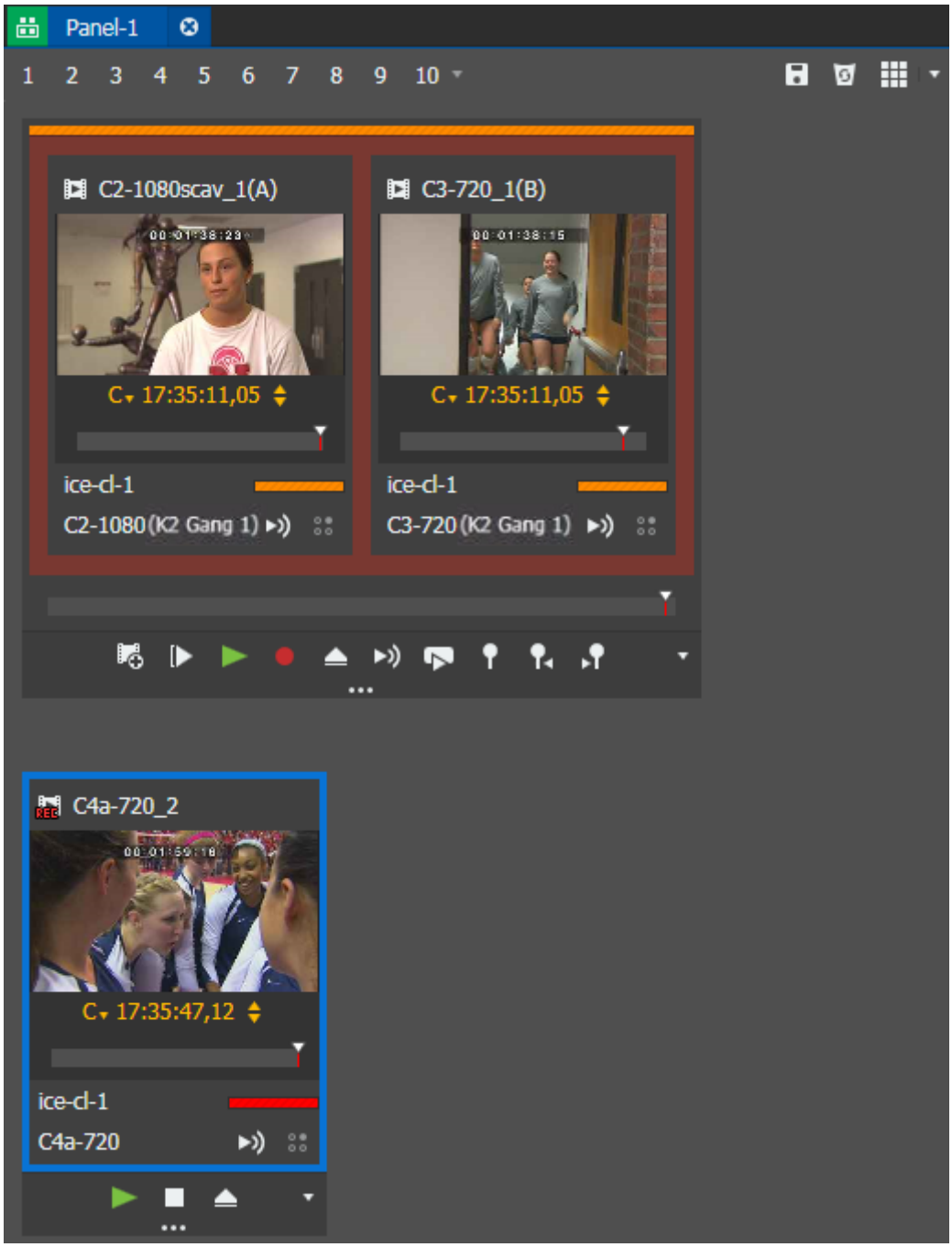
Launch a Channel Panel as follows:

1. In the Navigator, expand the **Tools** node and select **Channel Panels**.
   Your Channel Panel configuration is displayed in the Asset List.

2. Right-click the Channel Panel configuration and select **Launch**.

   The Channel Panel opens.

   NOTE: If a user on the* GV STRATUS *workstation is using Channel Panel, it is not recommended to log into EDIUS application as the same user on the same workstation.



3. To close the Channel Panel, click the **X** button on the title bar.

   The Channel Panel closes and one of the following occurs, based on Channel Panel user preferences:

   - Channel operations continue, which allows any record or play operations currently underway to continue.
   - Channels close, which stops any record or play operations currently underway.

Related Topics

Configuring K2 Channels User Preferences on page 1073

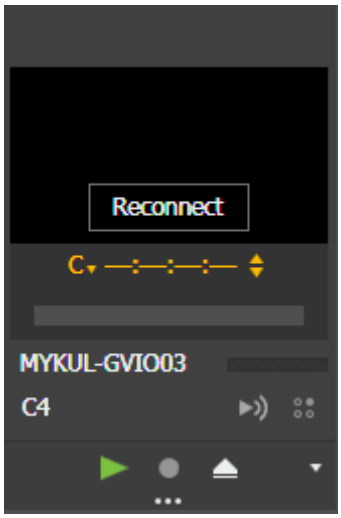
Modifying a Channel Panel while in use

After you have launched one or more Channel Panels, you can use drag and drop operations within a Channel Panel or between Channel Panels to change channels and gangs. You can do this while channel operations are underway.

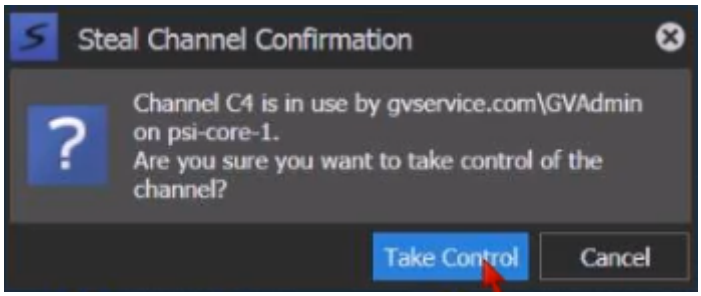
1. Click on the top bar of a channel and drag it as follows:

   - To create a gang, drag a single channel on top of another single channel. A gang opens that contains the two channels.
   - To remove a channel from a gang, drag the channel to a location outside of the gang. The channel becomes a single channel in the Channel Panel.
   - To remove a channel from the Channel Panel, drag the channel to the **Trash** button in the toolbar.
   - To add a single channel to a gang, drag the channel to the gang.
   - To remove a gang, drag all the channels in the gang to a location outside of the gang. When the last channel is removed from the gang, the gang is removed from the Channel Panel.

2. To take control of a channel, click **Reconnect**.



The Steal Channel Confirmation dialog opens.



3. Click **Take Control**.
4. To change the working bin, do the following:
   a) Right-click anywhere within the channel and select **Edit Working Bin**.
      The Channel Panel configuration opens in the Inspector and the working bin control expands.
   b) Select the working bin.
      NOTE: The working bin is set for all the channels from the same K2 system used in the Channel Panel.
5. Click the the **Save** button in the toolbar.
6. Click **OK**.
   This updates the current Channel Panel configuration with your changes.

If you close and then launch the Channel Panel your changes remain in effect.

Related Topics

Channel Panel ganging limitations on page 1097

Resizing channels and gangs

- To resize channels, in the Channel Panel toolbar identify the **View Mode** button and use it as follows:
  - Click the button to toggle between small, medium, and large size channels.
  - Click the drop-down arrow and select Small, Medium, or Large.
  - Click the drop-down arrow and drag the slider to the desired size.
- To resize a gang, drag the sides, bottom, or lower right corner of the Channel Panel window.

  Channels automatically align horizontally or vertically as you resize.

Modifying a Channel Panel configuration

You can use the Channel Panel configuration to change the channels included in a Channel Panel and the gangs to which they are assigned.

1. In the Navigator panel expand the **Tools** node and select **Channel Panels**.

   Your Channel Panel configuration is displayed in the Asset List.
2. Right-click the Channel Panel configuration and select **Open**.

   Channel Panel settings open.
3. Change settings as desired.
4. Do one of the following:
   - To save your changes when the Channel Panel is launched, click **Apply**. The changes take effect in the Channel Panel.
   - To save your changes when the Channel Panel is not launched, click **Launch**. The Channel Panel launches with the changes in effect.
   - To discard your changes, click **Revert**. The settings present when you opened the Channel Panel configuration are restored.

Copying a Channel Panel configuration

You can use the Channel Panel to copy a Channel Panel configuration.

1. In the Navigator panel expand the **Tools** node and select **Channel Panels**.

   Your Channel Panel configuration displays in the Asset List.
2. Right-click on the Channel Panel configuration and select **Copy**.
3. Right-click again on the Asset List and select **Paste**.

   The copy of the Channel Panel configuration displays in the Asset List.
4. If you want to rename the Channel Panel configuration, right-click on it and select **Rename**.

You can double-click the Channel Panel configuration to view its settings in the Inspector panel. After that, you can edit the channel configuration and save it by clicking the **Apply** button.

Related Topics

Creating a Channel Panel on page 1075
Launching and closing a Channel Panel on page 1076

About recording clips in a Channel Panel

You have the following options for recording clips:

- Crash Record — Start a recording without specifying a clip name. The GV STRATUS application gives the clip a default name based on User Preference settings.
- New clip — Create and name a clip before recording starts.

Indicators that the recording is underway are as follows:

- Timecode increments.
- Tally indicators display a red color.
- The clip thumbnail displays.

The function of the **Record** button toggles. While the channel is recording, clicking the **Stop** button stops the recording. While the channel is not recording, clicking the **Record** button begins recording.

When the channels in a gang are not on the same K2 Summit system, there can be a brief pause before the record operation begins.

If quota is configured on the K2 system bin, ensure you have enough disk space before recording starts.

It is recommended to set the quota on a destination bin to at least 2GB. Records will not begin if there is less than 1GB of free space remaining in the destination bin.

Refer to K2 system documentation for more details about recording clips.

Related Topics

Configuring K2 Channels User Preferences on page 1073

Recording on a single channel using crash record

- If quota is configured on the K2 system bin, ensure you have enough disk space before recording assets.
- It is recommended to set the quota on a destination bin to at least 2GB. Records will not begin if there is less than 1GB of free space remaining in the destination bin.

1. Launch a Channel Panel.

2. Click the **Record** button on a single channel. (**F12**)

   The following occurs:

   - The application creates a new clip and gives it a default name based on User Preference settings.
   - Recording begins on the channel.
   - The clip records to the current working bin.

While recording, if the bin in which a growing asset exists reaches its quota, the clip will be forced to stop recording but will remain in the bin.

Related Topics

Configuring K2 Channels User Preferences on page 1073

About keyboard shortcuts and input focus in a Channel Panel on page 1093

Recording on a single channel using new clip

- If quota is configured on the K2 system bin, ensure you have enough disk space before recording assets.
- It is recommended to set the quota on a destination bin to at least 2GB. Records will not begin if there is less than 1GB of free space remaining in the destination bin.

1. Launch a Channel Panel.
2. Right-click on the server/channel name and select **New Clip**.

   A New Clip dialog box opens.

3. Accept the default clip name or enter a clip name and then click **OK**.

   A new clip is loaded into the channel.

   You can configure the default clip name in User Preferences.

4. Click the **Record** button . (**F12**)

   The following occurs:

   - Recording begins on the channel.
   - The clip records to the current working bin.

While recording, if the bin in which a growing asset exists reaches its quota, the clip will be forced to stop recording but will remain in the bin.

Related Topics

Limitations for creating and naming assets and bins on page 1428

About keyboard shortcuts and input focus in a Channel Panel on page 1093

Configuring K2 Channels User Preferences on page 1073

Recording on ganged channels using crash record

- If quota is configured on the K2 system bin, ensure you have enough disk space before recording assets.

- It is recommended to set the quota on a destination bin to at least 2GB. Records will not begin if there is less than 1GB of free space remaining in the destination bin.

1. Launch a Channel Panel.
2. Click the **Record** button . (**F12**) on a gang.

   The following occurs:

   - The application creates new clips and gives them default names based on User Preference settings.
   - Recording begins on all channels in the gang.
   - The clips record to the current working bin.
   - The Channel Panel automatically assigns an **Angle** property for each clip.

While recording, if the bin in which a growing asset exists reaches its quota, the clips will be forced to stop recording but will remain in the bin.

Related Topics

Configuring K2 Channels User Preferences on page 1073

About keyboard shortcuts and input focus in a Channel Panel on page 1093

Recording on ganged channels using new clip

- If quota is configured on the K2 system bin, ensure you have enough disk space before recording assets.
- It is recommended to set the quota on a destination bin to at least 2GB. Records will not begin if there is less than 1GB of free space remaining in the destination bin.

1. Launch a Channel Panel.
2. Click the **New Clip** button on a gang.

   A New Clip dialog box opens.
3. Accept the default clip name or enter a clip name and then click **OK**.

   New clips are loaded into the gang channels.

   You can configure the default clip name in User Preferences.
4. Click the **Record** button. (**F12**)

   The following occurs:

   - Recording begins on all channels in the gang.
   - The clips record to the current working bin.
   - The Channel Panel automatically assigns an **Angle** property for each clip.

While recording, if the bin in which a growing asset exists reaches its quota, the clips will be forced to stop recording but will remain in the bin.

Related Topics

About keyboard shortcuts and input focus in a Channel Panel on page 1093

Configuring K2 Channels User Preferences on page 1073

Recording on an individual channel in a gang using crash record

- If quota is configured on the K2 system bin, ensure you have enough disk space before recording assets.
- It is recommended to set the quota on a destination bin to at least 2GB. Records will not begin if there is less than 1GB of free space remaining in the destination bin.

1. Launch a Channel Panel.
2. Double-click on the thumbnail of an individual channel in a gang.

   The overlay transport controls appear.
3. Click the **Record** button. (**F12**)

   The following occurs:

   - The application creates a new clip and gives it a default name based on User Preference settings.
   - Recording begins on the channel.
   - The clip records to the current working bin.

While recording, if the bin in which a growing asset exists reaches its quota, the clip will be forced to stop recording but will remain in the bin.

Related Topics

About keyboard shortcuts and input focus in a Channel Panel on page 1093

Recording on an individual channel in a gang using new clip

- If quota is configured on the K2 system bin, ensure you have enough disk space before recording assets.
- It is recommended to set the quota on a destination bin to at least 2GB. Records will not begin if there is less than 1GB of free space remaining in the destination bin.

1. Launch a Channel Panel.
2. Right-click on the thumbnail of an individual channel in a gang and select **New Clip**.

   A New Clip dialog box opens.
3. Accept the default clip name or enter a clip name and then click **OK**.

   A new clip is loaded into the channel.

   You can configure the default clip name in User Preferences.
4. Click the **Record** button. (**F12**)

   The following occurs:

   - Recording begins on the channel.
   - The clip records to the current working bin.

While recording, if the bin in which a growing asset exists reaches its quota, the clip will be forced to stop recording but will remain in the bin.

Related Topics

Limitations for creating and naming assets and bins on page 1428

About keyboard shortcuts and input focus in a Channel Panel on page 1093
Configuring K2 Channels User Preferences on page 1073

Recording on ChannelFlex channels

- If quota is configured on the K2 system bin, ensure you have enough disk space before recording assets.
- It is recommended to set the quota on a destination bin to at least 2GB. Records will not begin if there is less than 1GB of free space remaining in the destination bin.

When your K2 system channel is configured for ChannelFlex Multi-Cam, two record inputs are available for the channel.

1. Launch a Channel Panel that contains ChannelFlex channels, or add ChannelFlex channels to the Channel Panel.

   The timecode control, transport controls, and slider bar operate both record inputs at the same time.

2. Do one of the following record operations:

   - Record using crash record.
   - Record using new clip.

   Record operations are similar to those on a channel that is not configured for ChannelFlex.

A channel configured for ChannelFlex Multi-Cam is a record-only channel so you cannot load assets into the channel.

While recording, if the bin in which a growing asset exists reaches its quota, the clip will be forced to stop recording but will remain in the bin.

Related Topics

Recording on a single channel using crash record on page 1081
Recording on a single channel using new clip on page 1082

About playing clips in a Channel Panel

You have the following options for playing clips:

- Playback — Plays the clip once and stops at the end of the clip. You can do this on a single channel, on all the channels in a gang, or on an individual channel in a gang.
- Loop play — Plays the clip in a continuous loop until you manually stop the playout. You can do this on a single channel or on all the channels in a gang.

Indicators that playback is underway are as follows:

- Timecode increments.
- Tally indicators display a green color.
- The scrub bar slider moves from left to right.

The function of the **Play** button ▶ toggles. While the channel is playing, clicking the **Pause** button ⏸ stops the playback. While the channel is not playing, clicking the **Play** button ▶ begins playback.

When the channels in a gang are not on the same K2 Summit system, there can be a brief pause before the play operation begins.

Refer to K2 system documentation for more details about playing clips.

Related Topics

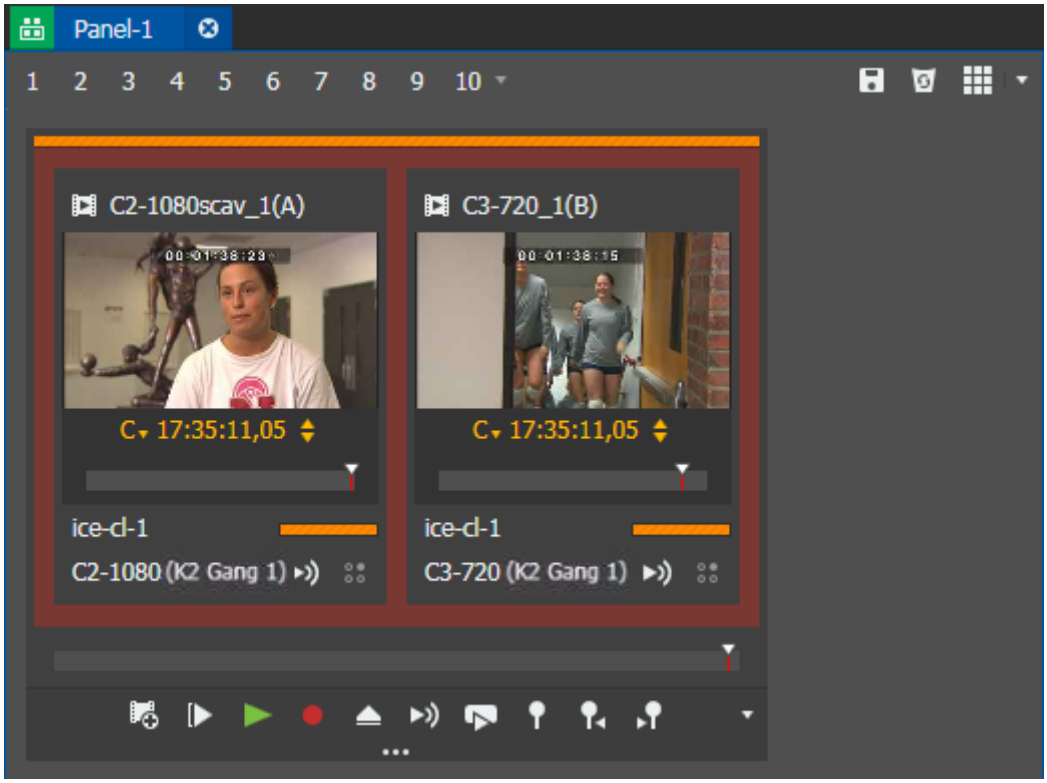
Using mouse wheel for transport control on page 1144

Loading an asset for playback in a Channel Panel

1. Launch a Channel Panel.
2. In the Navigator panel, select the bin containing the asset to play.
   The asset appears in the Asset List.

3. Do one of the following:

   - To load the asset into a single channel, drag the asset from the Asset List to a channel's thumbnail display area. You can do this on a single channel or on a channel that is part of a gang.
   - To load the same asset into multiple channels of a gang, drag the asset from the Asset List to the gang background or to the gang tally indicator. The channel name includes K2 gang info, when the channel is a part of a K2 gang.
   - To load the asset that is in one channel into another channel, drag the asset type icon from one channel to another.



The mouse pointer displays a no-drop icon for channels that are incompatible with the clip's video standard or format.

The following occurs:

- The asset is loaded on the channels that have access to the asset. If a gang includes channels from multiple K2 systems that have separate storage, the asset loads on the channels from those K2 systems that contain the asset in their storage. The asset does not load on channels from K2 systems that do not contain the asset.
- Each loaded channel displays a thumbnail of the media.
- Tally indicators display an orange color to indicate that media is cued up and ready to play.

Related Topics

Locating a loaded clip or playlist on page 1091

Playing a clip on a single channel

1. Launch a Channel Panel.
2. Load an asset into a channel so that it is cued up and ready to play.
3. Click the **Play** button. (**W**)

   Playback begins on the channel.

Related Topics

Loading an asset for playback in a Channel Panel on page 1086
About keyboard shortcuts and input focus in a Channel Panel on page 1093

Playing clips on ganged channels

1. Launch a Channel Panel.
2. Load assets into channels so they are cued up and ready to play. You can load the same asset on all channels or load different assets on individual channels.
3. Click the **Play** button. (**W**)

   Playback begins on the channels in the gang.

Related Topics

Loading an asset for playback in a Channel Panel on page 1086
About keyboard shortcuts and input focus in a Channel Panel on page 1093
Channel Panel ganging limitations on page 1097

Playing ganged clips and camera angles on a single channel

1. Launch a Channel Panel.
2. Load a ganged recorded asset or a clip that is part of a K2 Dyno camera angle set into a channel so that it is cued up and ready to play.
3. Click the **Play** button. (**W**)

   Playback begins on the channel.

4. On the player, hover your mouse pointer on the top right of the asset.

   The **Camera Angle** selector overlay displays.

   NOTE: You can only toggle between angles for playback of ganged recorded assets or K2 Dyno camera angle assets.

5. Select the desired angle on the overlay display.

   The clip of the selected angle displays.

   You can also toggle camera angles of audio only assets. The player displays thumbnail of the audio only asset, and the **Camera Angle** selector overlay displays available angles that you can select.

Related Topics

Toggling between camera angles in Inspector and Channel Panel on page 1002
Browsing camera angles on page 977

Playing a clip on a single channel in loop play

1. Launch a Channel Panel.
2. Load an asset into a channel so that it is cued up and ready to play.
3. Click the **Loop Playback** button.

   The channel is now cued in loop play mode, as indicated by the highlighted loop play button.
4. Click the **Play** button. (**W**)

   Loop play begins on the channel. When the clip reaches its end, it automatically starts to play again from its beginning.
5. Control loop play as follows:
   - To pause loop play, click the **Pause** button.
   - To resume loop play, click the **Play** button. When loop play restarts it begins at the point from which it stopped.
   - To stop loop play when it reaches the end of the clip, click the **Loop Playback** button. Playout continues normally and stops at the end of the clip.

Spacebar = Play/Pause. Toggles between play and pause.

Related Topics

About keyboard shortcuts and input focus in a Channel Panel on page 1093
Configuring K2 Channels User Preferences on page 1073

Playing ganged channels in loop play

1. Launch a Channel Panel.
2. Load assets into channels so they are cued up and ready to play. You can load the same asset on all channels or load different assets on individual channels.
3. Click the **Loop Playback** button.

   The gang is now cued in loop play mode, as indicated by the highlighted loop play button.
4. Click the the **Play** button. (**W**)

   Loop play begins on the channels. When each clip reaches its end, it automatically starts to play again from its beginning.

5. Control loop play as follows:
   - To pause loop play, click the **Pause** button.
   - To resume loop play, click the **Play** button. When loop play restarts it begins at the point from which it stopped.
   - To stop loop play when it reaches the end of the clip, click the **Loop Playback** button. Playout continues normally and stops at the end of the clip.

   Spacebar = Play/Pause. Toggles between play and pause.

Related Topics

About keyboard shortcuts and input focus in a Channel Panel on page 1093
Configuring K2 Channels User Preferences on page 1073
Channel Panel ganging limitations on page 1097

Toggling between camera angles in Inspector and Channel Panel

If a clip is a part of a K2 Dyno camera angle set or a GV STRATUS gang record set, in Inspector player and in Channel Panel player you can toggle between the associated clips in the set.

1. On the player, hover your mouse pointer on the top right of the asset.

   The **Camera Angle** selector overlay displays.

   NOTE: You can only toggle between angles for playback of ganged recorded assets or K2 Dyno camera angle assets.

2. Select the desired angle on the overlay display.

   The clip of the selected angle displays.

   You can also toggle camera angles of audio only assets. The player displays thumbnail of the audio only asset, and the **Camera Angle** selector overlay displays available angles that you can select.

Related Topics

Browsing camera angles on page 977

Controlling an individual channel in a gang

1. Launch a Channel Panel.
2. If desired, begin a record or a play operation on the gang.
3. Double-click on the thumbnail of an individual channel in the gang.

   The overlay channel transport controls appear.
4. Use the overlay channel transport to control the channel as desired.

   You can stop a play operation and then use the scrub bar to navigate to a location in the clip.

5. Consider the following when controlling an individual channel in a gang:

   - Operating the individual channel does not affect the ongoing operation of the gang.
   - When you pause and then resume playback on an individual channel, playback starts at the point it was stopped. The channel does not re-sync with the ongoing playback of the other channels in the gang.

   The individual channel's tally indicator displays the color that indicates its current operational status.

Related Topics

Channel Panel ganging limitations on page 1097

Locating a loaded clip or playlist

In Channel Panel or Playlist Editor, if you want to quickly access the location of the currently loaded clip or playlist, the GV STRATUS application can show you the location.

1. Identify the K2 Summit system name and channel name in the lower left section of the channel.
2. Click in the section in one of the following ways:

   - Double-click in the section.
   - Right-click and select **Locate Playlist** or **Locate Clip**.

The GV STRATUS application shows the location as follows:

- In the Navigator panel the bin that contains the clip or playlist is selected.
- The bin's Asset List opens with the clip or playlist selected.

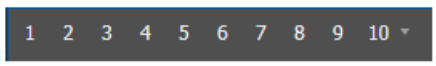
About salvos

A salvo is a pre-defined set of clips to load into the channels of a Channel Panel. You can use a salvo when you repeatedly set up the same channels to play the same clips as part of your show.

The salvo is saved as a part of the Channel Panel configuration. One Channel Panel configuration can have ten saved salvos.

Creating a salvo

1. Load clips in the channels of your Channel Panel.
2. Identify the salvo buttons in the Channel Panel toolbar.



3. Determine the salvo button to use for your new salvo as follows:
   a) Identify buttons with numbers that are a lighter color (not bold). These buttons do not have a salvo assigned.
   b) Hover your mouse pointer over a salvo button.

      A tooltip displays the salvo name or "Unassigned".

4. Right-click the salvo button and select **Create Salvo**.
   A dialog box opens and prompts for a salvo name.
5. Enter the name of the salvo and then click **OK**.
   The application displays this name as a tooltip to identify the salvo button.
   The salvo is saved as part of the Channel Panel configuration.

You must save the Channel Panel configuration to save the new salvo.

Loading a salvo

1. Identify the salvo to load by hovering your mouse pointer over a salvo button.
   A tooltip displays the salvo name.
2. Click the **Salvo** button. 1
   The clips load into the channels.

Deleting a salvo

1. Identify the salvo to delete by hovering your mouse pointer over a salvo button.
   A tooltip displays the salvo name.
2. Right-click on the salvo's button and select **Remove Salvo**.

The salvo button now has no salvo assigned.

You must save the Channel Panel configuration to save the salvo button with no salvo assigned.

Modifying a salvo

1. Identify the salvo to modify by hovering your mouse pointer over a salvo button.
   A tooltip displays the salvo name.
2. Click the **Salvo** button 1 to load the salvo, if it is not already loaded.
3. Eject or load clips to modify the salvo.
4. Right-click the salvo button and select **Create Salvo**.
   A dialog box opens and prompts you for a salvo name.
5. Click **OK**.
   Do not change the salvo name, so your modifications overwrite the salvo.
   The modified salvo is saved as part of the Channel Panel configuration.

You must save the Channel Panel configuration to save the modified salvo.

Configure router settings in Channel Panel

Before doing this task, make sure that in GV STRATUS Control Panel your router connection settings are configured.

You can set the router source and destination for a channel in a Channel Panel, and save the setting with the Channel Panel configuration.

1. Launch a Channel Panel.
2. Identify the channel for which you are making router settings.

   You can make router settings for a channel in a gang or for a channel not in a gang.
3. Right-click the channel and select **Router Settings**.

   The **Router Settings** dialog box opens.
4. Configure router settings as follows:

   - **Source**: The feed coming into the router, such as from a camera.
   - **Destination**: The port coming out of the router, connecting to the K2 system channel.
5. Click **OK** to save settings and close.
6. Repeat steps to configure router settings on other channels in the Channel Panel as desired.
7. Click the the **Save** button in the toolbar.
8. When prompted to confirm, click **Replace**.

   This updates the current Channel Panel configuration with your changes.

The next time you launch the Channel Panel, channels have routers already configured. To determine a channel's router settings, repeat steps to open the **Router Settings** dialog box. Router settings are not displayed in Channel Panel configuration.

About keyboard shortcuts and input focus in a Channel Panel

A keyboard shortcut takes effect for the channel or gang with the input focus. You must make sure that the channel or gang that you want to control has the input focus before you use a keyboard shortcut.

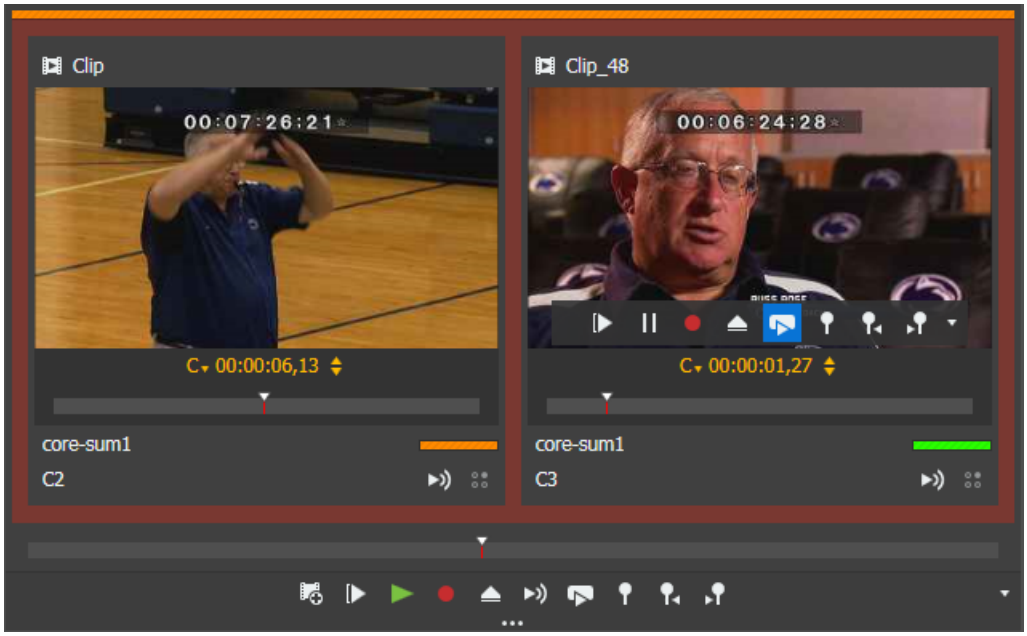
A blue border indicates the channel or gang with the input focus.

You can give a channel or gang the input focus as follows:

- To give a gang the input focus, click once anywhere on the gang.
- To give a single (un-ganged) channel the input focus, click once anywhere on the channel.

For an individual channel in a gang, an input focus is not indicated by a blue border.

- To give an individual channel in a gang the input focus, double-click on the channel. This also displays the overlay transport controls for the channel in focus.



Related Topics

Channel Panel keyboard shortcuts on page 1407

Modifying the clip name in a Channel Panel

You can change the name of the clip currently loaded in a channel.

1. Press the **Alt** key and click on the clip name at the top of the channel.
2. Type in the new name for clip.

   The name must conform to asset and bin name limitations.

   The name change must not be a change in capitalization only.
3. Press **Enter** or **Tab** or click anywhere outside of the clip name to put the change into effect.

Related Topics

Limitations for creating and naming assets and bins on page 1428

Loading an asset into the Inspector from a Channel Panel

1. Load an asset into a channel, if not already loaded.

2. Identify the asset type icon on the channel and do one of the following:
   - Double-click the icon.
   - If the Inspector panel is open, drag the icon to the Inspector.

   The asset opens in the Inspector panel.

Using the scrub bar to navigate through a clip

You can use the scrub bar to navigate through clips in ganged channels, single channels, and individual channels in a gang.

- Drag the scrub bar slider to navigate through the clip.
- Click at any point along the scrub bar to jump the slider to that location in the clip.

Related Topics

Using mouse wheel for transport control on page 1144

Identifying and selecting the timecode type

Where timecode is displayed, you can view and change the timecode type.

1. To identify the timecode type, interpret the label next to the timecode display as follows:

C	Current Timecode
I	Mark In
O	Mark Out
D	Duration
E	Elapsed
R	Remaining
d	Marked Duration
r	Remaining to Mark Out
e	Elapsed from Mark In

2. To change the timecode type, right-click the timecode display or label and select the type of timecode.

Selecting timecode type to navigate and mark clips

You can use the timecode display to navigate and mark clips in single channels, and individual channels in a gang.

1. On the timecode display, select one of the following timecode types:

   - **C**: Current Timecode
   - **I**: Mark In
   - **O**: Mark Out
   - **D**: Duration
   - **d**: Marked Duration

   You cannot navigate or set marks using the following timecode types.

   - Elapsed
   - Elapsed from Mark In
   - Remaining
   - Remaining to Mark Out

2. **Alt + Click** on the timecode display.

   Timecode goes into edit mode, as indicated by the up/down buttons.

3. Do one of the following:

   - Enter time code values.
   - Click up/down buttons to go to your desired timecode position.

4. Press **Enter** or click outside the timecode display.

   The playback point moves to the specified timecode, as indicated by the scrub bar. If timecode type is mark in or mark out, marks are set at the specified timecode. If timecode type is duration, the mark out point is set.

Channel panel markers

When you add a marker to a clip in a Channel Panel, behavior can vary depending on the state of the clip and if the channel is in a gang.

If the clip is currently recording, the marker is added and appears on the scrub bar. As the clip continues to record and its length increases, the marker moves to the left on the scrub bar, as its position relative to the end of the clip changes.

You can add a marker to a clip in an individual channel. This includes an individual channel that is not in a gang as well as an individual channel that is in a gang. If you add a marker to a clip in an individual channel that is in a gang, the marker is not applied in the other clips in the gang and it does not appear on the gang scrub bar.

In order to add a marker to a gang and have the marker applied to all the clips in the gang simultaneously, the gang must be as follows:

- All channels must be recording, all channels must be cued, or all channels must be playing.

- All the clips in the gang must be of the same length.
- Recording channels must have started at the same timecode value.
- Cued channels must have the same starting and ending timecode values.

Also, it is strongly recommended that all channels be frame accurate and use the same timecode source.

If you start your ganged channels recording as one gang record and as long as all the clips continue to be same length during the recording process, you can add a gang marker to all the clips in the gang. These markers appear on the individual channel scrub bar and on the gang scrub bar.

If the clips in a gang are not the same length, you cannot add a marker to the gang. This occurs if you start/stop recordings of individual channels in the gang or if you cue already recorded clips of different length/timecode into the gang.

If you load a ganged clip into the Inspector panel and add a marker there, the marker appears on that individual channel's scrub bar in the gang. However, that marker does not appear on the gang scrub bar, since the marker was not added to the gang.

Related Topics

Adding markers on page 1146

Navigating to keywords or markers in an asset on page 1150

Hiding transport controls

- You can show/hide transport controls on a gang or a single channel by clicking the **Show/Hide Control Tray** button. ... This opens the control tray.
- You can show/hide transport controls on an individual channel in a gang by double-clicking in the thumbnail display area.

Managing Channel Panel configurations

1. In the Navigator panel expand the **Tools** node and select **Channel Panels**.

   Your Channel Panel configuration displays in the Asset List.

2. In the Asset List, right-click the Channel Panel configuration and do the following:

   - To delete the Channel Panel configuration, select **Delete**.
   - To open the Channel Panel configuration in the Inspector panel, select **Open With | Inspector**.
   - To launch the Channel Panel, select **Launch**.

Related Topics

Channel Panel ganging limitations on page 1097

Channel Panel ganging limitations

The following limitations apply to ganging in the Channel Panel tool.

- For frame accurate playback, all K2 Summits must have the Time of Day (TOD) set to an LTC input and all channels must have the same TOD timecode source.

- On each K2 Summit client, the channel that has the LTC TOD input on it should be used exclusively for playout or record, not both. (Switching between record and play can cause a disruption in the TOD source, which can impact scheduled operations for all channels on the device.)
- Do not daisy-chain the LTC TOD source between K2 Summits, i.e. have a LTC output from one K2 summit connected to a LTC input of another K2 Summit. (This can result in the TOD for downstream K2 Summits falling slightly behind.)
- If K2 Summits have LTC inputs that are daisy-chained, all subsequent K2 Summits in the daisy-chain can have the TOD affected for a few seconds as well.
- The first and last K2 Summits that are LTC daisy-chained can be off by a field or frame if the daisy-chain exceeds ~5 or more K2 Summit devices.

Channel status indicators

The application displays icons with messages in a channel's thumbnail area to indicate the current status of the channel, as follows:

Icon	Status
	Normal, no clip loaded.
	Warning
	Error

Reconnecting channels

If status indicators report that a channel is no longer connected to a K2 or GV I/O appliance system, you can trigger the channel to reconnect.

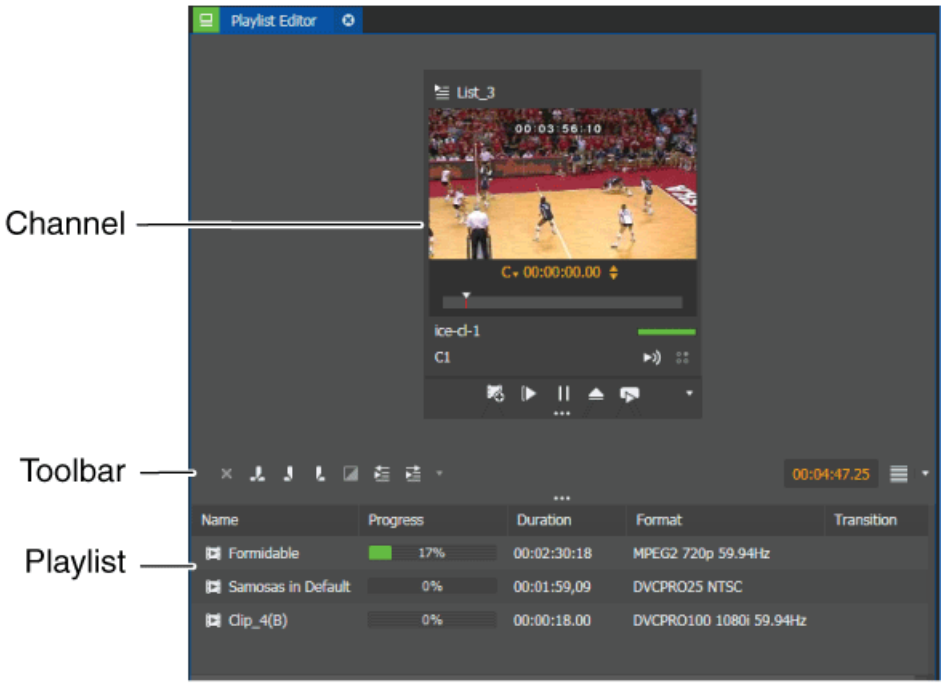
1. In the Channel Panel, identify the disconnected channel as indicated by the channel status indicator and message in the channel's thumbnail area.
2. Click the **Reconnect** button.

   One of the following occurs:

   - If Channel Panel failed to connect to the server, the channel connects to the K2 or GV I/O appliance system. Other channels in the Channel Panel attempt to reconnect as well, if those channels were previously connected to that same system.
   - If the channel is currently owned, an "...Are you sure...?" message appears and provides information about the user and system that currently owns the channel. Click **Yes** to disconnect the current owner and connect to the K2 or GV I/O appliance system.

The Playlist Editor tool

The Playlist Editor allows you to assemble and edit a Playlist. You can launch the Playlist Editor as a panel from a bin, from an Asset List, and the tool section of the Navigator panel.



You can drag assets into the panel to create or add to a Playlist. Assets in the panel are called *events*.

The panel has the following features:

- Channel — Controls a K2 system channel for playback of lists.
- Toolbar — Performs operations on events in the list.
- Playlist — Displays events and allows editing of events.

If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets, and metadata that do not have read permissions are not visible. Markers and segments permissions must be set to **Allow** in order to create, update, or delete markers and segments.

Editor Panel buttons

These buttons located on the toolbar let you perform various functions:

Delete: Deletes the selected item or items. Disabled if delete rights denied in GV STRATUS Control Panel.

Split: Splits the item at the current position.

Trim In: Trims the start of the event at the current position.

Trim Out: Trims the end of the event at the current position.

Add Transition: Adds a transition to the event.

Show/Hide Transition Panel: Edit current transition settings

Go to Previous: Goes to the previous transition in the playlist or sequence.

Go to Next: Goes to the next transition in the playlist or sequence.

These transport control buttons let you control the channel:

New Playlist: Creates a new playlist.

Cue Start: Cues to the beginning of the asset.

Play: Plays the clip. Toggles with the Pause button.

Pause: Pauses the play operation. Toggles with Play button.

Eject: Ejects the current asset.

These buttons located on the channel extend the functionality of transport controls:

Loop Playback: Loops the current asset between mark in to mark out.

Hide Markers and Keywords: Hides marker and keyword indicators on the scrub bar.

Show/Hide Control Tray: Shows or hides the control tray.

Live Streaming Video: Enables/disables the display of the live video stream.

Live Streaming Audio: Enables/disables the audio of the live video stream.

Related Topics

Using mouse wheel for transport control on page 1144
Arranging control tray buttons on page 971
Adding and removing transitions on page 1159

About playlists and sequences

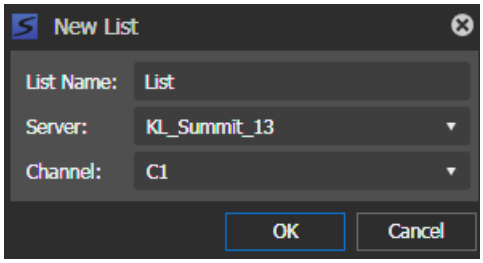
You can create or modify playlists and sequences as follows:

- The Playlist Editor creates and modifies playlists. When you use the Playlist Editor you are online, which means you are using a K2 system channel for the playlist. A playlist is always an asset in K2 storage and is saved automatically as you modify it.
- The Storyboard Editor creates and modifies sequences. When you use the Storyboard Editor you are offline, which means you are not using a K2 system channel. You can save the sequence as a playlist into K2 storage and play it on a K2 system channel.

Creating a playlist

1. Open the Playlist Editor as follows:
   a) Do one of the following:
      - Right-click a bin on the K2 Summit system and select **New | Playlist**.
      - Right-click in the empty space of an Asset List and select **New | Playlist**.
      - Select an asset or select multiple assets (Ctrl + Click) in an Asset List and then right-click and select **New | Playlist from Clips**. When you use this option assets are added to the playlist in the order selected.

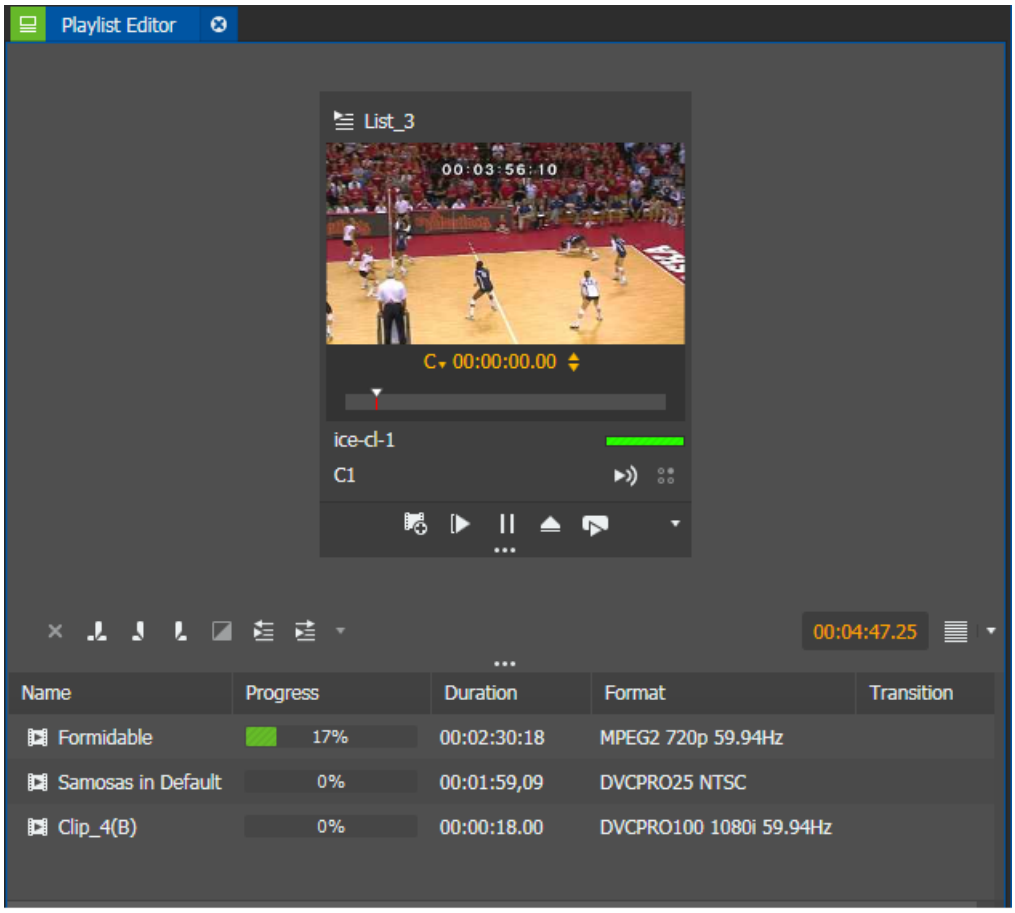
      A New List dialog box opens.



   b) Enter the name of your playlist and select the K2 system and channel on which you are creating your playlist, then click **OK**.
      The Playlist Editor opens.
2. In a K2 bin in Asset List , select an asset and drag it to the Playlist Editor panel.
   The asset displays.

   If needed, you can also drag it to the Inspector panel.
3. To preview the asset, click the **Play** button or use the appropriate transport controls.

4. Drag the asset if you want to rearrange the playlist in the lower section of the Playlist Editor.



The asset is now referred to as an *event* in the Playlist.

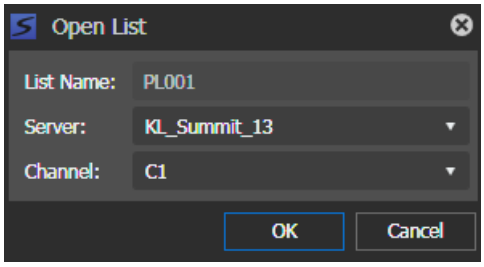
NOTE: If you leave the asset loaded in the* Inspector *and make additional changes, such as changing the mark-in or mark-out points, these changes are not reflected in the* Playlist Editor *unless you drag the asset to the* Playlist Editor *again.

5. Repeat above steps to add additional events.
6. In the panel, use the toolbar buttons to modify events.

To play the Playlist, use the transport controls in the Playlist Editor's channel.

Opening a Playlist

1. In an Asset List, right-click on a playlist and select **Open With | Playlist Editor**.
   The Open List dialog box opens.



2. Select the K2 system and channel on which to open the playlist.
3. Click **OK**.
   The Editor Panel opens.

After opening the playlist, use the toolbar buttons to modify events and transport controls to control playback in the Playlist Editor's channel.

Loading a playlist into the Playlist Editor

1. From an Asset List, drag a playlist into the Playlist's channel.
   The playlist loads into the Playlist Editor.

   If the Playlist Editor was previously loaded with a different playlist, the playlist you drag in replaces the previous playlist.
2. After loading the playlist, use the toolbar buttons to modify events and transport controls to control playback in the Playlist Editor's channel.

Related Topics

Locating a loaded clip or playlist on page 1091

Rearranging or deleting events in a playlist

Select the event in the panel and choose one of the following actions:

- To delete the selected event, click the **Delete** button.
- To move the selected event, drag the event to a new location in the panel.

There is no Undo feature for these operations.

Splitting an event

1. Navigate to the desired location in the event.
2. Select the **Split** button.

The event is divided into two events with identical names.

There is no Undo feature for these operations.

Importing, Exporting, and Transferring

About importing, exporting, and transferring

This section defines the different terms used when transferring files or assets to or from Grass Valley systems or between Grass Valley devices.

- Import — copy files from a file system to a Grass Valley system.
- Export — copy assets from a Grass Valley system to a folder on a network drive.
- Transfer — move or copy assets within or between Grass Valley devices.
- Remote transfer — copy all or part of an asset from a remote site to the local site.

Creating an export share

This procedure provides a share on a GV STRATUS client PC so that you can use the drive as a destination for export from the GV STRATUS application.

1. On a GV STRATUS client PC, create a folder to be used for the export from the GV STRATUS application. For example, create the folder *C:\STRATUSExport*.
2. Access the folder's properties and share the folder.
3. Make sure that permissions are set to allow read and write access to the internal system account, which by default is GVAdmin.

   If the GV STRATUS client PC is on a domain, it should have the internal system account, which by default is GVAdmin. If not, create the account.

You can now use the share as a destination for export from the GV STRATUS application.

Importing files to a Grass Valley system

- If importing from a folder on the GV STRATUS client PC C: drive, the drive must be a network-mapped C$.
- File format must be supported for import to the Grass Valley system.
- If quota is configured on the K2 system destination bin, ensure you have enough disk space before importing clips.
- It is recommended to set the bin quota to at least 2GB for the destination bin. You are not allowed to begin importing into a bin if there is less than 1GB of space remaining in that bin.

You can import files to a Grass Valley system through a context menu in the Navigator panel, send assets from a network-mapped drive to a bin on a Grass Valley system, or drag and drop assets directly into a folder.

This procedure describes using the context menu.

1. In the Navigator panel, select the source folder on the network-mapped drive.

2. Right-click on the asset or assets that you want to import and select the appropriate command:
   - **Copy To** or **Copy/Paste** — Copies the asset or assets, leaving the original in the source folder.
3. Select the destination bin, and click **OK**. If the destination bin is grayed out, it is not a valid destination.

   The transfer is initiated. If transferring multiple assets, transfer jobs are queued.
4. To monitor the status of the transfer, open the Jobs List.

   While transferring, if the destination quota is reached, the transfer job will fail gracefully in the Jobs Monitor and the partial asset will be deleted from the destination.

   NOTE: Due to Microsoft Windows limitations, files and directories from network shares are not updated automatically.

Related Topics

Formats supported for import and export on page 1429
Creating an export share on page 1104
Monitoring imports, exports, or transfers on page 1115

Exporting assets from a K2 Summit system

- If exporting to a folder on the C: drive, the drive must be a network share allowing read and write access to the internal system account, which by default is GVAdmin.

In the Navigator panel, you can export assets through a context menu, or by dragging and dropping the assets, from a Grass Valley system bin to a network-mapped drive. This procedure describes using the context menu.

1. In the Navigator panel, select the source bin on the K2 system.
2. Right-click on the asset or assets that you want to export and select the appropriate command:
   - **Copy To** or **Copy/Paste** — Copies the asset or assets, leaving the original in the source folder.
3. Select the destination bin, and click **OK**.

   To export, you can also drag and drop assets into the destination bin.

   The Export Options dialog box displays.
4. Use the drop-down arrow to select the export format and click **OK**.

   The export is initiated. If exporting multiple assets, transfer jobs are queued.
5. To monitor the status of the export, open the Jobs List.

Related Topics

Formats supported for import and export on page 1429
Creating an export share on page 1104
Monitoring imports, exports, or transfers on page 1115

Transferring between bins using drag and drop

- If quota is configured on the K2 system bin, ensure you have enough disk space before transferring assets.

You can move and copy assets to and from bins on a Grass Valley system. You can drag and drop the assets from one bin to another, or you can use the context menu. To move or overwrite (delete) an asset, you must be assigned with **Move Rights**, **Delete Rights** or the **Media Manager** role in GV STRATUS Control Panel. If not assigned, menu selections and operations are disabled. Where appropriate, the copy operation is substituted for the move operation.

1. In the Navigator panel, select the source bin on the Grass Valley system.
2. To transfer with drag and drop, do the following:
   a) In the Navigator panel, expose the destination bin on the Grass Valley system.
   b) Select one or more assets.

      NOTE: You can also select an asset that is still recording.

   c) Drag the asset or assets from source to destination bin.

      Cursor indicators identify a move, copy, or disallowed operation. By default, assets are moved. If the move operation is not allowed, only the copy operation is available.

   d) If both move and copy are available, you can hold down a modifier key to specify the desired operation:

      - **Shift**: Move
      - **Ctrl**: Copy

   e) Drop the asset or assets on the destination bin.
3. If prompted by a **Rename Policy** dialog box, do the following:
   a) Specify the rename or overwrite behavior if the assets exists.

      NOTE: The rename policy will not rename the logical asset with multiple hi-res associations. Only the new hi-res association will be renamed.

      This behavior applies when you transfer a single asset or multiple assets.

      To overwrite an asset, you must be assigned **Move Rights**, **Delete Rights**, or the **Media Manager** role in GV STRATUS Control Panel. If not assigned, selections are disabled.

   b) If you want this behavior to apply to all transfer operations in the future without being prompted, select the **Do not ask again** box.

      User Preferences allows you to reset hidden windows to display the **Rename Policy** dialog box again.

   c) Click **OK**.

   The **Rename Policy** dialog box is available only if you have the **Rename Asset Rights**, **Delete Rights**, or the **Media Manager** role.
4. If prompted by a **Security** dialog box, configure security options as desired, then click **OK**.

   The **Security** dialog box is available only if you have the role of Security Manager or you are the Owner.

The transfer is initiated. If transferring multiple assets, transfer jobs are queued.

To monitor the status of the transfer, open the Jobs List.

While transferring, if the destination quota is reached, the transfer job will fail gracefully in the Jobs Monitor and the partial asset will be deleted from the destination.

Transferring assets between bins using the context menu

- If quota is configured on the K2 system bin, ensure you have enough disk space before transferring assets.

You can move and copy assets to and from bins on a Grass Valley system. You can drag and drop the assets from one bin to another, or you can use the context menu. To move or overwrite (delete) an asset, you must be assigned with **Move Rights**, **Delete Rights** or the **Media Manager** role in GV STRATUS Control Panel. If not assigned, menu selections and operations are disabled. Where appropriate, the copy operation is substituted for the move operation.

1. In the Navigator panel, select the source bin on the Grass Valley system.
2. To transfer with the context menu, do the following:
   a) In the Asset List, right-click on the asset or assets that you want to transfer and select a command as follows:
      - **Copy** — Copies the asset or assets, leaving the original in the source bin.
      - **Copy To** — Copies the asset or assets, leaving the original in the source bin. Opens a **Copy To/Move To** dialog box in which you can browse to the desired destination bin.
      - **Move To** — Moves the asset or assets from one bin to another, removing the original from the source bin. Opens a dialog box in which you can browse to the desired destination bin.

   b) Select the destination bin or right-click and select **Paste**.

      If GV STRATUS security is enforced, settings are available as follows:

      - On the **Copy To/Move To** dialog box, if you have adequate permissions, click **Security** and configure security options as desired, then click **OK**.

      The **Security** dialog box is available only if you have the role of Security Manager or you are the Owner.

3. If prompted by a **Rename Policy** dialog box, do the following:
   a) Specify the rename or overwrite behavior if the assets exists.

      NOTE: The rename policy will not rename the logical asset with multiple hi-res associations. Only the new hi-res association will be renamed.

      This behavior applies when you transfer a single asset or multiple assets.

      To overwrite an asset, you must be assigned **Move Rights**, **Delete Rights**, or the **Media Manager** role in GV STRATUS Control Panel. If not assigned, selections are disabled.

   b) If you want this behavior to apply to all transfer operations in the future without being prompted, select the **Do not ask again** box.

      User Preferences allows you to reset hidden windows to display the **Rename Policy** dialog box again.

   c) Click **OK**.

   The **Rename Policy** dialog box is available only if you have the **Rename Asset Rights**, **Delete Rights**, or the **Media Manager** role.

The transfer is initiated. If transferring multiple assets, transfer jobs are queued.

To monitor the status of the transfer, open the Jobs List.

While transferring, if the destination quota is reached, the transfer job will fail gracefully in the Jobs Monitor and the partial asset will be deleted from the destination.

Transferring using Send Destination

- If quota is configured on the K2 system bin, ensure you have enough disk space before transferring assets.

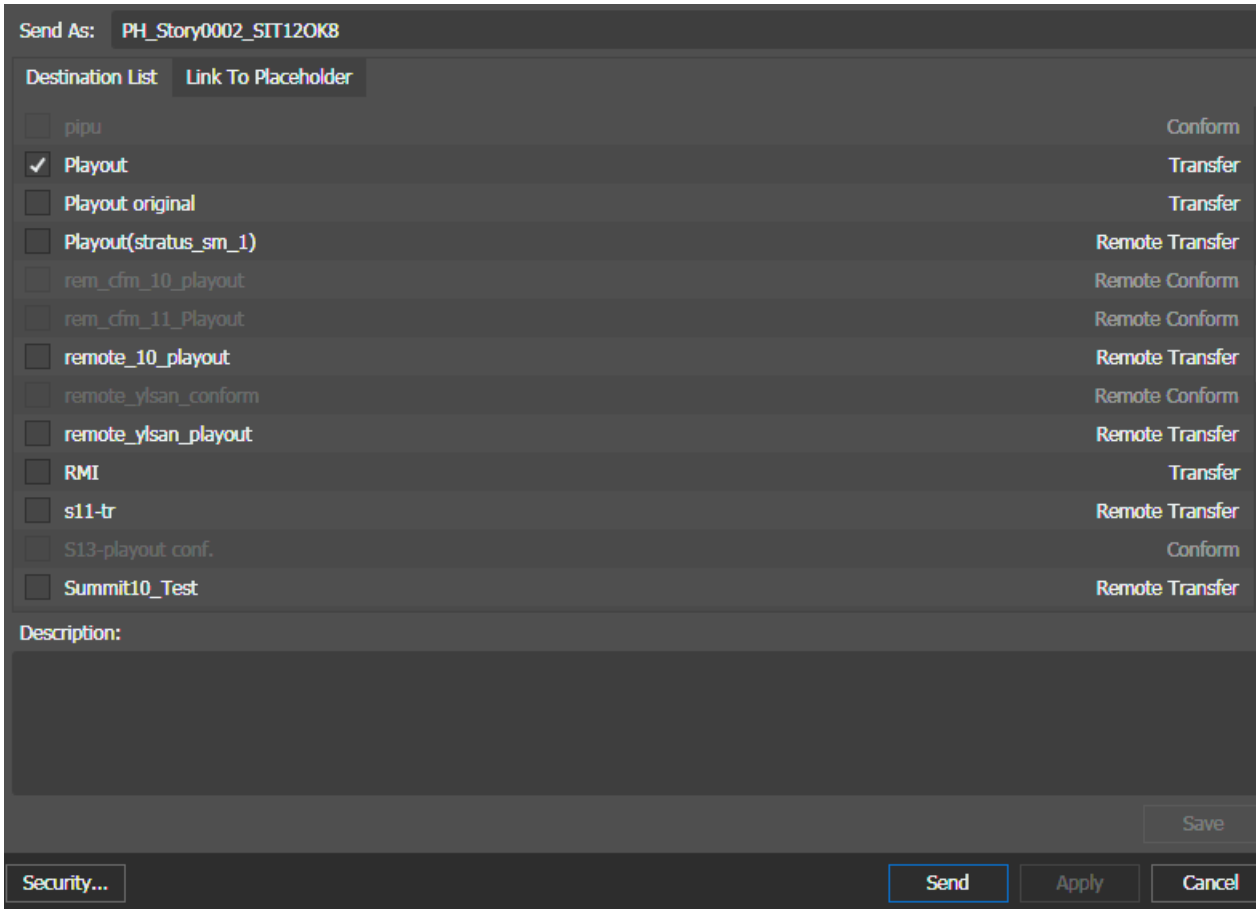
You can transfer assets to pre-configured destination locations using the Send Destination feature. The destination locations are configured in GV STRATUS Control Panel. The only formats available are those compatible with the Reference Standard currently configured in Format settings.

If the send destination is configured for conform, a complex asset can be flattened as part of the send operation to become a simple clip. You can configure the format of flattened asset in the Format setting of GV STRATUS Control Panel. You can also set the start timecode of the resultant simple clip according to EDIUS Start Timecode setting in GV STRATUS Control Panel. For same-format conforms (e.g.: 720p to 720p); if the **Restripe Timecode** checkbox is not selected during Send Destination configuration, the original timecode of the clip is preserved. For mixed-format conforms (e.g.: combination of 720p and 1080i); the resultant clip always consists of restriped timecode according to EDIUS Start Timecode setting in GV STRATUS Control Panel.

1. In the Navigator panel, select the source bin location.

   The assets in the bin are displayed in an Asset List.

2. Right-click on the asset that you want to transfer and select **Send** (**F11**).
   The Send Destinations dialog box opens and displays a list of destinations.



3. If desired, in the **Send As** field, enter a different name for the asset at the destination location.
4. In the **Destination List**, select one from the following:

   - Select one or more transfer destinations
   - Select one or more conform destinations

   You are not allowed to select both transfer and conform destinations at the same time.

   NOTE: If a local transfer destination is labeled as 'Remote Transfer', you need to re-save the send destination configuration on* GV STRATUS Control Panel *to get the correct label.

5. If configured for a Newsroom Computer System, you can also link the asset to a local or remote placeholder.
   - If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, and metadata.
   - In order to link to a placeholder, you must be assigned with the **Rename Asset Rights** role and write permission for the **Name** property in Metadata section of GV STRATUS Control Panel.

   a) On the **Link To Placeholder** tab, select a placeholder.

   If a remote placeholder, expand the remote site node.

   If already linked to a placeholder, you can select a different placeholder.

   b) If desired, in the **Placeholder Description** field, enter text and click **Save**.

   The placeholder description is updated. It is not necessary to click **Send** to update the placeholder description.

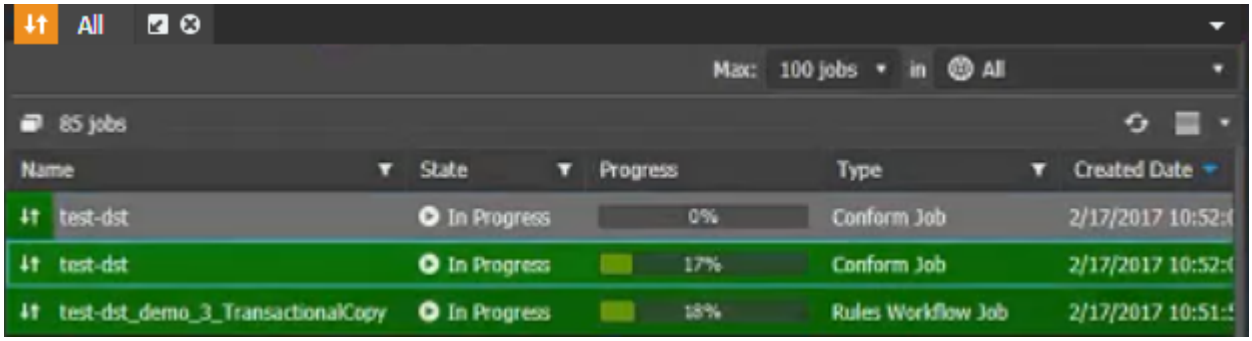
6. If you have adequate permissions, click **Security** and configure security options as desired, then click **OK**.

   The **Security** dialog box is available only if you have the role of Security Manager or you are the Owner.

7. Click **Send**.

   The Send order is translated into a rules workflow job. All subsequent jobs (conform(s), transfer(s), asset creation, metadata and marker copy) are managed by the rules workflow job.

To view the status of the transfer, open the Jobs Monitor.



The Rules Workflow job progress provides the overall status of the send order. Subsequent jobs like Conform or Transfer have their individual progress state.

In case assets would exist at the destination with the same name, the rules workflow job handles that gracefully. In case one of the subsequent jobs would fail, the rules workflow job rolls back all other subsequent jobs in a transactional fashion.

Transferring an asset from a remote site

Make sure no other asset with the same name exists in the local destination folder. If there is, rename the local asset before starting the remote asset transfer or select another local destination folder.

1. In Navigator, browse a remote GV STRATUS site and load a remote clip into Inspector.

2. If you want to transfer only part of the asset, in Inspector set Mark In and Mark Out points to define the portion you want to transfer.
3. In Inspector, click **Actions | Copy To**.

   A **Copy To** dialog box opens.
4. Select one of the following:

   - **Entire Asset**: Copies the entire asset from the remote site to the local site.
   - **Partial Asset**: Copies the portion of the asset between Mark In and Mark Out points from the remote site to the local site.
5. Select the destination on the local GV STRATUS to which the asset is going to be copied.
6. Click **OK**.

The asset is copied from the remote site to the local site. Progress is reported in the Monitors Jobs List.

Preservation of asset metadata after the remote transfer is as follows:

	Preserved	Not preserved
Asset metadata	• Protection Status • Rating • Tags • Approval Status • Description • Angle • Comments • Markers/Keywords	• Restored Date • Rules Applied • Import Location • Created Date - is set to the date and time when the new clip is created. • Modified Date - is set to the date and time when the new clip is modified. It is also set to the same date and time of **Created Date** when first created.

Transferring an asset to a remote site

- If quota is configured on the K2 system bin, ensure you have enough disk space before transferring assets.

1. In the Navigator panel, select the source bin on the Grass Valley system.
2. Do the following:
   a) In the Asset List, right-click on the asset or assets that you want to transfer and select a command as follows:

      - **Copy** — Copies the asset or assets, leaving the original in the source bin.
      - **Copy To** — Copies the asset or assets, leaving the original in the source bin. Opens a **Copy To** dialog box in which you can browse to the desired destination bin.

The transfer is initiated. If transferring multiple assets, transfer jobs are queued.

> ***NOTE: The transfer to a remote site always overwrites an asset if the remote site account does not have media manager role.***

To monitor the status of the transfer, open the Jobs List.

While transferring, if the destination quota is reached, the transfer job will fail gracefully in the Jobs Monitor and the partial asset will be deleted from the destination.

Sending assets for playout

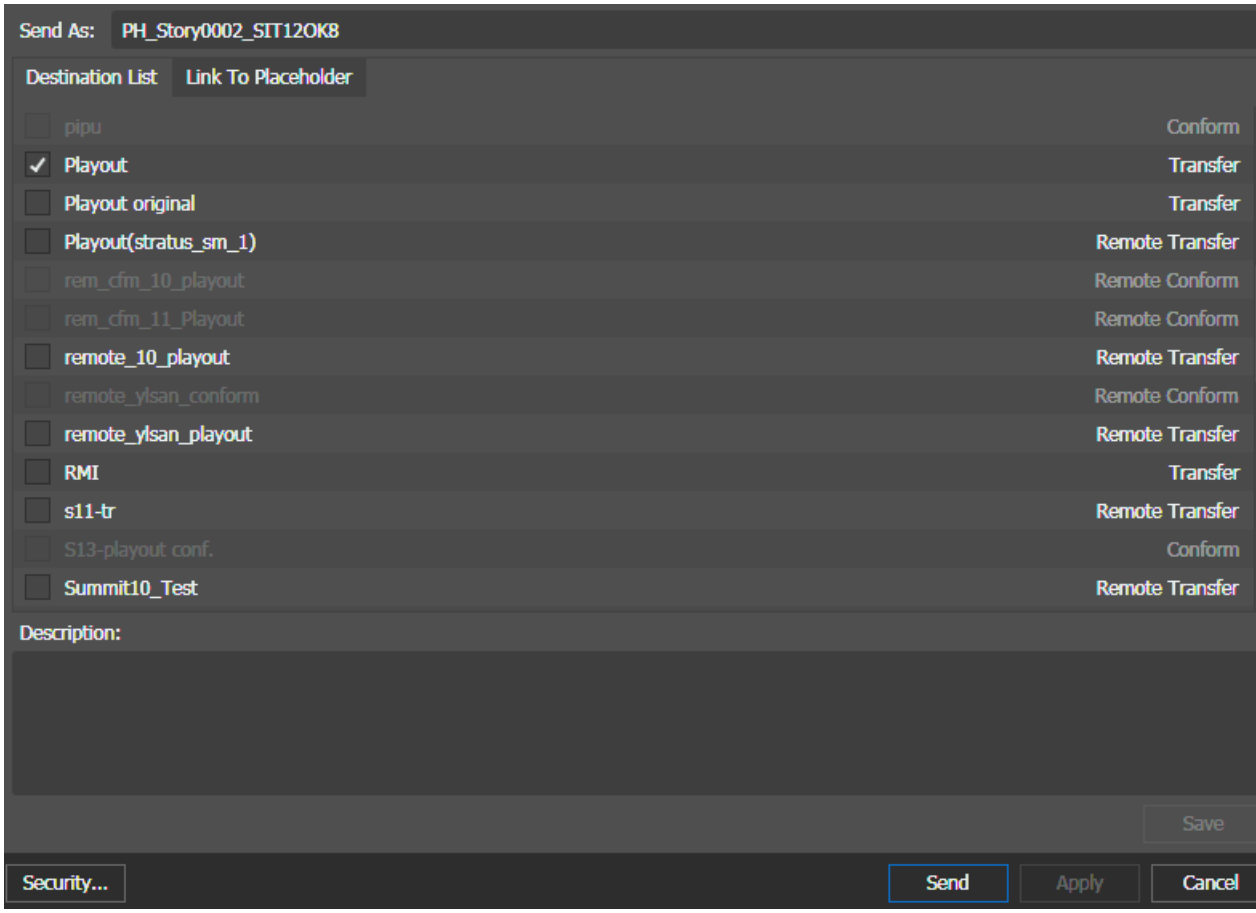
- If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, and metadata.
- In order to link to a placeholder, you must be assigned with the **Rename Asset Rights** role and write permission for the **Name** property in Metadata section of GV STRATUS Control Panel.
- If quota is configured on the K2 system bin, ensure you have enough disk space before transferring assets.
- It is recommended to set the bin quota to at least 2GB to a destination bin. You are not allowed to begin transferring into a bin if there is less than 1GB of space remaining in that bin.

You can send a completed clip or and edited sequence for playback in your operation. You can transfer assets to pre-configured destination locations using the Send Destination feature. The destination locations are configured in GV STRATUS Control Panel. The only formats available are those compatible with the Reference Standard currently configured in Format settings. Before sending the clip, you can link your asset to a placeholder.

1. In the Navigator panel, select the source bin location.

   The assets in the bin are displayed in an Asset List.

2. Right-click on the asset that you want to transfer and select **Send** (**F11**).
   The Send Destinations dialog box opens and displays a list of destinations.



3. If desired, in the **Send As** field, enter a different name for the asset at the destination location.
   If the asset is previously linked to a placeholder, the name of the placeholder appears in the **Send As** field. However, you can still modify the name of the placeholder in this dialog.
4. In the **Destination List**, select one from the following:
   - Select one or more transfer destinations
   - Select one or more conform destinations

   You are not allowed to select both transfer and conform destinations at the same time.

5. If configured for a Newsroom Computer System, you can also link the asset to a local or remote placeholder.
   - If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, and metadata.
   - In order to link to a placeholder, you must be assigned with the **Rename Asset Rights** role and write permission for the **Name** property in Metadata section of GV STRATUS Control Panel.

   a) On the **Link To Placeholder** tab, select a placeholder.

      If a remote placeholder, expand the remote site node.

      If already linked to a placeholder, you can select a different placeholder.

   b) If desired, in the **Placeholder Description** field, enter text and click **Save**.

      The placeholder description is updated. It is not necessary to click **Send** to update the placeholder description.

6. If you have adequate permissions, click **Security** and configure security options as desired, then click **OK**.

   The **Security** dialog box is available only if you have the role of Security Manager or you are the Owner.

7. Click **Send**.

   The transfer is initiated. If transferring multiple assets, transfer jobs are queued.

The asset is sent to the playout server. The placeholder status changes to **READY** in the Assignment List, and the number of missing items in the Assignment List decreases by one.

To monitor the status of the transfer, open the Jobs Monitor.

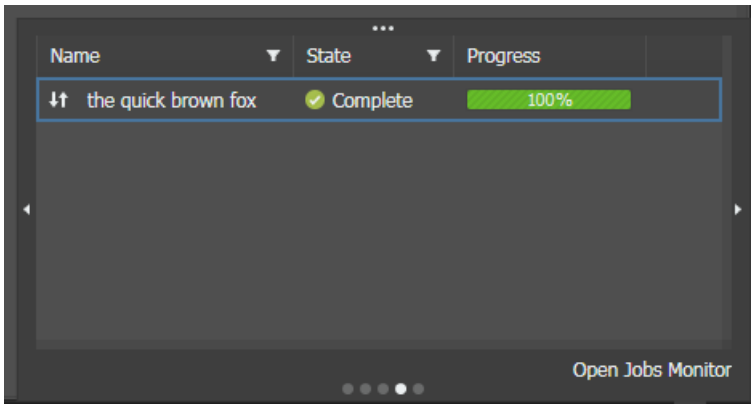
Monitoring imports, exports, or transfers

You can monitor the status of import, export, transfer, conform, and transcode jobs.

1. To monitor only the recent transfer jobs that you have triggered, do the following:
   a) In the lower-right GV STRATUS application Status bar, click the **My Transfer Jobs** button.

      If there are no recent transfer jobs that you have triggered, the icon for the button is not displayed.

   b) The Notification pop-up panel opens to the My Transfer Jobs page.



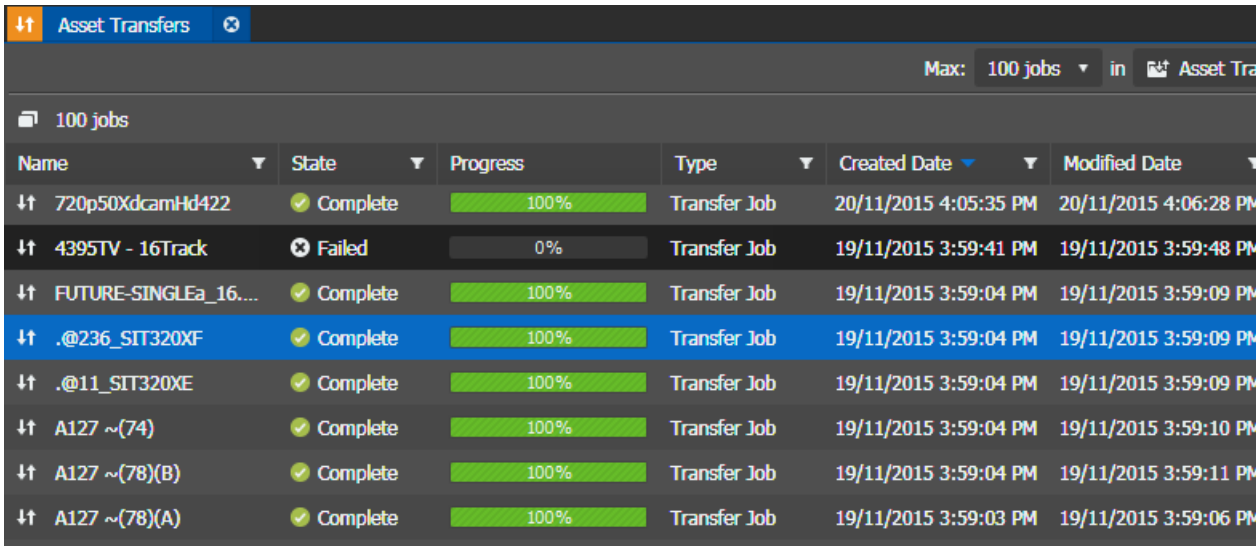
   NOTE: All recent jobs are only displayed in the pop-up panel for 5 minutes after completion. After that, you can still view them in the Jobs Monitor.

   c) To close the Notification pop-up panel, click the down-arrow on the top edge of the panel or click the **My Transfer Jobs** button again.
   d) To view a longer history and more information for all GV STRATUS system jobs, view the Jobs List by doing one of the following:

      - On the My Transfer Jobs page, click **Open Jobs Monitor**.
      - Proceed with the next step in this task.

2. To monitor GV STRATUS system jobs triggered by you and by others, in the GV STRATUS application Navigator panel, do one of the following according to the types of jobs you are monitoring:

   - Double-click **Monitors | Jobs** and sort on the **Type** column.
   - Double-click one of the nodes under **Monitors | Jobs**.



   The Jobs List displays GV STRATUS operations that can be monitored. Operations that are currently in progress or have failed are also displayed.

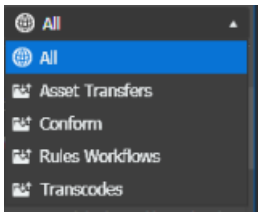
   Detailed transcode jobs are displayed if configured in General User Preferences.

   While transferring, if the destination quota is reached, the transfer job will fail gracefully in the Jobs Monitor and the partial asset will be deleted from the destination.

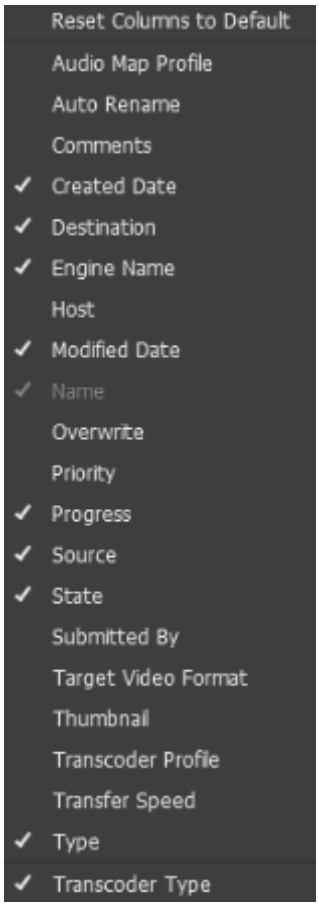
   You can also click the drop-down to select the maximum number of jobs to be displayed.

   The maximum number of jobs are limited to 2000 in the GV STRATUS 32-bit application, and 5000 in the 64-bit application.

3. Click the drop-down on the toolbar to filter the list and choose the type of job you want to monitor.



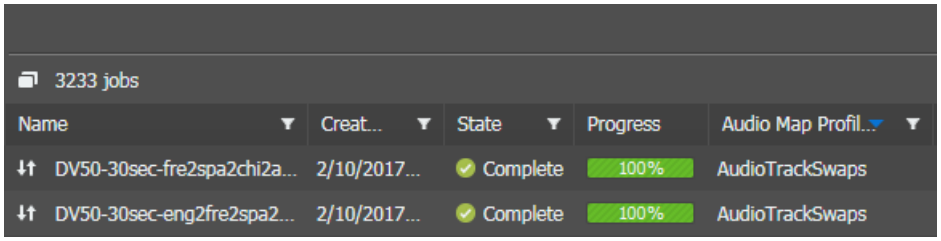
4. Right-click and select **Columns** to display specific column on the Jobs Monitor.



If **Transfer Speed** is selected, the column displays an instantaneous transfer speed in Mbit/sec during the transfer and then goes to 0 when finished.

NOTE: The transfer speed is not available for transfers of Import jobs.

If **Audio Map Profile** is selected, the column displays the list of profiles used for export Rules in the Asset Transfers monitor.



5. To change the position of an upcoming job in queue of jobs waiting to be processed, right-click an upcoming job, select **Change Priority**, and then select one of the following:

Options	Description
High	The job moves to the top of the queue, to be processed next, immediately after the currently processing job completes.
Normal	The job remains at its current position in the queue.
Low	The job moves to the bottom of the queue, to be processed last.

   You must be assigned the Queue Management role in GV STRATUS Control Panel in order to change job priority. If not assigned, menu selections are disabled.

6. To stop the GV STRATUS system from running an upcoming job, right-click an upcoming job and select **Cancel**.
7. To navigate to the asset of a specific job, do one of the following:
   - Right-click on the job and select **View Related | Asset**.

     The asset displays in the Asset List. Double-click the asset to view it in the Inspector.
   - Double-click the job in Jobs Monitor.

     The job and asset properties display on separate tabs in the Inspector. Click on the **Asset** tab, and double-click the asset to view it in the Inspector.
8. To retry a transfer from the list, right-click an aborted or failed job and select **Retry**.

   The job requeues and the retransfer starts shortly after. However the **Retry** option is only available for manually-triggered jobs, and not supported on jobs triggered by rules.
9. To remove a completed job from the list, right-click a completed job and select **Delete**.
10. Click the **Refresh** button if the Jobs List is not updated.

Related Topics

Configuring User Preferences on page 1387

Conforming a complex asset to a simple clip

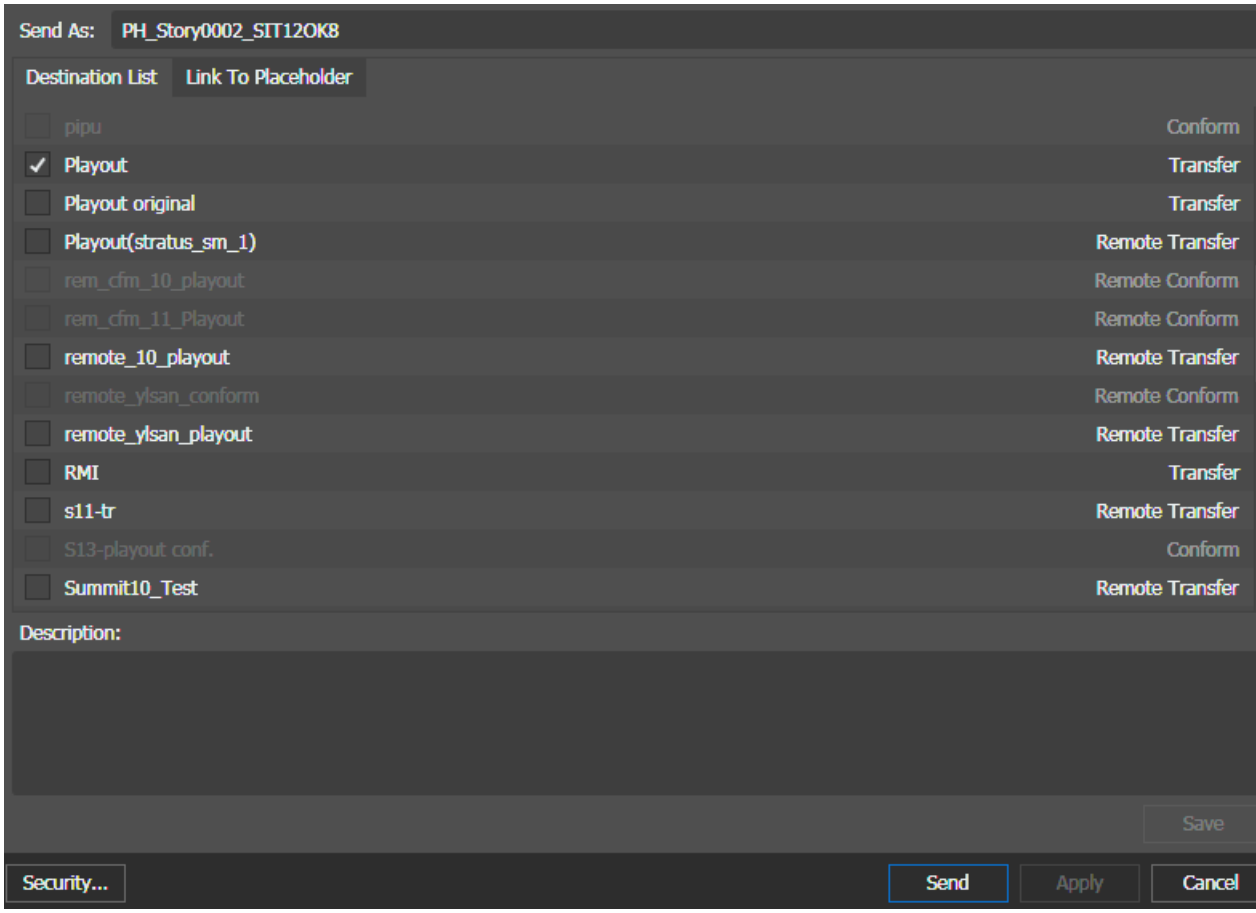
- If quota is configured on the K2 system bin, ensure you have enough disk space before transferring assets.

You can transfer assets to pre-configured destination locations using the Send Destination feature. The destination locations are configured in GV STRATUS Control Panel. The only formats available are those compatible with the Reference Standard currently configured in Format settings.

If the send destination is configured for conform, a complex asset can be flattened as part of the send operation to become a simple clip. You can configure the format of flattened asset in the Format setting of GV STRATUS Control Panel. You can also set the start timecode of the resultant simple clip according to EDIUS Start Timecode setting in GV STRATUS Control Panel. For same-format conforms (e.g.: 720p to 720p); if the **Restripe Timecode** checkbox is not selected during Send Destination configuration, the original timecode of the clip is preserved. For mixed-format conforms (e.g.: combination of 720p and 1080i); the resultant clip always consists of restriped timecode according to EDIUS Start Timecode setting in GV STRATUS Control Panel.

Before you can do this task, in the GV STRATUS Control Panel a destination must be configured to conform on send.

1. In the Navigator panel, select the source bin location.
   The assets in the bin are displayed in an Asset List.
2. Right-click on the asset that you want to transfer and select **Send** (**F11**).
   The Send Destinations dialog box opens and displays a list of destinations.



3. If desired, in the **Send As** field, enter a different name for the asset at the destination location.
4. In the **Destination List**, select destinations as follows:
   - Select one or more conform destinations

   You cannot select both transfer and conform destinations at the same time.

5. If configured for a Newsroom Computer System, you can also link the asset to a local or remote placeholder.
   - If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, and metadata.
   - In order to link to a placeholder, you must be assigned with the **Rename Asset Rights** role and write permission for the **Name** property in Metadata section of GV STRATUS Control Panel.

   a) On the **Link To Placeholder** tab, select a placeholder.

      If a remote placeholder, expand the remote site node.

      If already linked to a placeholder, you can select a different placeholder.

   b) If desired, in the **Placeholder Description** field, enter text and click **Save**.

      The placeholder description is updated. It is not necessary to click **Send** to update the placeholder description.

6. If you have adequate permissions, click **Security** and configure security options as desired, then click **OK**.

   The **Security** dialog box is available only if you have the role of Security Manager or you are the Owner.

7. Click **Send**.

   The transfer is initiated. If transferring multiple assets, transfer jobs are queued.

To monitor the status of the transfer, open the Jobs Monitor.

Considerations for conforming assets

Depending on formats and the application triggering a conform job, the resultant simple clip can have different specifications.

When a source complex asset (sequence or list) is conformed, the conform job falls into one of the following categories:

- Same-format:
  - The source format is the same for all clips in the complex asset AND the destination format to which the asset is conformed is also that same format.
- Mixed-format:
  - The source format is the same for all clips in the complex asset AND the destination format to which the asset is conformed is a different format.
  - -OR-
  - There are at least two different source formats in the complex asset.

Formats include SD, 720p, and 1080i.

The following are examples:

- When a source sequence or list with multiple SD clips is conformed to a simple SD clip, it is a same-format conform job.

- When that same source sequence or list with multiple SD clips is conformed to a simple 720p (HD) clip, it is a mixed-format conform job.
- When a source sequence or list with at least one 720p clip and at least one 1080i clip is conformed, it always a mixed-format conform job, regardless of the destination format to which it is conformed.

	Same-format job	**Mixed-format job**
Ancillary data	Inherited	Inherited from source formats that are the same as the destination format. Dropped in these conditions below: • When conforming from progressive to interlace or vice versa. • When conforming from 4:3 to 16:9 aspect ratio format or vice versa. • When conforming to multiple destinations with different format for each destination.
Start timecode	Configured according to the selection of **Restripe timecode** option in **Locations Config | K2-Send Destinations** settings in the GV STRATUS Control Panel. • When the **Restripe timecode** check-box is not selected, the start timecode of the conformed clip is preserved according to the original timecode. • When the **Restripe timecode** check-box is selected, the start timecode of the conformed clip is set according to EDIUS **Start Timecode** setting in GV STRATUS Control Panel.	Configured in the EDIUS **Start Timecode** setting in the GV STRATUS Control Panel.

	Same-format job	Mixed-format job
Marker timecode	Configured according to the selection of **Restripe timecode** option in **Locations Config | K2-Send Destinations** settings in the GV STRATUS Control Panel. • When the **Restripe timecode** check-box is not selected, the marker timecode of the conformed clip is preserved according to the original timecode. • When the **Restripe timecode** check-box is selected, the marker timecode on the conformed clip is shifted according to its position from the new start timecode as configured in EDIUS **Start Timecode** setting in GV STRATUS Control Panel.	Configured to new marker timecode from the new start timecode according to EDIUS **Start Timecode** setting in the GV STRATUS Control Panel.
Audio tags	Inherited	Inherited

Related Topics

EDIUS Settings on page 159

About archiving assets

You can store your assets on a permanent archive, thus allowing you to remove high-resolution material from your K2 system. You can archive a single asset or several assets at once via FTP to the archive location. During the archiving process, you can monitor the progress on the Jobs panel. Archiving lets you optionally remove assets that are not for immediate playout from your online location, thus also freeing your K2 system storage.

Depending on your system, you can archive assets into:

- Oracle Digital DIVArchive
- FlashNet archive
- Masstech archive
- Filezilla server
- Nearline K2 SAN
- Common RESTful archive server

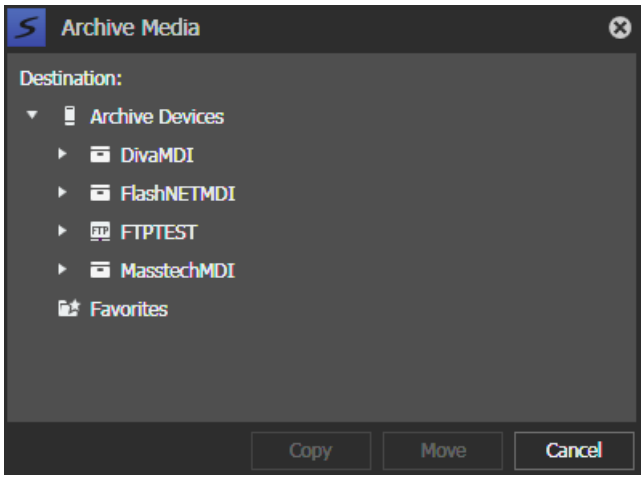
Refer to this Topic Library for information on supported formats.

Archiving an asset

You can only archive an asset if you are assigned with the archive role. When you want to archive an asset, you can choose whether to copy or move the asset to an archive location.

NOTE: A list must be conformed before it can be archived. If a rule is used to archive a list, the list is conformed by default.

1. In the Asset List panel, select an asset.
2. Right-click and select **Archive Media**.
3. Select the archive location.



NOTE: You cannot archive two assets with the same name at the same archive location. But you can select Rename Automatically in the Archive Rename Policy dialog box.

Tip: If you plan to archive or transfer assets frequently to the same folder, add that folder to your favorites. This allows you to select that folder directly from the Favorites menu instead of browsing to the archive location.

4. Click **Copy** or **Move**.

   NOTE: A copy operation archives a copy of the asset to the archive location. A move operation archives the asset and deletes it from its online location.

   You can also archive an asset via copy and paste, or drag and drop assets directly into a bin in your archive directory.

5. From the Navigator, select **Monitors | Jobs** to track the progress of the archive operation.

   If the Jobs List is not updated, click the **Refresh** button.

Upon completion of the archive operation, the **High-Res Status** column in the Asset List indicates the online or archive status of the asset.

A protected asset can be archived via the copy operation, but a move operation is not allowed as the high resolution media cannot be deleted.

Related Topics

Asset indicators on page 977

Archive system set up process on page 874

Searching archived assets

Use the advanced search tool to find specific content that have been archived.

Search for archived assets by setting a search condition for High-Res Status in the advanced search. This search finds archived assets, and also assets with both archived and online status.

Related Topics

Searching assets with the advanced search tool on page 992

About restoring assets

Once your assets are transferred to an archive system, you can restore those archived assets to the K2 Summit/SAN system as needed.

You can restore the whole asset, or only part of the asset. Partial restore is based on the asset's mark in and mark out points. To ensure that you select the correct asset to restore, preview the proxy of the asset in the Inspector panel or the Source Viewer tool.

If an asset is archived by other means than the GV STRATUS application, you can still restore the asset to the K2 Summit/SAN system. The proxy is automatically generated for the restored asset if you have a GV STRATUS server doing proxy encoding in your operation.

Refer to this Topic Library for information on supported formats.

Related Topics

Viewing a video asset on page 996

Restoring archived assets

You can restore assets if you are assigned with the restore role. Only archived assets can have their high resolution material restored into the K2 Summit/SAN system. However, you cannot restore or partial restore an asset if the high resolution material for that asset already exists in the K2 Summit/SAN system.

If you are logged on with the Media Manager role assigned, permission is granted to move assets from an archive system to the GV STRATUS system. Without this permission, assets may be copied but not moved.

1. In the Asset List panel, select the asset or assets you want to restore as follows:
   - Right-click a single asset to open a context menu.
   - Use **Ctrl + Click** to select multiple assets, then right-click to open a context menu.
2. In the context menu, select **Restore Media**.

   The Restore Media dialog opens.

3. Select the desired restore destination and click **OK**.
4. From the Navigator, select **Monitors | Jobs** to track the progress of the restore operation.

   If the Jobs List is not updated, click the **Refresh** button.

Upon completion of the restore operation, the Asset List displays a High-Res Status indicator.

Related Topics

Asset indicators on page 977

Partially restoring an asset

You can partially restore an asset to get a specific part of the high resolution material from the archive system and restore it into the K2 Summit/SAN system.

Refer to this Topic Library for information on supported formats.

1. Load the asset you are partially restoring into the Inspector.
2. Set Mark In and Mark Out points on the asset.
3. Click **Actions** on the Inspector panel and select **Restore Media**.

   The Restore Media dialog opens.
4. Select **Partial Asset** to partially restore the asset.

   Verify that the mark in and mark out points specified on the Restore Media dialog are correct.
5. Enter a new name in the **Asset Name** box if desired.

   If not, **_PR** is appended to the name of the asset by default to indicate partial restore.
6. Select the desired destination to restore the asset.
7. Click **OK**.

   NOTE: Restore operations are not always immediate.
8. Verify the status of your restore operation and the names of the assets that are restored by launching **Monitors | Jobs** from the Navigator.

Upon completion of the restore operation, the Asset List displays a High-Res Status indicator.

A partially restored asset uses the originally created proxy. The Inspector panel Associations tab provides information on paths, association types, and device locations.

Related Topics

Using mark-in and mark-out points on page 1145

Asset indicators on page 977

Restoring assets from keywords

You can restore assets if you are assigned with the restore role.

You can also partially restore assets from existing keywords and restore them into the K2 Summit/SAN system.

1. In the Asset List panel, select an archived asset with keywords that you want to restore.

   The asset loads in the Inspector.

2. In the Inspector panel, click on the **Markers** tab.

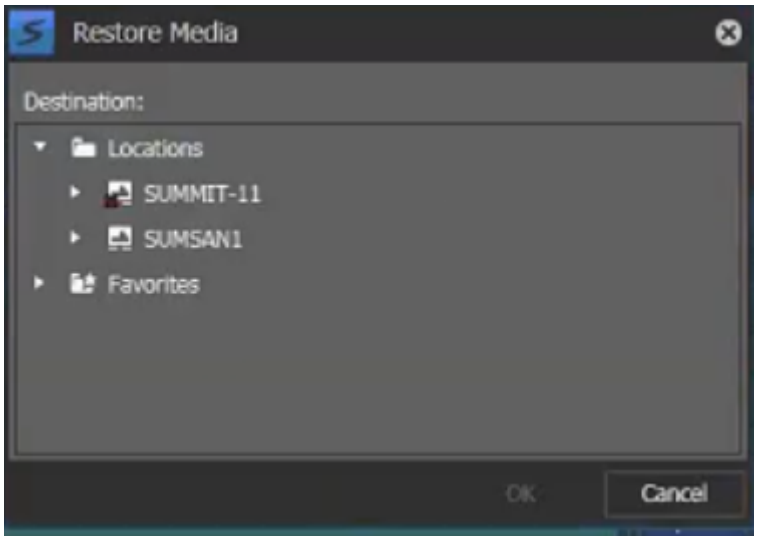
   The list of markers and keywords displays on the **Markers** tab.

3. Select a keyword or multiple keywords as follows:

   - Right-click a single keyword to open a context menu.
   - Use **Ctrl + Click** to select multiple keywords, then right-click to open a context menu.

4. In the context menu, select **Restore from Archive**.

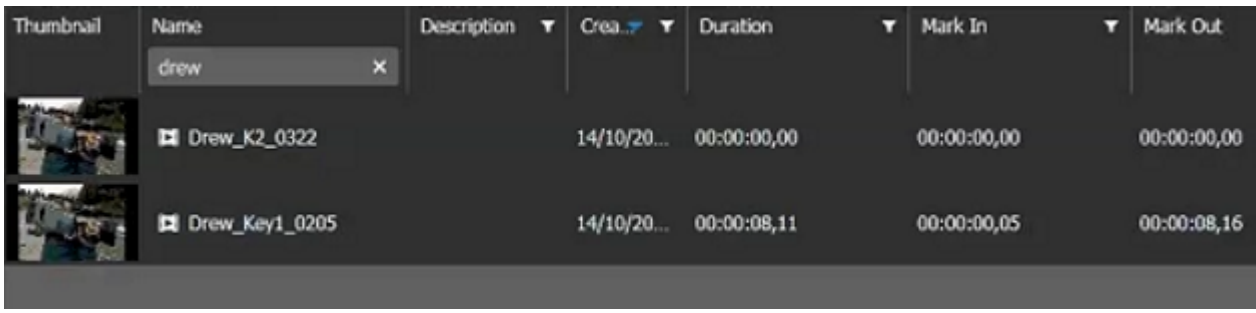
   The Restore Media dialog opens.



5. Select the desired restore destination and click **OK**.

   You can select whether to rename the restored asset automatically, or to overwrite an existing asset with the restored asset.

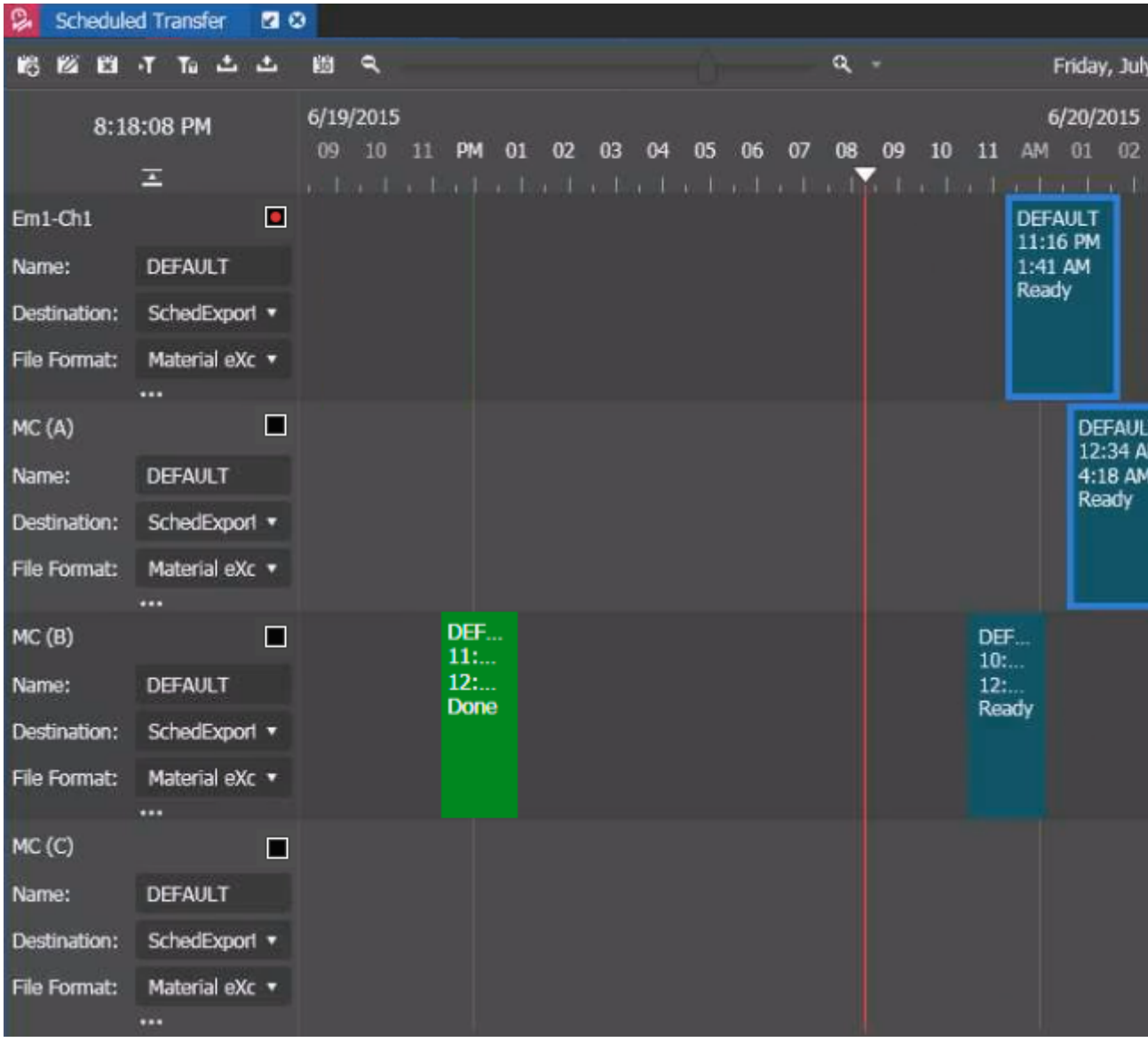
   Assets from those keywords are restored at the selected destination. Each keyword name is appended to the asset name to differentiate restored assets from multiple keywords.



Upon completion of the restore operation, the Asset List displays a High-Res Status indicator.

The Scheduled Transfer tool

The Scheduled Transfer tool allows you to schedule asset transfers into a repository. The Scheduled Transfer tool appears in the application as a panel that can be accessed from the Window menu or the tools section of the Navigator panel.



The Scheduled Transfer tool features are as follows:

- Clock — Shows current time according to the system time of the GV STRATUS core server. If the client PC time is in a different timezone than the server, the server time is converted to the client PC timezone.
- Timeline — Shows dates and hours to guide transfer scheduling. A maximum of four days' worth of events can be shown on the timeline at any given time.

- Available channels — Shows channels that are configured to transfer assets according to the recording schedule.
- Channel status indicator — Shows channel status whether it's idle, cued, recording, or playing.
- Scheduler toolbar — Consists of buttons for scheduling and viewing transfer events.
- Current time indicator — Moves along the timeline according to the current time.
- Scheduled events — Shows events that have been added to the Scheduled Transfer tool.
- Scheduled Transfer engine status — Shows the status of Scheduled Transfer engine.

With the tool, you can schedule transfer events in advance, by specifying the date, time, and duration of the event.

By default, the Scheduled Transfer tool opens to the current day, date, and time according to your system time.

Scheduled Transfer buttons

These buttons located on the Scheduled Transfer toolbar let you perform various functions.

Add Event: Adds a scheduled event.

Modify Event: Modifies the selected event.

Delete Event: Deletes the selected event.

Go to Current: Goes to the current time of day in the timeline.

Toggle Timelock: Goes to the current time of the day in the timeline and turns on the timelock mode.

Import: Imports selected transfer events to the assigned bin.

Export: Exports selected transfer events to the assigned bin.

Go to Date: Goes to the current day in a calendar.

Zoom In: Zooms in the view of the timeline. The slider between **Zoom In** and **Zoom Out** also zooms the view of the timeline.

Zoom Out: Zooms out the view of the timeline. The slider between **Zoom In** and **Zoom Out** also zooms the view of the timeline.

Record details toggle: Toggles display of the record details for all channels.

Expand: Shows/hides settings and lists.

Transfer Event status colors

Each event displays in a color that identifies its status in the Scheduled Transfer tool.

Event Color	Event Status
Teal	READY
Red	TRANSFERRING
Green	SUCCESSFULLY TRANSFERRED

Event Color	Event Status
Grey	NO ACTION MODE
Black	TRANSFER FAILED

Adding a transfer event

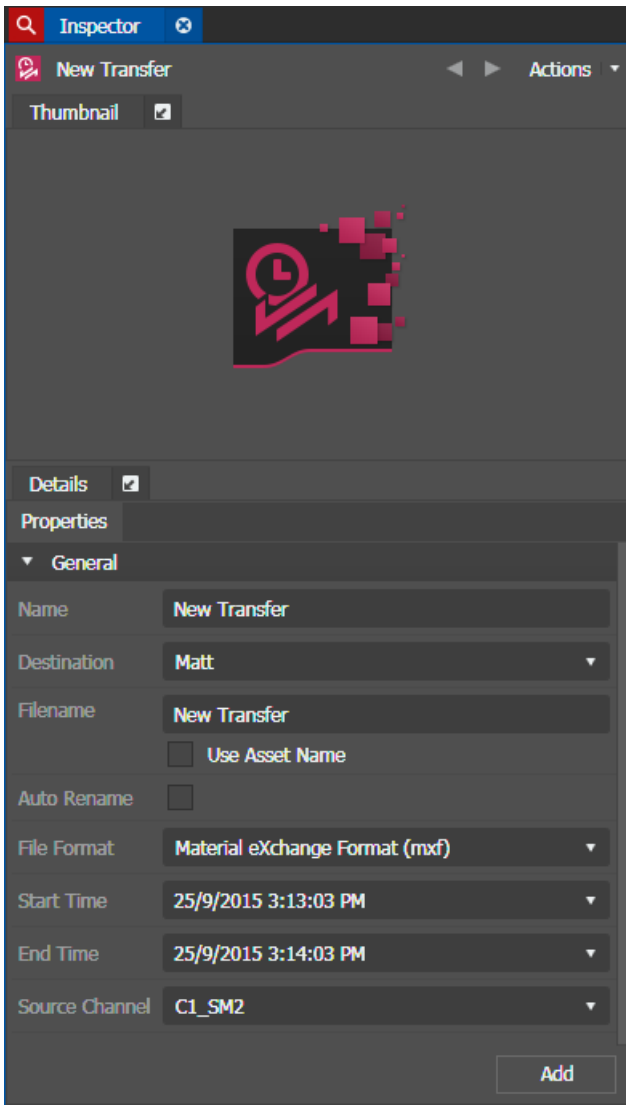
- If quota is configured on the K2 system bin, ensure you have enough disk space before transferring assets.

- It is recommended to set the bin quota to at least 2GB to a destination bin. You are not allowed to begin transferring into a bin if there is less than 1GB of space remaining in that bin.

To schedule transfers, add an event in the Scheduled Transfer tool for each asset that needs to be transferred.

1. Do one of the following:
   - Click the **Add Event** button.
   - Right-click and select **Add Event**. (**A**)

   The Inspector panel loads event properties.



2. Fill in properties of your event according to the following:
   a) Name — Enter a name for the transfer event that displays on the Scheduled Transfer tool.
   b) Destination — Select a destination bin for the transfer from the drop-down list.

      Destination availability depends on the location configuration of Scheduled Transfer in your GV STRATUS Control Panel. Once a location is configured, it appears automatically in the **Destination** drop-down list. If the bin has security access permissions configured, the recorded clip inherits those permissions.

   c) File Name — Enter the name of the file to be transferred. If you want the file name to be the same as the asset name, select the **Use Asset Name** checkbox.
   d) Auto Rename — Select the checkbox if you want the file name to be renamed automatically if the same name exists at the destination. Additional suffix will be automatically added to the file name if you selected the checkbox.
   e) File Format — Select the format of the file to be transferred from the following:

      - GXF: General Exchange Format
      - MXF: Material Exchange Format
      - MOV: QuickTime Movie
      - MOV Reference: QuickTime Reference Movie

   f) Start Time — Enter the date and time you want the transfer to start. The default date is the current date. You can also select your start date from the calendar when you click the drop-down arrow. Enter the time using the format **hour:minutes:seconds**. However, overlapping events are not supported.

      NOTE: The timecode source of the K2 channel must be set to Time of Day for scheduled transfers to work. Time of Day is usually from the Windows system clock, or from LTC/VITC timecode sources that are set to the system clock.

      Transfers will only be successful if a matching time is found between the event time and the clip timecode.

      Clock synchronization is required on all GV STRATUS servers and K2 Summit/SAN systems. Ensure that K2 Summit/SAN systems are locked to house reference and clocks on all machines are kept in sync. This is especially important as systems must be kept in sync between the GV STRATUS Core server and K2 Summit/SAN system channels.

   g) End Time — Enter the date and time you want the transfer to end. You can also select your end date from the calendar when you click the drop-down arrow.

      NOTE: The event duration must be more than 1 minute to ensure frame accurate transfers in your operation.

   h) Source Channel — Channel availability depends on the configuration in your system. You can only see and select channels that have been configured for the Scheduled Transfer tool. Once a channel is configured in the GV STRATUS Control Panel, the channel appears automatically in the **Source Channel** drop-down list and on the Scheduled Transfer timeline. Make sure that the channel is not in Continuous Record mode.

      If configured as a Multicam channel in the GV STRATUS Control Panel, two or three input sources can be selected depending on your configuration. You can also schedule overlapping event transfers on two or three different input sources within the same Multicam channel.

By default, the Scheduled Transfer tool opens to the current day, date, and time according to your system time. The time of day format within the Scheduled Transfer is directly from the current time of day format of your machine.

To set the 24 hour format to your Scheduled Transfer, change the time format of your Windows client by selecting **Start | Control Panel | Clock, Language and Region**, and change the time format accordingly.

NOTE: Changes to the* Scheduled Transfer*'s time format can only be seen after a restart of the GV STRATUS application.

3. Click the **Add** button in the Inspector panel.

   The event is added to the Scheduled Transfer tool.

   While recording, if the bin in which a growing asset exists reaches its quota, the clip will be forced to stop recording but will remain in the bin.

4. To add another transfer event, in the Inspector panel, fill in properties and other information as in the steps earlier in this procedure, then click the **Add** button.

To delete an event, refer to "Deleting an event" topic.

Related Topics

Deleting an event on page 1052
Configure Scheduled Transfer send locations on page 402

Adding a transfer event using Quick Schedule

- If quota is configured on the K2 system bin, ensure you have enough disk space before transferring assets.

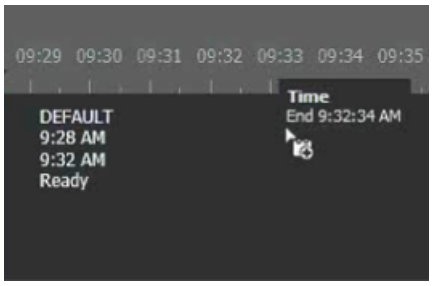
- It is recommended to set the bin quota to at least 2GB to a destination bin. You are not allowed to begin transferring into a bin if there is less than 1GB of space remaining in that bin.

With Quick Schedule, you can add events directly on the scheduling interface.

1. Right-click on a channel timeline and select **Quick Schedule**. (**Q**)

   Once you are in the Quick Schedule mode, your mouse pointer turns into the **Add Event** icon with time tooltip for your reference.

2. Click to select the start time, and drag your mouse to the right to select the end time.



3. Release the mouse after the end time is selected.

   The event displays on the timeline of the Scheduled Transfer tool.

   Each channel default options are included in the event properties when events are created on the respective channel's timeline. The Auto-rename flag is also checked by default for all Quick Schedule events.

4. Right-click on the event, and select **Modify Event** to add other properties to the event.

   The Inspector loads the event properties.

5. Edit properties of the event.
6. Click the **Modify** button to commit your changes.

The event adds to the Scheduled Transfer tool with a **Ready** status.

Modifying a transfer event

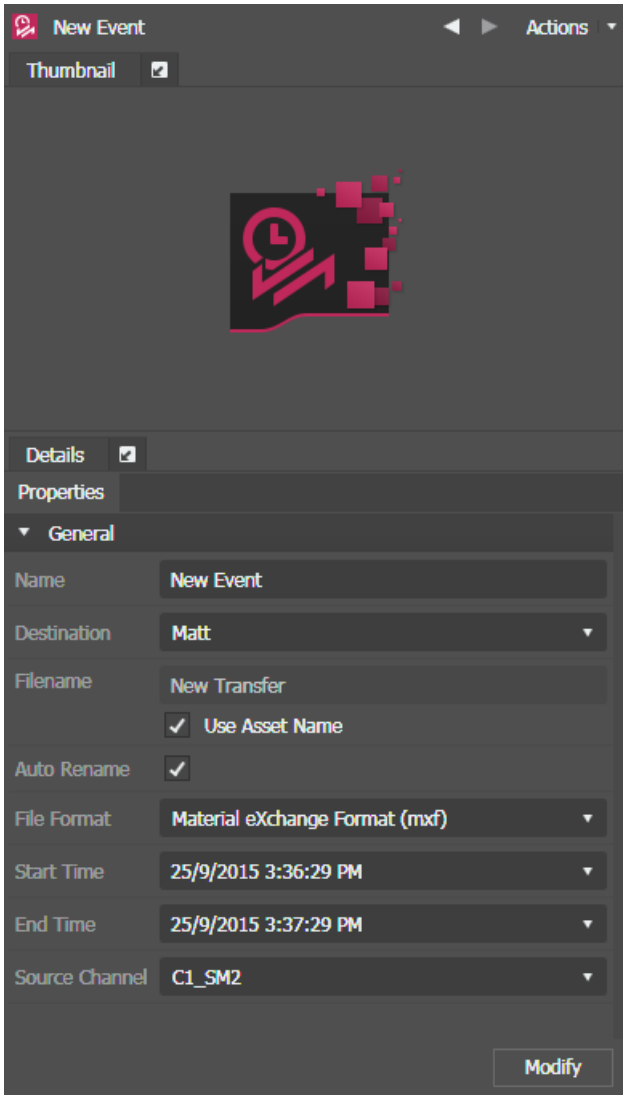
You can modify an event by changing the event name, transfer destination, file name, timing information, or source channel. However, an event can only be modified before the transfer starts.

1. Select the event you want to modify on the Scheduled Transfer tool.

2. Do one of the following:

   - Click the **Modify Event** button.
   - Right-click and select **Modify Event**. (**M**)
   - Double-click the event.
   - Drag and drop the event into the Inspector.

   The event opens in the Inspector panel.



   Event properties display in the **Properties** tab of the Inspector.

3. Modify the event properties.
4. Click the **Modify** button.

The transfer event updates with those changes on the Scheduled Transfer tool.

Moving a transfer event

You can move a scheduled transfer event via drag and drop within the same channel or to a different channel. This is useful when the current channel is not available, or another event needs to be in a particular channel at the same time.

NOTE: Move of past events, combination of past and future events, and overlapping of events are not supported.

1. Select the event you want to move on the Scheduled Transfer tool.
2. Press the **Ctrl** button and drag the event to a future time or into another channel.

   Once you drag the event, a tooltip appears to help you decide the start time of the event.
3. Drop the event to a new location and release the **Ctrl** button.

   A dialog box opens for you to confirm the move of the event.
4. Click **Yes**.

   The Scheduled Transfer tool updates the event change.

Retrying a transfer event

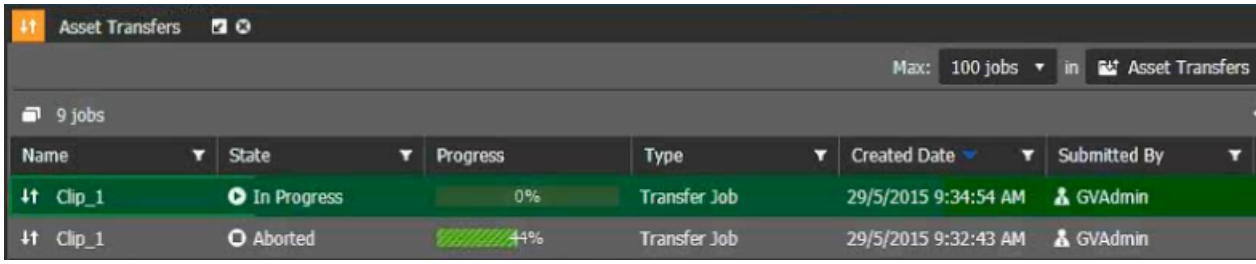
You can retry an event transfer after a failed, aborted, or completed event transfer. A still transferring event must be canceled before the event transfer could be retried.

NOTE: The Retry Event option is not available if the transfer event is in 'Ready' or 'Transferring' state.

1. Select the event you want to re-transfer on the Scheduled Transfer tool.
2. Right-click on the event and select **Retry Event**.

   The event status changes to **Ready** and **Transferring**.

   The progress of the event transfer can be viewed on the Jobs monitor.



If you aborted the previous event transfer, you can see that transfer is abandoned. Then the retried event transfer appears on the Jobs monitor.

Exporting Scheduled Transfer events

1. Select an event or multiple events in the Scheduled Transfer user interface.

   To select multiple events, hold the **Shift** key down and select all events between two selected events; or hold the **Ctrl** key down and select events randomly.

   To deselect any event, hold the **Ctrl** key down and click on the event to be unselected.

2. Do one of the following:

   - Click the **Export** button.
   - Right-click and select **Export Event**.

   The Export Event dialog box displays.

3. Enter the file name for those events and select the destination folder.
4. Click **Save**.

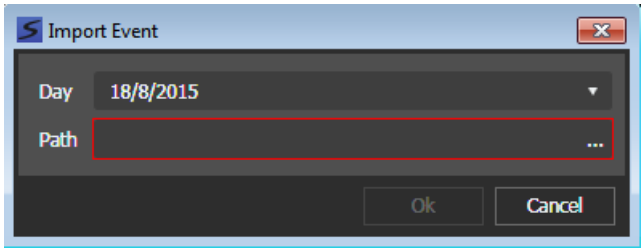
   Events are exported and saved in the `*.sts` file format.

Importing events into Scheduled Transfer

1. Do one of the following:

   - Click the **Import** button.
   - Right-click and select **Import Event**.

   The Import Event dialog box displays.



2. Select the Day for events to be imported from the calendar display.
3. Browse to select the Path to `*.sts` file that you want to import and click **Open**.

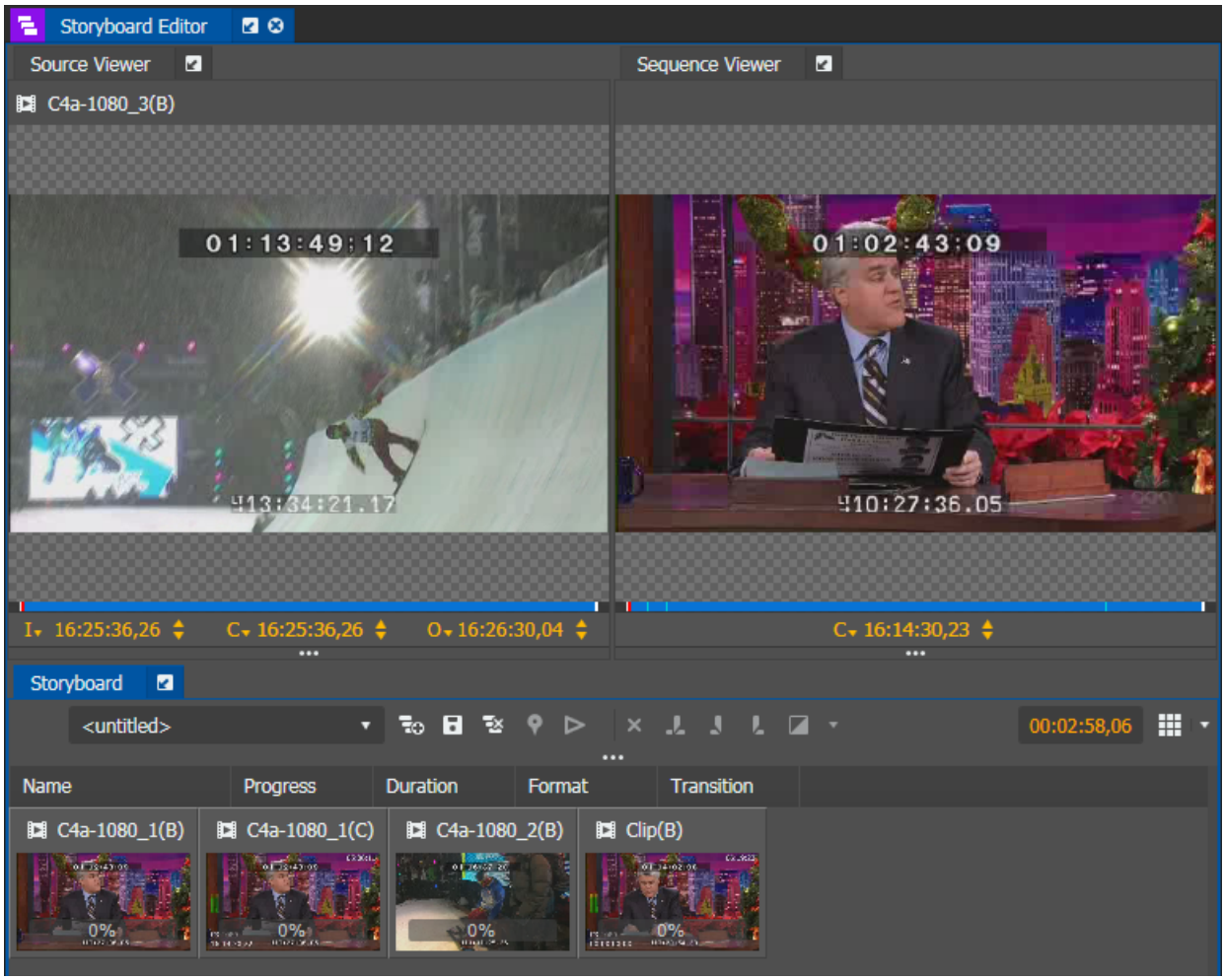
   Events are imported and displayed on the Scheduled Transfer user interface.

Editing

The Storyboard Editor tool

Launch the Storyboard Editor tool to access the editing workspace.

The Storyboard Editor tool launches as a composite panel inclusive of Source Viewer, Sequence Viewer, and Storyboard.



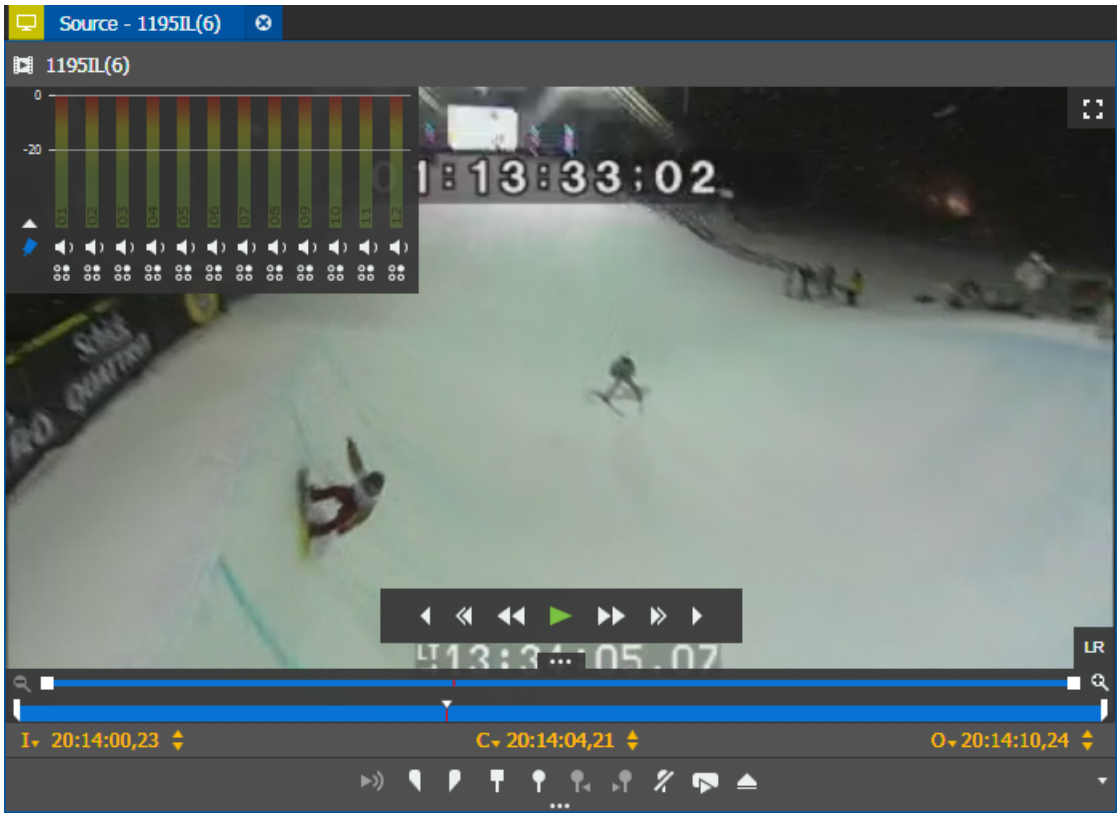
If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets, and metadata that do not have read permissions are not visible. Markers and segments permissions must be set to **Allow** in order to create, update, or delete markers and segments.

Opening a Storyboard

1. In an Asset List, right-click on a playlist and select **Open With | Storyboard Editor**.
   The Storyboard Editor Panel opens.
2. In the Storyboard panel, use the toolbar buttons to modify events.

The Source Viewer

The Source Viewer allows you to preview assets, both assets already recorded and assets currently being recorded. The Source Viewer appears in the application as a standalone panel when you select it in the Navigator panel or from the **Window | Panels** menu. However, the Source Viewer appears in a composite panel when you launch Advanced Logging or Storyboard Editor.



The Source Viewer includes the following components :

- Overlay Controls — Transport controls navigate through the asset. Visible when you hover the mouse pointer over the asset. Movable with drag-and-drop. Not all controls are displayed when the panel is not fully expanded.
- Clip Viewer — Displays the asset.
- Audio Overlay — Displays the audio settings embedded with the asset.
- Show/Hide Controls — Shows and hides the controls.
- Scrub Bar — Scrubs through the asset.

- Controls — Allows you to mark up the asset.
- Add/Remove Buttons — Allows you to choose which Control buttons to display.
- Timecode Controls — Allows you to select the mark in/out and other timecode types to display. Also lets you navigate through the clip to a specific timecode. If desired, the timecode controls can also be expanded and resized in the panel.

Related Topics

Identifying and selecting the timecode type on page 1095

Viewer buttons

These buttons and controls located on the Source Viewer and the Inspector let you perform various functions:

Show/Hide Control Tray: Shows or hides the control tray.

Live Streaming Video: Enables/disables the display of the live video stream.

Mark In: Sets the Mark In point.

Mark Out: Sets the Mark Out point.

Add Keyword: Logs an item from mark in to mark out.

Add Marker: Logs an item for the current position.

Go to Previous Marker: Goes to previous keyword/marker.

Go to Next Marker: Goes to next keyword/marker.

Hide Markers and Keywords: Hides marker and keyword indicators on the scrub bar.

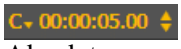
Loop Playback: Loops the current asset between mark in to mark out.

Eject: Ejects the current asset.

Full Screen: Displays the video player in full screen.

Restore: Restores player window to the normal size.

Next Display: Displays the video player on the next display monitor.



Timecode: Displays timecode and allows you navigate to a specific timecode. Also lets you select the timecode type for display. In the Viewer, displays the timecode for the mark-in point, mark-out point, and current timecode.

These transport control buttons let you move through the selected asset:

-1 Frame: Goes back one frame.

-10 Frames: Goes back ten frames.

Rewind: Rewinds the current asset. First press, rewinds -8x speed. Second press, increases to -16x speed.

Play: Plays the clip. Toggles with the Pause button.

Fast Forward: Fast Forwards the current asset. First press, fast forwards to 8x speed. Second press, increases to 16x speed.

+10 Frames: Goes forward ten frames.

+1 Frame: Goes forward one frame.

These control buttons on the audio overlay let you control the audio of the selected asset:

Mute: Silences the selected audio channel.

Solo: Isolates the selected audio channel.

Pin Audio: Always display audio channels.

Collapse Audio: Collapses display of audio channels.

Related Topics

Arranging control tray buttons on page 971

Using Source Viewer

Source Viewer allows you to preview assets that you can add to a sequence. You can also add keywords, markers, or mark-in and mark-out points to the asset. These are preserved when the asset is added to the sequence.

1. In the Navigator panel, select **Tools** and double-click **Source Viewer**.

   The **Source Viewer** panel opens.

2. In the Navigator panel, click **Assets** and select the bin containing the asset to previewed.

   The asset appears in the Asset List.

3. Do one of the following:

   - Drag the asset into the Source Viewer.
   - Double-click the asset to open it in the Source Viewer.

4. To navigate through the asset or to add or modify keywords, markers, or mark in and mark out points, use the appropriate transport controls or keyboard shortcuts.

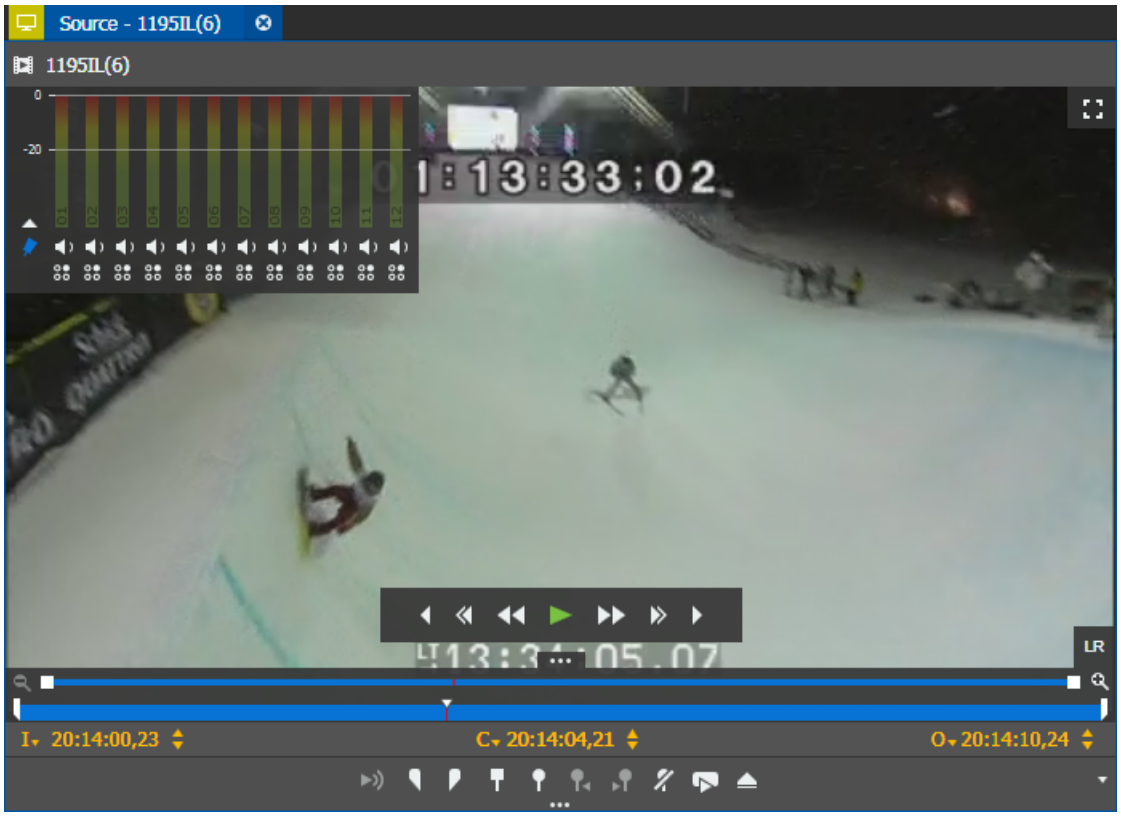
Using the Audio Overlay

The audio overlay is available on the Source Viewer, the Sequence Viewer, and the Inspector. The number of audio meter display depends on the number of audio tracks associated with the asset.

You can load and play assets up to 64 audio tracks if viewing a high-resolution clip, but only up to 32 audio tracks if viewing a low-resolution clip.

1. On the Source Viewer, the Sequence Viewer, or the Inspector player, hover your mouse pointer on the top left of the asset.

   The audio overlay of the asset displays. Each audio meter bar is labeled with the audio track number for easy reference.

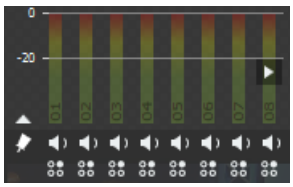


2. You can manage audio for the asset by clicking the appropriate button:

   - To mute specific audio channels, click the **Mute** button.
   - To isolate the selected audio channel while muting others, click the **Solo** button.

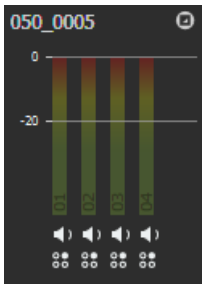
   Meters on muted channels will continue to display audio levels.

3. Click the **Pin Audio** button to pin the audio overlay and fix it in place.
4. Click the **Collapse Audio** button to show or hide meter bar display of audio channels.
5. Click the arrow button to go to the next page if there are multiple pages in the audio overlay.



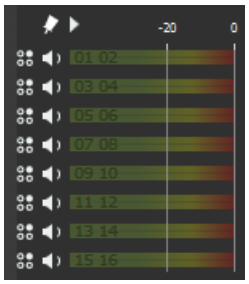
6. Drag the audio overlay off the viewer panel, if desired.

   The audio overlay is re-sizable and can be undocked. The clip name displays on the audio overlay if it is off the viewer panel.



7. To return the audio overlay to its original position on the viewer, click the **Redock** button.

The audio meter settings can be configured by selecting **Edit | User Preferences | Player**.



You can set the audio meter grouping to **Stereo** as shown above with 2 audio labels in combined channels. To toggle the audio meter display between **Mono** and **Stereo**, use these shortcut keys: **Shift + Alt + G**

You can also set the audio meter orientation to be stacked horizontally or vertically in User Preferences settings. The default is set to be stacked horizontally.

GV STRATUS supports the display of audio tags if already configured in the User Preferences settings. Audio tags can be selected from drop-down lists on the **Audio Tags** tab of the Inspector and automatically displayed on the audio meter.

Related Topics

Configuring Player User Preferences on page 1008

J, K, L keyboard shortcuts for transport control

The three keycaps J, K, and L on a standard keyboard can be used as transport control hotkeys in Source Viewer. These three keys can be used to play video and audio forward, in reverse, and vary speed as described below.

1. Load a video asset (clip) into an Inspector, Source Viewer, or Storyboard Editor tool.
2. Press the **J** key to start playing the clip in reverse.
3. Each time you press **J**, the reverse speed increases by 1X, 1.5X, 2X, 5X, 8X, 16X.
4. Hold down both the **J** and **K** keys.

   This increases the speed of the video play in reverse by 1/10.
5. Press and hold down the **K** key while pressing **J**.

   Now each press of **J** moves the video in reverse by one frame.
6. Press the **K** key to pause the video.
7. Press the **L** key to start playing the video forward.

8. Each time you press **L**, the forward speed increases by 1X, 1.5X, 2X, 5X, 8X, 16X.
9. Hold down both the **L** and **K** keys.

   This increases the speed of the video forward play by 1/10.

10. Press and hold down the **K** key while pressing **L**

    Now each press of **L** moves the video forward by one frame.

Using mouse wheel for transport control

A PC mouse wheel can be used as a transport control to advance the position of media so that jogging can be quick and efficient.

1. Select the asset in any window with transport controls using the mouse pointer.
2. Use the mouse wheel to move the media in both forward and reverse directions at the speed desired.

Using the ShuttlePro Controller with GV STRATUS viewers

GV STRATUS supports the use of ShuttlePro Controller with the Source Viewer and Inspector.

Any commands you send using the Shuttle Pro Controller apply to the currently active panel or window, which is considered to have focus. When a window has focus, you can perform tasks such

as navigating through a clip or trimming a clip. Always bear in mind that you need to give focus to a panel or window before you can apply the ShuttlePro Controller commands.

1. Plug the ShuttlePro controller into a USB connector on the GV STRATUS client.

   A default layout has been provided with pre-configured keys. Keyboard shortcut keys are as below:

   - Forward speeds:

Keyboard shortcuts	Forward Speed
Shift + F1	0.1
Shift + F2	0.3
Shift + F3	0.5
Shift + F4	1.0
Shift + F5	1.5
Shift + F6	2.0
Shift + F7	4.0
Shift + F8	8.0
Shift + F9	16.0

   - Reverse speeds:

Keyboard shortcuts	Reverse Speed
Ctrl + F1	0.1
Ctrl + F2	0.3
Ctrl + F3	0.5
Ctrl + F4	1.0
Ctrl + F5	1.5
Ctrl + F6	2.0
Ctrl + F7	4.0
Ctrl + F8	8.0
Ctrl + F9	16.0

2. Use the ShuttlePro Controller to scroll through, add markers or keywords, and trim clip in the Source Viewer or Inspector.

Using mark-in and mark-out points

- If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, metadata, markers, keywords, and segments.

- Create Marker and Update Marker permissions must be set to **Allow** for you to create and update markers.

1. Navigate to the desired starting point using the scrub bar, and click the **Mark In** button. (**I**)
2. Navigate to the desired end-point using the scrub bar, and click the **Mark Out** button. (**O**)

   Trim Asset is enabled when the asset has a mark-in or mark-out point. It is disabled if the asset does not have a mark-in or mark-out point.

   NOTE: If a clip is a part of Dyno record train sequence, Mark In and Mark Out points should not be set beyond the limit of the guard band, as configured for the record train sequence.

3. To clear a mark-in or mark-out point, click the drop-down arrow by the respective button and select **Clear Mark In** (**Shift + I**) or **Clear Mark Out**. (**Shift + O**)
4. To navigate to a mark-in or mark-out point, click the drop-down arrow by the respective button and select **Goto Mark In** (**Ctrl + I**) or **Goto Mark Out**. (**Ctrl + O**)

Adding markers

- If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, metadata, markers, keywords, and segments.
- Create Marker, Update Marker, and Write permissions must be set to **Allow** for you to create and update markers.

You can add markers to assets that are loaded in GV STRATUS Viewers. In the Sequence Viewer tool and the Channel Panel tool you can add markers but not keywords.

1. Load an asset into the Viewer or Channel Panel.

   If a Channel Panel, record a clip or load an already recorded clip.

2. If the logging controls are not shown, do the following:

   - If a Viewer, individual Channel Panel, or Channel Panel gang, click the **Show/Hide Control Tray** button ... to show the controls, then the drop-down arrow at the right of the control tray and **Add/Remove** buttons if necessary.
   - If a channel in a Channel Panel gang, double-click the channel to show the controls.

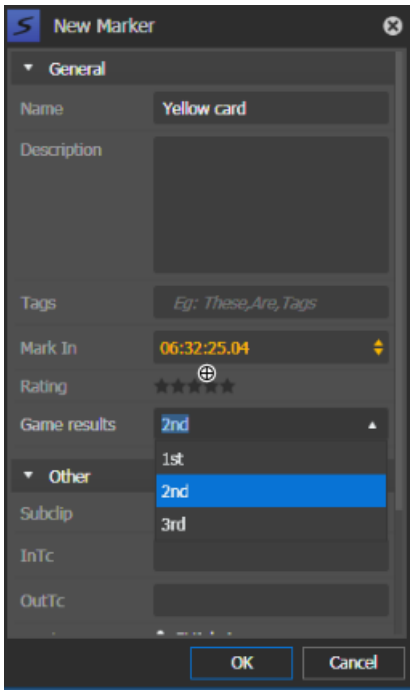
3. Click the **Add Marker** button. ( )

   The New Marker dialog box opens.

4. Enter the name of the marker.

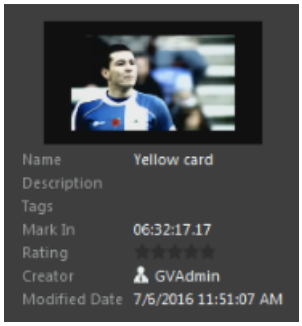
   You can also add the description, tags, rating, and angle if needed.

   If custom metadata had been specified for markers and keywords in the GV STRATUS Control Panel, you can select a custom value for the marker.



5. Click **OK**.

The marker is added to the asset. A symbol indicates its location. If you select a symbol the thumbnail associated with that point is loaded into the Viewer, and the slider is moved to that position.



If you hover the mouse pointer over a symbol, its thumbnail and properties appear.

Related Topics

Adding keywords on page 1148

Adding markers to a playlist on page 1155

Adding keywords

- If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, metadata, markers, keywords, and segments.
- Create Marker, Update Marker, and Write permissions must be set to **Allow** for you to create and update keywords.

You can add keywords to assets that are loaded in GV STRATUS Viewers. In the Sequence Viewer tool and in the Channel Panel tool you cannot add keywords, but you can add markers.

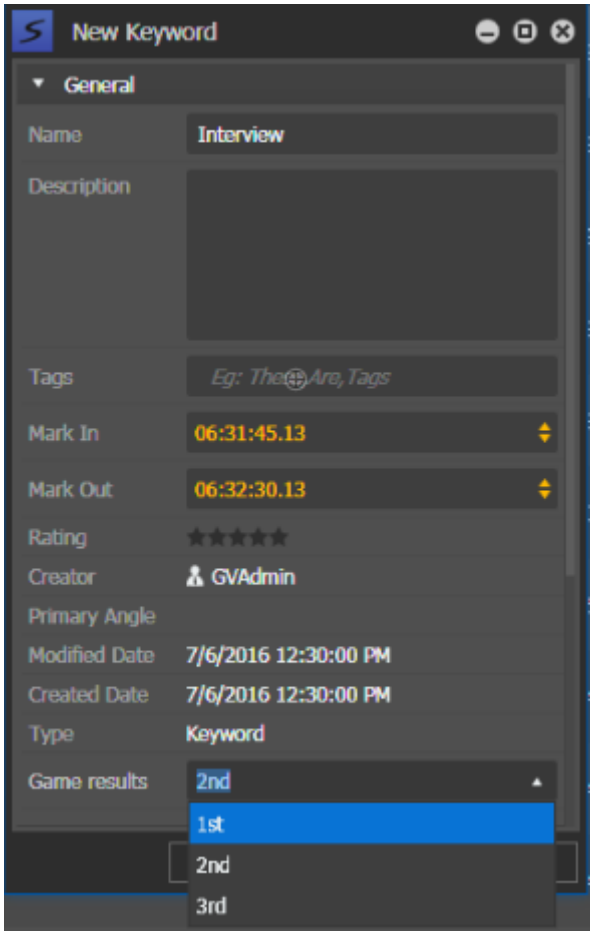
1. Load the selected asset into the Viewer.
2. If the logging controls are not shown, click the **Show/Hide Control Tray** button ... to show the controls, then the drop-down arrow at the right of the control tray and **Add/Remove** buttons if necessary.
3. Navigate to the desired starting point using the scrub bar, and click the **Mark In** button. (**I**)
4. Navigate to the desired end-point using the scrub bar, and click the **Mark Out** button. (**O**)
5. Click the **Add Keyword** button. ( )

   The New Keyword dialog box opens.

6. Enter the name of the keyword.

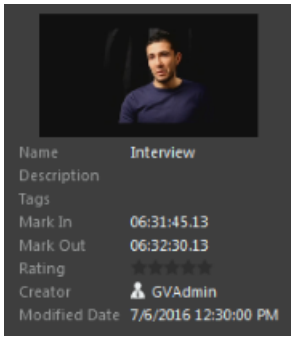
   You can also add the description, tags, rating, and angle if needed.

   If custom metadata had been specified for markers and keywords in the GV STRATUS Control Panel, you can select a custom value for the keyword.



7. Click **OK**.

The keyword is added to the asset. A symbol indicates its location. If you select a symbol the thumbnail associated with that point is loaded into the Viewer, and the slider is moved to that position.



If you hover the mouse pointer over a symbol, its thumbnail and properties appear.

Related Topics

Adding markers on page 1146
Adding markers to a playlist on page 1155

Navigating to keywords or markers in an asset

1. Load the asset in the Viewer or Channel Panel.
   Keywords or markers are indicated by symbols along the scrub bar.
2. Navigate through the asset using the appropriate buttons:
   - To go forward, use the **Go to Next Marker** button. (**H**)
   - To go backward, use the **Go to Previous Marker** button. (**G**)

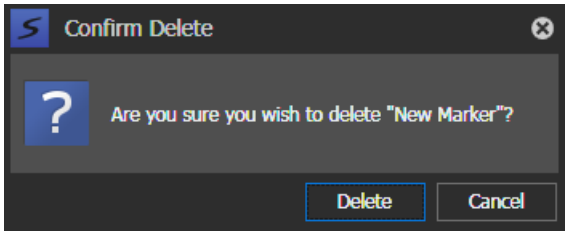
Deleting a marker

- Delete Marker permission must be set to **Allow** for you to delete markers.

1. Select a marker or multiple markers that you want to delete.

   To select multiple markers on the **Markers** tab of the Inspector, hold the **Shift** key down and select all markers between two selected markers; or hold the **Ctrl** key down and select markers randomly.
2. Right-click and select **Delete**. (**Delete**)

   The Confirm Delete dialog opens.



3. Click **Delete**.

Selected marker or markers are deleted from the **Markers** tab.

Create a subclip

- Subclips can be created on any K2 SAN, as long as the K2 SAN contains a high-resolution association of the clip.

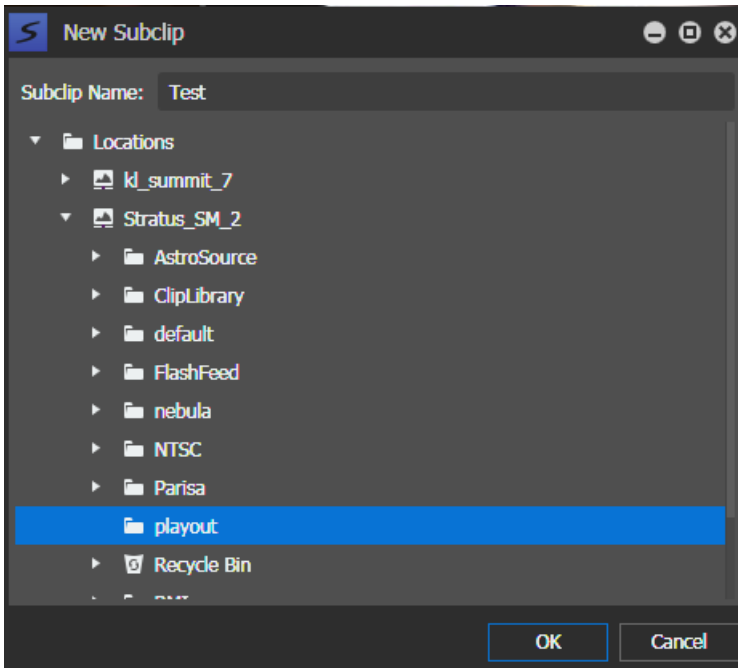
1. Load an asset into the Viewer.
2. Navigate to the desired starting point using the scrub bar, and click the **Mark In** button. (**I**)
3. Navigate to the desired end-point using the scrub bar, and click the **Mark Out** button. (**O**)

   Trim Asset is enabled when the asset has a mark-in or mark-out point. It is disabled if the asset does not have a mark-in or mark-out point.

   NOTE: If a clip is a part of Dyno record train sequence, Mark In and Mark Out points should not be set beyond the limit of the guard band, as configured for the record train sequence.

4. Right-click on the scrub bar and select **Create Subclip**. (**F4**)

   The **New Subclip** dialog box opens.



5. Enter a name for the subclip.
6. Navigate and select a location to save the subclip.

   NOTE: The last path from the previous subclip operation is automatically remembered as the starting point to save subsequent subclips. If there was no prior subclip operation, the starting path is automatically the same with the loaded asset.

7. Click **OK**.

The subclip is created in the specified location. The following is inherited from the parent clip:

- Rating

- Tags
- Description
- Angle
- Comments
- Markers and keywords that are between mark in and mark out
- Custom metadata

The following is not inherited:

- Approval Status
- Protection Status

Related Topics

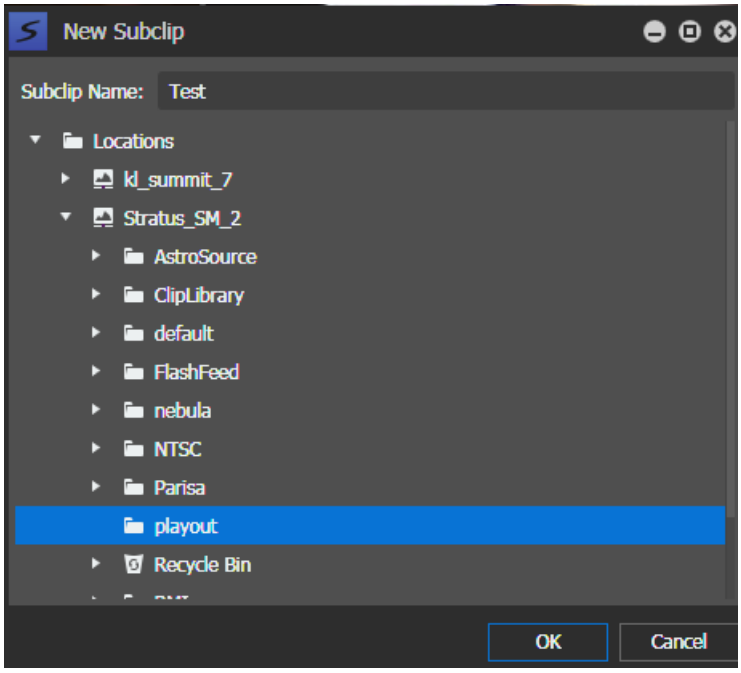
About GV STRATUS markers, Dyno markers, and the K2 database on page 419
Conforming a complex asset to a simple clip on page 1118

Create subclips from keywords

- Subclips can be created on any K2 SAN, as long as the K2 SAN contains a high-resolution association of the clip.

1. Load an asset with several keywords into the Inspector.
2. Click on **Markers** tab to view the list of keywords and markers.
3. Select a keyword or multiple keywords from the list.
4. Right-click on the keyword(s) and select **Create Subclip**.

   The **New Subclip** dialog box opens.



5. Enter a name for the subclip.

6. Navigate and select a location for the subclip.

   NOTE: The last path from the previous subclip operation is automatically remembered as the starting point to save subsequent subclips. If there was no prior subclip operation, the starting path is automatically the same with the loaded asset.

7. Click **OK**.

The subclip is created at the selected destination. If multiple subclips are created from multiple keywords, a suffix will be appended to the next and subsequent subclips.

Trimming a clip in Inspector

If GV STRATUS security is enforced, your credentials must give you adequate permissions. You can only view assets with read permissions, and edit assets with write permissions. If read permissions are denied on specific assets, those assets will not be available for viewing.

When you trim an asset, you change the length of the viewable asset, restricting it to the material between the Trim In and Trim Out points. The material outside the trim marks is not deleted. It remains on disk but is not viewable. To use the Trim Asset operation, you must be logged on with a user account to which the Trim Rights role is assigned. If the role is not assigned, the Trim Asset operation is not available.

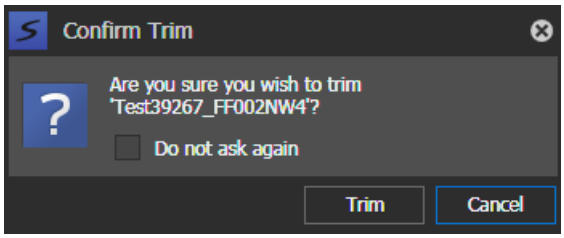
1. Load the asset into the Inspector.
2. Navigate to the desired starting point using the scrub bar, and click the **Mark In** button. (**I**)
3. Navigate to the desired end-point using the scrub bar, and click the **Mark Out** button. (**O**)

   Trim Asset is enabled when the asset has a mark-in or mark-out point. It is disabled if the asset does not have a mark-in or mark-out point.

   NOTE: If a clip is a part of Dyno record train sequence, Mark In and Mark Out points should not be set beyond the limit of the guard band, as configured for the record train sequence.

4. Click on the **Actions** drop-down arrow, and select **Trim Asset**.

   The **Confirm Trim** dialog box appears.

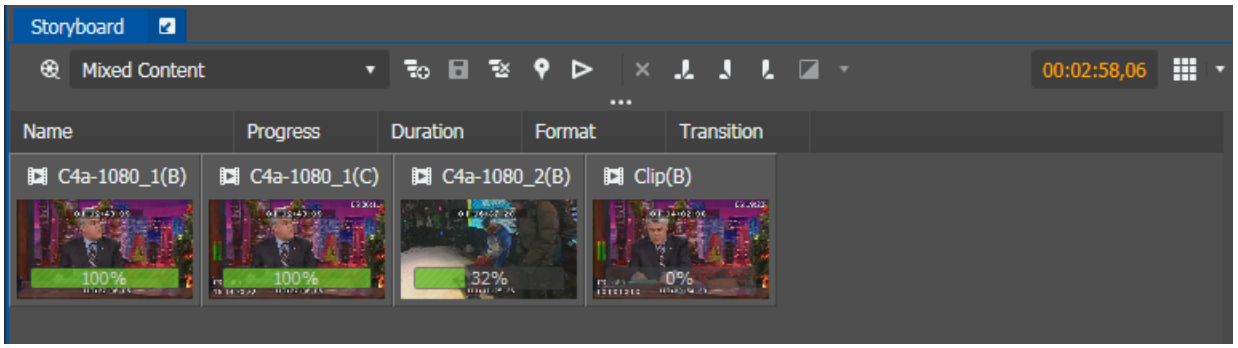


5. Select the **Do not ask again** checkbox to prevent recurring display of the **Confirm Trim** dialog box.
6. Click **Trim** to confirm the trimming of the asset.

The Storyboard

The Storyboard Editor tool allows you to assemble and edit a Sequence. You can launch the Storyboard Editor as a composite panel when you select it in the **Windows | Panels** menu.

The Storyboard appears in the application as a panel in the Storyboard Editor tool. You can drag assets into the panel to create or add to a Sequence. Assets in the panel are called *events*.



The panel has the following features:

- Toolbar — Edits the series of events.

Once you have assembled the Sequence, you can preview it in the Sequence Viewer. In the Storyboard, the progress bar next to an event indicates whether that event is currently being played in the Sequence Viewer, and if so where the current play location is.

If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets, and metadata that do not have read permissions are not visible. Markers and segments permissions must be set to **Allow** in order to create, update, or delete markers and segments.

Related Topics

About playlists and sequences on page 1100

Storyboard buttons

These buttons and controls located on the Storyboard let you perform various functions:

New Sequence: Creates a new sequence.

Save Sequence: Saves selected sequence.

Close Sequence: Closes selected sequence.

Locate Sequence: Navigate to this sequence in the Asset List viewer.

Launch in EDIUS: Launches the sequence in the EDIUS XS application.

Delete: Deletes the selected item or items. Disabled if delete rights denied in GV STRATUS Control Panel.

Split: Splits the item at the current position.

Trim In: Trims the start of the event at the current position.

Trim Out: Trims the end of the event at the current position.

Add Transition: Adds a transition to the event.

Show/Hide Transition Panel: Edit current transition settings

View Mode: Controls the display and size of the items in a list or panel.

Related Topics

Adding and removing transitions on page 1159

Adding markers to a playlist

- If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, metadata, markers, keywords, and segments.
- Create Marker, Update Marker, and Write permissions must be set to **Allow** for you to create and update markers.

You can add markers to a playlist in the Storyboard panel. These markers are added in addition to any markers inherited from sequences in the playlist.

1. In an Asset List, right-click on a playlist and select **Open With | Storyboard Editor**.

   The Storyboard Editor Panel opens.

2. In the Sequence Viewer, use the transport controls to navigate through sequences in the playlist.
3. In the Storyboard panel, right-click and select **Add Marker**.

   The New Marker dialog opens.

4. Enter the name of the marker.

   You can also add the description, tags, rating, and angle if needed.

5. Click **OK**.

The marker is added to the playlist. If the playlist is conformed to a flattened file and archived, the marker is preserved and can be found with advanced search.

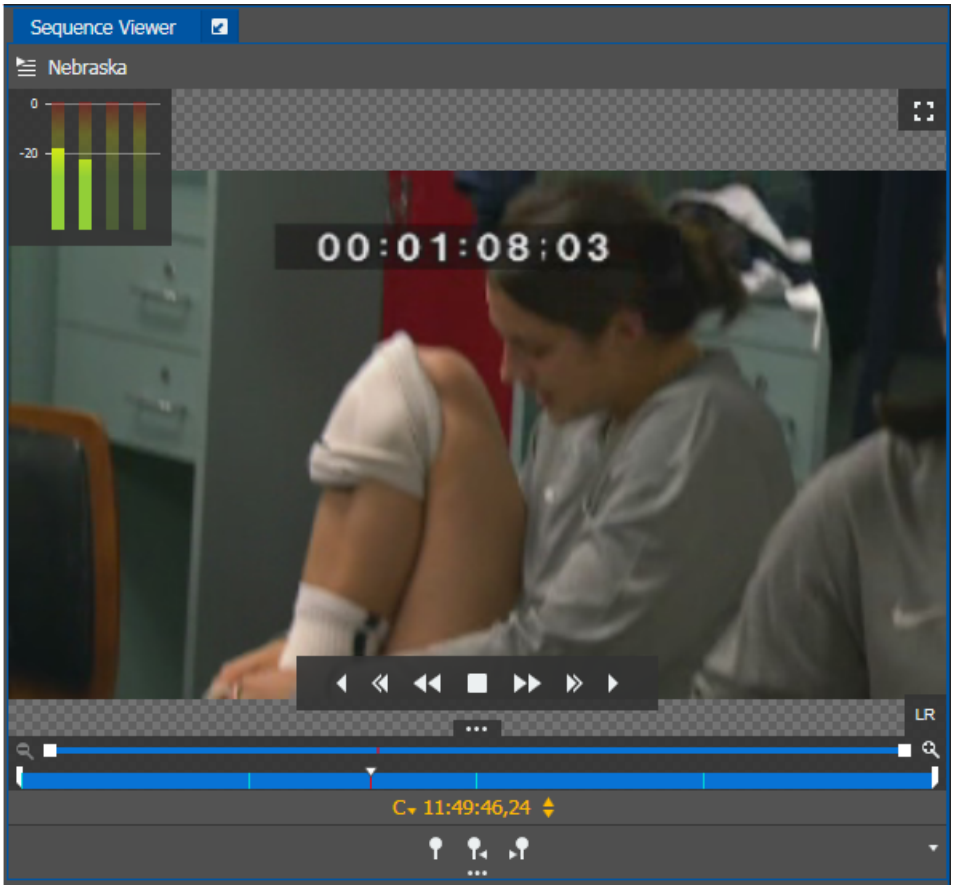
Related Topics

Adding keywords on page 1148

Adding markers on page 1146

The Sequence Viewer

The Sequence Viewer allows you to play assets (also called events) that have been assembled into a sequence in the Storyboard. The Sequence Viewer appears in the application as a panel in the Storyboard Editor tool.



The Sequence Viewer includes the following components:

- Title bar — Displays the name of the sequence.
- Viewer — Displays the event currently playing in the sequence.
- Overlay Transport controls — Navigates through the sequence. Visible when you hover the mouse pointer over the sequence.
- Audio meter overlay — Displays audio settings. Visible when you hover the mouse pointer over the sequence.
- Scrub bar — Lets you scrub through the sequence.
- Show/Hide Controls — Shows and hides the controls.
- Controls — Allows you to mark up the asset.
- Add/Remove Buttons — Allows you to choose which Control buttons to display.
- Timecode Controls — Allows you to select the mark in/out and other timecode types to display. Also lets you navigate through the clip to a specific timecode. If desired, the timecode controls can also be resized in the panel.

NOTE: Not all controls are displayed when the panel is not fully expanded.

You can navigate through the newly created sequence by using one of the transport controls. Each event in the sequence is indicated by a symbol in the scrub bar.

Related Topics

Identifying and selecting the timecode type on page 1095

Sequence Viewer buttons

These buttons and controls located on the Sequence Viewer let you perform various functions:

Show/Hide Control Tray: Shows or hides the control tray.

Add Marker: Logs an item for the current position.

Go to Previous Marker: Goes to previous keyword/marker.

Go to Next Marker: Goes to next keyword/marker.

Full Screen: Displays the video player in full screen.

Restore: Restores player window to the normal size.

Next Display: Displays the video player on the next display monitor.

Hide Markers and Keywords: Hides marker and keyword indicators on the scrub bar.

Timecode: Displays timecode and allows you navigate to a specific timecode. Also lets you select the timecode type for display.

These transport control buttons let you move through the selected asset:

-1 Frame: Goes back one frame.

-10 Frames: Goes back ten frames.

Rewind: Rewinds the current asset. First press, rewinds -8x speed. Second press, increases to -16x speed.

Play: Plays the clip. Toggles with the Pause button.

Fast Forward: Fast Forwards the current asset. First press, fast forwards to 8x speed. Second press, increases to 16x speed.

+10 Frames: Goes forward ten frames.

+1 Frame: Goes forward one frame.

These control buttons on the audio overlay let you control the audio of the selected asset:

Mute: Silences the selected audio channel.

Solo: Isolates the selected audio channel.

Pin Audio: Always display audio channels.

Collapse Audio: Collapses display of audio channels.

Creating a sequence

1. Open the Storyboard Editor tool and then do one of the following:
   - On the Storyboard toolbar, click the **New Sequence** button. A New Sequence dialog box opens. Enter the name of your sequence, select a K2 bin, and then click **OK**.
   - In the Navigator panel, right-click a K2 bin and select **New | Sequence**. A New Sequence dialog box opens. Enter the name of your sequence and then click **OK**.
   - Right-click in the empty space of a K2 bin in Asset List and select **New | Sequence**. A New Sequence dialog box opens. Enter the name of your sequence and then click **OK**.
2. Select an asset in a K2 bin in Asset List and drag it to the Source Viewer panel.

   The asset name displays in the title bar.
3. Choose one of the following actions:
   - To preview the asset, click the **Play** button or use the appropriate transport controls.
   - To create a mark-in point, click the the **Mark In** button.
   - To create a mark-out point, click the **Mark Out** button.
4. Drag the asset to the Storyboard. (**C**)

   The asset is now in the timeline of the Storyboard and referred to as an *event*.
5. Repeat above steps to add additional events.
6. In the panel, use the toolbar buttons to modify events.
7. Click the **Save** button to save the sequence. If you have not yet named the sequence, a Save As dialog box opens. Name the sequence and select the K2 bin in which to save the sequence.

To preview the sequence, use the transport controls in the Sequence Viewer.

Editing an event

1. Double-click an event on the timeline of the Storyboard.

   The event opens in the Source Viewer.
2. To edit, mark in and mark out the event.

The event duration automatically updates in the Storyboard.

There is no Undo feature for these operations.

Splitting an event

1. Navigate to the desired location in the event.
2. Select the **Split** button.

The event is divided into two events with identical names.

There is no Undo feature for these operations.

Configuring Storyboard Editor User Preferences

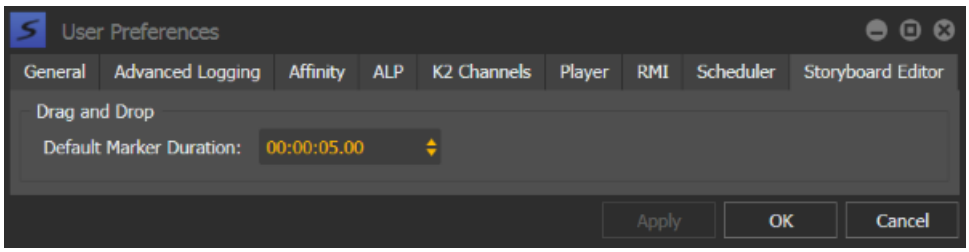
You can configure Storyboard Editor settings within the user settings preferences window.

1. Select **Edit | User Preferences**.

   The User Preferences dialog box opens.

   The GV STRATUS application shows or hides sections based on the roles assigned to your GV STRATUS log on credentials.

2. Select the **Storyboard Editor** tab.



3. Set the **Default Marker Duration** when markers are dragged and dropped as sequences into the Storyboard Editor.
4. To apply a change and continue editing user preferences settings, click **Apply**.
5. To accept any changes and close the dialog box, click **OK**.

   The dialog box closes.

Using keywords and markers to add an event to a sequence

Once you have keywords and markers to an asset, you can use those keywords and markers to add events to a sequence in the Storyboard Editor.

On the Source Viewer, Advanced Logging tool, or Markers tab in the Inspector, drag and drop the symbol associated with the keyword or marker into the Storyboard.

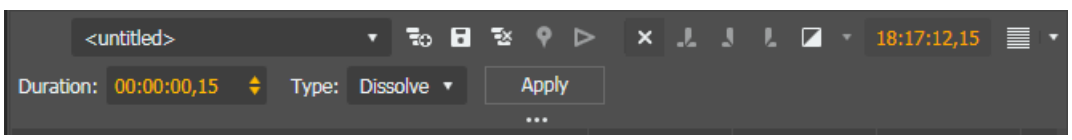
If you dragged a keyword to the Storyboard, the part of the asset between the mark-in and mark-out points is added to the sequence.

If you dragged a marker to the Storyboard, the marked part of the asset is added to the sequence. The marker duration is set according to the **Default Marker Duration** as configured in the User Preferences setting.

Adding and removing transitions

1. Click the the **Show/Hide Transition Panel** button. ...

   The transition settings open.



2. Configure transition settings as follows:
   a) Set the **Duration** of the transition.
   b) Select the **Type** of the transition.
   c) Click **Apply**.

   These settings define transitions subsequently applied with the the **Add Transition** button.
3. Select the event or events to which you are adding a transition.
4. Click the the **Add Transition** button.
   The transition is applied between each selected event and the next event.
   Transitions are indicated by icons in Thumbnails view and by text in Details and Tiles view.
5. To modify, do the following:
   a) Select an event or events, then right-click and select **Modify Transition**.
      The transition settings open, if they are not already open.
   b) Change settings and then click **Apply**.

   The changed setting is applied to the selected events.
6. To remove a transition, right-click an event and select **Delete Transition**.

Rearranging or deleting events in a sequence

Select the event in the panel and choose one of the following actions:

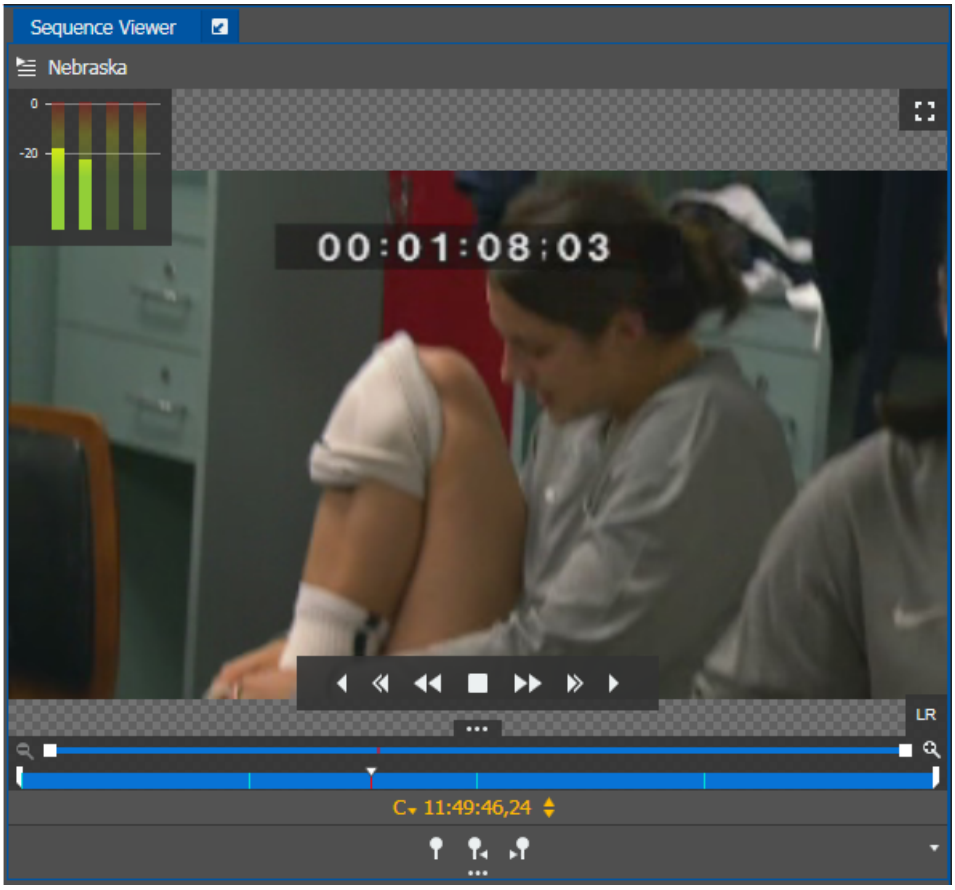
- To delete the selected event, click the **Delete** button.
- To move the selected event, drag the event to a new location in the panel.

There is no Undo feature for these operations.

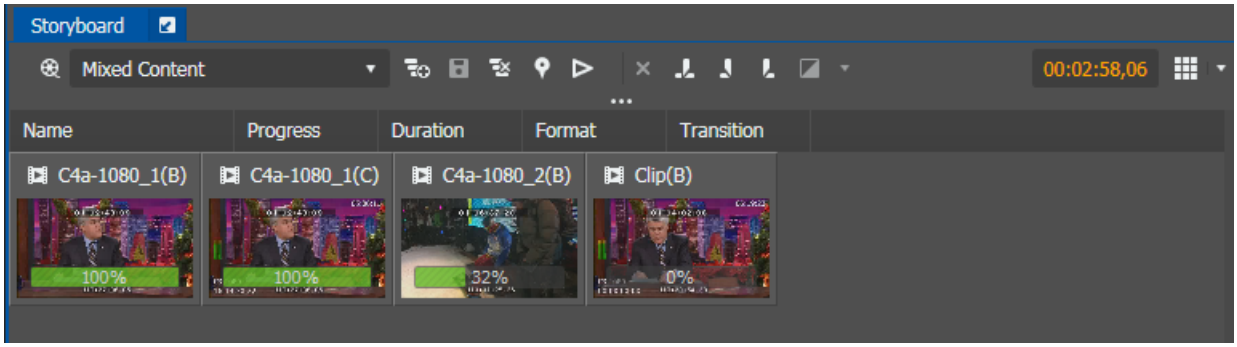
Playing a sequence

1. Drag the sequence from the Navigator to the Storyboard.

2. In the Sequence Viewer, use the transport controls to navigate through the sequence. Each event is indicated by a symbol in the scrub bar.



As the event plays in the Sequence Viewer, the event's progress indicator in the Storyboard displays the current location.



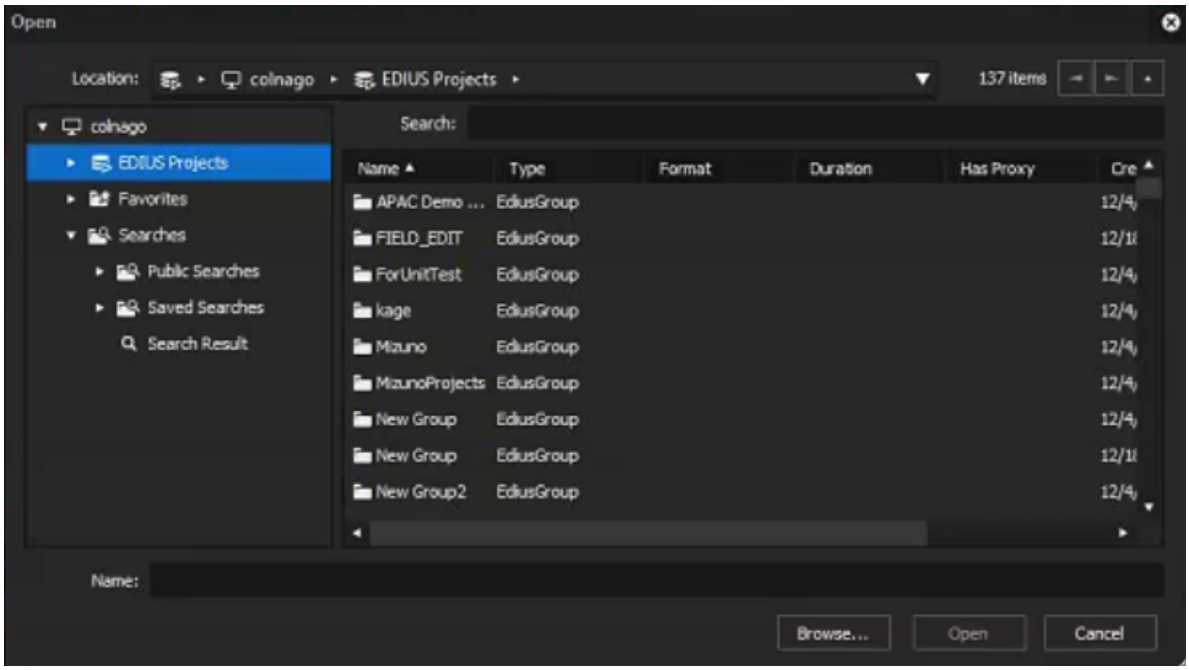
Launching a sequence in the EDIUS application

After creating a sequence in the Storyboard Editor, you can launch the sequence in the EDIUS application for further editing.

The **Launch in EDIUS** button is only available if you are assigned with the EDIUS XS role in the GV STRATUS Control Panel.

1. Create a sequence in the Storyboard Editor as you normally would.
2. Click the **Save Sequence** button.
3. Click the **Launch in EDIUS** button.
4. If you are not already logged on to GV STRATUS in the EDIUS application, a GV STRATUS logon dialog box opens. Enter your GV STRATUS credentials to log on.

   The Startup dialog appears.

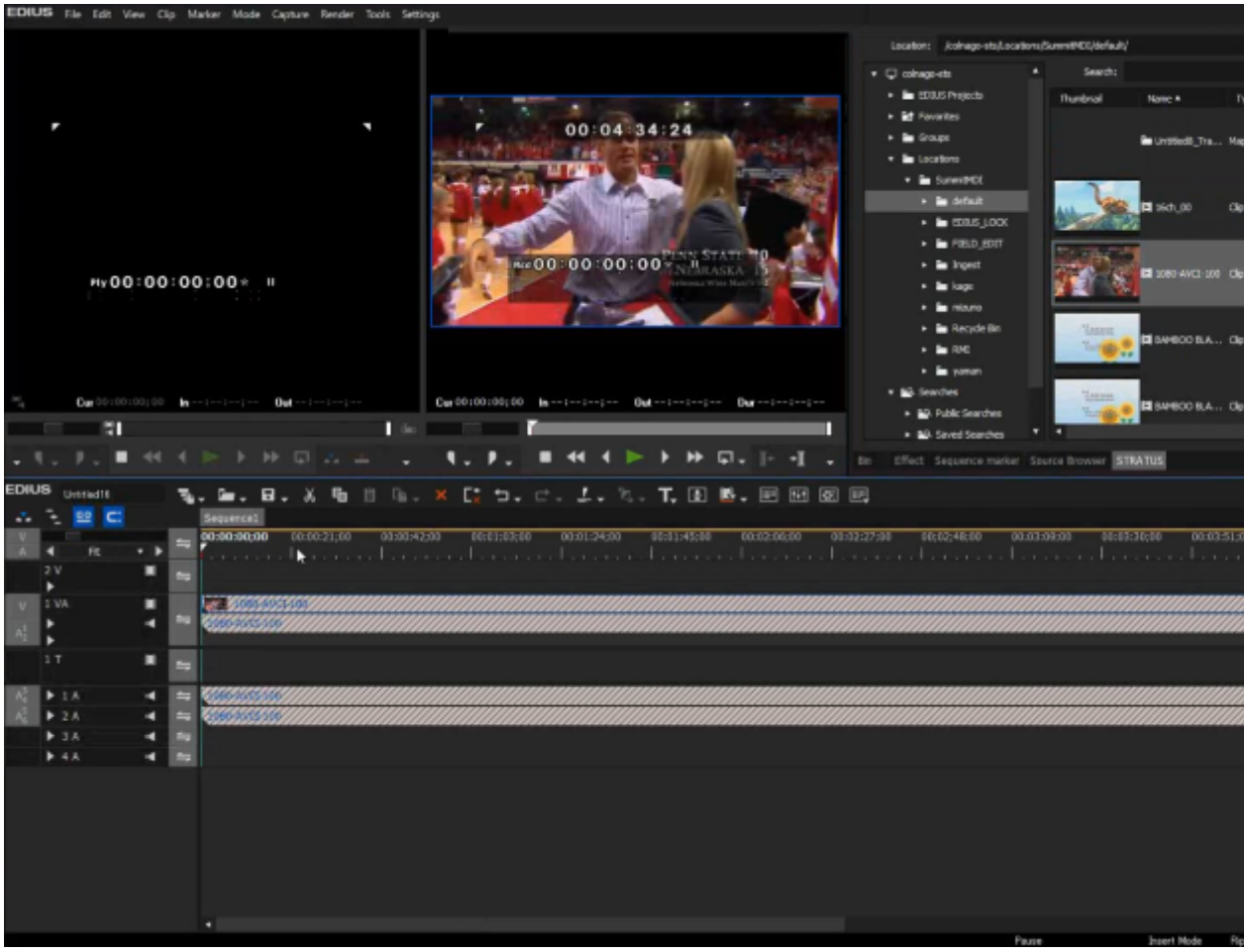


5. Select the project location.

   You can also set to other locations as long as the new location is under the default location path in EDIUS settings on the GV STRATUS Control Panel.

6. Enter the project name and click **Open**.

   The EDIUS application opens with the sequence loaded into the player and timeline.



Related Topics

Adding GV STRATUS assets to EDIUS timeline on page 1181
Sending EDIUS sequences to the K2 system on page 1189

Viewing the properties of an item

You can view the properties of an item in several locations in the application.

- To view basic asset properties as a tooltip, hover the mouse pointer over an item in the Asset List panel.
- To view more asset properties, open the asset in the Inspector panel and view the General section.
- To view properties of a playlist or sequence event, right-click on the event in the Editor Panel and select **Properties**, or drag the event to the Inspector panel.

  The event's properties display in the Inspector panel.

- To modify the display of properties in Tiles view, right-click on the Asset List panel, select **Tile Properties**, and reorder the top three items as desired.
- To view the properties associated with a keyword or marker, hover the mouse pointer over the symbol associated with that keyword or marker.

  The thumbnail and properties associated with the keyword or marker appear as an overlay tooltip.

Using EDIUS for GV STRATUS application

You can launch the GV STRATUS application as an ActiveX panel or STRATUS Browser within the EDIUS application. This allows you to use all GV STRATUS tools within EDIUS and consolidate your entire operation into one workspace.

Depending on licensing and system configuration, the EDIUS for GV STRATUS application launches as a high resolution editor (EDIUS Workgroup) or a low resolution proxy editor (EDIUS XS). The EDIUS for GV STRATUS application allows you to work with GV STRATUS assets. You can drag assets from the GV STRATUS Asset List and drop them into EDIUS player and timeline.

If GV STRATUS security is enforced, manage assets considering the following:

- If accessing assets with the GV STRATUS ActiveX panel or STRATUS Browser, GV STRATUS security applies. Your credentials must give you adequate permissions on bins and assets that are part of your workflow.
- If accessing high-resolutions assets using the EDIUS K2 Browser, GV STRATUS security does not apply. Be careful that you do not interfere with a workflow that is dependent on GV STRATUS security.

You can also undock the GV STRATUS panel from the EDIUS application window to customize the application workspace.

About high resolution and low resolution EDIUS for GV STRATUS

The EDIUS for GV STRATUS application can launch and operate as follows:

- A high resolution editor, identified as EDIUS Workgroup, which can operate in STRATUS mode or in standalone mode. In STRATUS mode, the EDIUS for GV STRATUS application can access GV STRATUS high resolution assets. In standalone mode, the EDIUS for GV STRATUS application cannot access GV STRATUS high resolution assets.
- A low resolution proxy editor, identified as EDIUS XS, which operates in a single mode that must access GV STRATUS proxy assets.

Requirements for the different launch modes and operations are as follows:

- High resolution EDIUS Workgroup:
  - Launch:
    - The GV STRATUS application must be installed.
    - All the following EDIUS licenses must be present on the local GV STRATUS/EDIUS client PC.
      - EDIUS Workgroup license
      - EDIUS K2 Option license
      - EDIUS STRATUS Option license
    - For the EDIUS Workgroup license activation, port number 80/443 or https access is required to connect to the Flexera server via the internet.
  - Operation:
    - The GV STRATUS/EDIUS client PC must be configured as a high resolution client in GV STRATUS Control Panel.
    - For STRATUS mode, the GV STRATUS/EDIUS client PC must have access to high resolution K2 storage, either with an iSCSI connection or a SMB connection.
- Low resolution EDIUS XS:
  - Launch:
    - The GV STRATUS application must be installed.
    - The EDIUS Workgroup license must not be present on the local GV STRATUS/EDIUS client PC. This is an EDIUS license, not a Sabretooth license.
  - Operation:
    - The user account logged on to GV STRATUS must have the EDIUS XS role assigned in GV STRATUS Control Panel.
    - The GV STRATUS/EDIUS client PC must have network access to low resolution proxy assets.

Create EDIUS project and shared folder

You must create a location for your EDIUS projects.

You must have a shared folder that both the GV STRATUS/EDIUS client PC and the GV STRATUS Render Engine server can access. Files like audio clips and still images can be located in this shared folder.

1. On the K2 media file system (the `V:\` drive), create a new project folder.
2. Name the folder with a meaningful name.

   For example create the following folder:

   ```
   V:\EDIUS_Projects
   ```

3. To create a shared folder, name the folder with a meaningful name.

   For example create the following folder:

   `V:\EDIUS_Projects\Shared items`

4. Make sure the folder is shared with permission granted so that your GV STRATUS/EDIUS client PCs and GV STRATUS Render Engine server can access the folder.

   On the GV STRATUS Render Engine server, the internal system account, which by default is GVAdmin, accesses the folder.

If you created several bins in your EDIUS project, the same bin structure will appear in the **Navigator** panel of GV STRATUS after you saved the project.

Related Topics

Access K2 storage for EDIUS using standard convention on page 282

Access K2 storage for EDIUS using standard convention on page 282

Applying User Settings to multiple EDIUS users

In some environments, there may be a need to create a pre-defined EDIUS user interface layout and settings, so that all users have the exact same working environment. This information is stored in EDIUS user settings, and it is possible to apply the same settings across all users, by understanding how Windows roaming user profiles work. This allows EDIUS settings to remain unchanged across all machines for all users in a shared editing environment.

To achieve this, once EDIUS has been set up as desired, user settings will be automatically saved on this path on the local machine: `C:\Users\UserName\AppData\Roaming\Grass Valley\EDIUS\9.00\User\User000\Setting`.

The file **Setting.esp** stores this information. When a new user logs in, it is possible to apply the same settings by simply copying the **Setting.esp** file over to their relevant user folder. Whenever this user closes the EDIUS application, the user settings are saved, both on the local machine and, if it exists, on the domain controller, as a roaming profile.

Secondly, some editing environments may prefer to have a single log-in for all editing users. In such case, wherever there is a Windows Domain Controller, the User Settings from the last log-out of such roaming profile will be saved to the domain controller. Hence, if a change is made to the user settings in EDIUS, it is important to update that user profile on all the machines before any of them shut down. This can be achieved by copying the **Setting.esp** file to the Setting folder indicated above.

The behavior of Microsoft Windows roaming profiles needs to be considered when setting up this type of infrastructure. Please refer to Windows-specific sources of information for more details.

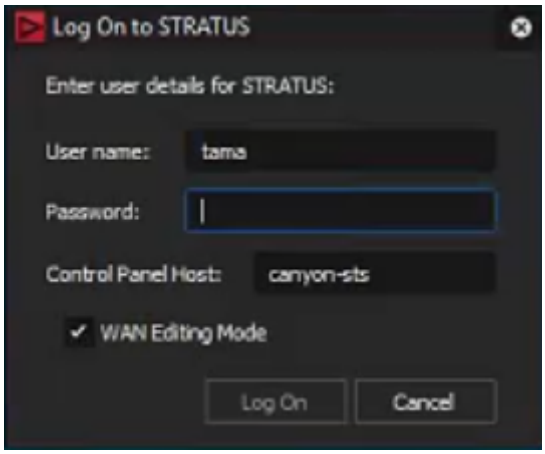
Logging on to EDIUS for GV STRATUS application

When you log on to the GV STRATUS system, the GV STRATUS application assigns GV STRATUS licenses and roles based on your user account credentials, as set by the system administrator in the GV STRATUS Control Panel application. If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins and assets that are part of your workflow. If GV STRATUS metadata access control is enforced, your credentials must give you adequate permissions

on metadata fields that are part of your workflow. Your credentials must also give you access to all your K2 systems.

1. From the Windows desktop, open the the **EDIUS** icon shortcut.

   A **GV STRATUS** Log On dialog box opens.



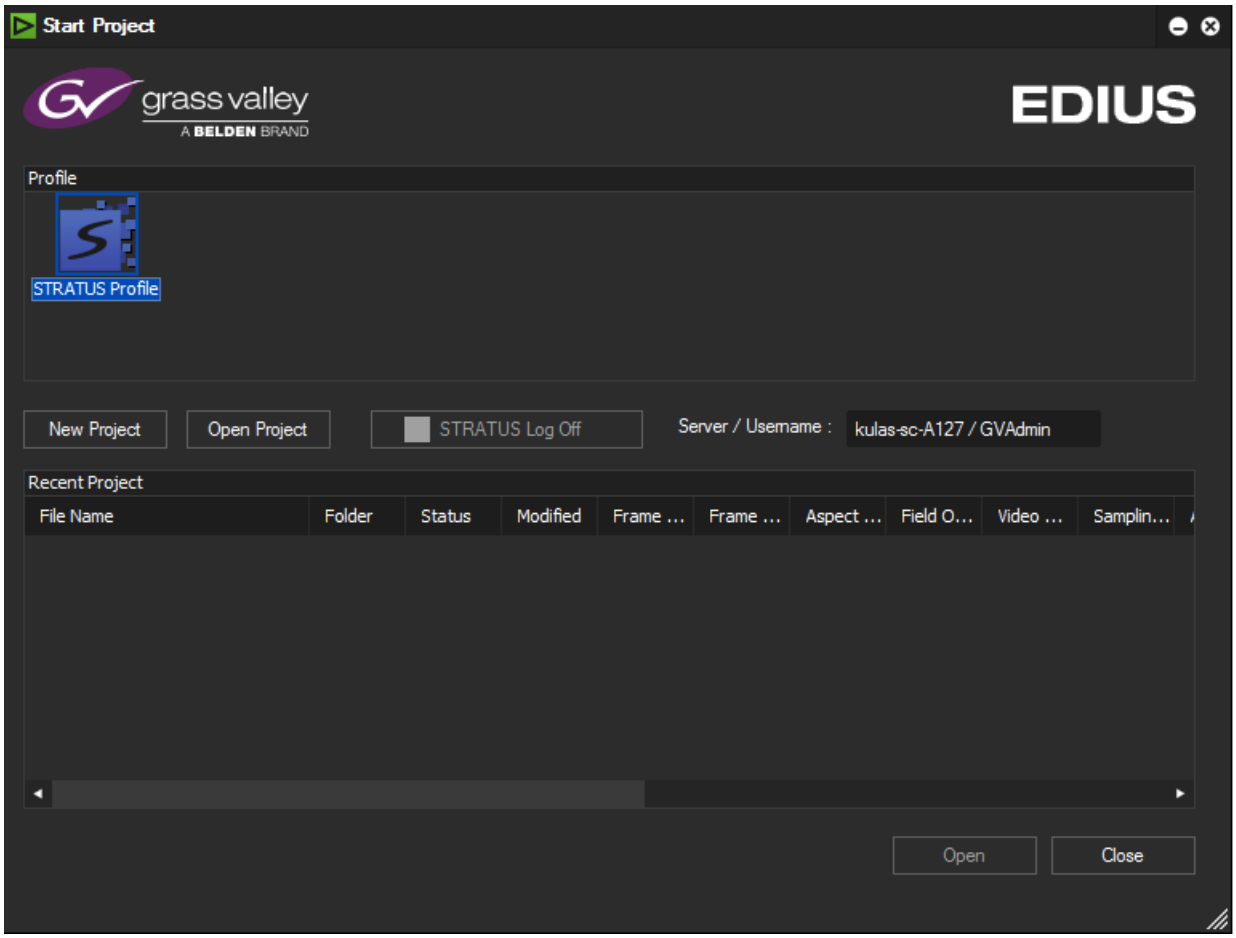
2. Enter your user name.

   If you use domain credentials, enter in format `<domain>\<username>`. For example, if your domain is "gv" and your username is "GVuser", enter `gv\GVuser`.

3. Enter your password.
4. Verify or enter the name of the Control Panel Host for the GV STRATUS Control Panel Service. In most systems, this is the main GV STRATUS Core server.
5. Select the **WAN Editing Mode** check-box if you want to work with assets procured in the field and add them to the timeline.

6. Click **Log On**.

   The **Start Project** dialog box displays.



   If the client PC is licensed for EDIUS Workgroup, the EDIUS application is now operating in STRATUS mode and can access high resolution assets. If not licensed, the EDIUS application accesses low resolution proxy assets only.

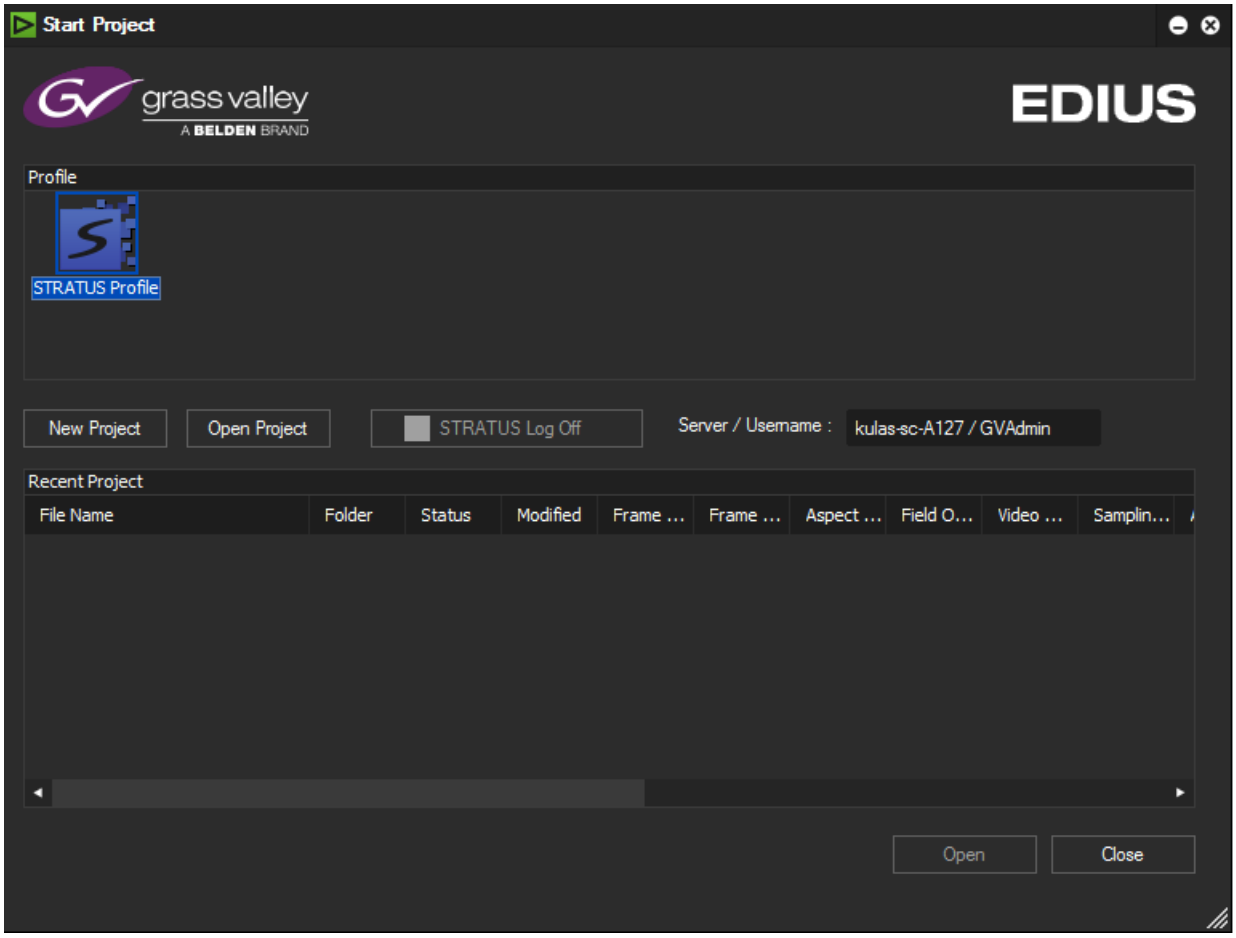
   NOTE: If a user is using the EDIUS application, it is not recommended to log into GV STRATUS's Channel Panel as the same user on the same workstation.

Related Topics

If you have trouble launching EDIUS XS on page 169

Opening an existing EDIUS project at application start

1. Open the EDIUS for GV STRATUS application and log on to the GV STRATUS system. The **Start Project** dialog box displays.

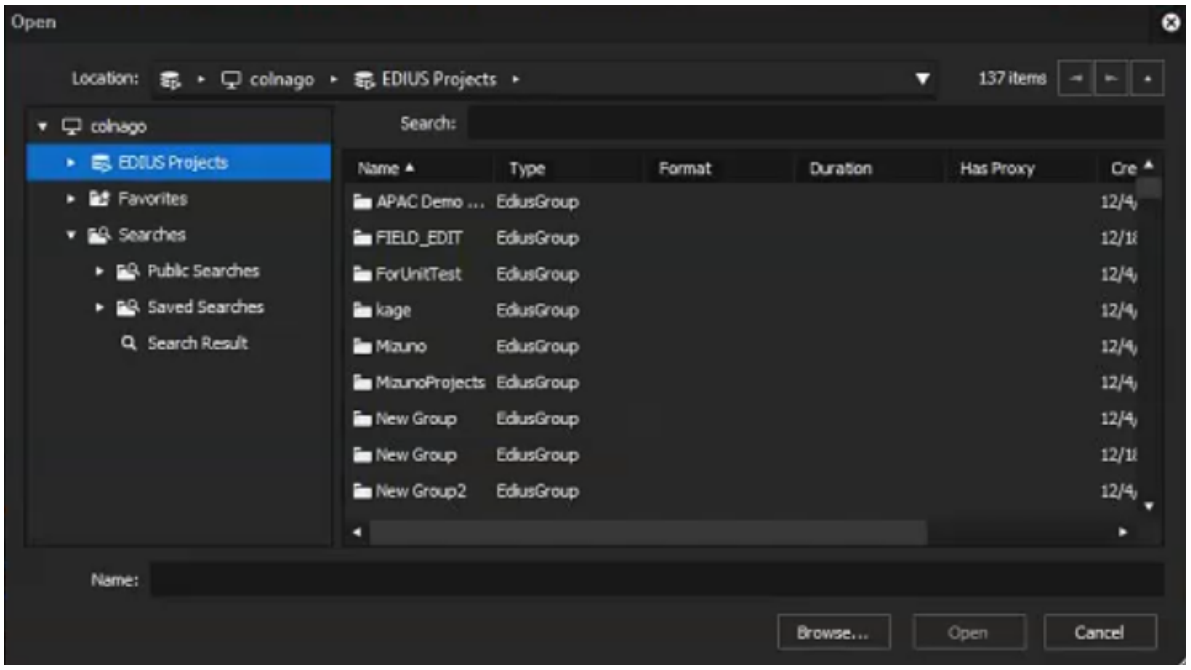


2. Proceed as follows:

   - If the desired project is listed in the **Recent Project** list, select the project and click **Open**.

     The project opens. No further steps are necessary.
   - If the desired project is not listed in the **Recent Project** list, click **Open Project** and continue with the remainder of this task.

   The **Open** dialog box opens.



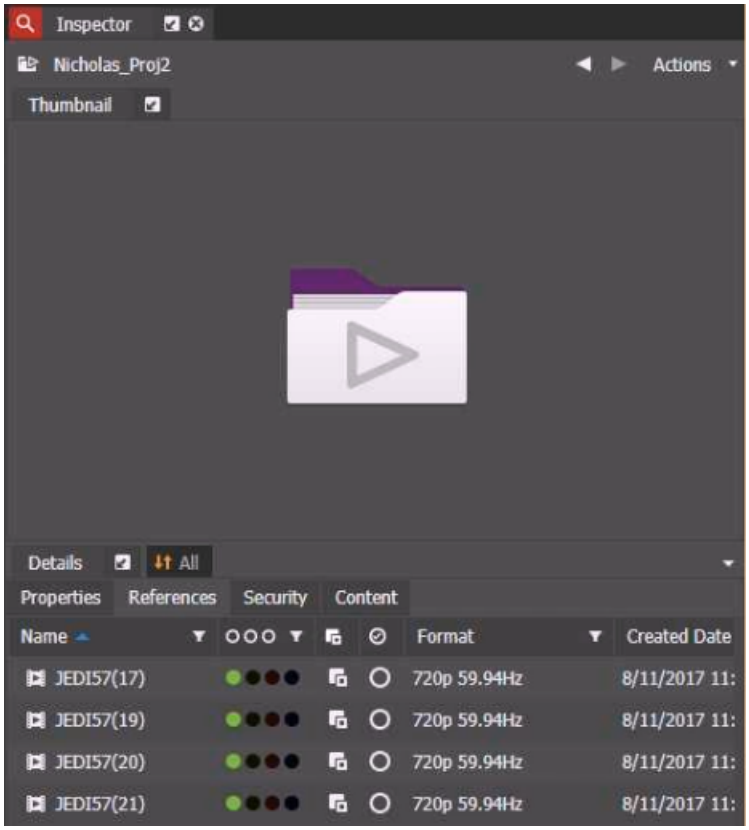
The project location is set by default to the **EDIUS Projects** folder in GV STRATUS.

3. Select a project in one of the following ways:
   - Select the project in **EDIUS Projects** folder, and click **Open**.
   - Enter the project name in the Search text box, select the project from the Search Result and click **Open**.
   - If the project is outside the managed EDIUS projects folder, click **Browse** to navigate to and select the project.

   The project opens.

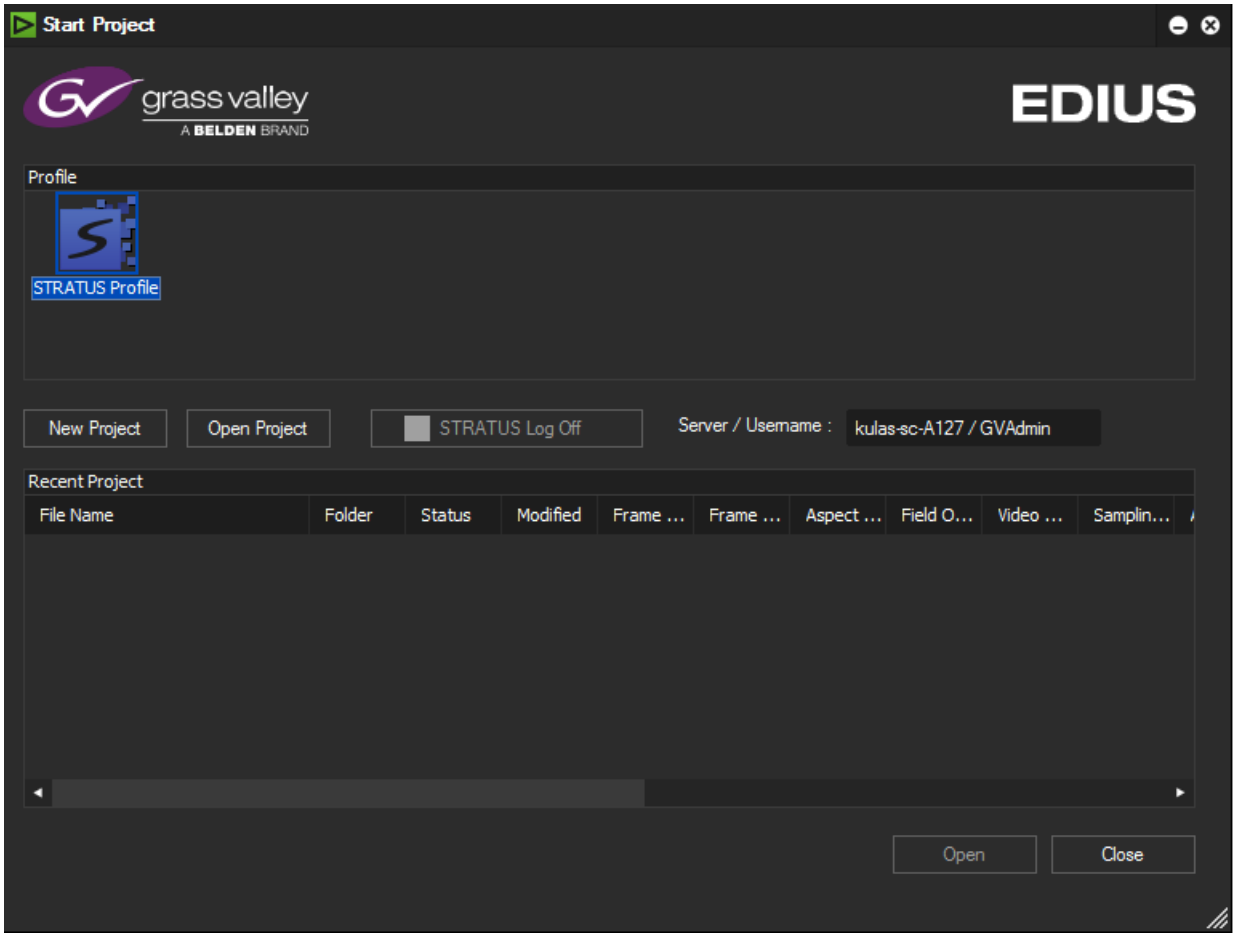
   While the EDIUS project is being edited, the project and its included sequences and clips are locked in the GV STRATUS application.

   You can view the project's list of sequences and clips on the **References** tab if you drag the EDIUS project into the Inspector.



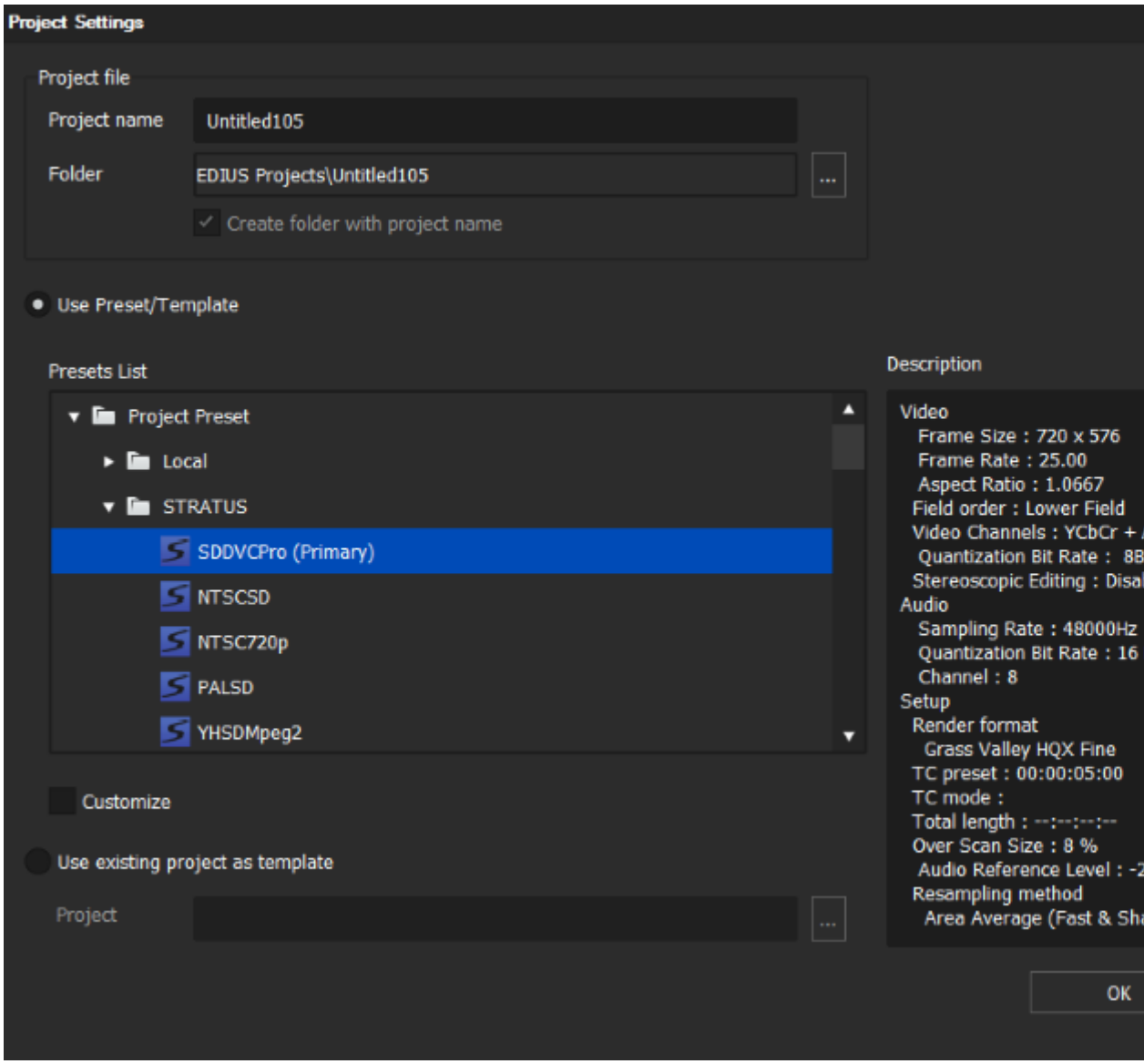
Creating a new EDIUS project at application start

1. Open the EDIUS for GV STRATUS application and log on to the GV STRATUS system. The **Start Project** dialog box displays.



2. Click **New Project**.

   The **Project Settings** dialog box displays.



3. Enter a project name.

   By default, the project folder is the **EDIUS Projects** folder in GV STRATUS and is set to create a sub-folder with the project name.

4. Set a project folder in one of the following ways:

   - Accept the default project folder with the project name.
   - Click **...** to navigate to and select another project folder.

   When logged on to the GV STRATUS system, the project folder must be under the **EDIUS Projects** folder.

5. To create the project with different settings from the project preset settings, select **Customize**. Refer to *related topics* in "EDIUS Online Manual".
6. Click **OK**.

   The new project opens.

   While the EDIUS project is being edited, the project and its included sequences and clips are locked in the GV STRATUS application.

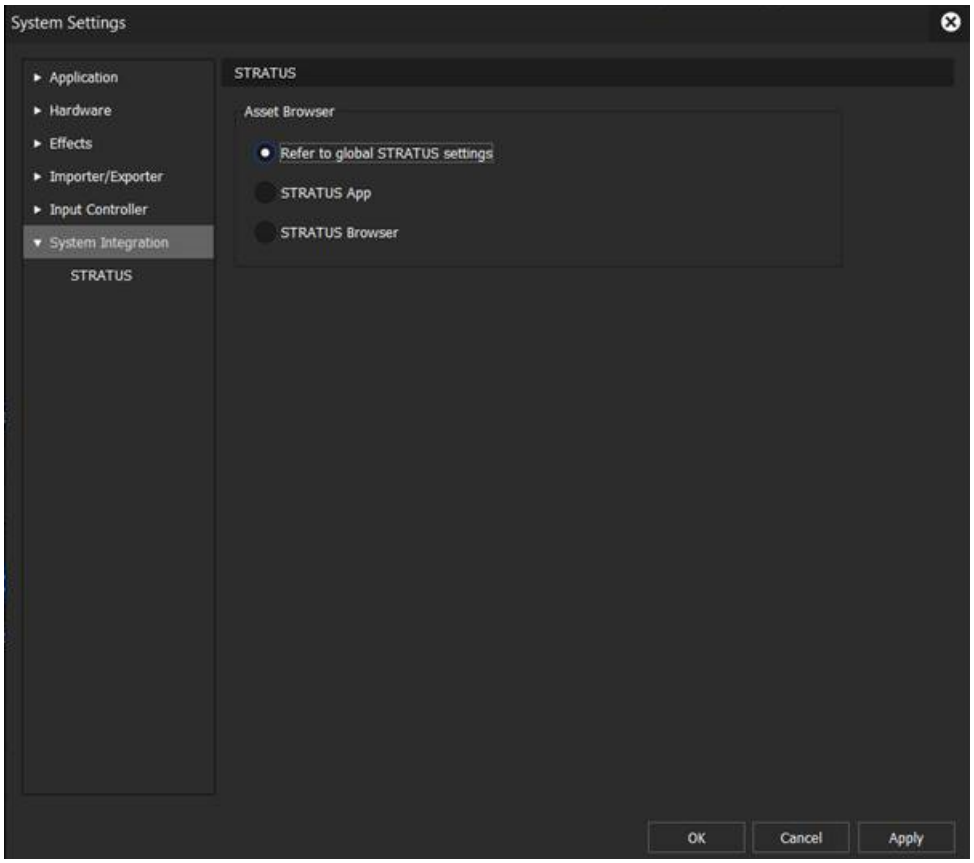
Related Topics

The Storyboard Editor tool on page 1137
Google

Opening the GV STRATUS panel in EDIUS

If you launch the EDIUS for GV STRATUS application in GV STRATUS mode, the GV STRATUS ActiveX Panel or the STRATUS browser opens by default. However, if it was previously closed, the result can be that it no longer opens automatically.

1. Click **Settings | System Settings | System Integration | STRATUS**.



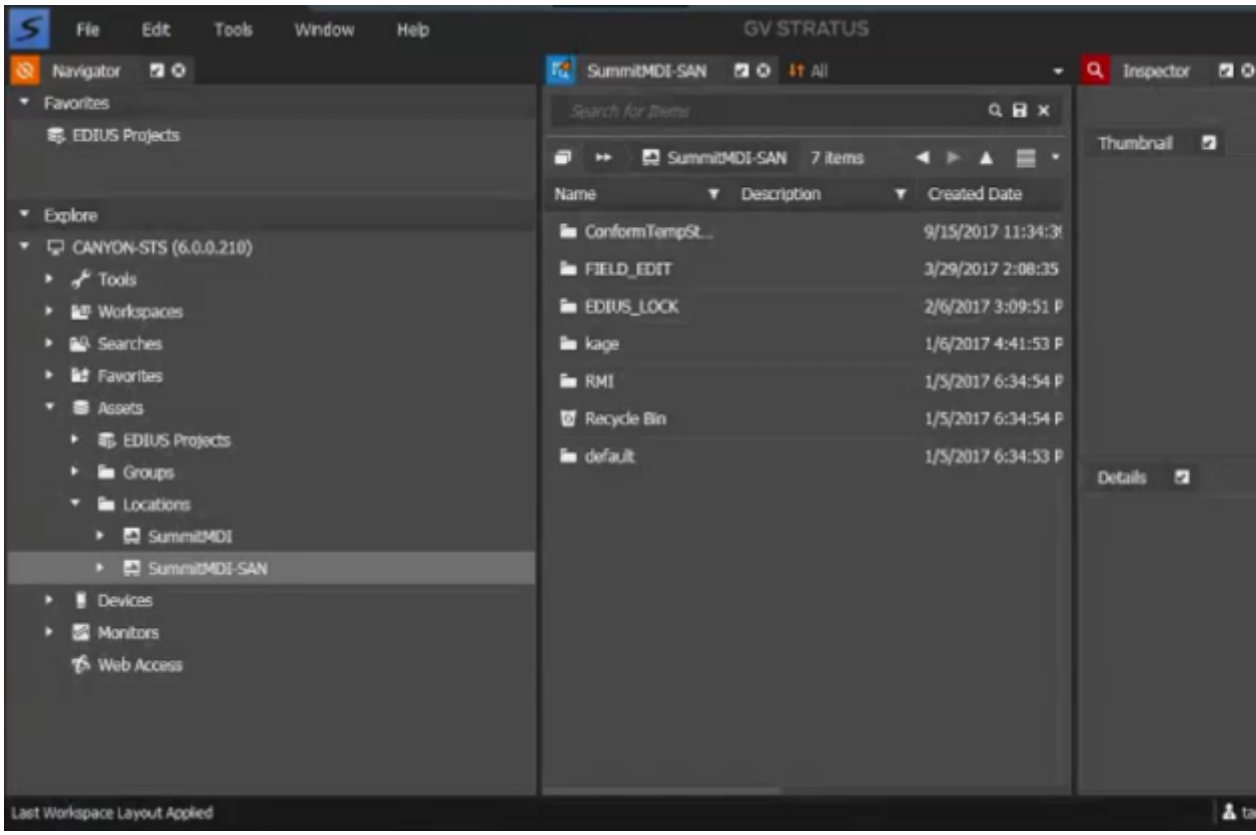
Select one from the following:

- Click **Refer to global STRATUS settings** to use the Asset Browser as configured via **EDIUS Client** settings in GV STRATUS Control Panel.
- Click **STRATUS App** to utilize GV STRATUS ActiveX panel in the EDIUS application.
- Click **STRATUS Browser** to only browse and search GV STRATUS assets in the EDIUS application.

2. If **STRATUS App** is selected, click on the **STRATUS** tab to view the GV STRATUS ActiveX panel.

   If the panel is hidden, click **View | Palette** and select **STRATUS**.

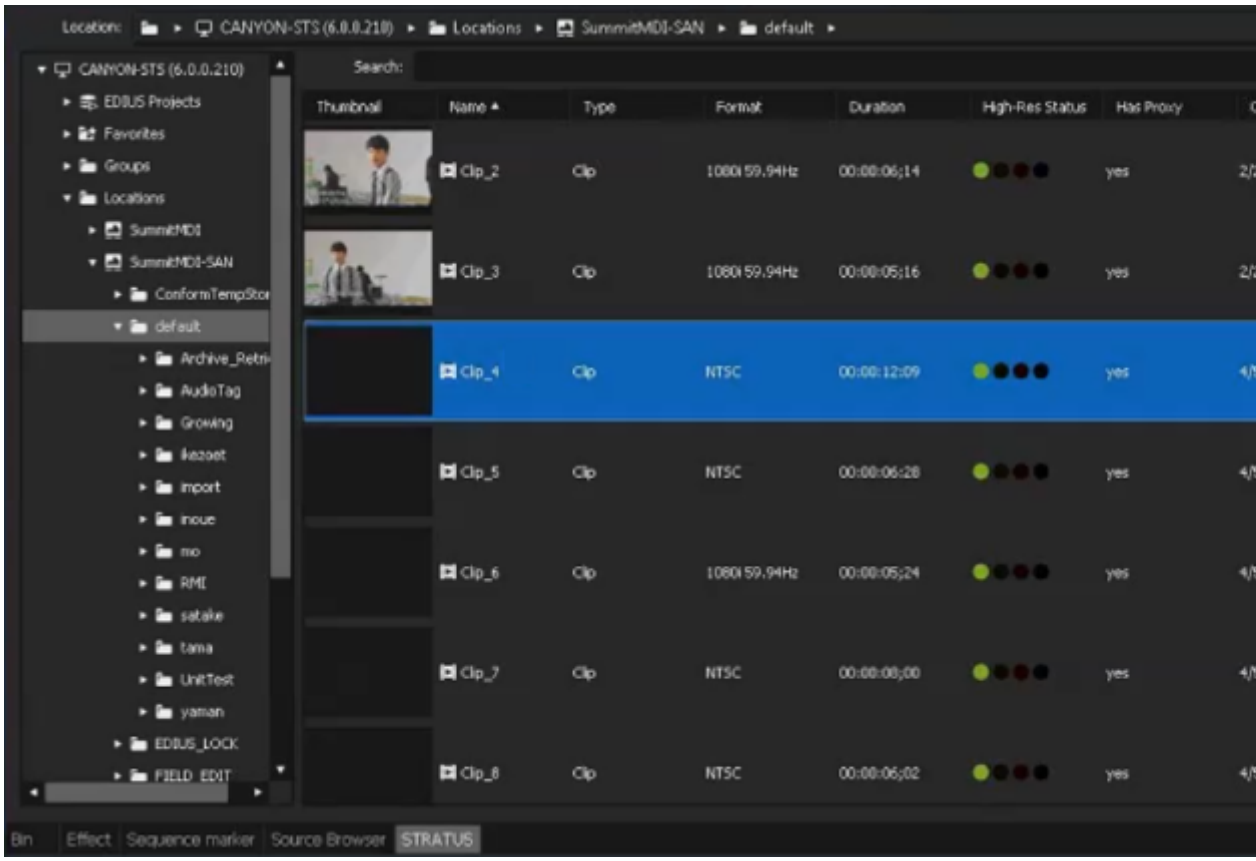
   The GV STRATUS ActiveX panel opens.



3. If **STRATUS Browser** is selected, click the **STRATUS** tab on the EDIUS browser.

   If the tab is hidden, click **View | Palette** and select **STRATUS**.

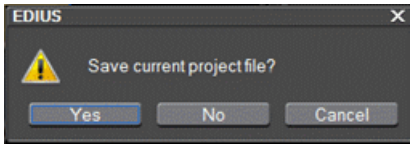
   The STRATUS Browser displays.



Opening GV STRATUS assets in the EDIUS for GV STRATUS application

1. In the GV STRATUS application, right-click an asset in an Asset List and select **Open With | EDIUS**.

   A dialog opens to confirm whether you want to save the current project.



2. Respond as appropriate for saving your project.

3. If the EDIUS for GV STRATUS application is not already open and you are not already logged on to the GV STRATUS system, log on as prompted.

   The currently opened project in EDIUS closes and the **Startup** dialog box opens.

   By default, the project location folder is the **EDIUS Projects** folder in GV STRATUS and it is set to create a folder with the project name.

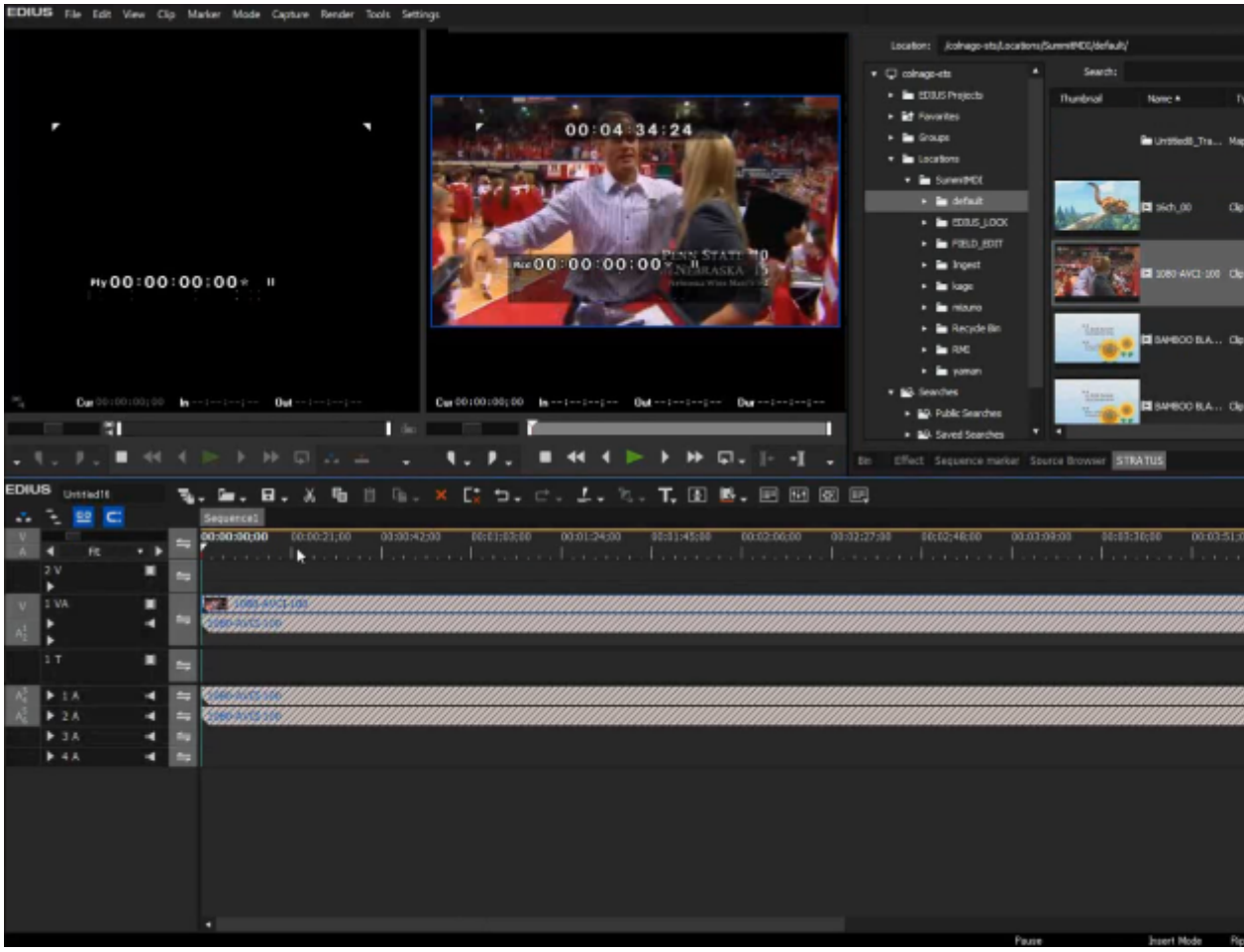
4. Set a project folder in one of the following ways:

   - Click **...** to browse and select an existing project in a sub-folder of the **EDIUS Projects** directory.
   - Click the drop-down arrow on the right of **...** to select a recently used project folder.

   You can also change the project name, if desired.

5. Click the **New** button.

   The project opens and the asset loads on the EDIUS timeline.



   You can also select to open multiple assets simultaneously on the timeline.

   In the STRATUS Browser, you can search for assets or select assets from **Saved Searches** and **Favorites** bin.

After adding assets to the timeline; you can edit, apply effects, and add voice overs to those assets.

Viewing GV STRATUS assets in the EDIUS for GV STRATUS application

If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets,

and metadata that do not have read permissions are not visible. Markers and segments permissions must be set to **Allow** in order to create, update, or delete markers and segments.

1. Drag an asset from the STRATUS tab within EDIUS, and drop it into the EDIUS Player window.

   The asset displays in the EDIUS Player window.

2. Navigate through the asset using the appropriate transport controls on the Player.

Adding GV STRATUS assets to EDIUS timeline

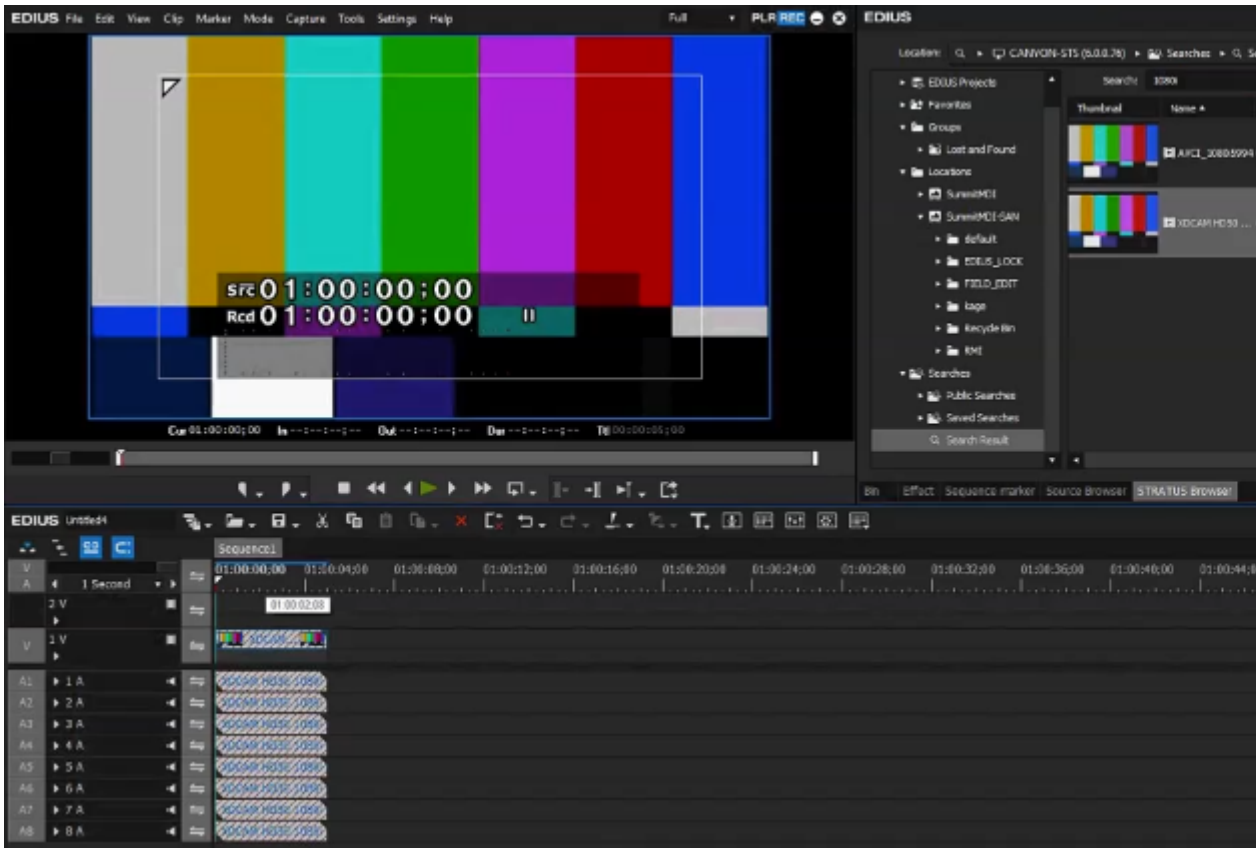
This topic applies to the EDIUS for GV STRATUS application.

If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets,

and metadata that do not have read permissions are not visible. Markers and segments permissions must be set to **Allow** in order to create, update, or delete markers and segments.

1. Drag an asset from the STRATUS tab within EDIUS, and drop it into the EDIUS timeline.

   The asset displays in the EDIUS Player window and timeline.



   You can also drag and drop multiple assets simultaneously into the timeline.

   If a low resolution client, proxy assets display in slash pattern on the timeline.

   NOTE: Copy and paste operation is not supported between the GV STRATUS panel and EDIUS application.

2. Repeat the above step until the sequence is complete.

While the EDIUS project is being edited, the project and its included sequences and clips are locked in the GV STRATUS application.

After adding assets to the timeline; you can edit, apply effects, and add voice overs to those assets.

If custom metadata is configured, red or yellow flags can be assigned to assets as follows:

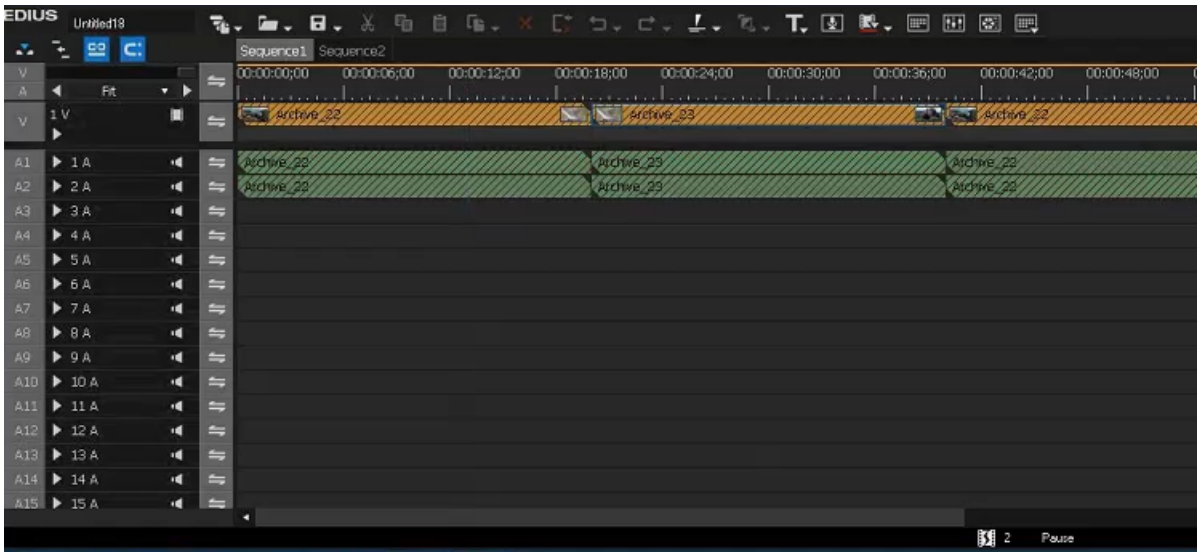
- **Red flag**: When assigned, playback and broadcast of the asset is prohibited. No video and audio are available when you load the asset.
- **Yellow flag**: When assigned, playback and broadcast of the asset should proceed with caution. Video and audio are available for the asset.

NOTE: Both red and yellow flag custom metadata are only supported for assets of type Clip and Subclip.

Restoring archived assets in EDIUS

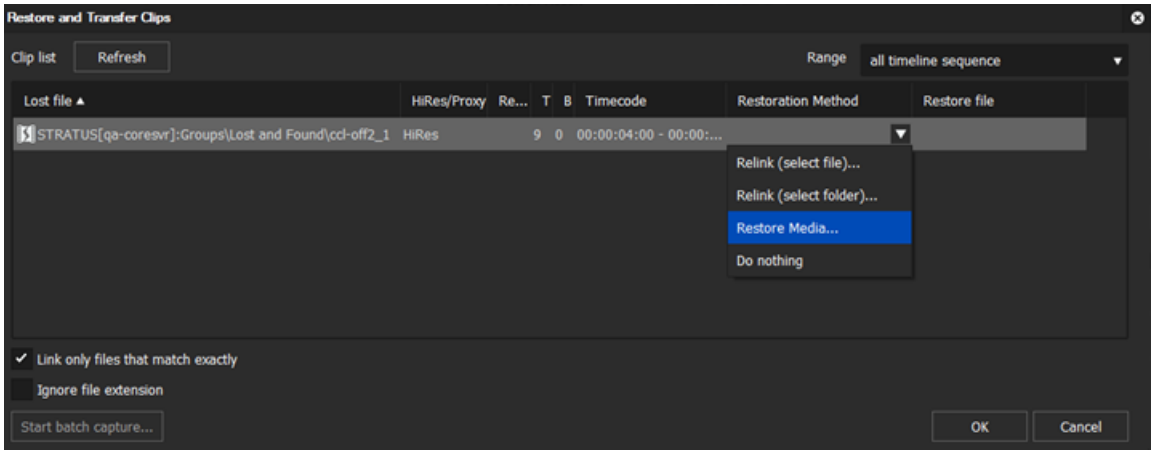
You can restore the high-resolution asset even if it has been archived by the GV STRATUS application.

1. Double-click the **Offline** icon on the status bar below the EDIUS timeline.



NOTE: The number of offline assets is also displayed next to the Offline icon.

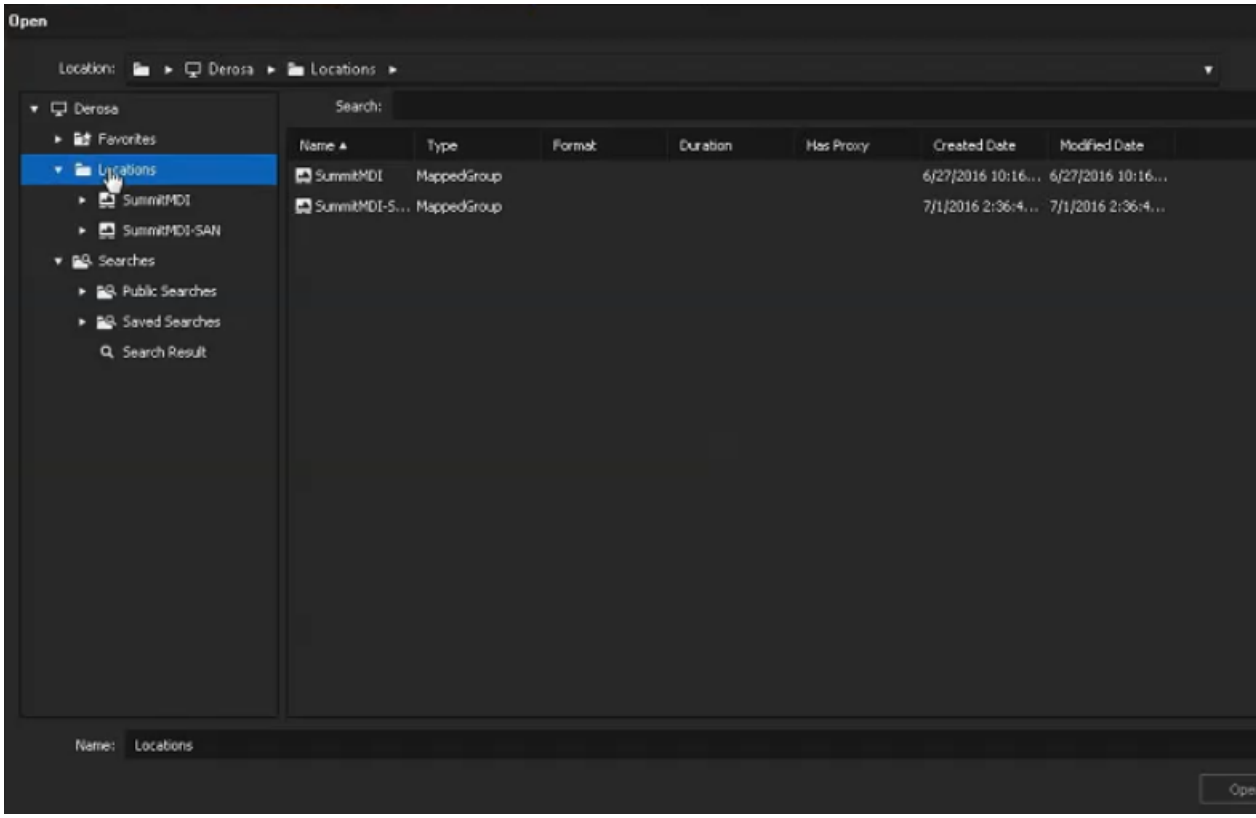
The **Restore and Transfer Clips** window opens.



2. Select the asset to be restored and click the drop-down list under the **Restoration Method** column.

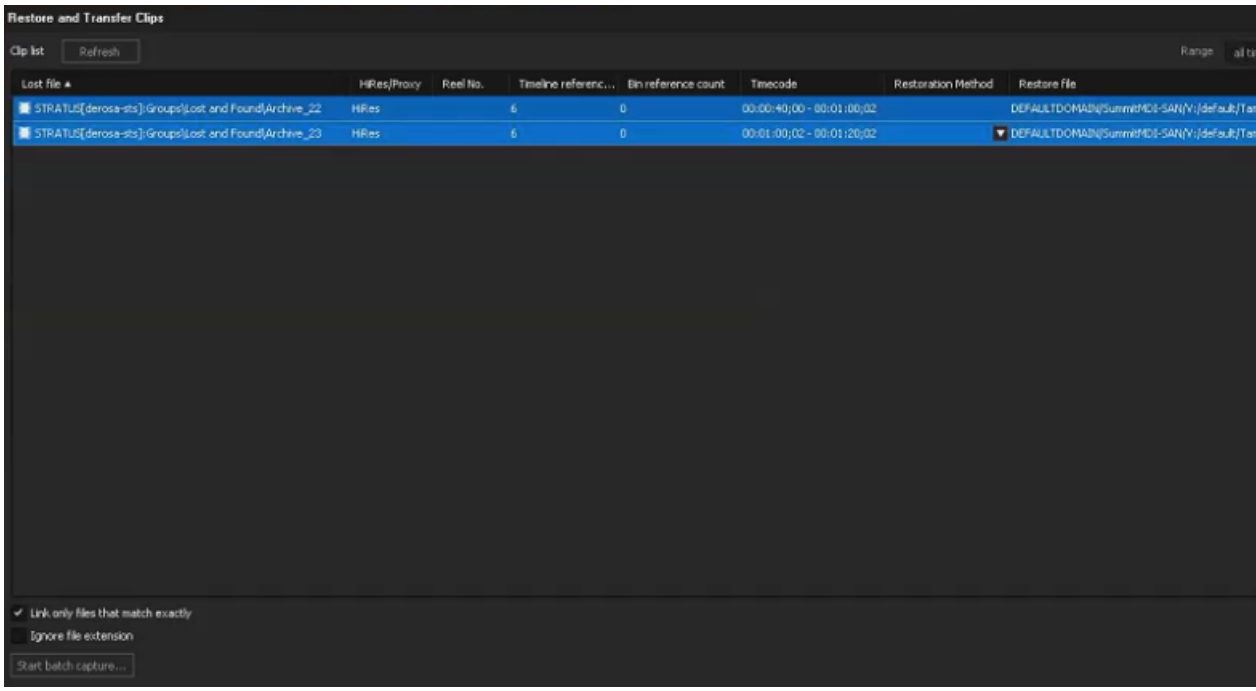
3. Select **Restore Media**.

   The **Open** window launches.



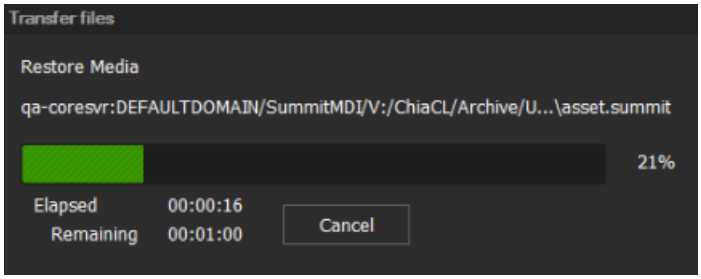
4. Select the destination of asset to be restored and click **Open**.

   The selected location displays under the Restore File column in the **Restore and Transfer Clips** window.



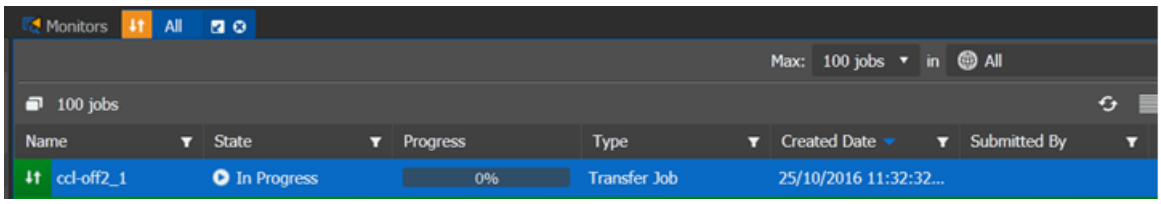
5. Click **OK**.

   EDIUS triggers the restore from archive system and transfer the high-resolution assets.

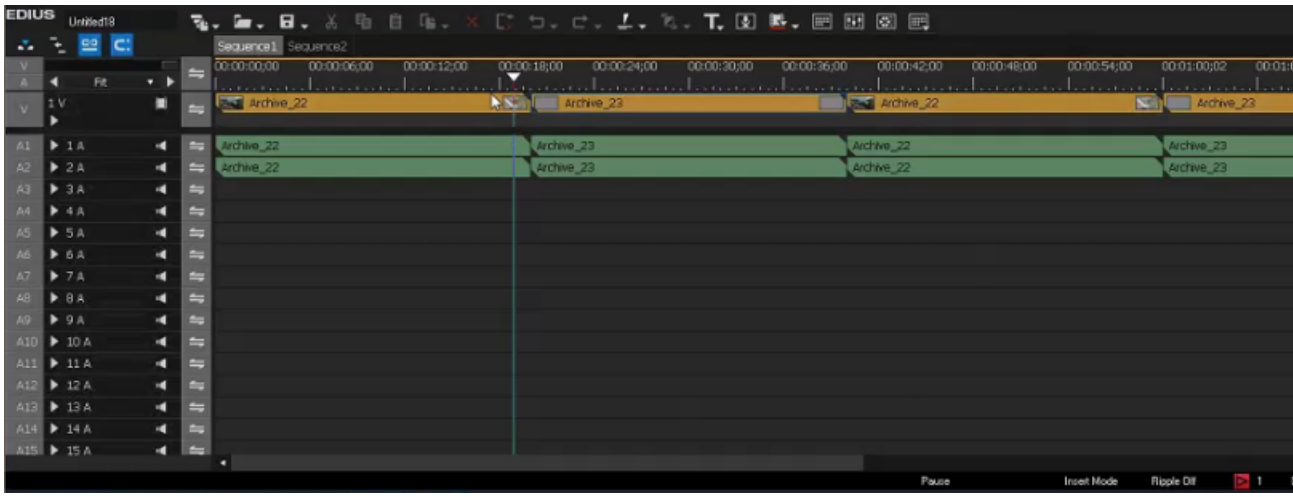


NOTE: Once in progress, cancellation of the Restore Media operation is not supported.

You can also monitor the transfer on the GV STRATUS Jobs Monitor.



After a successful transfer, assets appear as online on the EDIUS timeline.

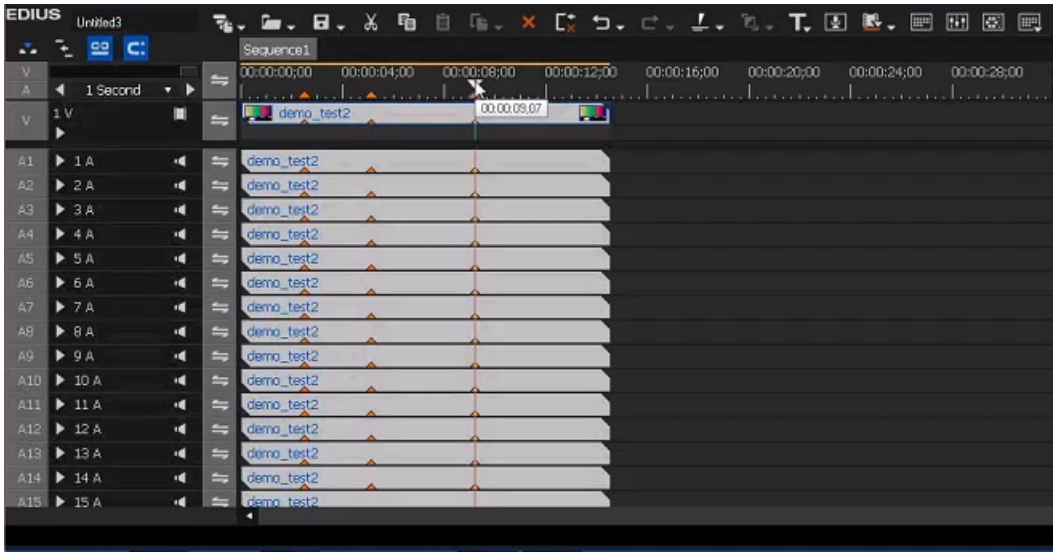


Sending EDIUS sequences with markers and keywords to GV STRATUS

1. Select a sequence on the EDIUS timeline.

   NOTE: Markers and keywords of the original source clip are not supported to be sent to the GV STRATUS system.

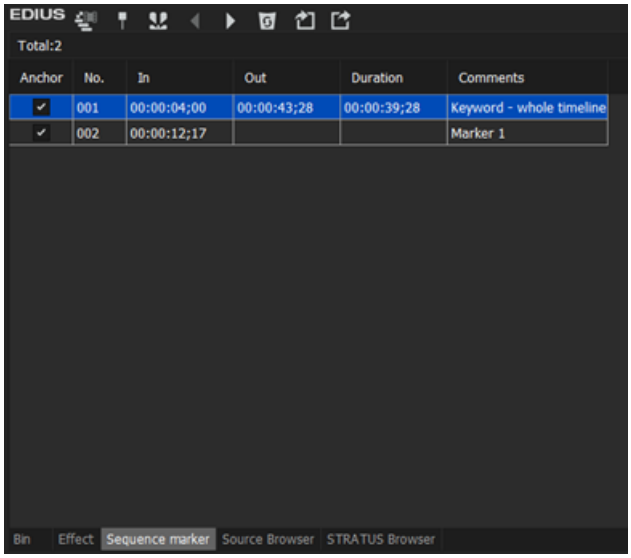
   However, if you create markers and keywords according to the following procedure; they will also be sent to GV STRATUS system together with the sequence.



2. To create markers/keywords on the EDIUS timeline, scrub the cursor to the desired time/duration, select the **Sequence Marker** tab and do the following:

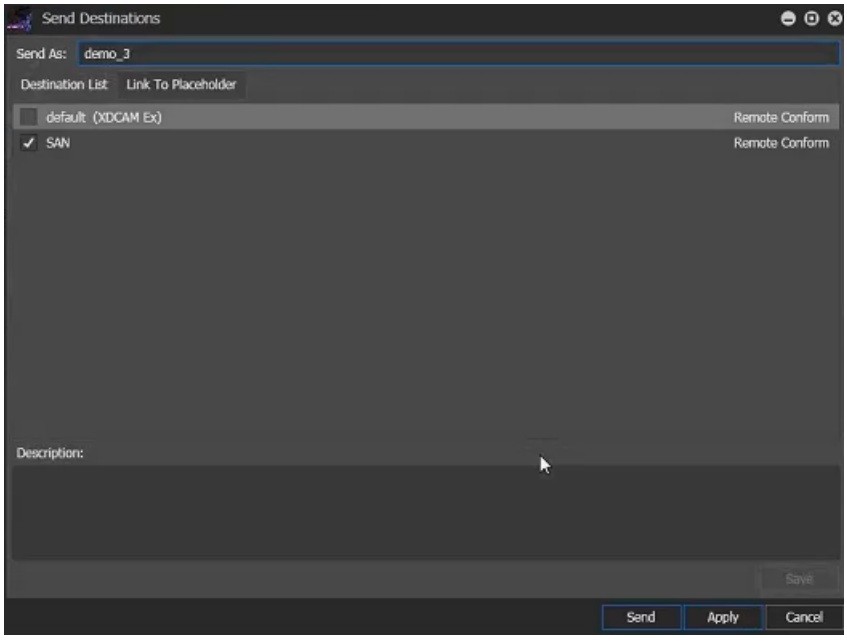
   - To create a marker, right-click on the **Sequence Marker** tab, and select **Set Mark**.
   - To create a keyword, right-click on the **Sequence Marker** tab, and select **Set Mark In/Out**.

   Markers and keywords display on the **Sequence Marker** tab.



3. Press the **F11** key.

   The **Send Destination** dialog box opens.



4. Enter the name of the sequence in the **Send As** box.
5. In the **Destination List**, select one or more conform destinations.

   NOTE: You cannot select both transfer and conform destinations at the same time.

6. If configured for a Newsroom Computer System, you can also link the sequence to a local or remote placeholder.
   - If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, and metadata.
   - In order to link to a placeholder, you must be assigned with write permission for the **Name** property in Metadata section of GV STRATUS Control Panel.

   a) On the **Link To Placeholder** tab, select a placeholder.

   If a remote placeholder, expand the remote site node.

   If already linked to a placeholder, you can select a different placeholder.

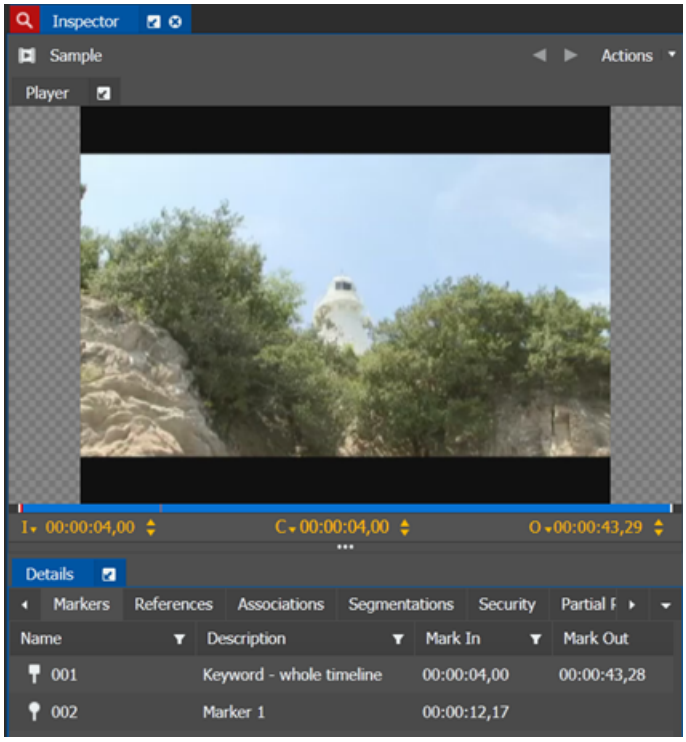
   b) If desired, in the **Placeholder Description** field, enter text and click **Save**.
   The placeholder description is updated.

7. Click **Send**.
   The transfer is initiated. If transferring multiple assets, transfer jobs are queued.

The sequence is sent to the GV STRATUS system.

You can check the progress of the transfer in the GV STRATUS Jobs Monitor.

Once the transfer is complete, you can view the asset in the Inspector.



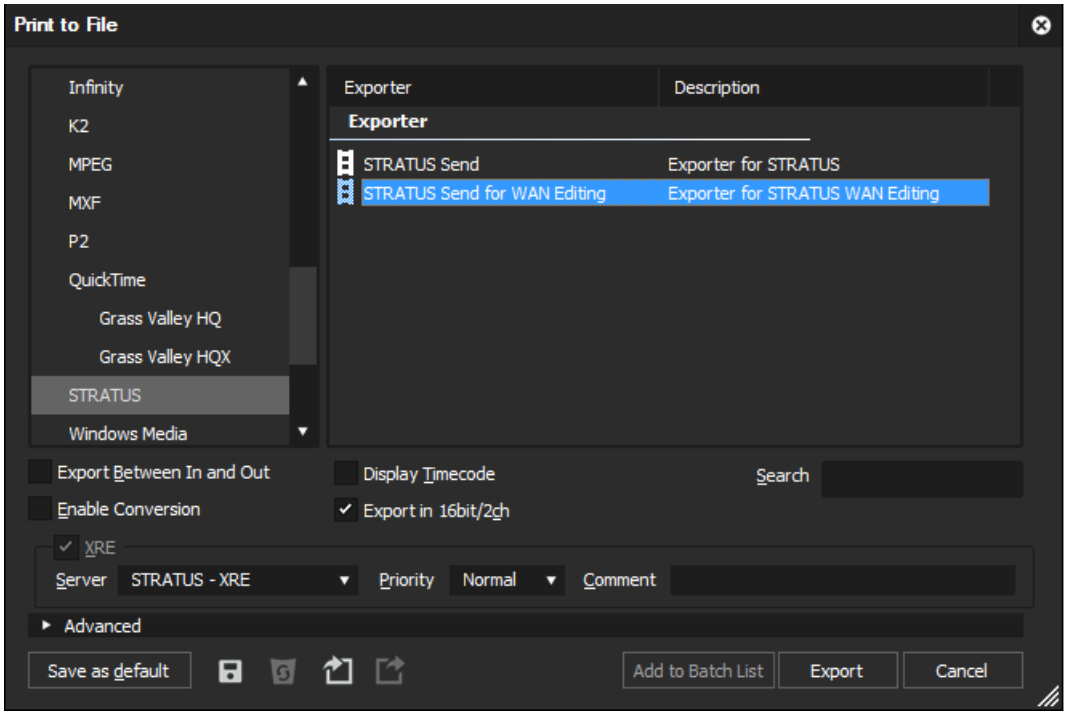
Markers and keywords created in EDIUS can be viewed on the Markers tab of the Inspector.

Sending EDIUS sequences to the K2 system

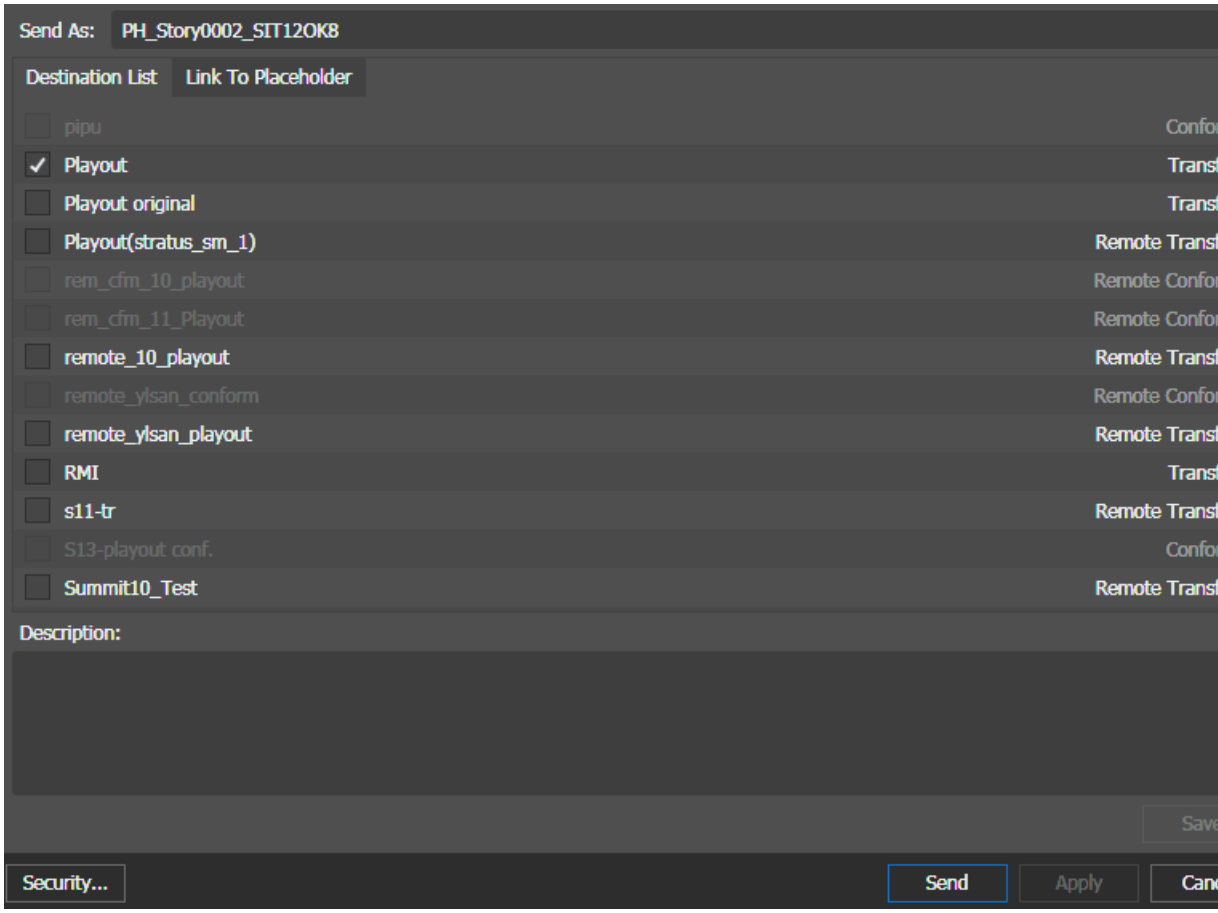
You can send a sequence in EDIUS directly to a playout bin on the K2 system. The sequence can only be sent via the GV STRATUS Render Engine server.

1. Select a sequence on the EDIUS timeline.

2. Press the **F11** key, then proceed as follows:
   - For the low-resolution EDIUS for STRATUS application (EDIUS XS), the **Send Destination** dialog box opens. Skip ahead to the next step.
   - For the high-resolution EDIUS for STRATUS application (EDIUS Workgroup), the **Print to File** dialog box opens. Do the following substeps:



   a) Make sure **XRE** is selected.
   b) In the Exporter section, select **STRATUS Send** and then click **Export**.
      The **Send Destination** dialog box opens.



3. Enter the name of the sequence in the **Send As** box.

   Asset and bin names must comply with K2 system specifications.

4. In the **Destination List**, select destinations as follows:

   - Select one or more transfer destinations
   - Select one or more conform destinations

   You cannot select both transfer and conform destinations.

5. If configured for a Newsroom Computer System, you can also link the asset to a local or remote placeholder.
   - If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, and metadata.
   - In order to link to a placeholder, you must be assigned with the **Rename Asset Rights** role and write permission for the **Name** property in Metadata section of GV STRATUS Control Panel.

   a) On the **Link To Placeholder** tab, select a placeholder.

   If a remote placeholder, expand the remote site node.

   If already linked to a placeholder, you can select a different placeholder.

   b) If desired, in the **Placeholder Description** field, enter text and click **Save**.

   The placeholder description is updated. It is not necessary to click **Send** to update the placeholder description.

6. Click **Send**.

   The transfer is initiated. If transferring multiple assets, transfer jobs are queued.

The sequence is sent to the playout server.

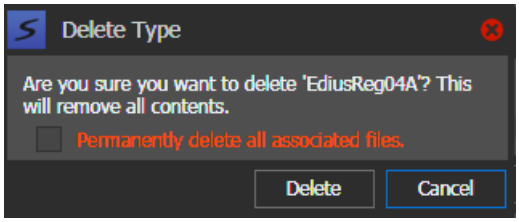
You can check the progress of the transfer in the GV STRATUS Jobs Monitor.

Deleting EDIUS Projects

Only users assigned with **EDIUS Project Management** and **Media Manager** roles are able to delete EDIUS Projects via the GV STRATUS application.

1. In an Asset List panel, right-click on the EDIUS project you are deleting and select **Delete**.

   A Delete Type dialog box opens.



   - If the **Permanently delete all associated files** check-box is selected, the entire EDIUS Project and all associated assets in the project will be permanently deleted in GV STRATUS database and the project location.
   - If the **Permanently delete all associated files** check-box is not selected, the EDIUS Project will only be deleted from the GV STRATUS database. The EDIUS Project and sequence are still accessible if you browse to the project location using Windows Explorer.

2. Click **Delete**.

The EDIUS project and associated assets in the project are deleted according to your selection. However, assets in the EDIUS sequence can only be deleted if the asset is not in use (for example, if the asset is loaded in a K2 Summit channel).

Importing still images and audio clip from EDIUS to GV STRATUS

Before performing this task, there must be a shared folder that both the GV STRATUS/EDIUS client PC and the GV STRATUS Render Engine can access. Files like audio clips and still images are located in this shared folder.

1. Open the EDIUS for GV STRATUS application.
2. In Window Explorer, open the shared folder.
3. Browse the folder and select the files that you want to copy to the timeline.
4. Drag the still images and audio files from the shared folder and drop them into the EDIUS timeline.
5. When editing is complete, send the sequence to the K2 system.

The sequence becomes a GV STRATUS system asset. The asset includes the still images and the audio clips.

Related Topics

Sending EDIUS sequences to the K2 system on page 1189

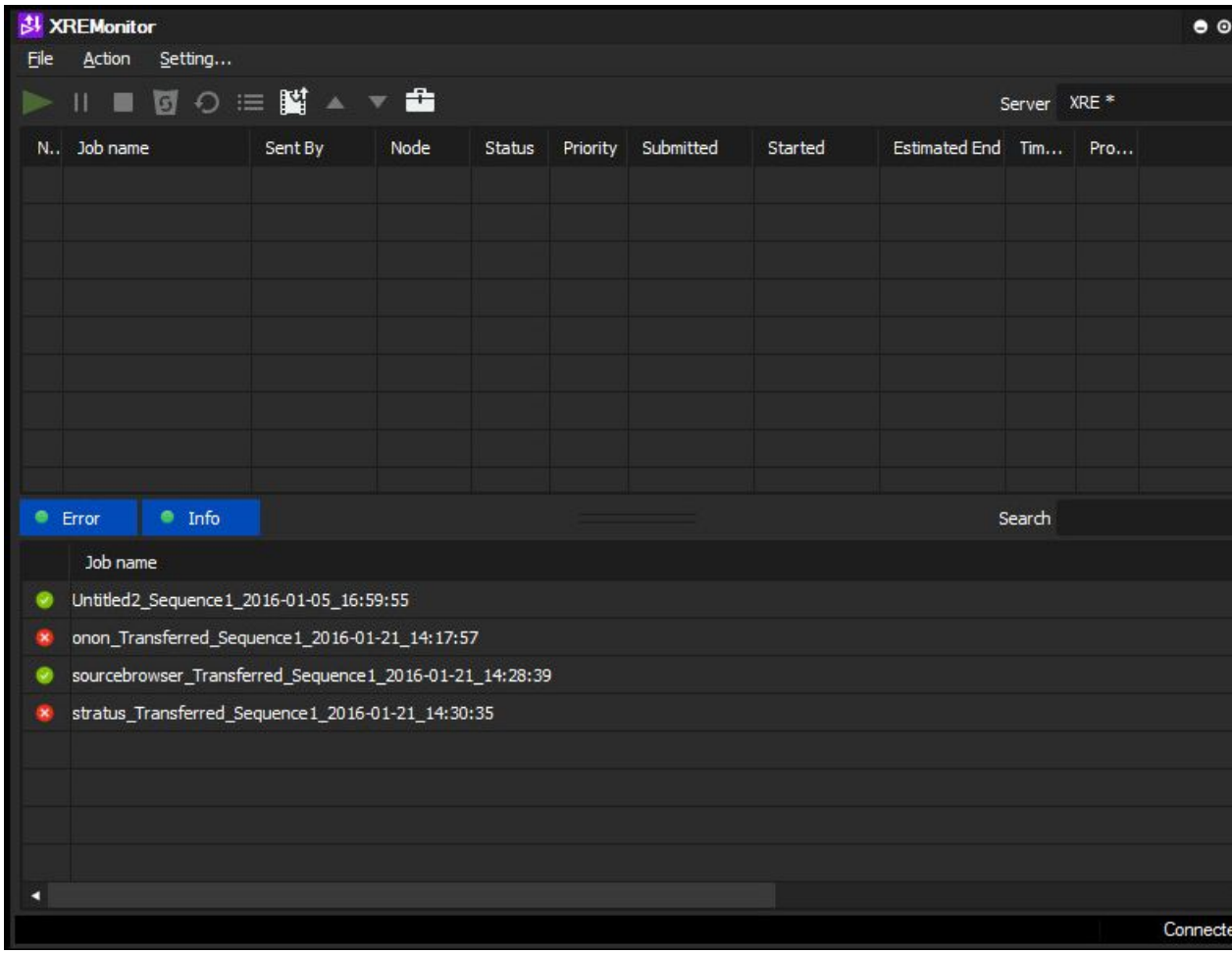
Using XRE Monitor

The XRE Monitor tracks the status of EDL files sent to a specified Render Engine Server, allowing you to quickly monitor multiple Render Engine Servers and their current job queue.

Once an item is in the queue, you can stop the current job if you need to reprioritize or re-edit a sequence. You can also filter the jobs that display in the XRE Monitor, letting you see only those jobs you need to monitor.

1. From the Windows desktop, click the **Start | All Programs | Grass Valley | XREMonitor** icon.

   The XRE Monitor opens.



2. View the progress of sent EDL files.

Field or button	Description
Server	A drop-down list of the Render Engine Servers available to you at your location
Setting | Add	Lets you add a Render Engine Server to the XRE Monitor
Setting | Delete	Lets you remove a Render Engine Server from the XRE Monitor
Stop/Continue	Stops or pauses the dynamic updates of the XRE Monitor; it has no impact on the Render Engine Server itself
No.	The XRE Monitor assigns a unique ID to each job that comes in; each job increments the ID by one
Job Name	Name of the clip as sent to the Render Engine Server
Sent By	Name of the machine that sent the job
Status	Gives updated status on the completion of a job; status messages include "Job completed successfully", "Job failed"; failure messages may provide information on some functions
Started	Indicates when the job began transferring
Progress	Specifies what percentage of the job has completed; updates automatically
Time Remaining	Specifies how long the job takes to finish the transfer process
Search	Lets you search what jobs to view; you can filter by Job name, Sent By, or by specified time in hours and minutes
Cancel	Click to cancel jobs you have selected
Close	Click to exit out of the XRE Monitor

About EDIUS WAN Editing

With an EDIUS Workgroup workstation in the field, you can integrate with the GV STRATUS system at your home site to combine both field and home assets on the same timeline.

EDIUS WAN Editing integration with GV STRATUS provides the following:

- Add assets you have procured in the field to the timeline. These are high-resolutions assets stored on the local EDIUS Workgroup workstation.
- Access assets from the home GV STRATUS system as proxy media.
- Mix the home site proxy assets and the local high-resolution assets on the same project/timeline.
- Send the completed project/sequence to the home GV STRATUS system. The project/sequence is rendered and becomes a GV STRATUS asset.

You can drag assets from the GV STRATUS Asset List and drop them onto the EDIUS timeline.

From the timeline that contains both high-resolution field assets and proxy home assets, you can create a project or a story. You can do this while you are in the field yet remotely connected to the GV STRATUS system at your home site.

EDIUS Workgroup allows mixed-format editing as it converts between HD and SD resolutions, aspect ratios, and frame rates in real time during rendering by the GV STRATUS Render Engine at the home site. In WAN editing mode, clips can be trimmed and transcoded using H.264 format.

The EDIUS Workgroup application automatically provides WAN editing capabilities as follows:

- The project must be saved in a location outside of the managed project location on the `V:` drive. Typically, the project is saved on the GV STRATUS/EDIUS client PC local drive. EDIUS Workgroup must be operating in WAN mode (not GV STRATUS mode) to create and save a project outside of the managed project location.
- The EDIUS timeline must be exported using the **Print to File** dialog box configured for **XRE** and **STRATUS Send for WAN Editing**. This sends to the home GV STRATUS system for rendering by the GV STRATUS Render Engine.

Field editing on the EDIUS timeline

You can use the proxy assets from the home GV STRATUS system and mix with high-resolution assets gathered in the field.

1. On the EDIUS Workgroup workstation, launch the EDIUS for GV STRATUS application.
2. Log on to the GV STRATUS system at application launch; in WAN Editing mode.

   NOTE: It is recommended to use WAN Editing mode to avoid unexpected traffic on the network. You can select the STRATUS Send for WAN Editing option when sending the asset later.

3. Create and save a project in a location outside of the managed project location on the `V:` drive.
4. In the EDIUS Workgroup Source Browser, select a local high-resolution asset and drag it onto the timeline.
5. Launch the STRATUS ActiveX panel or STRATUS Browser.
6. Log on to the GV STRATUS system when prompted.

   The GV STRATUS panel opens.

7. In the EDIUS Workgroup GV STRATUS panel, select a GV STRATUS proxy asset and drag it onto the timeline.

   The proxy asset on the timeline displays diagonal lines to indicate that it is proxy.

The timeline contains both high-resolution and proxy assets.

Next, edit the EDIUS project sequence as desired. Then send the project to the home GV STRATUS system.

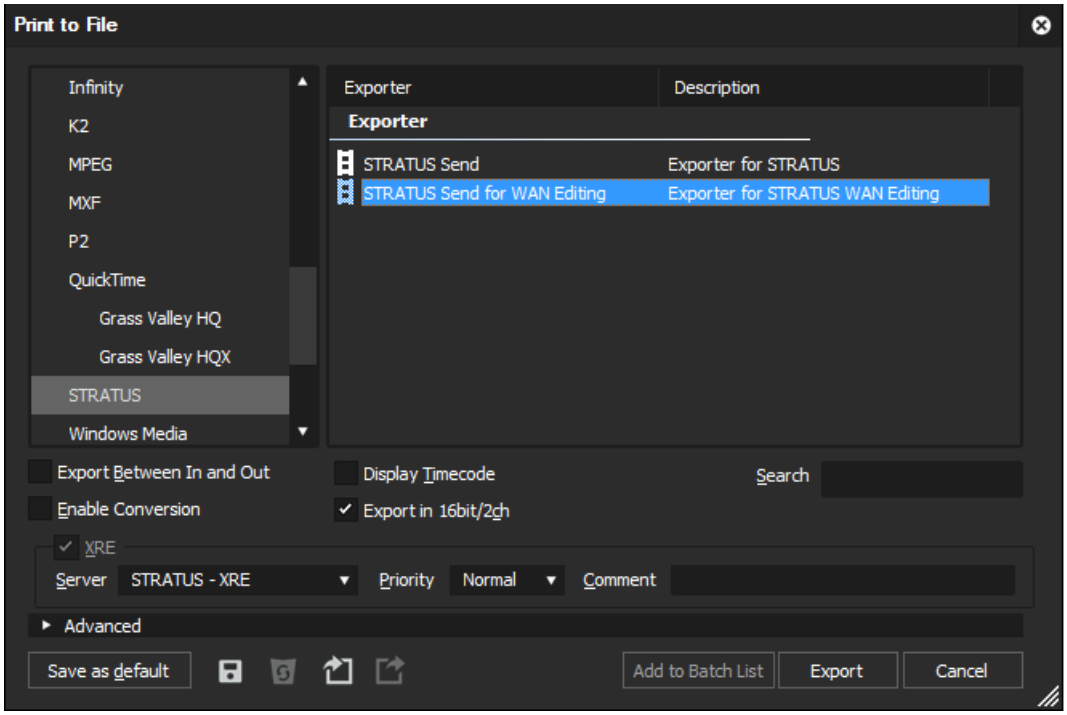
Related Topics

Sending the field EDIUS project to the home GV STRATUS system on page 1197

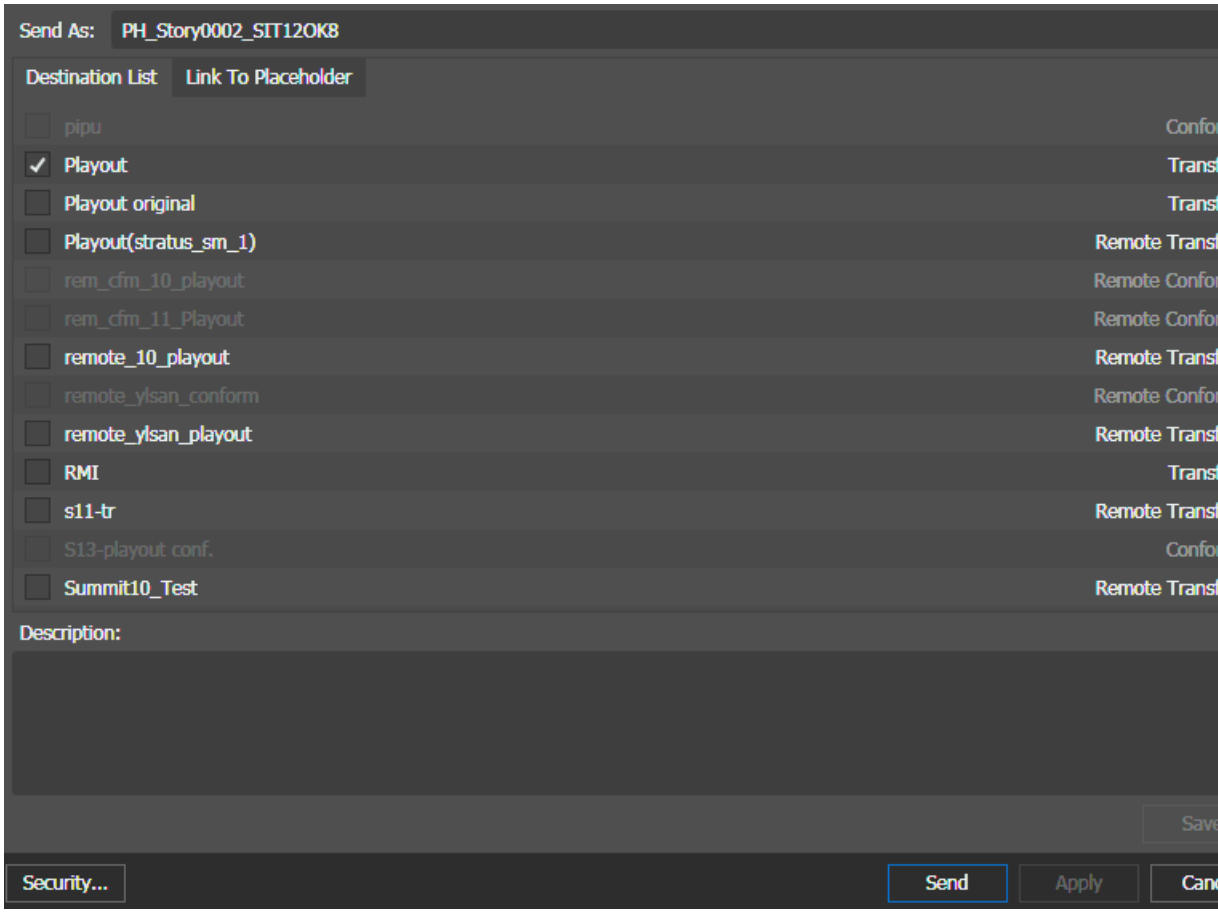
Sending the field EDIUS project to the home GV STRATUS system

- The project must be saved in a location outside of the managed project location on the `V:` drive.

1. Select a sequence on the EDIUS timeline.
2. Press the **F11** key.
   The **Print to File** dialog box opens.



3. On the **Print to File** dialog box, do the following substep:
   a) Select the **STRATUS Send for WAN Editing** Exporter and then click **Export**.
   The **Send Destination** dialog box opens.



4. Enter the name of the sequence in the **Send As** box.

   Asset and bin names must comply with K2 system specifications.

5. In the **Destination List**, select destinations as follows:

   - Select one or more transfer destinations
   - Select one or more conform destinations

   You cannot select both transfer and conform destinations.

6. If configured for a Newsroom Computer System, you can also link the asset to a local or remote placeholder.
   - If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, and metadata.
   - In order to link to a placeholder, you must be assigned with the **Rename Asset Rights** role and write permission for the **Name** property in Metadata section of GV STRATUS Control Panel.

   a) On the **Link To Placeholder** tab, select a placeholder.

      If a remote placeholder, expand the remote site node.

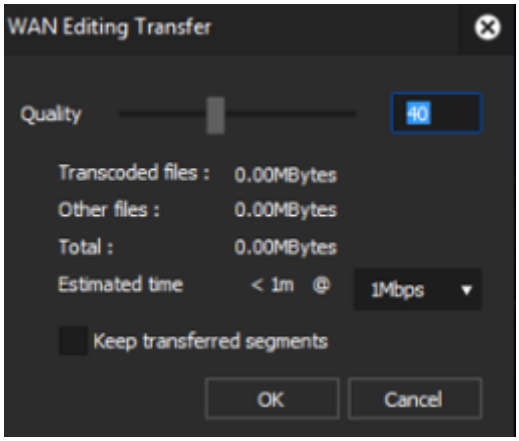
      If already linked to a placeholder, you can select a different placeholder.

   b) If desired, in the **Placeholder Description** field, enter text and click **Save**.

      The placeholder description is updated. It is not necessary to click **Send** to update the placeholder description.

7. Click **Send**.

   The WAN Editing Transfer dialog appears.

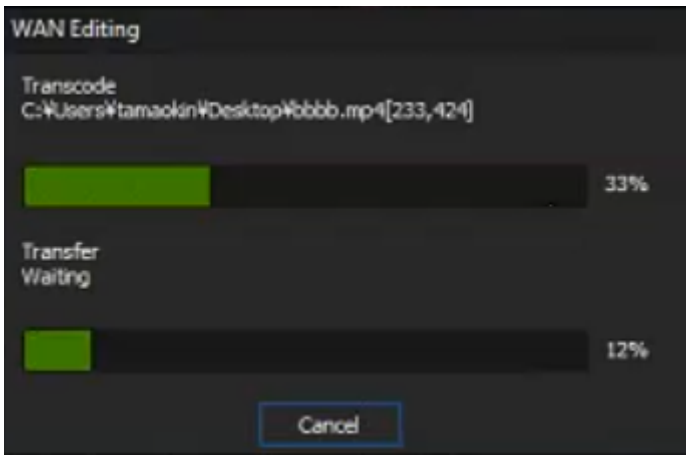


   You can drag the slider to set the quality of the transcoded file, and click on the drop-down list to set the speed of the transfer

   You can also select the **Keep transferred segments** check-box to re-use the transcoded file, if desired.

8. Click **OK**.

   The WAN Editing dialog appears.



The EDIUS Workgroup field-to-home site render process creates and transfer GV STRATUS asset from the EDIUS Workgroup project.

You can also check the progress of the transfer in the GV STRATUS Jobs Monitor.

Related Topics

EDIUS Workgroup field-to-home site render process on page 1200

EDIUS Workgroup field-to-home site render process

When you use the EDIUS WAN Editing with GV STRATUS to send a field project to the home site GV STRATUS system, the following occurs:

1. For proxy assets, EDIUS Workgroup sends project information to the home GV STRATUS system.
2. For high-resolution assets in a format supported by GV STRATUS, EDIUS Workgroup sends only the edited portion to the home GV STRATUS system. If the high-resolution asset is in a format not supported by GV STRATUS, EDIUS Workgroup sends the entire asset to the home GV STRATUS system.
3. EDIUS Workgroup sends high-resolution assets in H.264 format.
4. At the home GV STRATUS system, the Render Engine server receives the EDIUS project and related information.
5. For the proxy asset information received from EDIUS Workgroup in the field, the Render Engine server access the associated high-resolution asset on the home GV STRATUS system.
6. The Render Engine server combines the H.264 assets received from EDIUS Workgroup in the field with the high-resolution assets from the home GV STRATUS system and conforms the project to a GV STRATUS asset in the house format.

Optionally, if you are at the home site later and you connect the EDIUS Workgroup workstation that was in the field to the home GV STRATUS system, you can re-render the EDIUS Workgroup project. When you do so, the Render Engine server uses the high-resolution assets on the EDIUS Workgroup workstation that you procured in the field, rather than H.264 assets. The result is a higher resolution for the field assets in the conformed GV STRATUS asset.

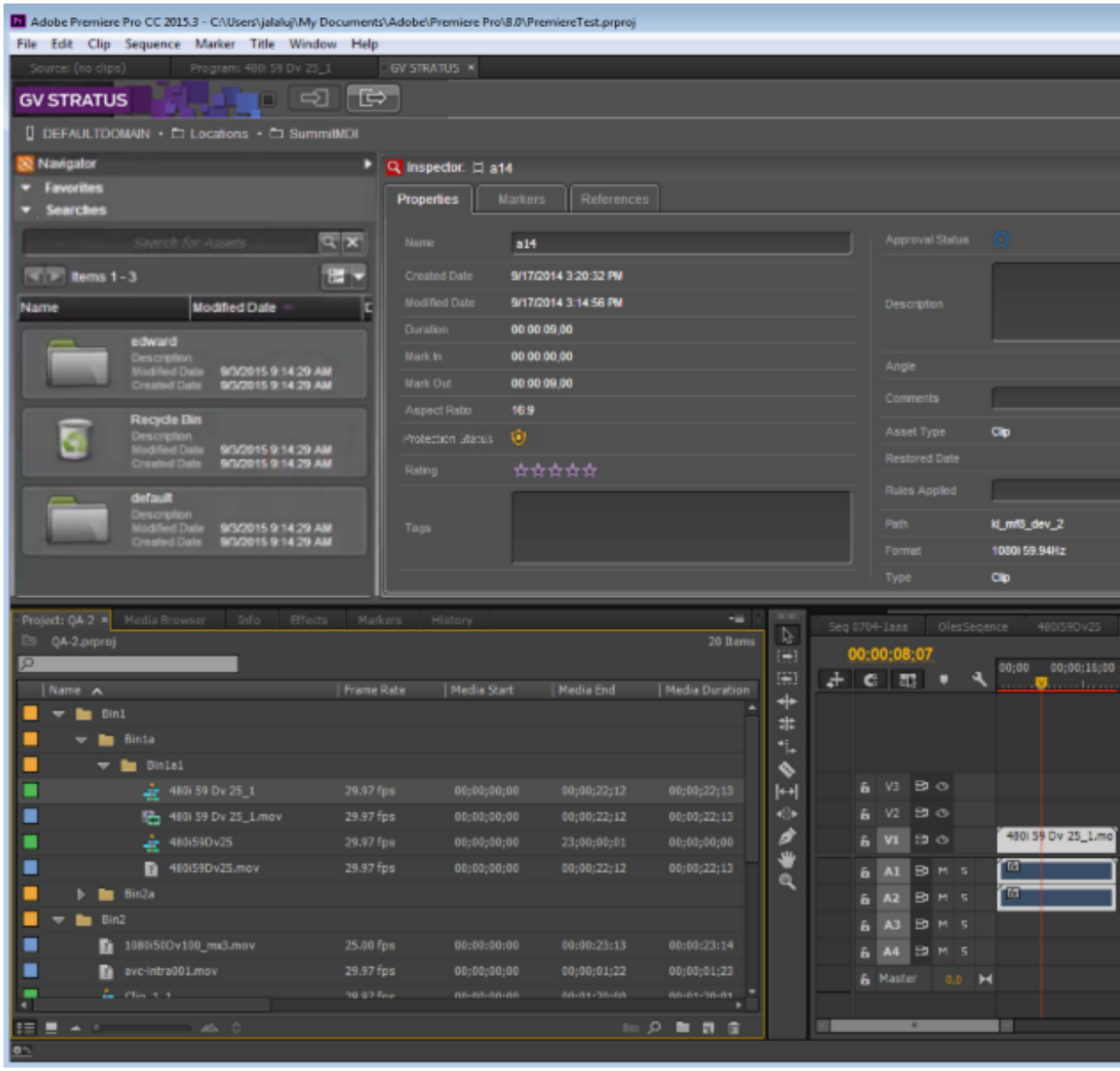
Using the GV STRATUS application in Adobe Premiere Pro CC

You can launch the GV STRATUS application as a plug-in within the Adobe® Premiere® Pro CC application. This allows you to use GV STRATUS to access assets in the K2 SAN system for an edit-in-place workflow and consolidate your editing operation in just one workspace.

The GV STRATUS plug-in consists of the Navigator and Inspector panels. You can search for assets, navigate to assets, view asset properties, modify asset properties, and import assets into your project and timeline using the GV STRATUS plug-in. With this workflow, you can easily access your high resolution media, edit sequences using the Adobe® Premiere® Pro CC application, and export sequences via GV STRATUS plug-in.

If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets, and metadata that do not have read permissions are not visible. Markers and segments permissions must be set to **Allow** in order to create, update, or delete markers and segments.

If GV STRATUS metadata access control is enforced, your credentials must give you adequate permissions. You can only view metadata with read permissions, and modify metadata with write permissions. If read or write permissions are denied, your metadata fields will be disabled.



Setting up K2 storage for Adobe Premiere Pro CC

Before installing GV STRATUS for Adobe® Premiere® Pro CC , set up the required support in K2 storage.

1. Ensure the Adobe Premiere Pro editor user accounts have access to the K2 media file system `V:` drive.

2. On the K2 Media Server with role of file system server (FSM), set up the Adobe directory.
   a) Share the `V:` drive with Everyone, Read/Write permissions.
   b) On the root of the `V:` drive, create a directory named `Adobe`.
   c) On the root of the `V:` drive, create a directory named `AdobeExporters`.
3. Set up a plan to periodically delete the files in the Adobe directory.

   For each asset imported from K2 storage into Adobe Premiere Pro, a temporary FCP XML file is created in the Adobe directory. Once the import succeeds the XML file is no longer needed. To maintain file system health, purge the directory on a regular basis.

License GV STRATUS for Adobe Premiere Pro

The Adobe Premiere Pro Sabretooth license is installed on the GV STRATUS server with role of Common Services. Typically the GV STRATUS Core server has the role of Common Services.

The Adobe Premiere Pro license is as follows:

- STRA-PREM-CONNECT

If you received your system pre-configured from Grass Valley, licenses are already installed, so you can skip these tasks. Otherwise, do the following:

1. Refer to the license sheet that you received with your GV STRATUS license. The license sheet has the Sales Order number that you need.
2. On the GV STRATUS server with role of Common Services, run the SabreTooth License Manager, generate a unique ID, and send the email to Grass Valley requesting your license or licenses.

   Refer to this Topic Library for detailed licensing procedures.
3. When you receive your license file, use SabreTooth License Manager and install it on the server.

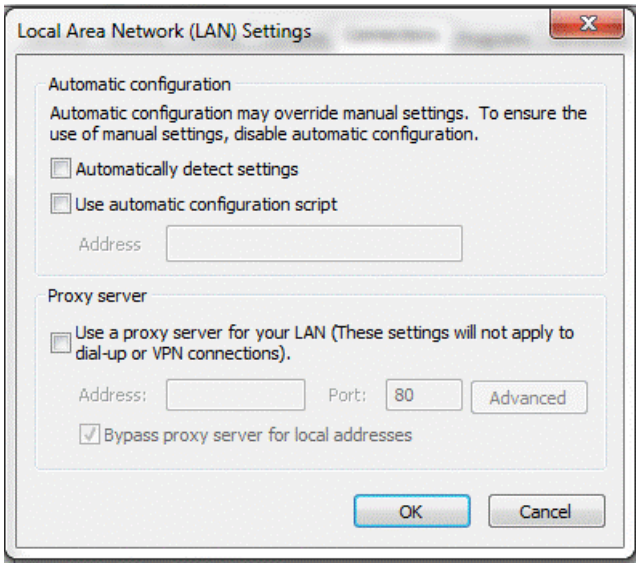
Installing Adobe Premiere Pro CC and GV STRATUS plug-in

- The GV STRATUS extension plug-in file must be accessible from your machine.
- The GV STRATUS Xcode Control Engine must be installed and configured on the GV STRATUS Core server.
- K2 storage must be set up with Adobe directories.
- The Adobe Premiere Pro SabreTooth License must be installed on the GV STRATUS Core server.

1. Install the Adobe Creative Cloud desktop application.
2. Launch the Adobe Creative Cloud and select **Apps**.
3. Select **Premiere Pro CC** in the Adobe Creative Cloud.
4. Click **Install** or **Update**, if appropriate.

   Premiere Pro CC installs and displays in the **Apps** section.

5. Launch your Windows Control Panel to select **Internet Options | Connections | LAN Settings** and clear the **Proxy server** setting as below:



   If this setting is enabled, the proxy server slows the performance of your Adobe Premiere Pro CC application.

6. To install the GV STRATUS Plug-in, you must get the Extension Manager Command Line tool (ExManCmd) from the *Adobe Exchange webpage*.
7. Select an installer according to your operating system, download and install the Extension Manager Command Line tool.

   Do take note of the install location.

8. Retrieve and place the GV STRATUS Plug-in installation file - **GV STRATUS_x.x.x.xx.zxp** file in the same folder as the Extension Manager Command Line tool (ExManCmd).
9. Launch the Command Prompt if you are using a Windows client, or the Terminal if you are on a Mac client. Then do the following:

   a) Go to *ExManCmd.exe* file location by entering: `cd <location of ExManCmd.exe>`

   - Example for Windows client: `cd C:\Users\Administrator\Desktop\ExManCmd_win\`
   - Example for Mac client: `cd /Users/Administrator/Desktop/Contents/MacOS`

   b) Once you are in the directory, install the "GV STRATUS.zxp" file by entering the following command:

   - Example for Windows client: `ExManCmd.exe /install "GVSTRATUS_x.x.x.xx.zxp"`
   - Example for Mac client: `./ExManCmd --install "GVSTRATUS_x.x.x.xx.zxp"`

10. Launch the Adobe Premiere Pro CC application.
11. Click **Window | Extensions | GV STRATUS**.

    The GV STRATUS plug-in appears in the Adobe® Premiere® Pro CC application.

12. If GV STRATUS security is enforced, ensure that user accounts have permissions on bins, assets, and send destinations that are part of your Adobe® Premiere® Pro CC workflow.

Installing the self-signed GV STRATUS security certificate for Adobe Premiere Pro

This is only required if you are using Adobe Premiere Pro application version 9.1 and above with GV STRATUS plug-in.

Installing the self-signed GV STRATUS security certificate on Windows clients

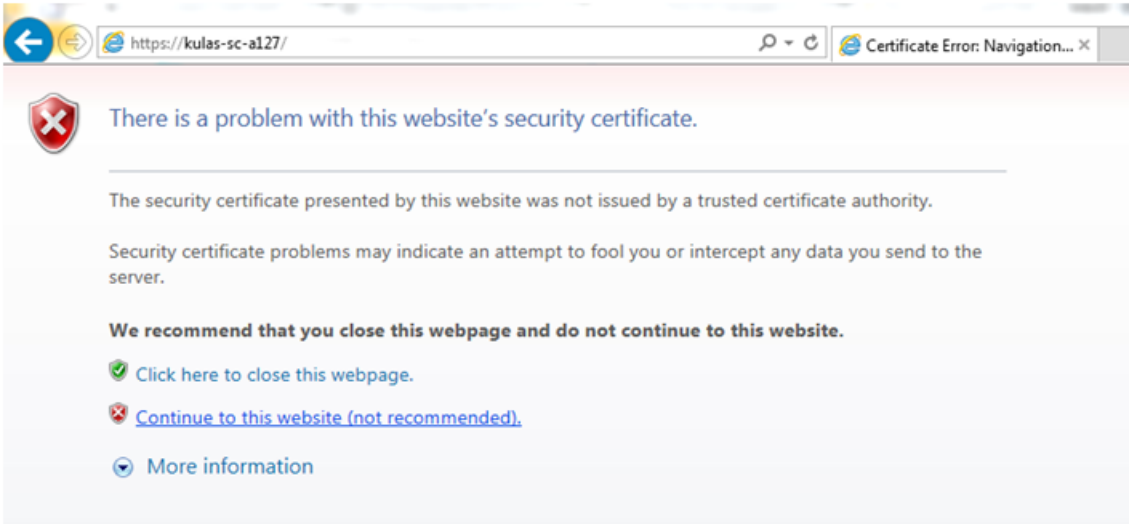
- The Adobe Premiere Pro version 9.2 must be installed on the Windows client.
- The GV STRATUS extension plug-in file must be installed on the Windows client.

1. Launch your Internet browser on the Windows client.
2. Enter the name of the GV STRATUS core server in the URL as follows:

   `https://{The name of the GV STRATUS core server}/`

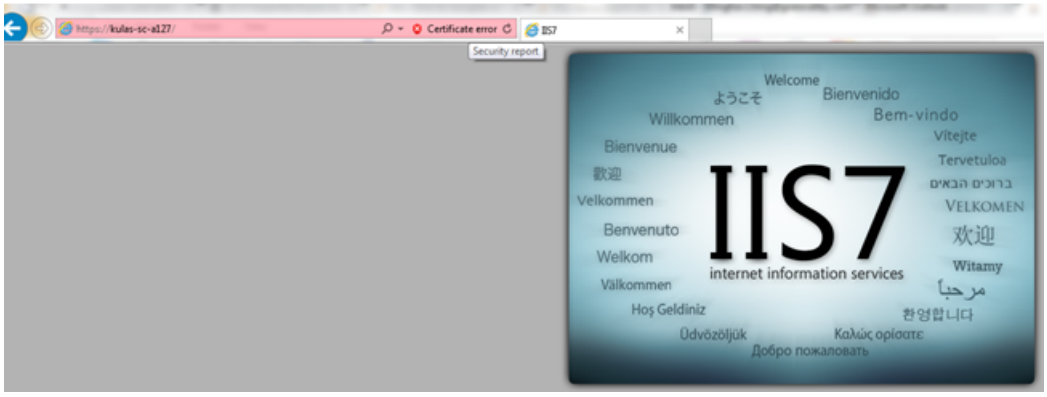
3. Press **Enter**.

   The Certificate Error page displays.



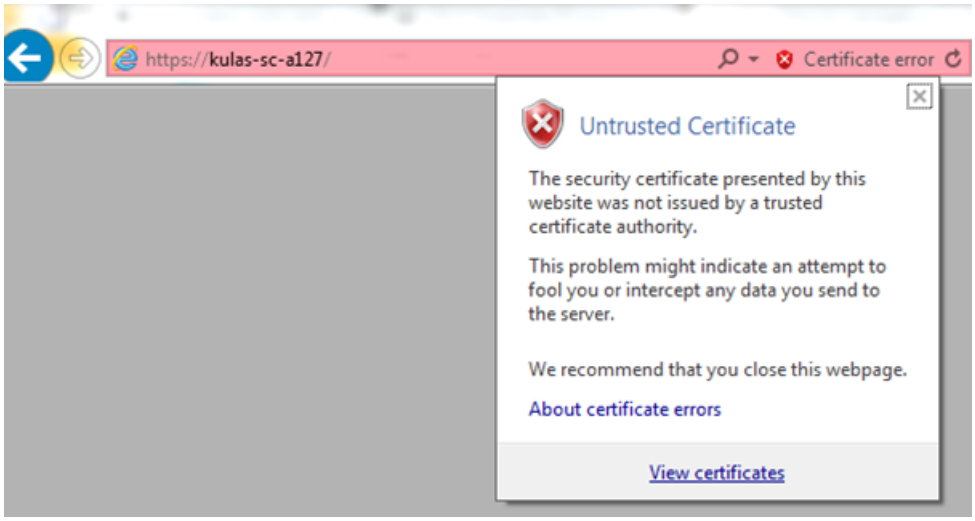
4. Click the **Continue to this website (not recommended)** link.

   The IIS page below displays.



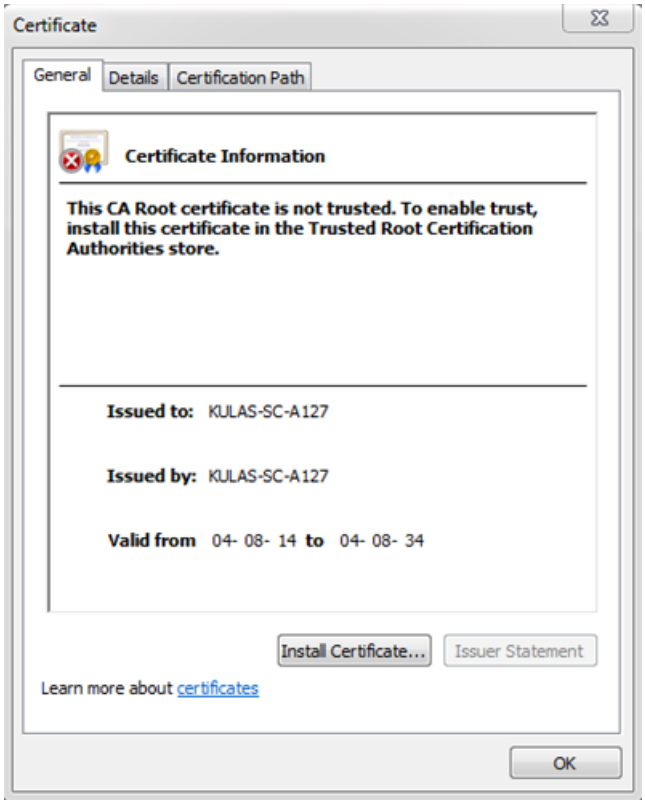
5. Click on the **Certificate error** display on the URL.

   The Untrusted Certificate page displays.

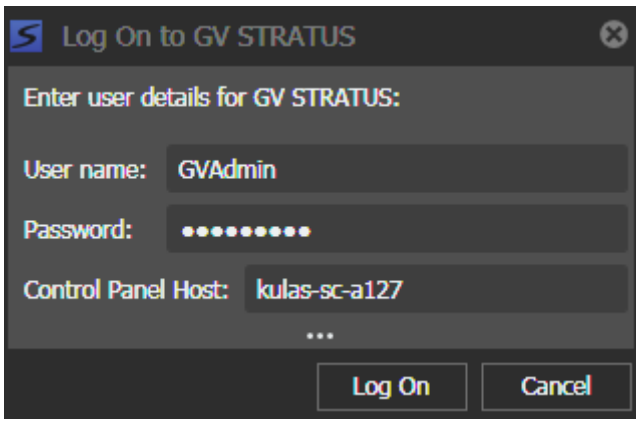


6. Click **View certificates**.

   The **Certificate** appears.



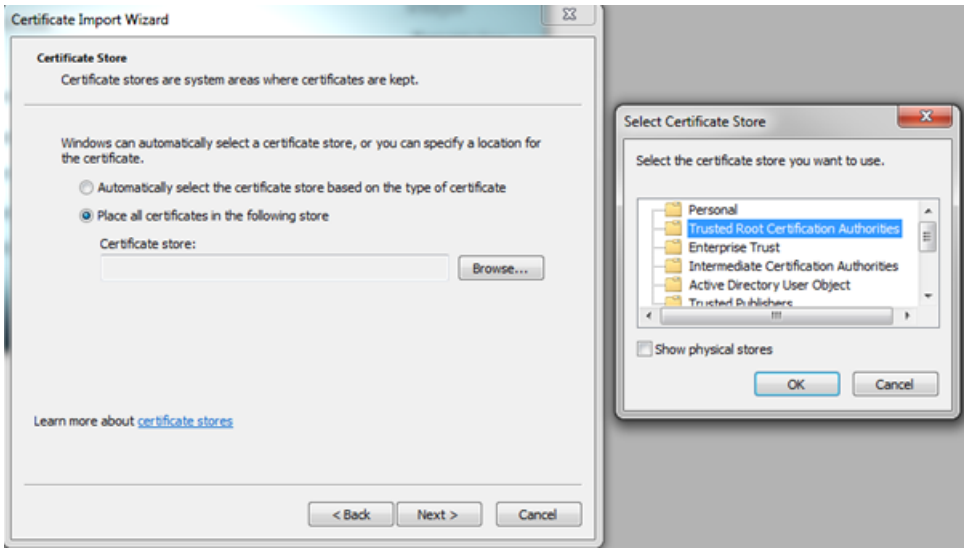
NOTE: Make sure that the certificate is issued to the same Control Panel Host you used to log on to GV STRATUS.



7. Click **Install Certificate**.

   The Certificate Import Wizard appears.

8. Click **Next** until the page for Certificate Store appears.



9. Select **Place all certificates in the following store** and click the **Browse** button.

   The Select Certificate Store window appears.

10. Select the **Trusted Root Certification Authorities** store and click **OK**.
11. Click **Next** on every page until the end, and click the **Finish** button.

    A Security Warning window appears.

12. Click **Yes**.

    A pop-up window displays **The import was successful**.

13. Click **OK**.

Installing the self-signed GV STRATUS security certificate on Mac clients

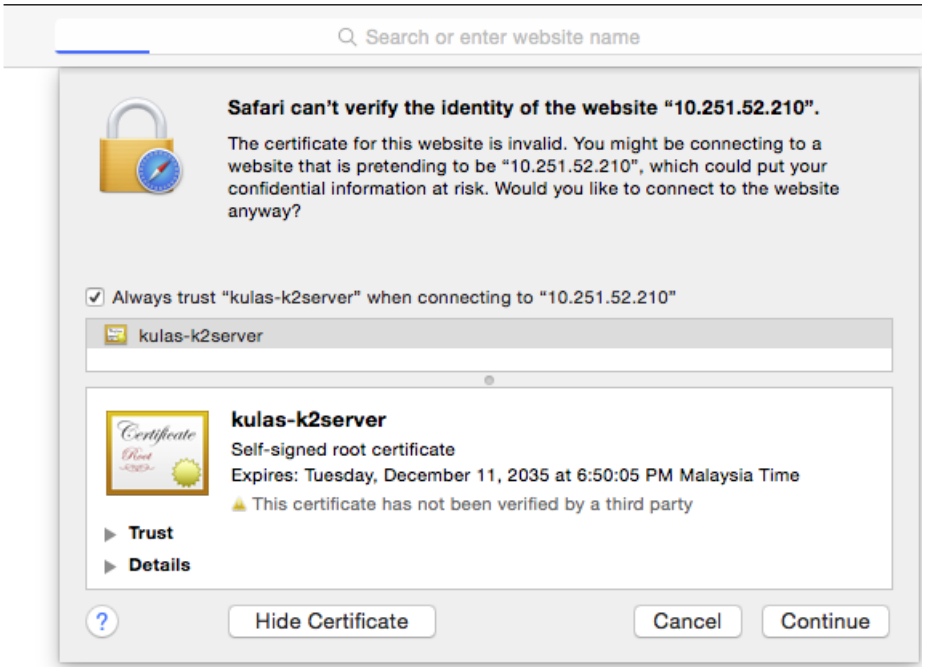
- The Adobe Premiere Pro version 9.2 must be installed on the Mac client.
- The GV STRATUS extension plug-in file must be installed on the Mac client.

1. Launch your Safari Internet browser on the Mac client.
2. Enter the name of the GV STRATUS core server in the URL as follows:

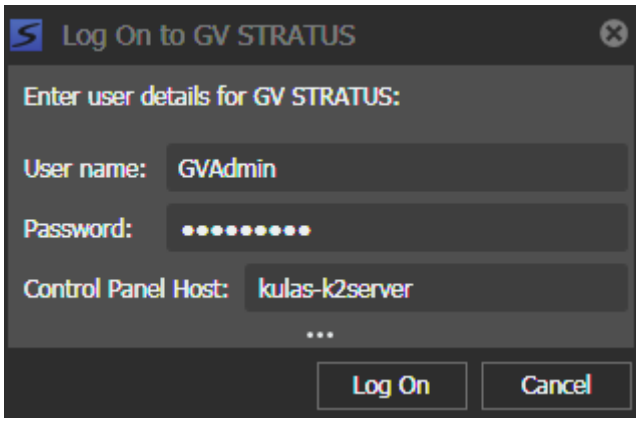
   https://{The name of the GV STRATUS core server}/

3. Press **Enter**.

   The page below displays.

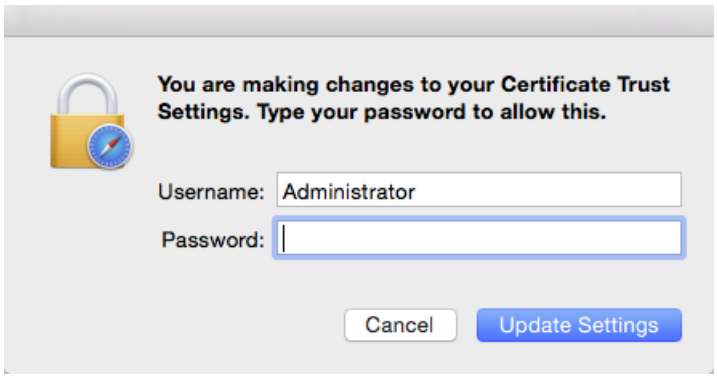


NOTE: Make sure that the certificate is issued to the same Control Panel Host you used to log on to GV STRATUS.



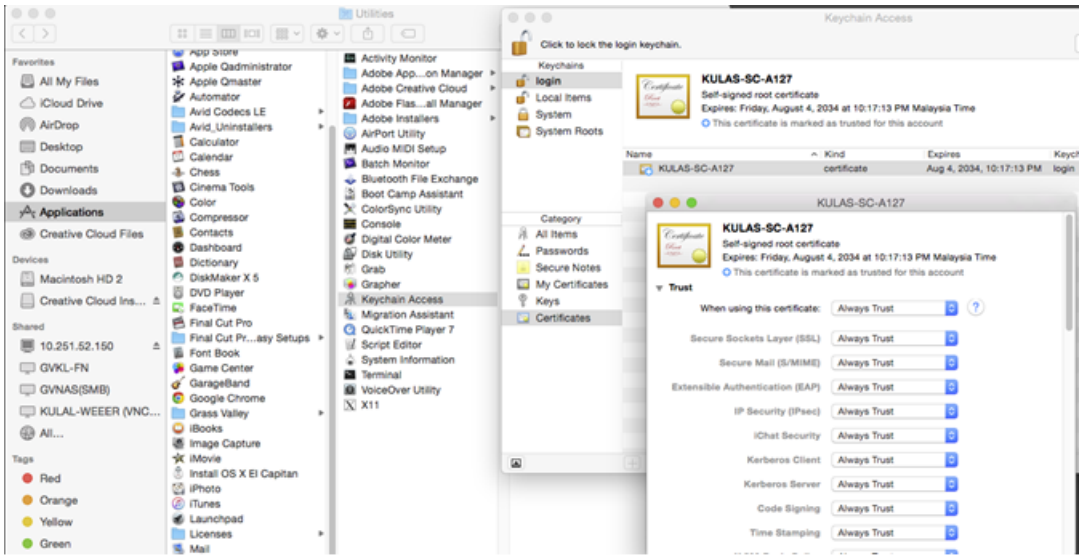
4. Select the **Always trust "{core server name}" when connecting to "{core server IP/name}"** check box and click the **Continue** button.

   The log-in page displays.



5. Enter your username and password, and click **Update Settings**.
6. On your Mac client, select **Applications | Keychain Access | login | Certificates** and select the certificate that you just imported.

   The certificate property window appears.



7. Select the Trust tab, and set all settings to **Always Trust**.
8. Then close the certificate property window.

Upgrading Adobe Premiere Pro CC and GV STRATUS plug-in

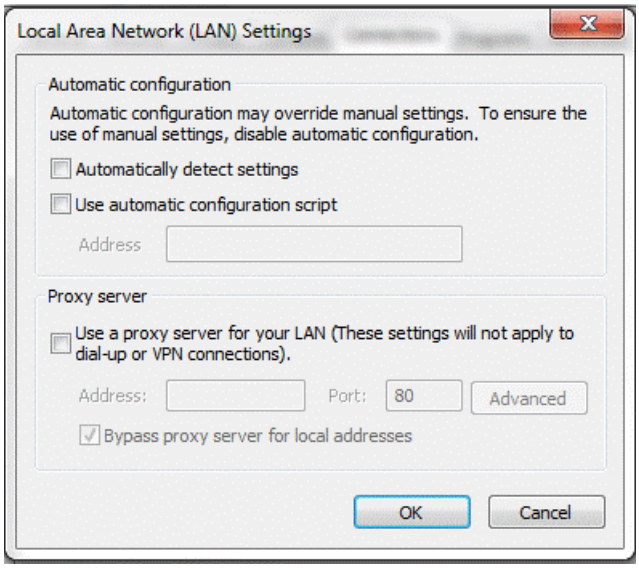
- The GV STRATUS plug-in file must be accessible from your machine.
- The GV STRATUS Xcode Control Engine must be installed and configured on the GV STRATUS Core server.
- K2 storage must be set up with Adobe directories.

- The Adobe Premiere Pro SabreTooth License must be installed on the GV STRATUS Core server.

1. Launch the Adobe Creative Cloud and select **Apps**.
2. Select **Premiere Pro CC** in the Adobe Creative Cloud.
3. Click the **Update** button.

   Premiere Pro CC installs and displays in the **Apps** section.

4. Launch your Windows Control Panel to select **Internet Options | Connections | LAN Settings** and clear the **Proxy server** setting as below:



   If this setting is enabled, the proxy server slows the performance of your Adobe Premiere Pro CC application.

5. To install the GV STRATUS Plug-in, you must get the Extension Manager Command Line tool (ExManCmd) from the *Adobe Exchange webpage*.
6. Select an installer according to your operating system, download and install the Extension Manager Command Line tool.

   Do take note of the install location.

7. Launch the Command Prompt if you are using a Windows client, or the Terminal if you are on a Mac client. Then do the following:

   a) Go to *ExManCmd.exe* file location by entering: `cd <location of ExManCmd.exe>`

   - Example for Windows client: `cd C:\Users\Administrator\Desktop\ExManCmd_win\`
   - Example for Mac client: `cd Desktop\Contents\MacOS`

   b) To install the latest GV STRATUS plug-in, enter the path to the "GV STRATUS.zxp" file:

   - Example for Windows client: `ExManCmd.exe /install "C:\Users\Administrator\Desktop\4.8.0.39\GVSTRATUS_4.8.0.39.zxp"`
   - Example for Mac client: `./ExManCmd --install "/Users/Administrator/4.8.0.39/GVSTRATUS_4.8.0.39.zxp"`

8. Launch the Adobe Premiere Pro CC application.
9. Click **Window | Extensions | GV STRATUS**.

   The GV STRATUS plug-in appears in the Adobe® Premiere® Pro CC application.
10. If GV STRATUS security is enforced, ensure that user accounts have permissions on bins, assets, and send destinations that are part of your Adobe® Premiere® Pro CC workflow.

Create Export Presets

The Adobe Premiere editing application uses the Adobe Media Encoder (included with the install of Adobe Premiere) to export files to K2 storage. The exports are based on presets which specify a K2-compatible video codec, resolution, frame rate, field order, and FTP destination. Each preset is built to correspond to a specific GV STRATUS Send Destination.

Presets are created by an admin-level advanced user and saved to shared location accessible by the Adobe Premiere editors. Multiple presets can be created, according to workflow needs and corresponding to GV STRATUS Send Destination locations.

1. Create presets according to the following specifications:

   - Create one preset file for each GV STRATUS Send Destination and name the preset with the exact name of the GV STRATUS Send Destination location.
   - The export preset file name must match the send destination location name you wish to export to. For example: `playout.epr` is created for the **playout** send destination location
   - Set format to MXF OP1a.
   - Do not Write XMP ID to Files on Import.
   - Do not export metadata.
   - Set a K2-compatible video codec. Your selection of a compatible video codec depends on K2 models, options, and licenses that are installed.

     For more info, refer to *Video codec description K2 Summit system* on page 1422 and *K2 Summit/Solo formats, models, licenses, and hardware support*.
   - Configure FTP settings as follows:

     - User Login: mxfmovie
     - Password: Leave blank
     - Server Address: IP address of the K2 Media Server with role of K2 FTP Server.
     - Remote Path: Desired destination bin on the K2 system.

2. Save to `V:\AdobeExporters`.

   NOTE: After every setting change, the .epr file must be exported and saved again. Only then, the settings will take effect. If you click the Test button to test the FTP connection, it may fail. However, it does not affect the media export to K2 storage.

Access K2 storage from workstations

Before exporting and importing assets from the Adobe Premiere Pro application, set up the required access into K2 storage.

Access K2 storage from a Windows workstation

On a Windows operating system workstation, do the following:

1. If the workstation is not connected to the K2 SAN as an iSCSI client, map the *V:* drive through Windows Explorer.
2. Select **Reconnect at logon**.

Access K2 storage from a Mac workstation

- On a Mac workstation with OSX version **10.11 and below**, connect to K2 SAN via SMB mount.

  Adobe Premiere connectivity to the K2 SAN storage is only supported via SMB connection. Currently, iSCSI and Fiber Channel connections are not supported.

  NOTE: K2-FCP-Connect license is not required for this connection.

  a) To connect to the K2 SAN media volume, mount the *V:* drive as follows:

     1. Launch the Terminal and log on as **Administrator**.
     2. Navigate to **/Volumes:** by entering the following command: `cd ../volumes`
     3. Create a new V drive using this command: `mkdir V`
     4. Mount the V drive using this command: `mount_smbfs //administrator@name-of-K2SAN/V V/`
     5. Enter the administrator password.

     The V drive is mounted at *../volumes/V/*

     You can check the content of the V volume by entering this command: `Volumes Administrator$ cd V`

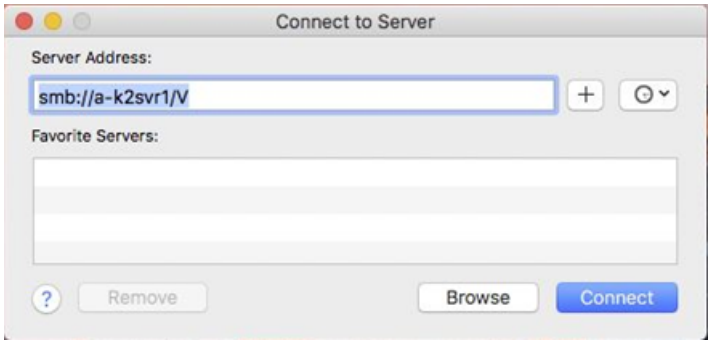
     Then followed by this command: `V Administrator$ ls`

     All folders inside the V volume will be displayed

  b) You can also click the mounted V volume icon on the desktop to access the V volume and its content.

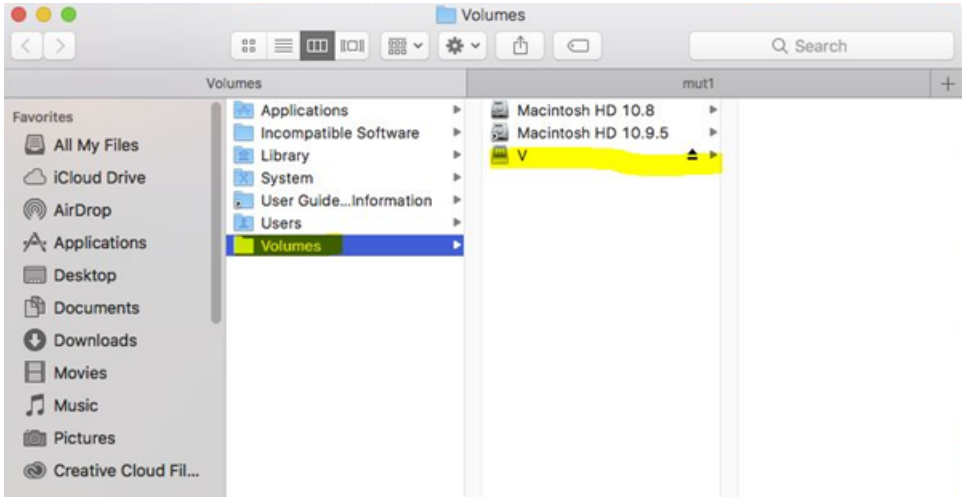
- On a Mac workstation with OSX version **10.12 and above**, connect to K2 SAN via the **Connect to Server** option.
  a) In the Finder, select **Go | Connect to Server**.

     The Connect to Server dialog box displays.
  b) Map the V drive for the K2 SAN in the **Server Address** field.



  c) Click **Connect**.
  d) Enter your user name and password, then click **Connect**.

     The V drive appears in your Volumes.



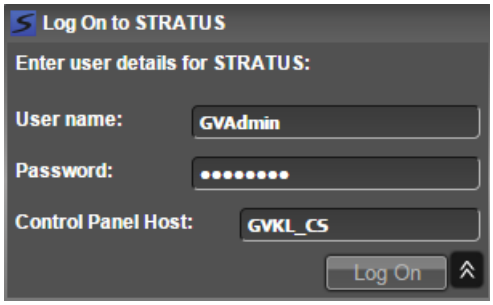
Launching the GV STRATUS plug-in

When you log on to the GV STRATUS system, the GV STRATUS application assigns GV STRATUS licenses and roles based on your user account credentials, as set by the system administrator in the GV STRATUS Control Panel application. If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins and assets that are part of your workflow. If GV STRATUS metadata access control is enforced, your credentials must give you adequate permissions on metadata fields that are part of your workflow. Your credentials must also give you access to all your K2 systems.

1. Launch the Adobe® Premiere® Pro CC application.
2. Start a new project or choose an existing project.

3. Select **Window | Extensions | GV Stratus**.

   A GV STRATUS Log On dialog opens.



4. Enter your user name.

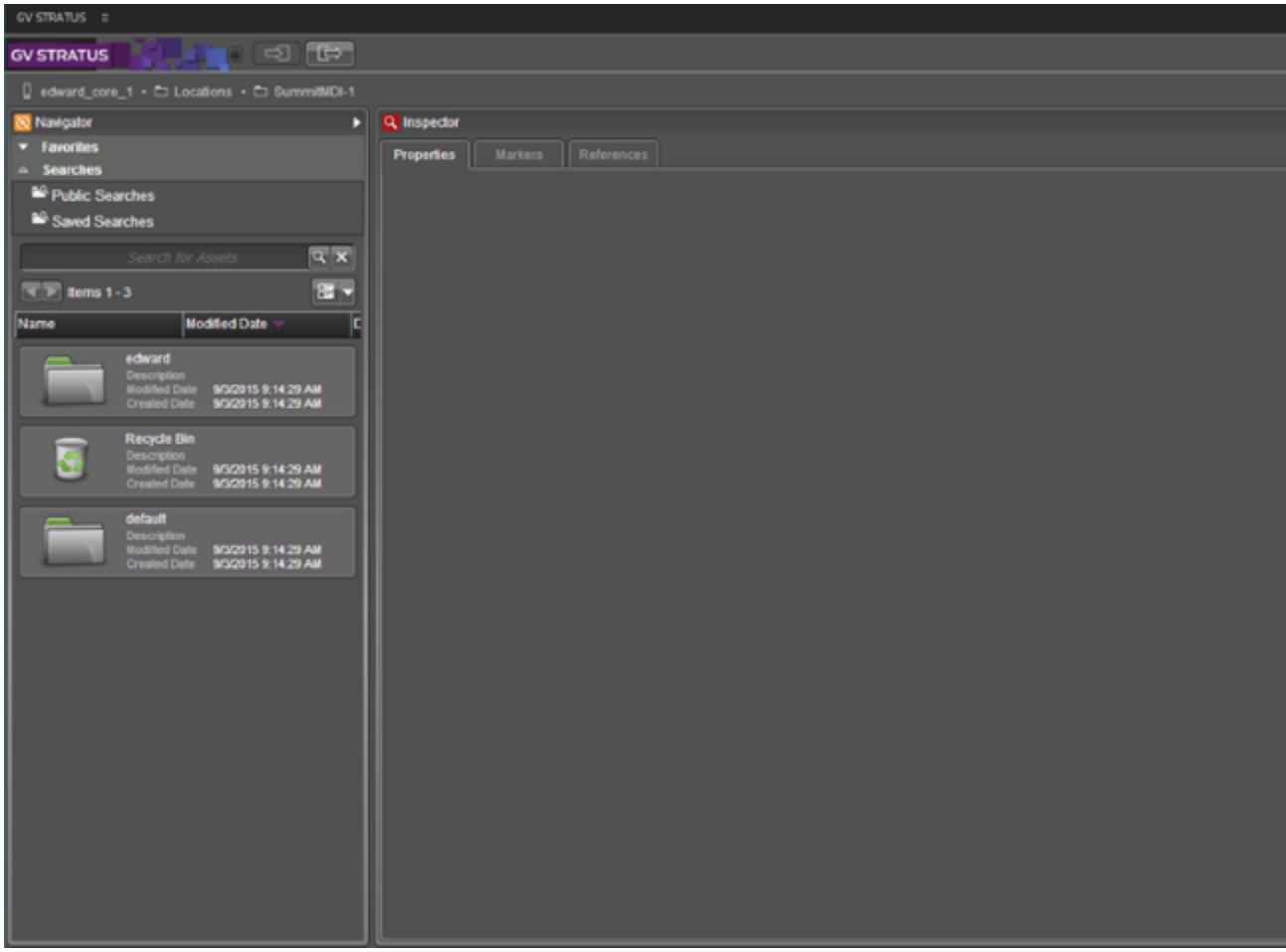
   If you use domain credentials, enter in format `<domain>\<username>`. For example, if your domain is "gv" and your username is "GVuser", enter `gv\GVuser`.

5. Enter your password.
6. For the Control Panel Host, enter the IP address of the GV STRATUS server with the SiteConfig role of GV STRATUS Control Panel Service.

   It must correctly point to the GV STRATUS Control Panel Services Host. In most systems this is the main GV STRATUS Core server.

7. Click **Log On**.

The GV STRATUS plug-in opens.

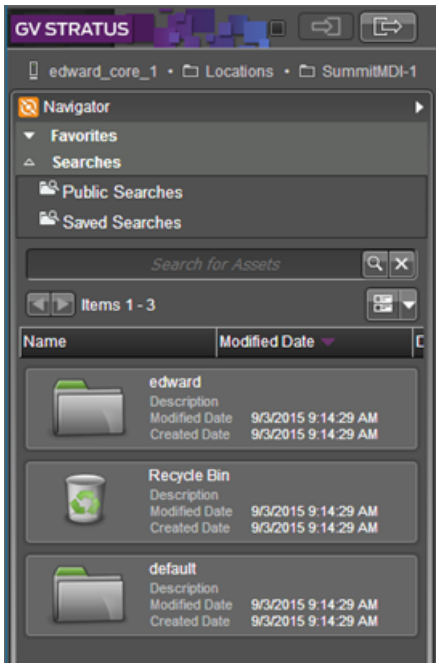

GV STRATUS
GV STRATUS
edward_core_1 • Locations • SummitMDI-1
Navigator
Favorites
Searches
Public Searches
Saved Searches
Search for Assets
Items 1 - 3
Name
Modified Date
edward
Description
Modified Date 9/3/2015 9:14:29 AM
Created Date 9/3/2015 9:14:29 AM
Recycle Bin
Description
Modified Date 9/3/2015 9:14:29 AM
Created Date 9/3/2015 9:14:29 AM
default
Description
Modified Date 9/3/2015 9:14:29 AM
Created Date 9/3/2015 9:14:29 AM
Inspector
Properties
Markers
References

Browsing assets

- If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins and assets. Bins and assets that do not allow read permissions are not visible.

You can browse and navigate into bins and sub-bins of the GV STRATUS system.

1. Double-click to browse through bins and sub-bins in the Navigator panel.



   The breadcrumb trail of your selected bin displays on the toolbar.

2. To navigate up the breadcrumb trail, click a bin on the toolbar.
3. To browse for assets, click on bins or sub-bins in the Navigator panel.

   Assets display in the Navigator panel. You can sort the display by **Name**, **Created Date**, **Modified Date**, and **Duration**.

Related Topics

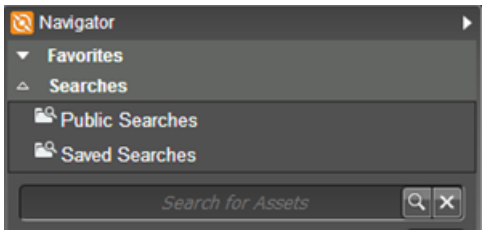
Asset indicators on page 977
Identifying asset permissions on page 480

Searching assets using the GV STRATUS plug-in for Adobe Premiere Pro CC

- If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins and assets. Bins and assets that do not allow read permissions are not visible.

You can search for assets in the GV STRATUS system using the Navigator panel.

1. For simple searches, in the Search tool of the Navigator, enter the word or a fragment of the word for your search.



   For a simple search you can enter text with advanced query syntax. Assets with names, tags, descriptions, comments, marker text, or custom text data that match the search are returned. Refer to related topics for more information.

2. For advanced searches, click the **Advanced Search Toggle** button ... next to the Simple Search tool.

   The advanced search options opened.

3. Configure an advanced search with the provided options. Refer to related topics for more information.
4. To start the search, click the **Search** button.
5. To clear the search, click **X**.

Assets matching the search criteria are displayed in the Navigator panel. Search of 1080p assets is also supported via the GV STRATUS plug-in.

However, unlike search results in the main GV STRATUS application; search results within the plug-in do not include these assets:

- Non SAN assets
- Assets in the Lost and Found directory
- EDIUS sequences

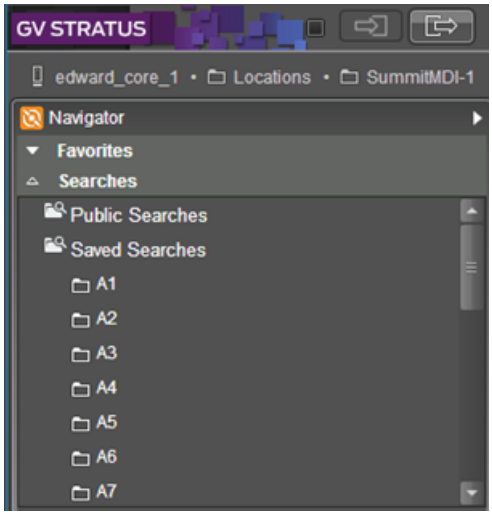
Related Topics

Search constraints and considerations on page 992

About advanced query syntax, advanced searches and custom expressions on page 423
Searching assets with the advanced search tool on page 992

Using a saved search in the GV STRATUS plug-in

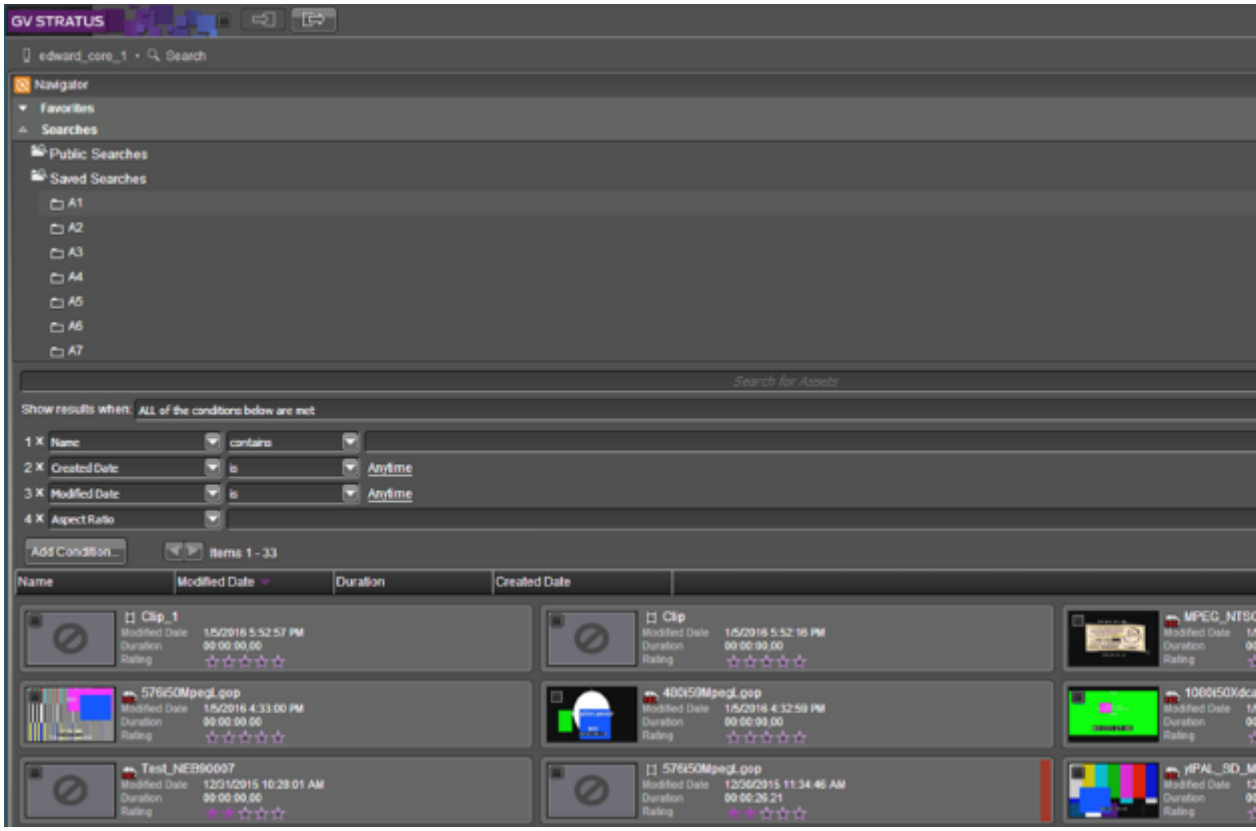
1. In the Navigator panel, expand the **Searches** node.



2. Find saved searches, organized as follows:
   - Public Searches: Searches saved as public by GV STRATUS system users with the role of Media Manager.
   - Saved Searches: Searches saved by users on GV STRATUS clients.

3. Select a saved search.

   Search results are automatically displayed in the Navigator panel.



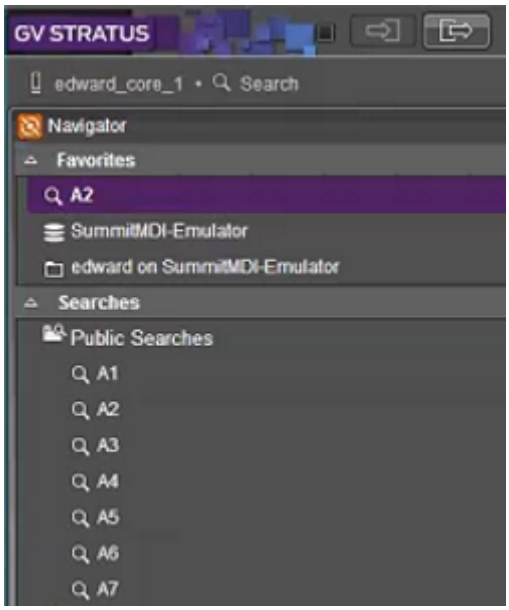
NOTE: If the name of public searches or saved searches started with non-alphanumeric characters, the order of display for those searches in* GV STRATUS *plug-in is not the same as displayed in* GV STRATUS *clients.

4. To re-run the search, click the **Search** button.

   You can also right-click on a saved search and select **Refresh** to update the search results.

5. To add the saved search into **Favorites** node, right-click on a saved search and select **Add to Favorites**.

   The saved search is now accessible under **Favorites** node in the Navigator panel.



Viewing asset metadata

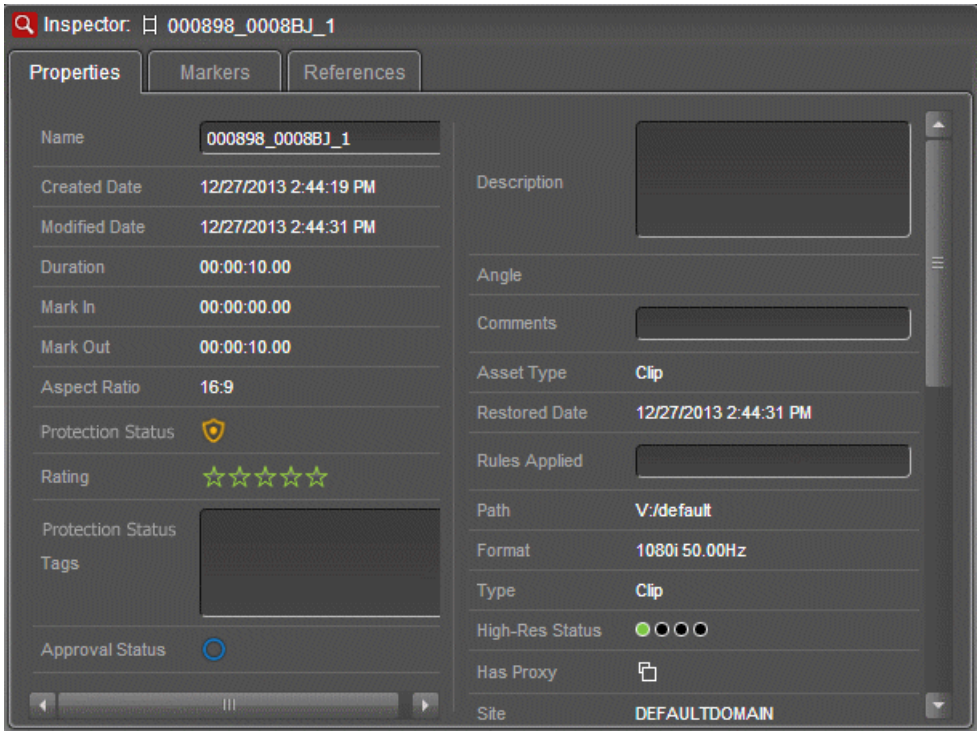
- If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, metadata, markers, keywords, and segments.

1. Locate the desired asset by browsing or using the Search tool.

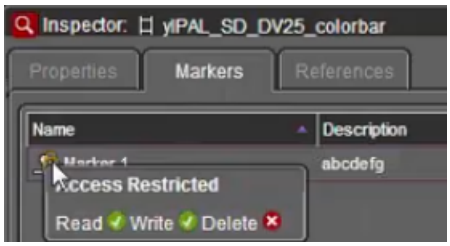
2. Double-click the asset to view its metadata.

   The asset metadata is displayed in the **Inspector** panel. You can also view custom metadata of the asset on the Properties tab.

   NOTE: Asset properties and custom metadata will not display for users without read permissions.

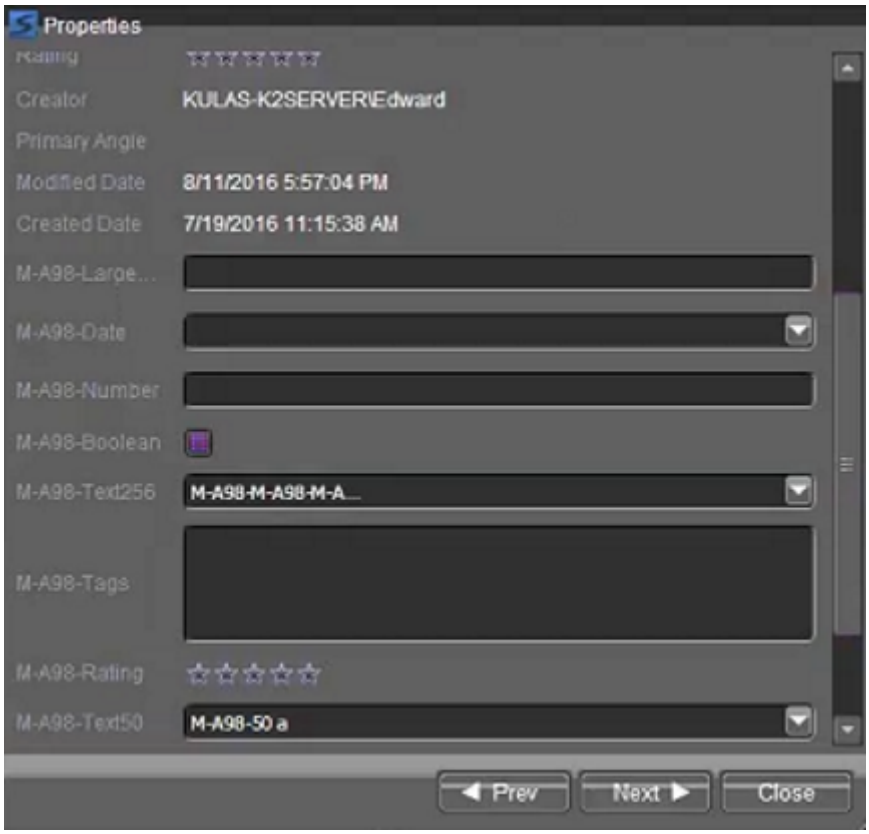


3. Click the **Markers** tab to view markers and keywords of the asset.



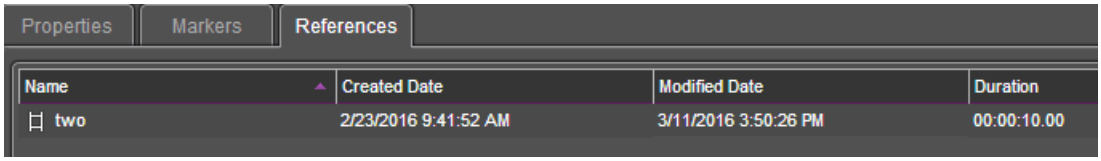
Markers and keywords must have appropriate permissions to be created, updated, or deleted. However, those permissions are only accessible via the main GV STRATUS application.

4. Double-click the marker to view its properties.



If custom metadata are assigned to markers and keywords in the GV STRATUS Control Panel, they can be viewed on the **Properties** window.

5. Click **Prev** or **Next** to view properties of other markers, and click **Close** to close the Properties window.
6. Click the **References** tab to view the list of related assets.



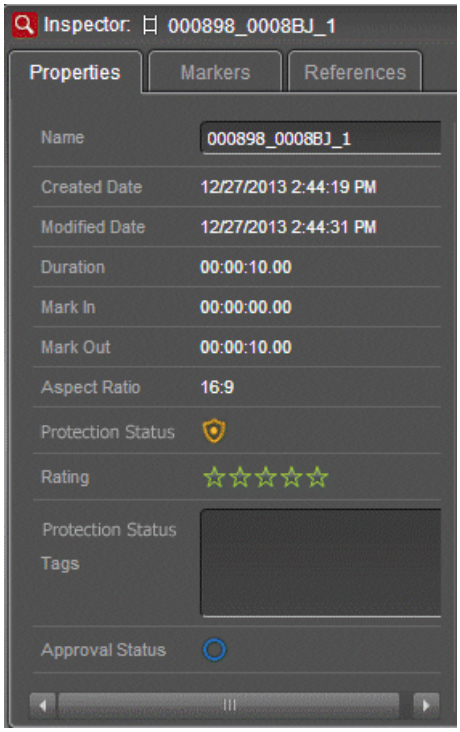
Modifying asset metadata

- If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, metadata, markers, keywords, and segments.

1. Double-click the asset.

   The asset properties display in the Inspector panel.

   NOTE: If write permissions are denied, your metadata fields will be disabled.



2. Key-in and modify the name, description, and tags of the asset.
3. Click the appropriate icon to modify the protection status, approval status, and rating of the asset.
4. On the Markers tab, you can also modify marker and keyword properties if you have the Update Marker permission.

   Marker permissions must be set to **Allow** for markers and keywords to be created, updated, and deleted.

Asset metadata is updated according to your changes.

Importing GV STRATUS assets

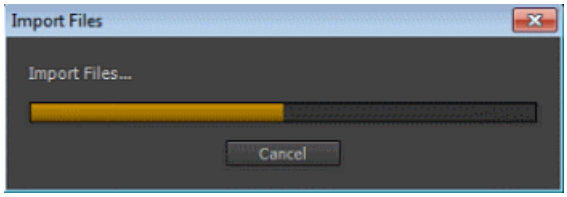
You can import GV STRATUS assets into your Adobe Premiere project to consolidate your editing operation.

1. In the Navigator panel, select the asset or assets you are importing.

   You can also select the **Select all assets in Navigator** checkbox on the toolbar if you want to import all assets in the bin.

2. Click the **Add selected asset into active bin** button to import the asset(s).

   A dialog box opens to show the progress of the import.



   Clips and subclips appear in the active project bin. Sequences, and all clips referenced by the sequences also appear in the active project bin.

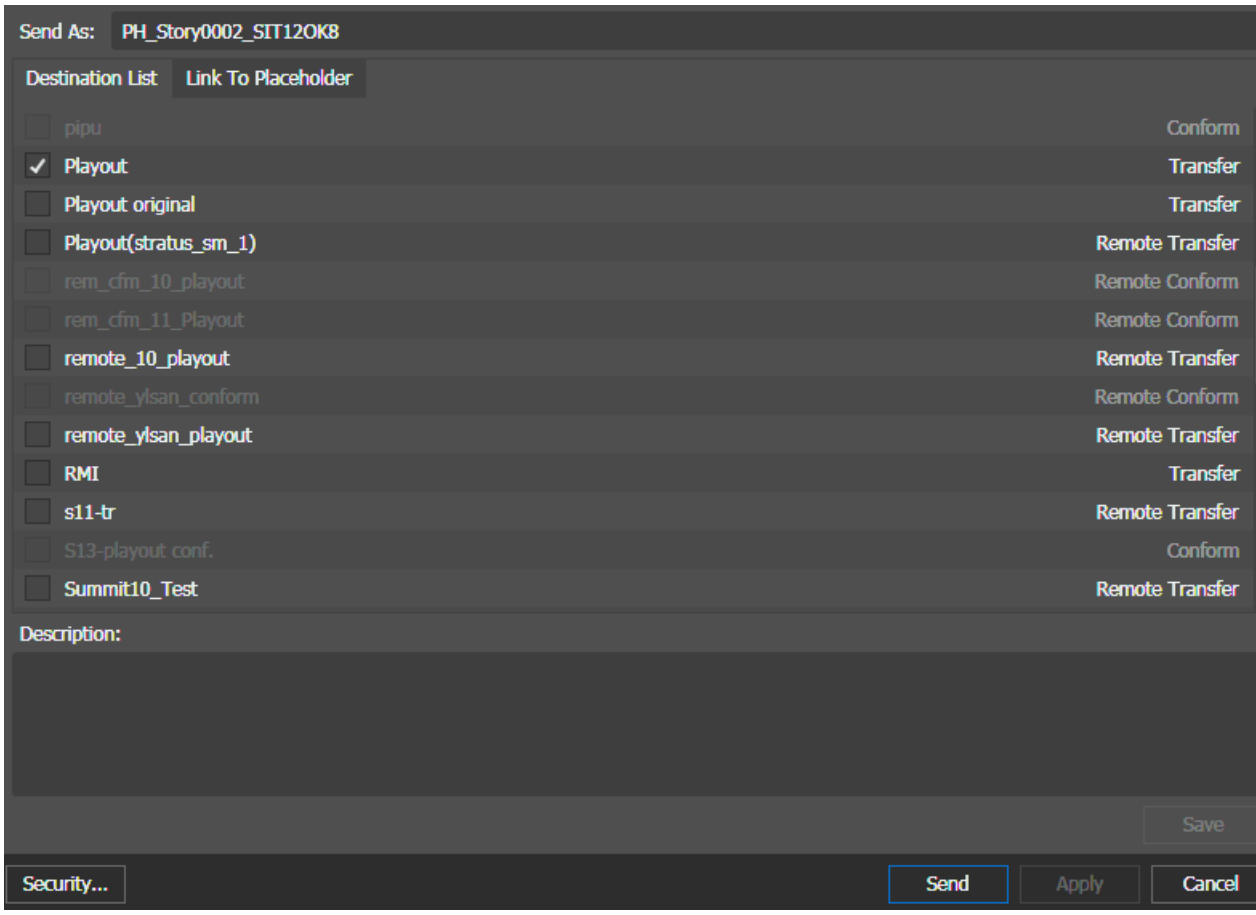
3. Double-click on a clip or subclip in the Adobe Premiere bin to load that clip or subclip into the source viewer.
4. Double-click on a sequence in the Adobe Premiere bin to open that sequence in the timeline.

Exporting Adobe Premiere sequences to GV STRATUS

- If GV STRATUS security is enforced, your credentials must give you write permissions on destinations. Destinations with inadequate permissions are disabled.
- If quota is configured on the K2 system bin, ensure you have enough disk space before transferring assets.

1. Load a sequence into the timeline area of the Adobe Premiere application.
2. On the GV STRATUS panel, click the **Export Active Timeline** button.

3. The **Send Destinations** dialog box opens.



4. Enter a name in the **Send As** field.
5. Select the desired Send Destinations.
6. If configured for a Newsroom Computer System, you can also link the asset to a local or remote placeholder.

   - If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, and metadata.
   - In order to link to a placeholder, you must be assigned with the **Rename Asset Rights** role and write permission for the **Name** property in Metadata section of GV STRATUS Control Panel.

   a) On the **Link To Placeholder** tab, select a placeholder.

   If a remote placeholder, expand the remote site node.

   If already linked to a placeholder, you can select a different placeholder.

   b) If desired, in the **Placeholder Description** field, enter text and click **Save**.

   The placeholder description is updated. It is not necessary to click **Send** to update the placeholder description.

7. Click **Send**.

The sequence is successfully sent to K2 storage via FTP.

If you're using Adobe Premiere with a Windows operating system, the Adobe Media Encoder shows a "Failed" status of the FTP transfer. This is a known file renaming problem and does not affect the exported asset. You can easily check in K2 storage to ensure the asset is successfully transferred.

The "Failed" status does not occur if you're using Adobe Premiere with Mac operating system.

NOTE: The Adobe Media Encoder does not delete the local asset after an export with a "Failed" status. If sending to multiple destinations when the asset exists locally with the same name, a suffix will be appended to the asset name at the new destination, and the next available default suffix will be appended at the next destination. Therefore, it is not recommended to send to multiple destinations via this workflow.

If sending to multiple destinations is required, choose the main destination to send from Adobe Premiere, and set up a GV STRATUS workflow rule that then transfers media from the main destination to subsequent destinations (e.g. to a main and then back up K2 system).

Related Topics

Adding an export rule on page 580

Using the GV STRATUS application with Avid

You edit GV STRATUS assets in the Avid Media Composer® application using a transfer workflow or using an edit-in-place workflow.

Opening a GV STRATUS asset in Avid using the transfer workflow

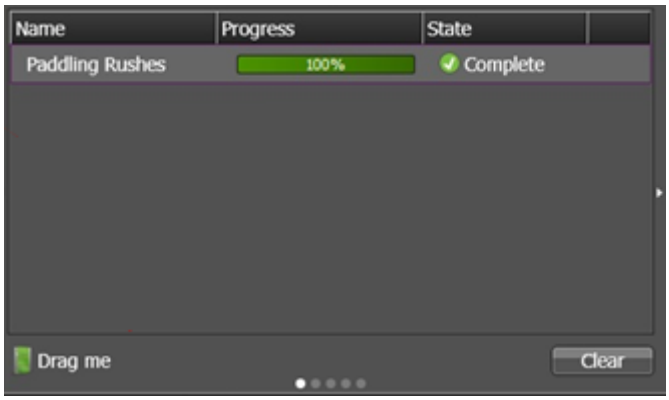
- The MEWS system must be installed and operational.
- The MEWS system must be configured in GV STRATUS Control Panel Engines settings.
- A Send Destination for each Avid Media Composer® workstation must be configured in GV STRATUS Control Panel.
- An import rule for each Avid Media Composer® workstation must be configured in GV STRATUS Control Panel.

- The GV STRATUS application and the Avid Media Composer® application must be running on the same client PC.

1. Select one or more clips or subclips in a GV STRATUS Asset List, right-click, select **Send to Avid**, and select the location for the Avid application running on the local PC from one of the following:

   - Avid ISIS
   - Avid MC
   - Avid Interplay

   You can see the progress of the asset transfer to the local PC.



   For assets sent to Avid Media Composer or ISIS (without Interplay), a **Drag me** button appears.

   For assets sent to Avid Interplay, there is no **Drag me** button display, as the assets are automatically transferred into the Interplay system.

2. When progress reports **100%**, select the **Drag me** icon in the **Sending to Avid** dialog box.

3. Drag and drop the icon to the Media Bin in the Avid application.

   The asset is available in the Avid Bin for editing in the Avid application.

4. For assets sent to Avid Interplay, navigate through to the relevant folder and open the assets in the Media Composer using the Interplay Window.

   Assets checked-in to Interplay will additionally check their GV STRATUS metadata as pre-configured in the GV STRATUS Control Panel.

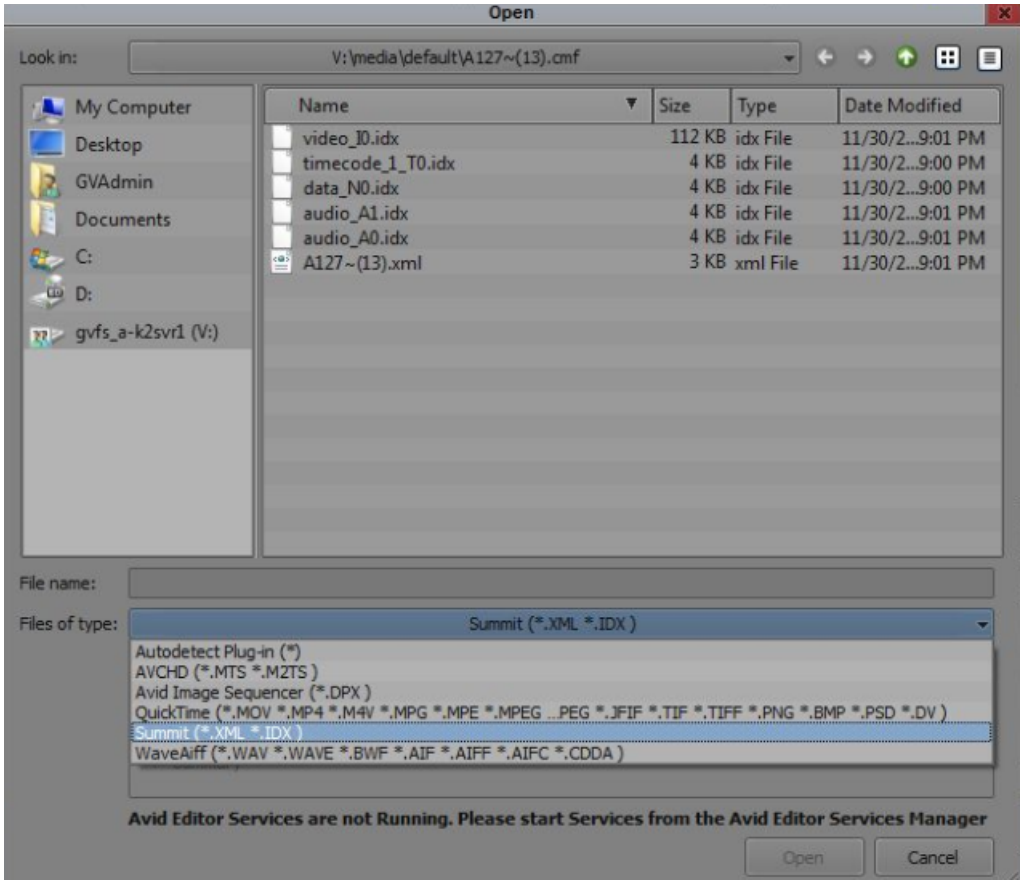
Related Topics

Setting up Avid workstations with GV STRATUS on page 661

Linking a GV STRATUS asset in Avid using the edit-in-place workflow

- The GV AMA plug-ins must be correctly installed and configured.
- The K2 storage volume must be mounted.
- The Avid Media Composer in your system is version 8.5 or lower. For versions higher than 8.5, refer to *Linking GV STRATUS assets in Avid* on page 1230.

1. To manually link to files, do the following:
   a) Open and select the bin in which you want the master clip or sequence to appear.
   b) Select **File | Input | Link to Media**, navigate to the filepath, and select the file or files for linking.



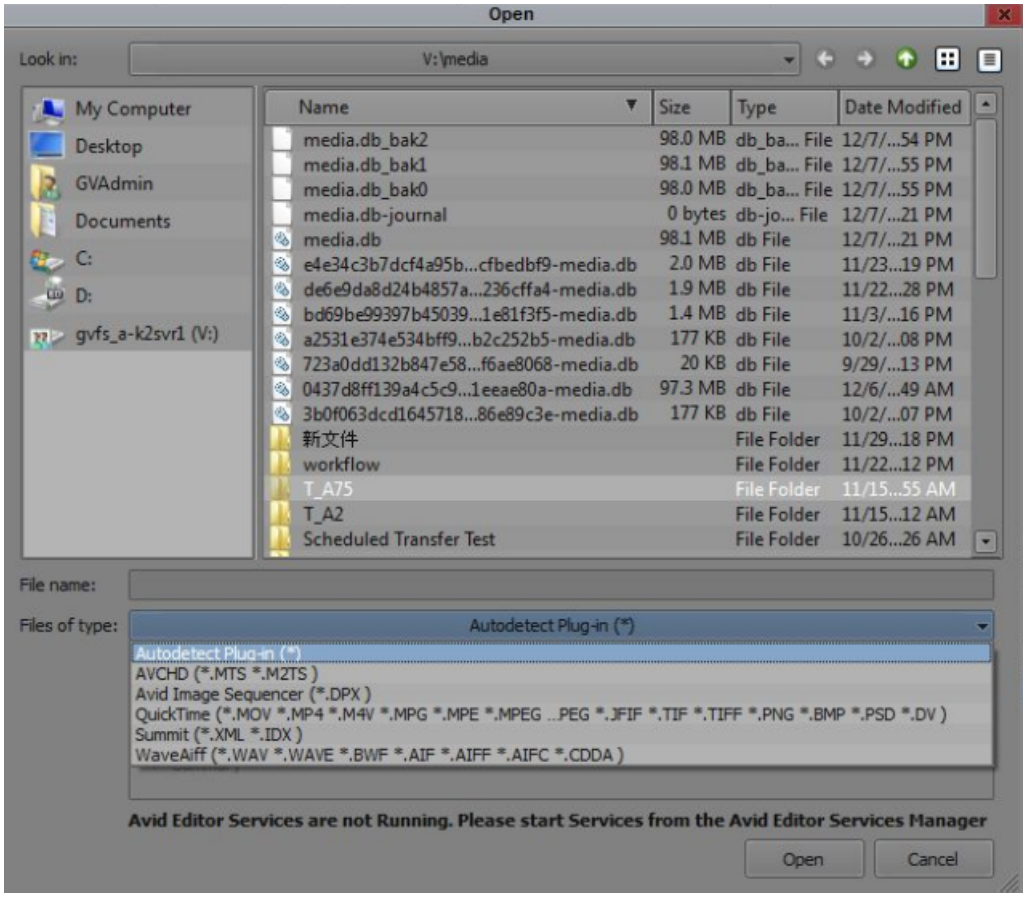
   c) Choose the file type for linking:

      - **Summit (*.XML, *.IDX)**: Creates a master clip or sequence which references all the media files and metadata as described by the XML.

   d) Click **Open**.

      The linked files appear as master clips or sequences.

2. To manually link to volumes (folders), do the following:
   a) Select **File | Input | Link to Media** and file type as below:



   - **Autodetect Plug-in (*)** for volume linking.

   b) Click **Open**.
   c) Navigate to the required folder, such as `V:\media\default`.

      A new bin is created and populated with all the assets found in the folder. The linked asset appears as master clips or sequences.

   d) To limit the number of assets in each folder, use **Link to files** and select only the files needed.

      When you link to volumes, only the content within a folder can be linked. All the assets within the selected folder are enumerated and linked. Master clips or sequences are created using all the media files and metadata as described by each of the assets XML found in the folder.

Related Topics

Setting up Avid workstations with GV STRATUS on page 661

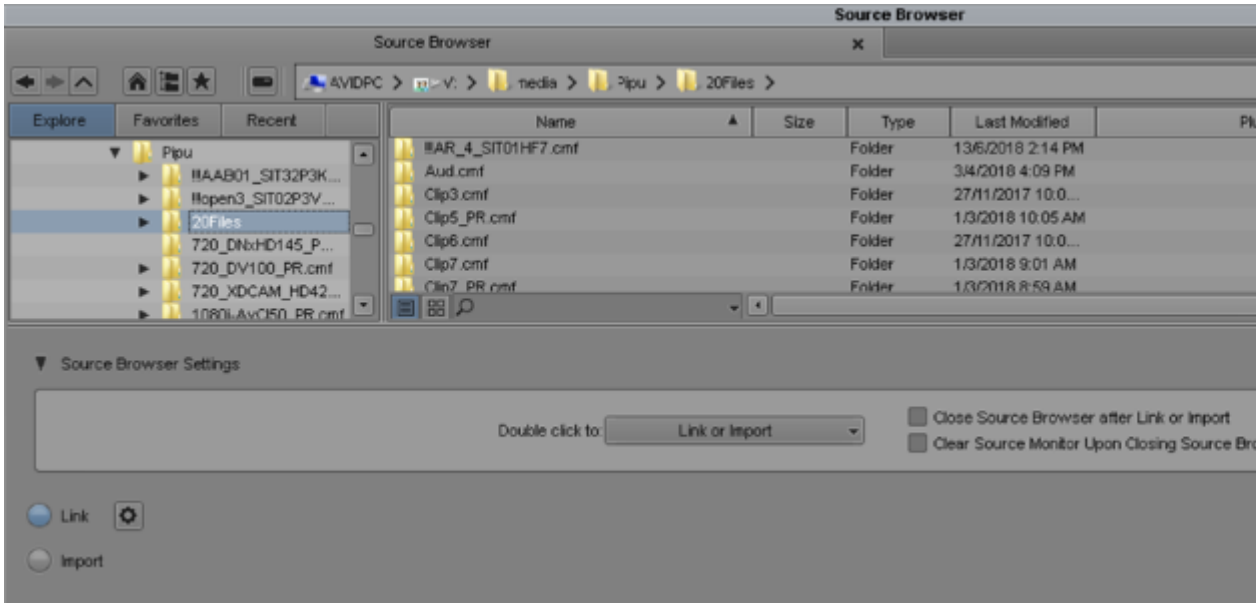
Linking GV STRATUS assets in Avid

- The GV AMA plug-ins must be correctly installed and configured.
- The K2 storage volume must be mounted.

- The Avid Media Composer in your system is higher than version 8.5. For version 8.5 and lower, refer to *Linking a GV STRATUS asset in Avid using the edit-in-place workflow* on page 1229.

1. In the Avid Media Composer, open the bin with GV STRATUS assets.
2. Right-click on the bin and select **Input | Source Browser**.

   The Source Browser window opens.



3. For single file linking, do the following:
   a) Navigate to the V: drive and open the asset CMF folder.

      Avid processes the folder and displays **MSP_GrassValley for 64Bit OS** for the supported *Assetname.xml* file in the **Plug-in** column of the Source Browser.

      If the file is not supported, the **Plug-in** column displays **Cannot be linked**.

   b) Select the XML file which references all the media files and metadata for the master clip or sequence.
   c) Under Source Browser Settings, select **Link or Import** from the drop-down list.
   d) Select the **Link** radio button on the left of the Source Browser window.
   e) Select **AMA** from the Target Bin drop-down list.
   f) Click the **Link** button on the right of the Source Browser window.

      The clip is AMA linked.

   g) Drag the clip into the Avid timeline.

      The linked file appears as a master clip or sequence in Avid. It is also available for playback.

4. For volumes (folders) linking, do the following:
   a) Navigate to the V: drive and select a bin with several GV STRATUS assets.
   b) Under Source Browser Settings, select **Link or Import** from the drop-down list.
   c) Select the **Link** radio button on the left of the Source Browser window.
   d) Select **AMA** from the Target Bin drop-down list.
   e) Click the **Link** button on the right of the Source Browser window.

      All clips in the bin are AMA linked.

      When you link to volumes, only the content within a folder can be linked. All the assets within the selected folder are enumerated and linked. Master clips or sequences are created using all the media files and metadata as described by each of the assets' XML files found in the folder.

      NOTE: Avid Media Composer version 8.7.2 does not support lists and sequence imports.

Export Avid clips or sequences to GV STRATUS

- The MEWS system must be installed and operational.
- The MEWS system must be configured in GV STRATUS Control Panel Engines settings.
- A Send Destination for each Avid Media Composer® workstation must be configured in GV STRATUS Control Panel.
- An import rule for each Avid Media Composer® workstation must be configured in GV STRATUS Control Panel.
- The GV STRATUS application and the Avid Media Composer® application must be running on the same client PC.

1. In the Avid application, right-click on the clip or sequence in the Avid Bin and select **Send to | GV STRATUS**.

   The **Send To** dialog box opens.

2. Configure as follows:
   a) For **Filename**, enter a new name for the exported file if desired.
   b) For **Destination**, click **Set** and browse to `C:\Avid MediaFiles\Export`.
   c) Leave other settings at default values.
   d) Click **OK**.

The MEWS services transcode the clip or sequence for compatibility with GV STRATUS and places the resulting files in the destination folder. The GV STRATUS rule detects the files in the destination folder and imports them into the GV STRATUS system.

Related Topics

Setting up Avid workstations with GV STRATUS on page 661

Avid/MEWS considerations

- GV STRATUS supports operation with multiple MEWS engines running on separate servers. Each MEWS engine supports up to 3 concurrent transcode jobs at a time.

- To ensure the MEWS Service machine(s) are correctly configured and the required license exists, you should check whether the resources provided per MEWS Service are registered in the GV STRATUS Control Panel via **Core | Resource Management | Resource Monitor**. The status of the MEWS license and MEWS Server machine should be **Online** on the Resource Monitor. Below are corresponding display of both MEWS licenses in SabreTooth and the Resource Monitor:

SabreTooth MEWS Licenses	SubResource Provider in Resource Monitor
STRATUS-XCODECONTROLMEWSEXT	MEWS
STRATUS-XCODECONTROLMEWS	MEWS-ELITE

- When editing HD material you must use an HD project. When editing SD material you must use an SD project.
- The GV STRATUS rule that imports an Avid sequence must use a transcode format that matches the Avid Media Composer Project window Format settings. If transcoding, an HD project must use an HD transcode format and an SD project must use an SD transcode format. If not transcoding, select **As Source**.
- The latest MEWS version supports AVC-Intra 100 1080p 50Hz format. Since Avid Media Composer is not supporting the format yet, the GV STRATUS Transcode Engine provides a transcode profile for MEWS to convert asset format from AVC-Intra 100 1080p 50Hz to **DNxHD 1080p (115/120/145 Mb/s)** for use in Avid systems.

  NOTE: AVC-Intra 100 1080p 60 Hz is not supported by MEWS.
- The Avid sequence can be of mixed codecs but they must be the same definition/standard.
- Assets transferred from GV STRATUS to Avid via MEWS retain GV STRATUS markers and keywords.
  - In Avid Media Composer, a GV STRATUS marker displays a red indicator and a GV STRATUS keyword displays a yellow indicator.
  - When transferred as AMT-Atom container, GV STRATUS Marker and Keyword names will be replaced by a valid Avid user name so that they can be imported into Avid. The original names will be added to the Avid *Comment field* together with the GV STRATUS description metadata, semicolon separated. The user name is extracted from the Location configuration in GV STRATUS Control Panel in the *Interplay Folder*.
  - Markers are only transferred if they exist in GV STRATUS before the transfer was initiated.
  - When transferring a still recording asset, markers will not display in the Avid system. Markers will only display if the clip is loaded into the Avid Media Composer after recording is stopped and the transfer is complete.
  - If the asset is already in the Avid Media Composer project bin, a refresh is required. In the context menu, select **Interplay | Update from Interplay** to refresh.
- Asset metadata are automatically transferred into Avid if configured in the **Metadata Export** tab of GV STRATUS Control Panel. Metadata fields can be selected under the Avid column, and automatically transferred when assets are sent from GV STRATUS.

- For a standalone Avid Media Composer workstation, configure Media Composer as follows:
  - In Media Creation settings, on every tab set **Video Drive** and **Audio Drive** to the *C:* drive.
  - In Export Settings, set **Export As** to **AAF** and for both **Video/Data Details** and **Audio Details**, do the following:
    - Set **Export Method** to **Consolidate Media**.
    - Set all Media Destinations to **Media Drive** and select **Use Media Creation Settings**.

- For a system with AVID ISIS, do the following:
  - Install Avid ISIS Client Manager on the following
    - The machine where the XCode Control Engine is running
    - The machine where MEWS is running
    - Every Avid Media Composer workstation
  - Configure Avid ISIS Client Manager as follows:
    - Map a drive, such as drive *Z:*, to the ISIS share.
    - Configure the user to the internal system account, which by default is GVAdmin
  - For an AVID ISIS Media Composer workstation, configure Media Composer as follows:
    - In Media Creation settings, on every tab set **Video Drive** and **Audio Drive** to the drive letter, such as drive *Z:*, mapped to ISIS.
    - In Export Settings, set **Export As** to **AAF** and for both **Video/Data Details** and **Audio Details**, do the following:
      - Set **Export As** to **AAF**.
      - Set **Export Method** to **Link to (Don't Export) Media**.
      - Set all Media Destinations to **Media Drive**.
  - Configure GV STRATUS as follows:
    - The GV STRATUS Xcode Control Engine Service and the MEWS Service must be installed to use the internal system account, which by default is GVAdmin.
    - In GV STRATUS Control Panel Locations Configuration settings, **Location Path** must point to the *\MXF* subfolder on Avid ISIS and **Host Name** must point to the hostname of the Avid Media Composer workstation.
    - Create an Import Rule Watchfolder, which is a share that can be accessed by the Rules Engine and the Avid Media Composer workstations.
    - Create an Import Rule as follows:
      - Source: The Import Rule Watchfolder
      - Destination: K2 folder
      - Transcode Format: a MEWS format that matches the Avid project.
      - Avid Server Type: Isis
      - Avid Media Host: The Isis server name
      - Set Rule Conditions to trigger on .aaf file extension

Refer to Avid Media Composer product documentation for more information.

Related Topics

SabreTooth MEWS license process on page 665

Resource Management settings on page 352

Installing K2 Avid Connect

What's new in K2-AvidTM/AMA

About K2/Avid Transfer Manager and Avid Media Access

K2/Avid Transfer Manager is Grass Valley's push and pull plug-in application that allows you to push and pull files stored on a K2 system to and from an Avid editor or shared-storage device.

It provides a seamless interface between GV STRATUS and K2 servers and Avid standalone and shared-storage environments. The K2 system enhances the Avid Workgroup solution in several ways:

- Provide a fast and reliable server for ingest and playout; once a story or a promo created using the Avid editor, you can send it to a K2 system for immediate playout.
- Seamless Avid Interplay nonlinear workflow engine; you can begin playout while the file is being streamed from your editor to a server.,
- Additional features to accelerate your workflow that lets you access a file while it's being transferred.
- A mirror option that lets you save to two servers (main and backup) in one operation.
- Ability to simultaneously transfer up to four files between the K2 and editing environments.

With GV AMA (Avid Media Access) plug-in for Media Composer and NewsCutter, you can access GV file-based media directly on the K2 Summit system media volume `V:`. It allows fast editing since you are not required to import the files before the media can be used.

What's new in version 7.3.5.249

Build 7.3.5.249

1. Added KT-8794 - K2-Avid Transfer Manager and GV AMA (Avid Media Access) plug-in support clips in Open-GOP XDCAM EX format.
2. Build for GV STRATUS version 6.5.
3. Build for Media Composer version 8.7.2.
4. Build for Interplay engine version 3.5.

Changes and features in previous releases

The following sections describe changes and features in past releases.

Build 7.0.0.163

1. Fixed DE7096 - AMA linked clips that are under construction should show up with the In Progress Icon in Media Composer. This fails if the under construction clip has a Mark-In greater than zero.
2. Build for GV STRATUS version 3.0.
3. Build for Media Composer version 6.5.2 and 7.0.2.
4. Build for Interplay engine version 2.7.5.

Build 7.0.0.162

1. Build for GV STRATUS version 3.0.
2. Build for Media Composer version 6.5.2 and 7.0.2.
3. Build for Interplay engine version 2.7.5.

Build 7.0.0.161

1. Build for GV STRATUS version 2.8.
2. Build for Media Composer version 6.5.2 and 7.0.2.
3. Build for Interplay engine version 2.7.5.

Build 7.0.0.150

1. Build for Interplay transfer engine 2.6 and 2.7 and AMA plugins build with AMA_SDK_3.1_2660.
2. Added new configuration utilities, TServerconfig and IngestConfig.

Build 7.0.0.149

1. Build for Interplay transfer engine 2.6 and 2.7 and AMA plugins build with AMA_SDK_3.1_2660.
2. Increased the ping timeout in AMA K2ConnectionHelper to 300ms, therefore avoiding devices erroneously getting declared offline.
3. Rolled the MVP and MSP PluginMinorVersion to 3.
4. Fixed XmlParser, now validates data before attempting string copy, preventing Media Composer from vaporising.

Build 7.0.0.148

1. Build for Interplay transfer engine 2.6 and 2.7 and AMA plugins build with AMA_SDK_3.0_2555.
2. Added Support for GV STRATUS metadata to the AMA MVP plugin.
3. Rolled the MVP and MSP PluginMinorVersion to 2.
4. Increased the DEFAULT_RCVBUF_SIZE and DEFAULT_SNDBUF_SIZE to (1024*1024)*2 to push the transfer speeds to around 85 to 100MB/sec. If the registry key is already set, then, this must be removed first.

Build 7.0.0.147

1. Build for Interplay transfer engine 2.6 and 2.7 and AMA plugins build with AMA_SDK_3.0_2555.
2. Updated install script to correctly register and unregister dlls.

Build 7.0.0.146

1. Build for Interplay transfer engine 2.6 and 2.7 and AMA plugins build with AMA_SDK_3.0_2555.
2. Added Support for GV STRATUS metadata to the GvgK2Setup.dll.
3. Added Support for GV STRATUS metadata to the AMA MSP plugin.
4. Fixed ncbug00076294: At Random transfer (SEND to PLAY BACK) aborts midstream.
5. User can now select the colour of the locators when ingesting asset via the DHM. This is done via the registry at *Software\\Grass Valley Group\\Applications\\K2-AvidTM\\SETUP* value LocatorColour. Set the values to:
   - 0 = Red
   - 1=Green
   - 2=Blue
   - 3=Magenta
   - 4=Cyan
   - 5=Yellow
   - 6=White
   - 7=Black

Build 7.0.0.145

1. Build for Interplay transfer engine 2.6 and 2.7.
2. Fixed ncbug00076584: Increased the GXF parser buffer size to handle the large MPEG frames produced by long GOP recording 50Mbit records.
3. Added support for AMA chase editing.

Build 7.0.0.144

- Build for Interplay transfer engine 2.6 and 2.7.

Build 7.0.0.143

- Build for Interplay transfer engine 2.5.

Build 7.0.0.142

- Special Build for Interplay transfer engine 2.2.

Build 7.0.0.141

1. Build for Interplay transfer engine 2.5.

2. Fixed ncbug00075587: Transfers of programs which includes empty audio tracks to Avid MC has audio distortion on the filler tracks. Added Audio fill for 24 bit audio and corrected for progressive formats.
3. Fixed ncbug00074984: Transfer from Avid Media Composer to K2 Summit system fails if part of the Sequence does not have video track. Added DNxHD and AVCi fill fame support. Corrected AVCi fill frame size.

Build 7.0.0.140

1. Build for Interplay transfer engine 2.5.
2. Fixed ncbug00075794: Audio corrupted for Avid sequence transferred to K2 Summit system.
3. Fixed ncbug00075795: Need change the default password for Avid TServer/DHM Ok.
4. Fixed ncbug00075603: K2Avid Explorer hangs if one of the K2 Summit system is rebooted and shutdown.
5. Fixed ncbug00075831: K2Avid Explorer hangs whenever I click on a bin of a K2 Summit system that has just shutdown.
6. Fixed ncbug00075623: K2 AvidExplorer errors during K2 Summit system boot up.

Build 7.0.0.139

1. Build for Interplay transfer engine 2.5.
2. Fixed ncbug00075824: Second round of fixes with the correct path.

Build 7.0.0.138

1. Build for Interplay transfer engine 2.5.
2. Fixed ncbug00075822: Software license agreement for K2 DHM/Ingest/Tserver installation needs to be updated (get rid of Thomson). Changed the Email address from `K2license@thomson.net` to `K2License@grassvalley.com` in the `K2-AvidTm.ini` to be used for License requests wizard.
3. Fixed ncbug00075824: K2-AvidTMLicense request wizard does not launch. Unable to locate `wizard.hta`.. Updated the path used by install shield.
4. Fixed ncbug00075785: Updated the license cutter to create licenses named K2-AvidTM instead of k2-DHM and updated the `TemporaryLicense.txt` to include K2-AVIDTM Evaluation license instead of SERVER-SOFTWARE-TEMPORARY. Updated the receiver and dhm dll to work with both k2-DHM and K2-AVIDTM.

Build 7.0.0.137

1. Build for Interplay transfer engine 2.5.
2. Fixed ncbug00075811: Newer version of Sabretooth license manager should be used for Avid DHM PC.

Build 7.0.0.135

- Fixed ncbug00075587 — Filler tracks had random noise. Problem caused by filler audio frame was not initialised to zero. Fixed by memset(pc,0,sizeof(char)*nSize).

Build 7.0.0.134

1. Fixed ncbug00075461 — AvidTServer install had the option show the install log at the end, but it doesn't work. Disabled the "Show the Windows Installer log check box" from the SetupCompleteSuccess dialogbox.

2. Fixed ncbug00075397 — Unable to transfer List or Program from K2 Summit system to Avid.Failures to transfer Lists are caused by additional video frames transferred for transition's. There is no way to handle this on the Avid side. So to address this, any attempt to transfer a list is now rejected.
3. Fixed ncbug00075137 — Sighting: K2 Avid Explorer had an unhandled exception.Added better exception handling and check to guard against accessing null objects.
4. Fixed ncbug00075398 — K2AvidExplorer crashes when user clicks on a bin that no longer exists. Fixed additional issues where bin would not update or wrong bin would be deleted.
5. Fixed ncbug00075399 — Audio misalignment (out of sync with video) on Programs transferred from K2 Summit system to Avid MediaComposer. Added code to correct the Audio sample used when dealing with Programs (sequences).
6. Fixed ncbug00075401 — Logviewer throws an error from K2AvidExplorer whenever the clip name is changed while it is still being recorded.
7. Fixed ncbug00074988 — Transfer of subclips from K2 Summit system to Avid Media Composer sometimes fail. This should be addressed by the fix in ncbug00075399.

Build 7.0.0.133

1. Fixed ncbug00075359 — Send to playback: Drop Frame time code does not drop frames.
2. Fixed ncbug00075439 — Send to playback: Media files are dumped in the Interplay transfer engine folder.

Build 7.0.0.132

- Final fix for Bottom field versus top field issue with DNxHD content.

Build 7.0.0.131

- Fixed Bottom field versus top field issue with DNxHD content.

Build 7.0.0.130

- Added new configurations utility to ease the configuration of the K2-AvidTM.

Build 7.0.0.129

1. First build to support Media Composer version 6.0.1 and Interplay engine 5.0.1.
2. Added support for DNxHD.
3. Changed the Tserver dependencies so it can be installed on the FSM.

Build 7.0.0.112

With the introduction of build 7.0.0.112 and Avid Interplay 2.2.1.1, K2-AvidTM now supports the following:

1. 16 channels of audio.
2. AVC-I ingest and Send to playback. 1080i & 720P, 50Mbit or 100Mbit.
3. Ingest of XDCAM.
4. MetaData can be displayed in Avid editor bin view.
5. Basic sorting on Colum view in K2-Avid Explorer.
6. K2-Avid Explorer no longer allows assets to be deleted or renamed.

Reference to system compatibility

Software version versus Avid Operating System support

Software Version	Windows NT4.0	Windows XP	WIN 7 32 bit	WIN 7 64 bit
7.0.0.104	Yes	Yes	No	No
7.0.0.105	Yes	Yes	No	No
7.0.0.112	No	Yes	Yes	Yes
7.0.0.129	No	No	No	Yes
7.0.0.130	No	No	No	Yes
7.0.0.131	No	No	No	Yes
7.0.0.132	No	No	No	Yes
7.0.0.133	No	No	No	Yes
7.0.0.134	No	No	No	Yes
7.0.0.135	No	No	No	Yes
7.0.0.136	No	No	No	Yes
7.0.0.137	No	No	No	Yes
7.0.0.138	No	No	No	Yes
7.0.0.139	No	No	No	Yes
7.0.0.140	No	No	No	Yes
7.0.0.141	No	No	No	Yes
7.0.0.142	No	No	Yes	No
7.0.0.143	No	No	No	Yes
7.0.0.144	No	No	No	Yes
7.0.0.145	No	No	No	Yes
7.0.0.146	No	No	No	Yes
7.0.0.147	No	No	No	Yes
7.0.0.148	No	No	No	Yes
7.0.0.149	No	No	No	Yes
7.0.0.150	No	No	No	Yes
7.0.0.161	No	No	No	Yes
7.0.0.162	No	No	No	Yes
7.0.0.163	No	No	No	Yes

Microsoft Windows Operating System supported by Profile and K2 Summit system

Software Version	Profile PVS series	K2 Series	K2 Summit/Solo system	K2 Summit 3G/Solo 3G system
Windows NT4.0	Yes	No	No	No
Windows XP	Yes	Yes	Yes	Yes
WIN 7 32 bit	No	Yes	Yes	Yes
WIN 7 64 bit	No	Yes	Yes	Yes
Windows 10 IoT LTSB	No	Yes	No	Yes (K2 Summit 3G only)

K2-AvidTM Software Version and Avid version matrix

Software Version	Interplay Transfer engine	NewsCutter	Media Composer
7.0.0.104	1.6.2 & 1.6.4	7.5.9	3.5.9
7.0.0.105	2.1	8.x	4.x
7.0.0.112	2.2.1.4	9.x	5.x
7.0.0.126	2.2.1.4	9.x	5.x
7.0.0.127	2.3.0.3	9.5.3	5.5.3
7.0.0.128	2.4.0.2	9.5.3	5.5.3
7.0.0.129	2.5.0.3	10.0.3	6.0.3
7.0.0.130	2.5.0.3	10.0.3	6.0.3
7.0.0.131	2.5.0.3	10.0.3	6.0.3
7.0.0.132	2.5.0.3	10.0.3	6.0.3
7.0.0.133	2.5.0.3	10.0.3	6.0.3
7.0.0.134	2.5.0.3	10.0.3	6.0.3
7.0.0.135	2.5.0.3	10.0.3	6.0.3
7.0.0.136	2.5.0.3	10.0.3	6.0.3
7.0.0.137	2.5.0.3	10.0.3	6.0.3
7.0.0.138	2.5.0.3	10.0.3	6.0.3
7.0.0.139	2.5.0.3	10.0.3	6.0.3
7.0.0.140	2.5.0.3	10.0.3	6.0.3
7.0.0.141	2.5.0.3	10.0.3	6.0.3
7.0.0.142	2.2.1.4	9.0.4	5.0.4

Software Version	Interplay Transfer engine	NewsCutter	Media Composer
7.0.0.143	2.7.0.2	10.5.2	6.5.2
7.0.0.144	2.7.0.2	10.5.2	6.5.2
7.0.0.145	2.7.0.2	10.5.2	6.5.2
7.0.0.146	2.7.0.2	10.5.2	6.5.2
7.0.0.147	2.7.0.2	10.5.2	6.5.2
7.0.0.148	2.7.0.2	10.5.2	6.5.2
7.0.0.149	2.7.0.2	10.5.2	6.5.2
7.0.0.150	2.7.0.2	10.5.2	6.5.2
7.0.0.161	2.7.0.2	10.5.2 & 11.0.2	6.5.2 & 7.0.2
7.0.0.162	2.7.0.2	10.5.2 & 11.0.2	6.5.2 & 7.0.2
7.0.0.163	2.7.0.2	10.5.2 & 11.0.2	6.5.2 & 7.0.2

K2-AvidTM Software Version and Video server version matrix

Software Version	Profile PVS series	K2 series	K2 Summit system	K2 Summit/Solo system	Notes
7.0.0.104	5.4.9.1328	3.3.2.1412	7.3.8.1432	7.3.8.1432	
7.0.0.105	5.4.9.1328	3.3.2.1412	7.3.8.1432	7.3.8.1432	
7.0.0.112	No support	3.3.2.1412	7.3.8.1432	7.3.8.1432	
7.0.0.126	No support	3.3.2.1412	9.x	9.x	DNxHD not supported.
7.0.0.127	No support	3.3.2.1412	9.x	9.x	DNxHD not supported.
7.0.0.128	No support	3.3.2.1412	9.x	9.x	DNxHD not supported.
7.0.0.129	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.130	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.131	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.132	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.133	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.

Software Version	Profile PVS series	K2 series	K2 Summit system	K2 Summit/Solo system	Notes
7.0.0.134	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.135	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.136	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.137	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.138	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.139	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.140	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.141	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.142	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.144	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.145	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.146	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.147	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.148	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.149	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.150	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.161	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.162	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.163	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.

Supported compression formats

K2-AvidTM Build 7.0.0.104 supports

Compression formats Supported on PVS1100 with software build 5.4.9.1328

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
DVCAM	Yes	Yes	Yes	Yes	8	Yes	Yes	No
DVCPRO25	Yes	Yes	Yes	Yes	8	Yes	Yes	No
DVCPRO50	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 30 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 40 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 50 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No

NOTE: For PVS, ingest & Send to playback are only supported if Windows XP operating system are used on the Avid editor and transfer manager.

Compression formats Supported on K2 with software build 3.3.2.1412

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
DVCAM	Yes	Yes	Yes	Yes	8	Yes	Yes	No
DVCPRO25	Yes	Yes	Yes	Yes	8	Yes	Yes	No
DVCPRO50	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 30 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 40 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 50 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No

Compression formats Supported on K2 Summit/Solo system with software build 7.3.8.1432

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
DVCAM	Yes	Yes	Yes	Yes	8	Yes	Yes	No
DVCPRO25	Yes	Yes	Yes	Yes	8	Yes	Yes	No
DVCPRO50	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 30 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 40 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 50 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No
DV100 1080I	Yes	Yes	Yes	Yes	8	Yes	Yes	No

K2-AvidTM Build 7.0.0.105 supports Interplay 2.1

Compression formats Supported on PVS1100 with software build 5.4.9.1328

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
DVCAM	Yes	Yes	Yes	Yes	8	Yes	Yes	No
DVCPRO25	Yes	Yes	Yes	Yes	8	Yes	Yes	No
DVCPRO50	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 30 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 40 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 50 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No

NOTE: For PVS, ingest & Send to playback are only supported if Windows XP operating system are used on the Avid editor and transfer manager.

Compression formats Supported on K2 with software build 3.3.2.1412

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
DVCAM	Yes	Yes	Yes	Yes	8	Yes	Yes	No
DVCPRO25	Yes	Yes	Yes	Yes	8	Yes	Yes	No
DVCPRO50	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 30 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 40 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 50 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No

Compression formats Supported on K2 Summit/Solo system with software build 7.3.8.1432

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
DVCAM	Yes	Yes	Yes	Yes	8	Yes	Yes	No
DVCPRO25	Yes	Yes	Yes	Yes	8	Yes	Yes	No
DVCPRO50	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 30 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 40 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 50 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No
DV100 1080I	Yes	Yes	Yes	Yes	8	Yes	Yes	No

K2-AvidTM Build 7.0.0.112 to build 7.0.0.128

Compression formats Supported on PVS1100 with software build 5.4.9.1328

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
DVCAM	Yes	Yes	Yes	Yes	16	Yes	No	No
DVCPRO25	Yes	Yes	Yes	Yes	16	Yes	No	No
DVCPRO50	Yes	Yes	Yes	Yes	16	Yes	No	No
D10 30 Mb.	Yes	Yes	Yes	Yes	16	Yes	No	No
D10 40 Mb.	Yes	Yes	Yes	Yes	16	Yes	No	No
D10 50 Mb.	Yes	Yes	Yes	Yes	16	Yes	No	No

NOTE: For PVS, ingest is only supported if Windows XP operating system are used on the Avid editor and transfer manager.

Compression formats Supported on K2 with software build 3.3.2.1412

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
DVCAM	Yes	Yes	Yes	Yes	16	Yes	Yes	No
DVCPRO25	Yes	Yes	Yes	Yes	16	Yes	Yes	No
DVCPRO50	Yes	Yes	Yes	Yes	16	Yes	Yes	No
D10 30 Mb.	Yes	Yes	Yes	Yes	16	Yes	Yes	No
D10 40 Mb.	Yes	Yes	Yes	Yes	16	Yes	Yes	No
D10 50 Mb.	Yes	Yes	Yes	Yes	16	Yes	Yes	No

Compression formats Supported on K2 Summit system with software build 7.3.8.1432

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
DVCAM	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
DVCPRO25	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
DVCPRO50	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
D10 30 Mb.	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
D10 40 Mb.	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
D10 50 Mb.	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
DV100 1080I	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
DV100 720P	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
AVCI 720P 50Mb	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
AVCI 720P 100Mb	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
AVCI 1080 50Mb	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
AVCI 1080 100Mb	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
XDCAM-HD 1080 18Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-HD 1080 25Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-HD 1080 35Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-HD422 1080 50Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-EX 1080 35Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-EX-HD422 720P 50Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-EX 720P 25Mb	No	No	No	No	No	No	No	No
XDCAM-EX 720P 35Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes

K2-AvidTM Build 7.0.0.129 and up supports Interplay Engine 2.5.0.1

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
DVCAM	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
DVCPRO25	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
DVCPRO50	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
D10 30 Mb.	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
D10 40 Mb.	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
D10 50 Mb.	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
DV100 1080I	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
DV100 720P	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
AVCI 720P 50Mb	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
AVCI 720P 100Mb	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
AVCI 1080 50Mb	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
AVCI 1080 100Mb	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
XDCAM-HD 1080 18Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-HD 1080 25Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-HD 1080 35Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-HD422 1080 50Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
XDCAM-EX 1080 35Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-EX-HD422 720P 50Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-EX 720P 25Mb	No	No	No	No	No	No	No	No
XDCAM-EX 720P 35Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
DNxHD 120 (HD1080i)	No	Yes	Yes	Yes	16	Yes	Yes	Yes
DNxHD 185 (HD1080i)	No	Yes	Yes	Yes	16	Yes	Yes	Yes
DNxHD 185x (HD1080i)	No	Yes	Yes	Yes	16	Yes	Yes	Yes
DNxHD 120 (HD720p)	No	Yes	Yes	Yes	16	Yes	Yes	Yes
DNxHD 185 (HD720p)	No	Yes	Yes	Yes	16	Yes	Yes	Yes
DNxHD 185x (HD720p)	No	Yes	Yes	Yes	16	Yes	Yes	Yes
DNxHD 145 (HD1080i)	Yes	No	Yes	Yes	16	Yes	Yes	Yes
DNxHD 220 (HD1080i)	Yes	No	Yes	Yes	16	Yes	Yes	Yes
DNxHD 220x (HD1080i)	Yes	No	Yes	Yes	16	Yes	Yes	Yes
DNxHD 145 (HD720p)	Yes	No	Yes	Yes	16	Yes	Yes	Yes
DNxHD 220 (HD720p)	Yes	No	Yes	Yes	16	Yes	Yes	Yes
DNxHD 220x (HD720p)	Yes	No	Yes	Yes	16	Yes	Yes	Yes

K2-AvidTM Build 7.0.0.143 and up supports Interplay Engine 2.7.0.2

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
DVCAM	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
DVCPRO25	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
DVCPRO50	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
D10 30 Mb.	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
D10 40 Mb.	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
D10 50 Mb.	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
DV100 1080I	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
DV100 720P	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
AVCI 720P 50Mb	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
AVCI 720P 100Mb	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
AVCI 1080i 50Mb	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
AVCI 1080i 100Mb	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
AVCI 1080p 100Mb	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
XDCAM-HD 1080 18Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-HD 1080 25Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-HD 1080 35Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-HD422 1080 50Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-EX 1080 35Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-EX-HD422 720P 50Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-EX 720P 25Mb	No	No	No	No	No	No	No	No
XDCAM-EX 720P 35Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
DNxHD 120 (HD1080i)	No	Yes	Yes	Yes	16	Yes	Yes	Yes
DNxHD 185 (HD1080i)	No	Yes	Yes	Yes	16	Yes	Yes	Yes
DNxHD 185x (HD1080i)	No	Yes	Yes	Yes	16	Yes	Yes	Yes
DNxHD 120 (HD720p)	No	Yes	Yes	Yes	16	Yes	Yes	Yes
DNxHD 185 (HD720p)	No	Yes	Yes	Yes	16	Yes	Yes	Yes
DNxHD 185x (HD720p)	No	Yes	Yes	Yes	16	Yes	Yes	Yes
DNxHD 145 (HD1080i)	Yes	No	Yes	Yes	16	Yes	Yes	Yes
DNxHD 220 (HD1080i)	Yes	No	Yes	Yes	16	Yes	Yes	Yes
DNxHD 220x (HD1080i)	Yes	No	Yes	Yes	16	Yes	Yes	Yes
DNxHD 145 (HD720p)	Yes	No	Yes	Yes	16	Yes	Yes	Yes
DNxHD 220 (HD720p)	Yes	No	Yes	Yes	16	Yes	Yes	Yes
DNxHD 220x (HD720p)	Yes	No	Yes	Yes	16	Yes	Yes	Yes

Installation and configuration

Installation instructions

Follow the installation instructions in K2 Avid Plug-in manual PN. 071-8551-02 for detail over how to install and configure build 7.0.0.104 or 7.0.0.105.

Installation of build 7.0.0.112 is much simpler as it only support Avid Interplay Transfer engine 2.2.1.1 but it's still highly recommended you refer to the K2 Avid Plug-in manual PN. 071-8551-02.

Installing Avid Media Access

Do the following steps to install Grass Valley AMA (Avid Media Access):

1. Install SNFS client software on the device hosting the Editing application.

   This provides guaranteed bandwidth, thereby ensuring smooth playback in the Editing application.

2. Use SMB mounted `v:` volume on standalone K2 Summit system.

   It is recommended for you to use the latest generation K2 Summit system hardware since older hardware may not have the required hardware resources to sustain smooth playback in the Editing application.

3. Use media files on removable media if the original folder and file structure are kept intact.

   If the removable media cannot provide adequate edit playback, transcode or consolidate the media into one of Avid's native codec formats.

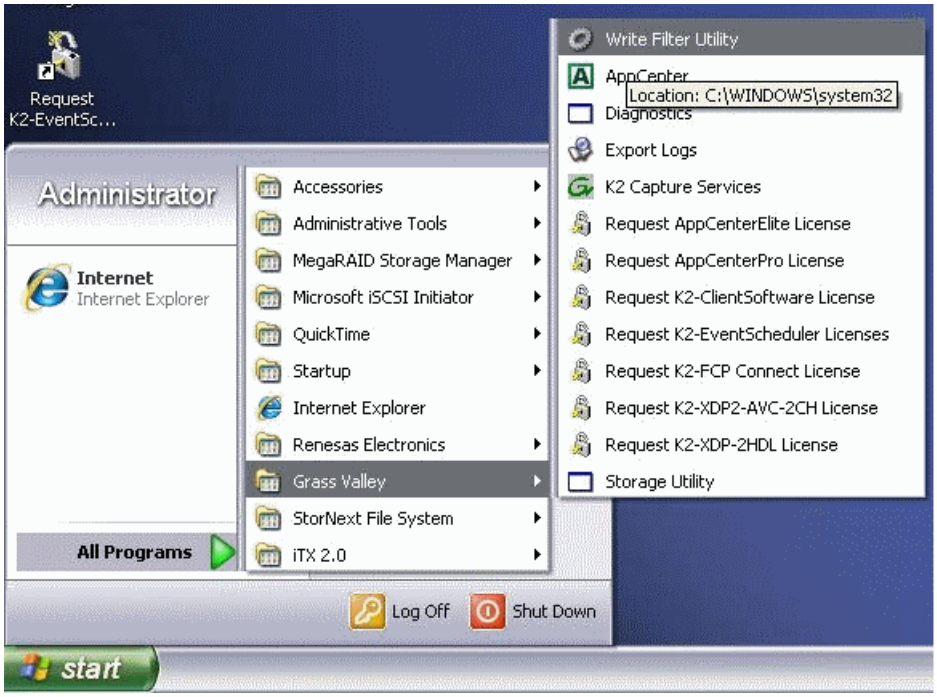
Installing TServerSvc on the K2 Media Clients and K2 Summit Production Client

If you previously had the TserverSvc installed, then uninstall this prior to installing the new version.

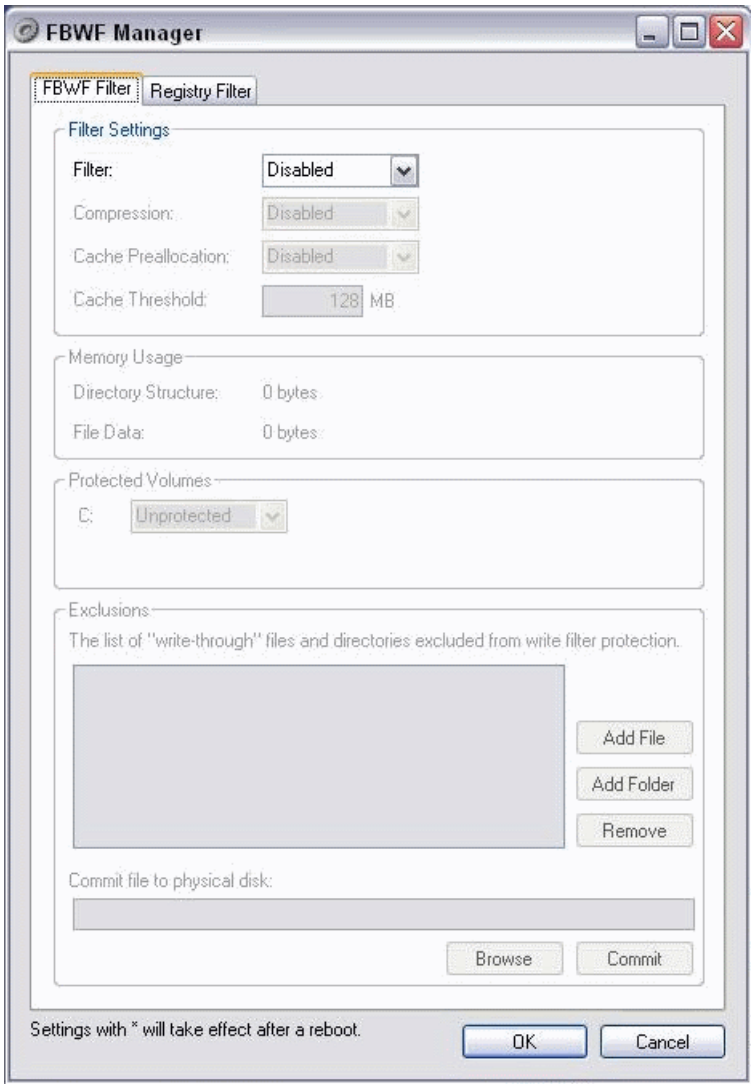
- For K2 Summit systems with Microsoft Windows that use McAfee embedded security, you need to put the system in Update mode before installing the new software.

The TServerSvc can be installed on standalone K2 Media Clients, K2 Summit Production Clients, K2 Summit 3G Production Clients or K2 Media Servers (with the role of FTP servers) when configuring systems with external (shared) storage.

1. Navigate to the Write Filter Utility and launch the application.



2. Under Filter Settings, set the Filter to **Disabled** as shown.



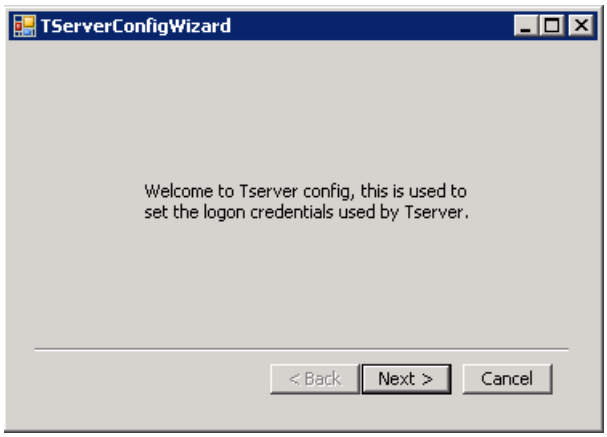
   If the filter setting is changed then you will be requested to reboot the K2 Summit Production Client before proceeding with the K2Tserver installation.

3. Browse the folder with the installers and access the folder \K2Tserver\.
4. Double-click Setup.exe.
5. Click **Next** in the "Welcome to the InstallShield Wizard for Grass Valley K2 AvidTM K2 Tserver" dialog box.

   Next the License Agreement is displayed.

6. Select "I accept the terms in the License agreement" and click **Next**.
7. Click **Install** to start the installation or **Cancel** in the "Ready to install" dialog box.
8. The status dialog then displays the progress of the installation.

9. The following Configuration Wizard is then displayed.



- This is used to override the default credentials.

10. Click **Next** to walk through the wizard.
11. To set the credential using the wizard, do one of the following:

Options	Description
Default credentials	• Username: Administrator • Password: Administrator password
If installing on a K2 Summit system version earlier than 8.x, use this default credentials	• Username: Administrator • Password: Administrator password

12. Click **Next** and **Finish** to complete the wizard.

This wizard can be run at any time from `C:\profile\TserverConfigWizard.exe`.

13. Click **Finish** when installation completes in the "InstallShield Wizard Completed" dialog box.

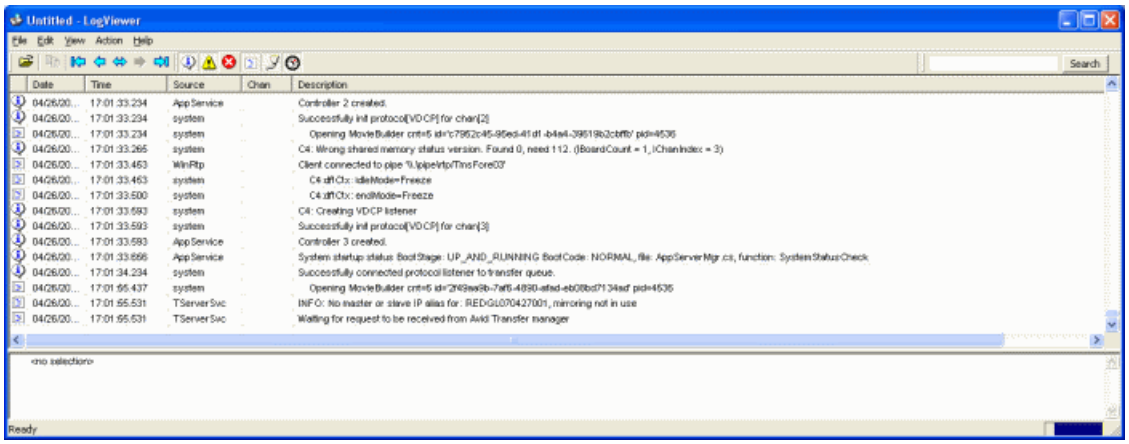
Verify TserverSvc is installed correctly

1. On the K2 Media Client or K2 Summit Production Client, open the Logviewer program in `c:\profile\log.exe`.

   NOTE: Make sure no filters are selected.

2. Then look for the following TServerSvc messages.

   - INFO: No master or slave IP alias for: DeviceHostName, mirroring not in use.
   - Waiting for request to be received from Avid Transfer manager.



This indicates the service is installed and running.

3. Repeat the above steps for each K2 Media Client or K2 Summit Production Client you wish to use.

   NOTE: Default username administrator and password adminK2 are used by the Tserver. You can overwrite the default credentials by running `C:\profile\TserverConfigWizard.exe`.

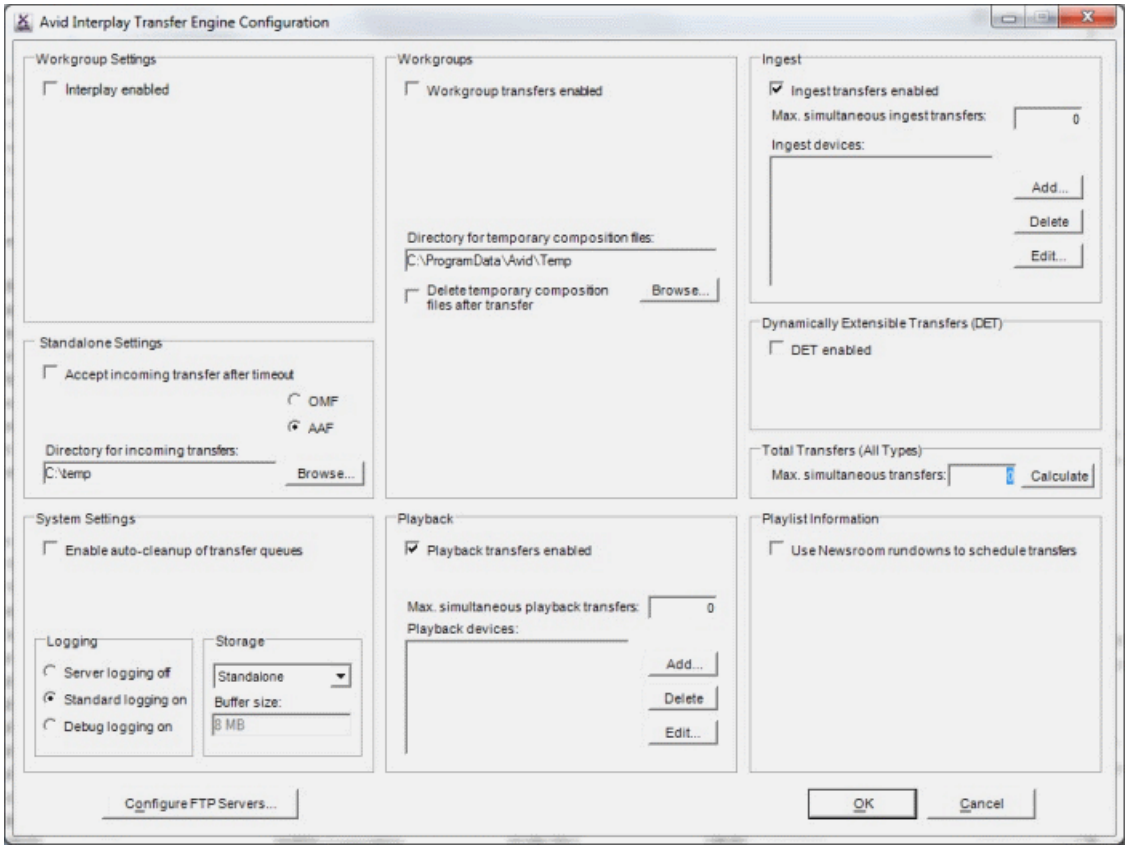
Prerequisites for installation of K2-AvidTM Software on Avid devices

1. NewsCutter® or MediaComposer® software is installed on editor clients.
2. Each Editor has Avid Interplay Transfer Client software installed.
3. Avid Interplay Transfer Engine software is installed.
4. Each Editor is configured for Transfers.
5. Transfer Engine has been configured with a valid Storage Type.
6. SNFS client software has been installed and configured if GV AMA is used to link to media files on GV SAN FS (K2 media file system).

Configuring Avid Interplay Transfer Engine

The following configuration is for a standalone Interplay Transfer Engine.

1. Open the Avid Interplay Transfer Engine Configuration by doing one of the following:
   - Click the icon on the desktop.
   - Find the configuration in `C:\Program Files\Avid\Avid Interplay Transfer Engine\TRANSFERMGRSERVERCONFIG\tmconfig.exe`.



2. Set the **Standalone Settings** by doing the following:
   a) Select the **Accept Incoming transfers after timeout** check box.
   b) Select **AAF**.
   c) Select the directory for incoming transfers.

3. Set the **System Settings** by doing the following:
   a) Select the **Enable auto-cleanup of transfer queues** check box.
   b) Set the Storage Type to **Standalone**.
4. Set the **Playback** by doing the following:
   a) Select the **Playback transfers enabled** check box.
   b) Set the **Max simultaneous playback transfers** to 4.
   c) Do not select the**Long GOP transfers enabled** check box.
5. Set the **Ingest** by doing the following:
   a) Select the **Ingest transfers enabled** check box.
   b) Set the **Max simultaneous ingest transfers** to 4.
6. Click **Calculate** to update the Max. Simultaneous Transfers in the **Total Transfers (All Types)** section.
7. Click **OK** to save the configuration or click **Cancel** to discard the changes.
8. If the Interplay engine is running, terminate and restart to use the new configuration.

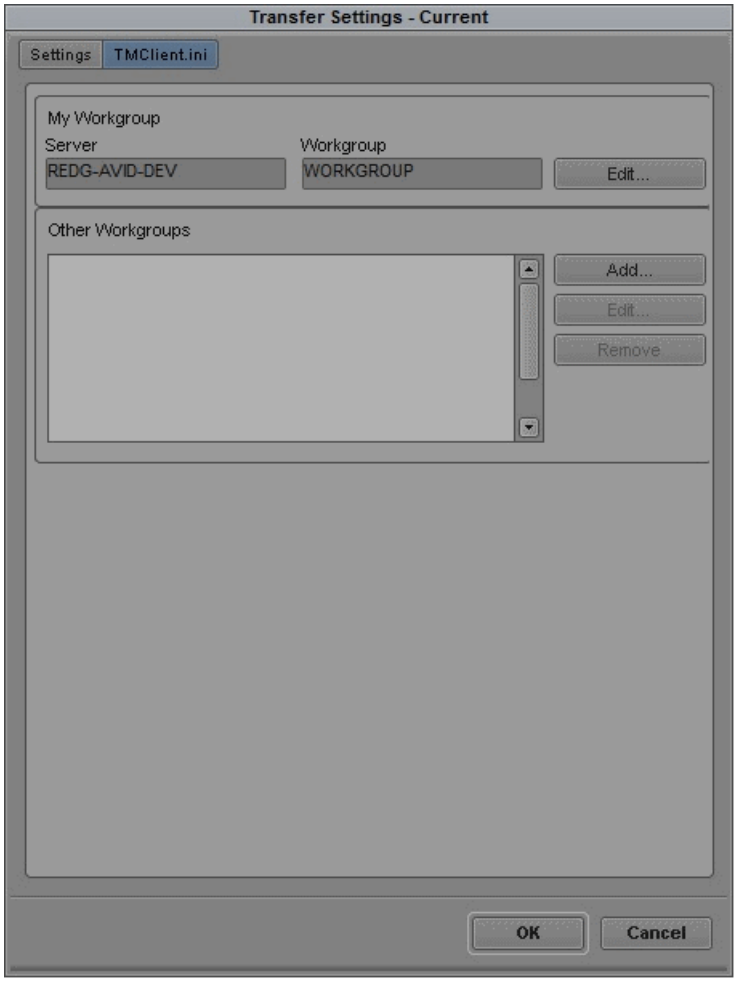
Configuring the Avid Editor for Transfers

The following configuration uses the Avid Media Composer.

1. Start the Avid Media Composer.
2. Click the **Edit** menu, and then select **Preferences**.
3. Select **Transfer** under the Settings tab.
4. In the Send To Playback, locate the Output Audio Mix and select **Direct channel output or Stereo output**.
5. Click on the TMClient.ini tab and click **Add**.

6. Add the host name of the device which is running the Avid Interplay Transfer Engine. In this example **REDG-AVID-DEV**, and set the Workgroup to **WORKGROUP**.

   NOTE: The names must match the names used to configure the Avid Interplay Transfer Engine.



7. Click **OK** to save and exit.
8. Restart the Editor.

   Configuration of the editor is complete.

Installing the K2AvidDHM software

Do the following steps to install the K2AvidDHM software on the PC that runs the Avid Interplay Transfer Engine.

1. Browse the folder of installers and navigate to `\K2AvidDhm\Disk1\`.
2. Double-click **Setup.exe**.
3. Click **Next** in the "Welcome to the InstallShield Wizard for K2AvidDHM" dialog box.

   The License Agreement dialog box is displayed.

4. Select the **I accept the terms in the License agreement** check box.

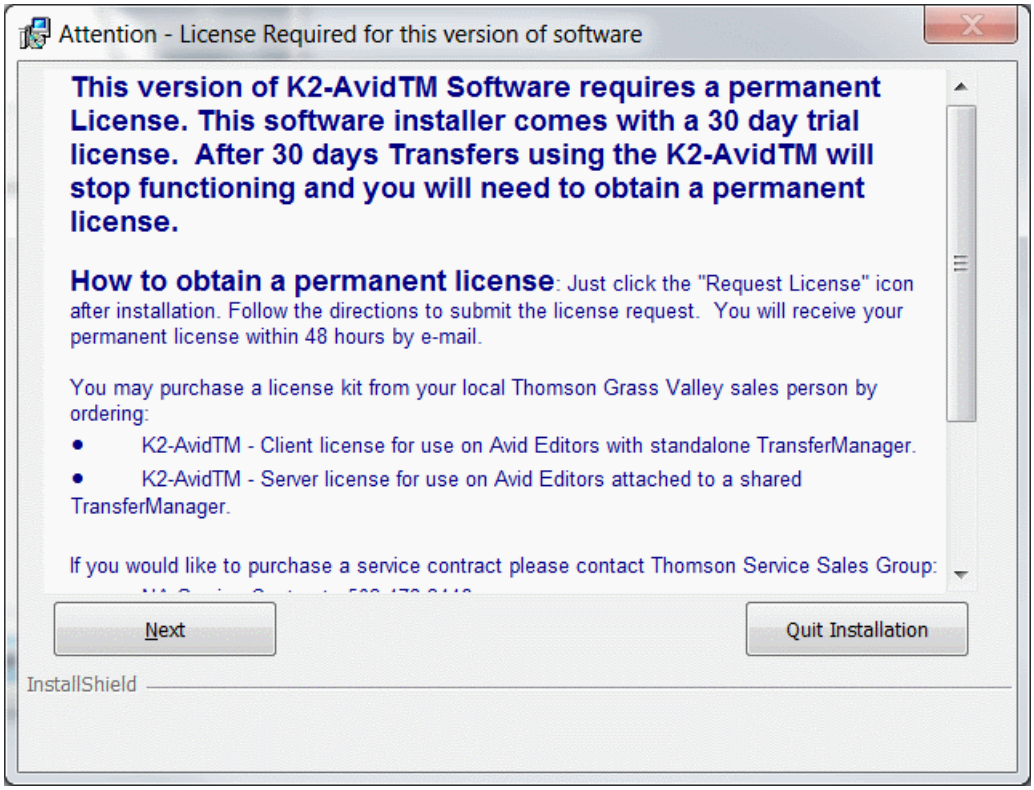
5. Take the time to read the information provided on the license agreement and click **Next**.
6. Click **OK** if you get the following message when you are attempting to install on a device which do not have any Avid Interplay Transfer Engine installed.

NOTE: Ensure that you have installed Avid Interplay Transfer.

Likewise a message will be displayed if both Transfer Manager and Interplay Transfer engine are installed.

7. Click **Install** to start the installation in the "Ready to Install" dialog box.

8. Do take the time to read the information provided in the "License Required for this version of software" dialog box and click **Next**.



   The status dialog then displays the progress of the installation.

9. Click **Finish** when the install is completed.
10. Restart the Avid Interplay Transfer Engine to complete the DHM installation.

Verify K2 Avid DHM is installed correctly

1. Start the License Manager and verify licenses are installed.
2. On the Avid Transfer manager / Interplay engine device, locate the License manager icon on the desktop and double click to start this.
3. If you are upgrading from a previous version and a permanent license was previously installed, then verify that it is still present. Otherwise add the license which was backed up previously and verify that it is still valid.

4. If you do not have a permanent license, check if a temporary license was installed during the setup. Otherwise you can add a temporary license which can be found in:

Options	Description
32-bit Operating System	*C:\Program Files\Grass Valley\SabreTooth\TemporaryLicense.txt*
64-bit Operating System	*C:\Program Files (x86)\Grass Valley\SabreTooth*

NOTE: You will need a permanent license to operate beyond the 30 day trial period. Details on how to obtain permanent license can be found elsewhere in this manual.

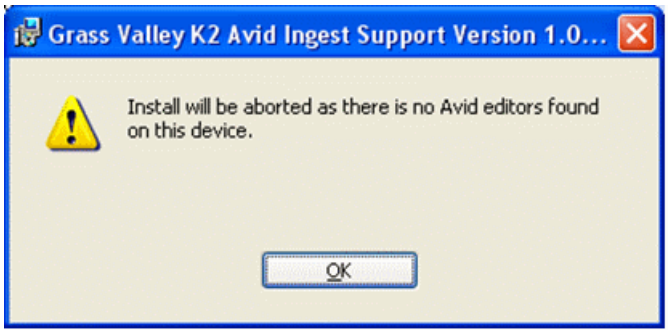
Installing the K2 Avid Ingest software

1. Browse the folder of installers and navigate to *\K2ingest\Disk1*.
2. Double-click **Setup.exe**.
3. Click **Next** in the "Welcome.." dialog box.

4. Click **OK** if you get one of the following below:

   Please refer to *Prerequisites for installation of K2-AvidTM Software on Avid devices* on page 1254 if you encounter any of the following error warnings.

   a) You may get the following message if you are attempting to install on a device which does not have an Avid Editor installed.



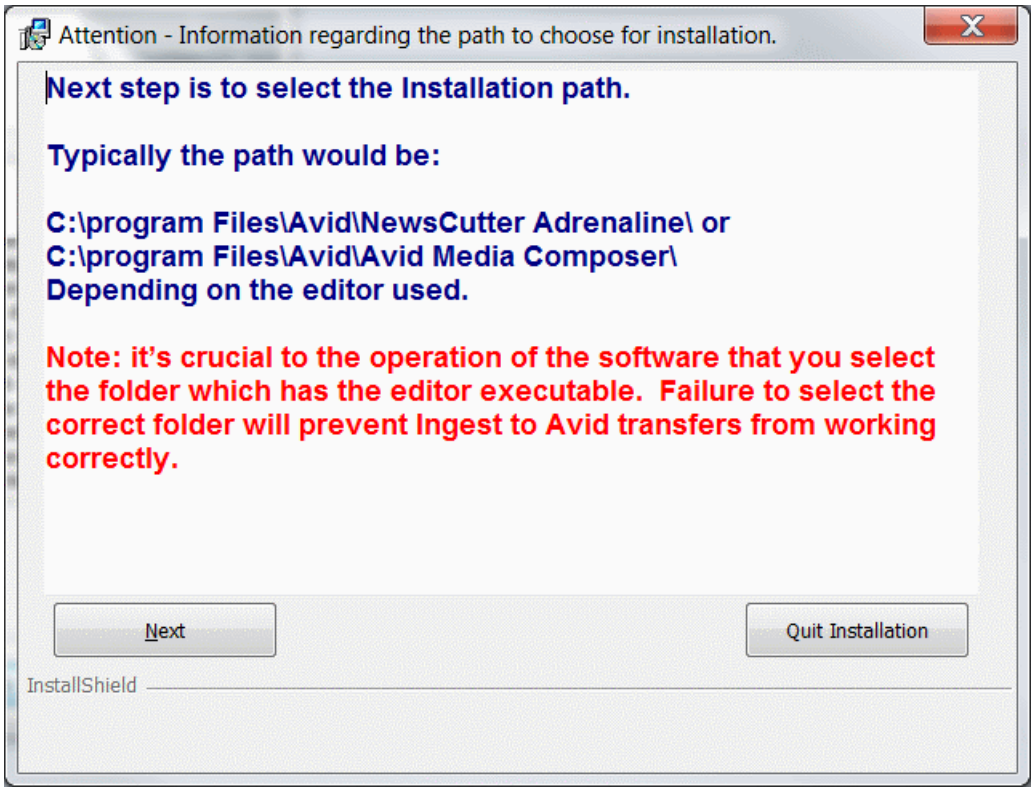
   b) You may get the following message if you are attempting to install on a device which has both AvidNewsCutter and Avid MediaComposer installed.

   c) Or if there is no TransferManager Clients or Avid Interplay Transfer Clients installed, you may see the following message.

   The "License Agreement" dialog box is displayed.

5. Select the **I accept the terms in the License agreement** check box.
6. Take the time to read the information provided on the license agreement and click **Next**.
7. Select the installation path. Take a moment to find out where the Avid Editor executable is located.

   NOTE: The Install program will attempt to locate the Avid editor executable and use the path found.

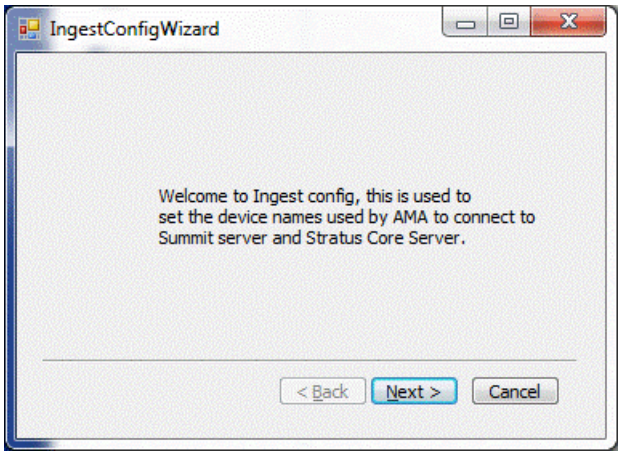


8. Click **Next**.

   The next dialog box displays the path found.
9. Verify that the path is correct, and click **Next**. Otherwise, click **Change** and browse to the correct destination folder.
10. Click **Install** to begin the installation.

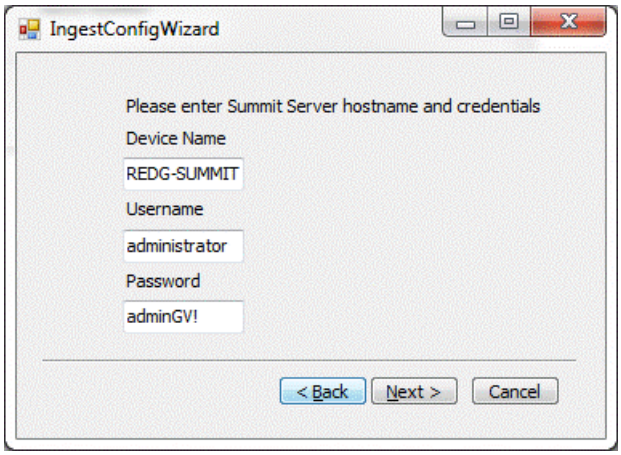
    The status dialog then displays the progress of the installation.

11. The following Configuration Wizard is then displayed.

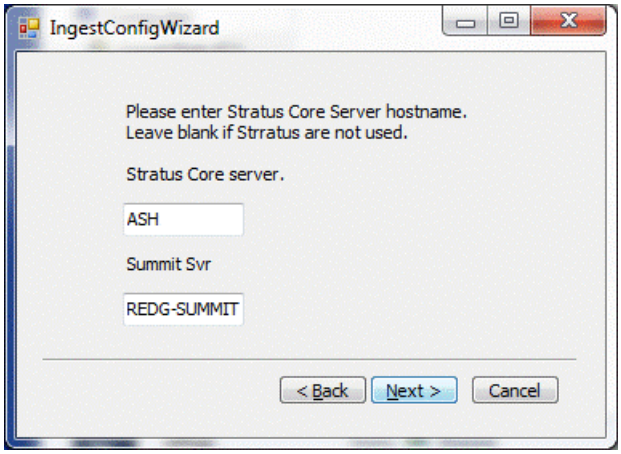


This is used to set the hostname of the K2 Media Server (FSM) used for AMA linking.

12. If GV STRATUS is used, you need to set the Core Server hostname and the hostname of the device the Grass Valley Media Server MDI is connecting to.
13. Click **Next** to walk through the wizard.
14. Enter the hostname of the FSM and credentials if AMA is used, otherwise leave blank and click **Next**.

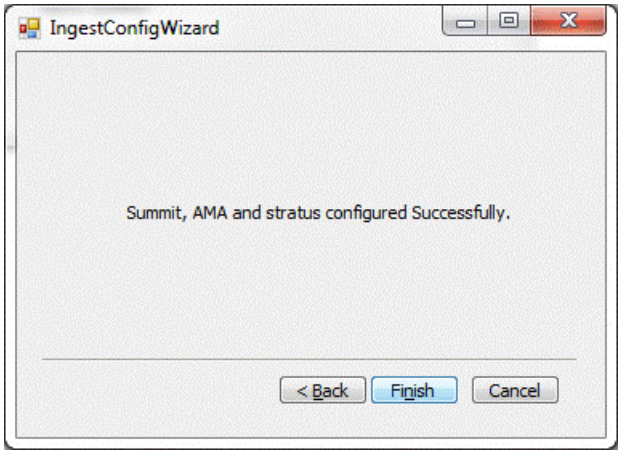


15. Enter the hostname of the Core Server and host name of the K2 Summit server used by the Grass Valley Media Server MDI.



Leave the space blank if GV STRATUS integration is not used.

16. Click **Next** to complete this Wizard.



This can be run at any time from `C:\Program Files\Avid\Avid Media Composer\IngestConfig64.exe`.

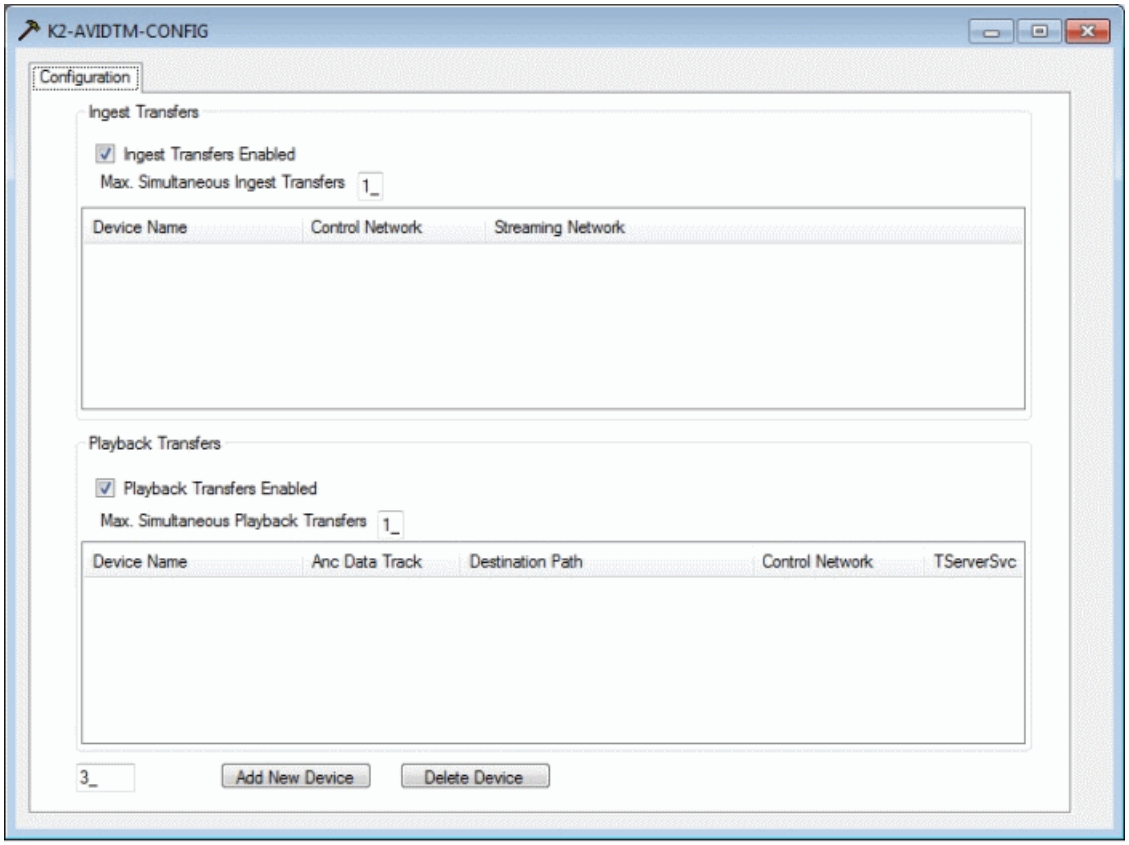
17. Click **Finish** when the install is completed.

NOTE: Default username "Administrator" and password are used by the Ingest software.

Add and configure devices for Ingest and Playback

1. Start the K2-AVIDTM-CONFIG.

   If there are no configured devices, it will appear as shown below.

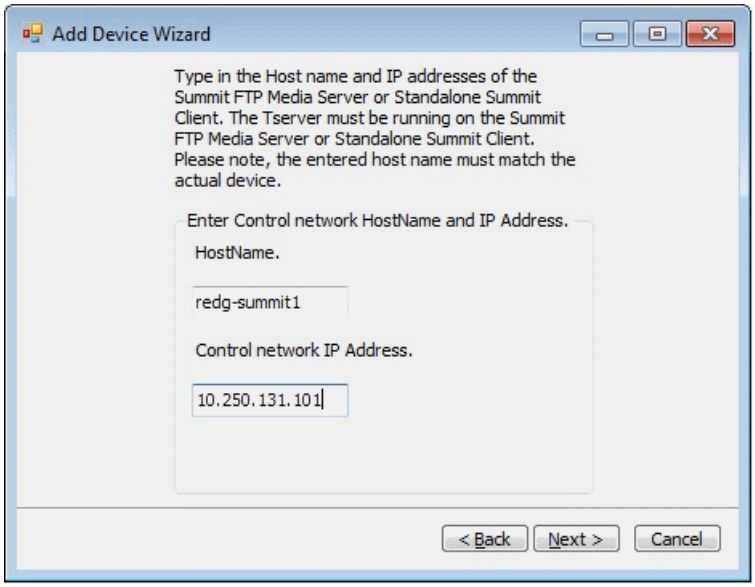


2. Click **Add New Device**.

   The Add Device Wizard displays.

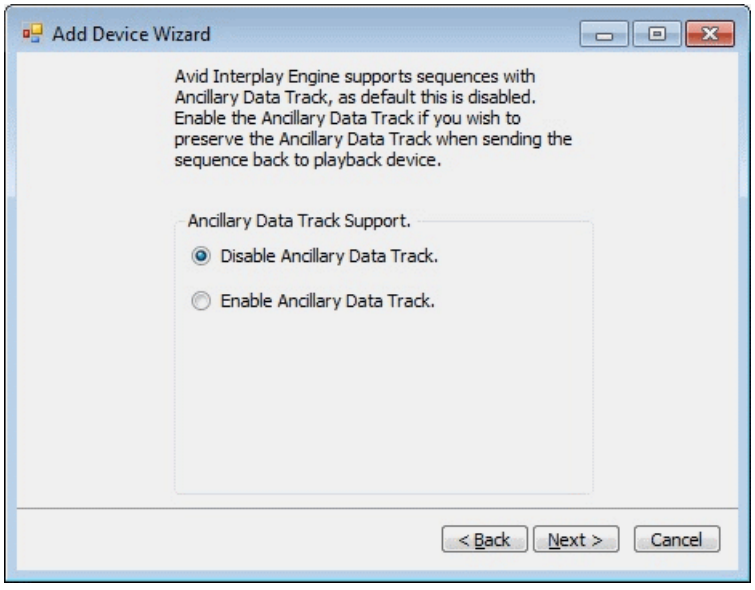
3. Select the type of network configuration.

4. Enter the host name of the standalone K2 Summit system or the host name of the K2 Media Server with the role of FTP server.



NOTE: The host name used must match the actual device name.

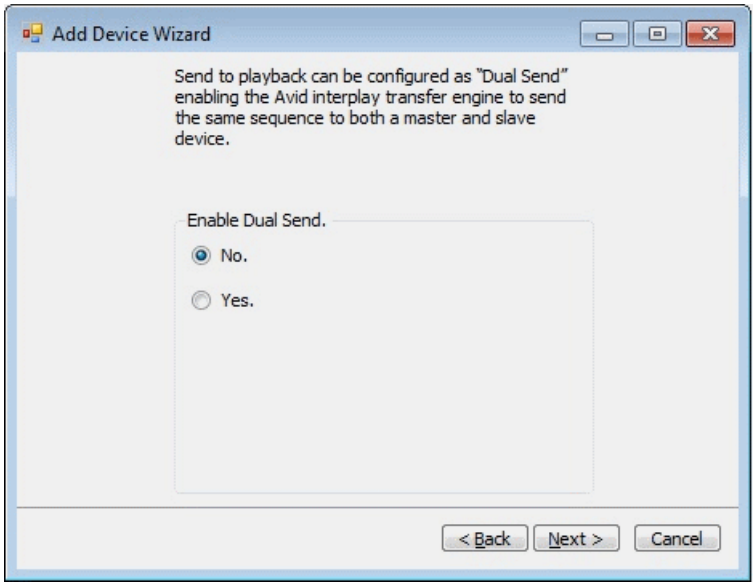
5. Select to enable Ancillary Data Track support if you want to preserve Ancillary data when sending sequences back to the playback device.



6. Select **Yes**, if you wish to send back to a different folder than default.

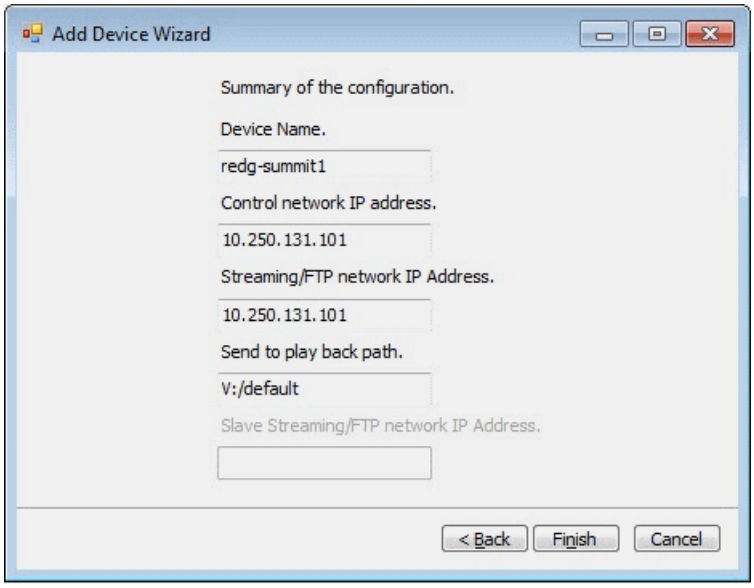
NOTE: You need to run the wizard twice when overwriting the folder. Once with no overwrite and then once more for the overwrite.

7. Select **Yes** if you want dual send support.



8. Click **Next**.

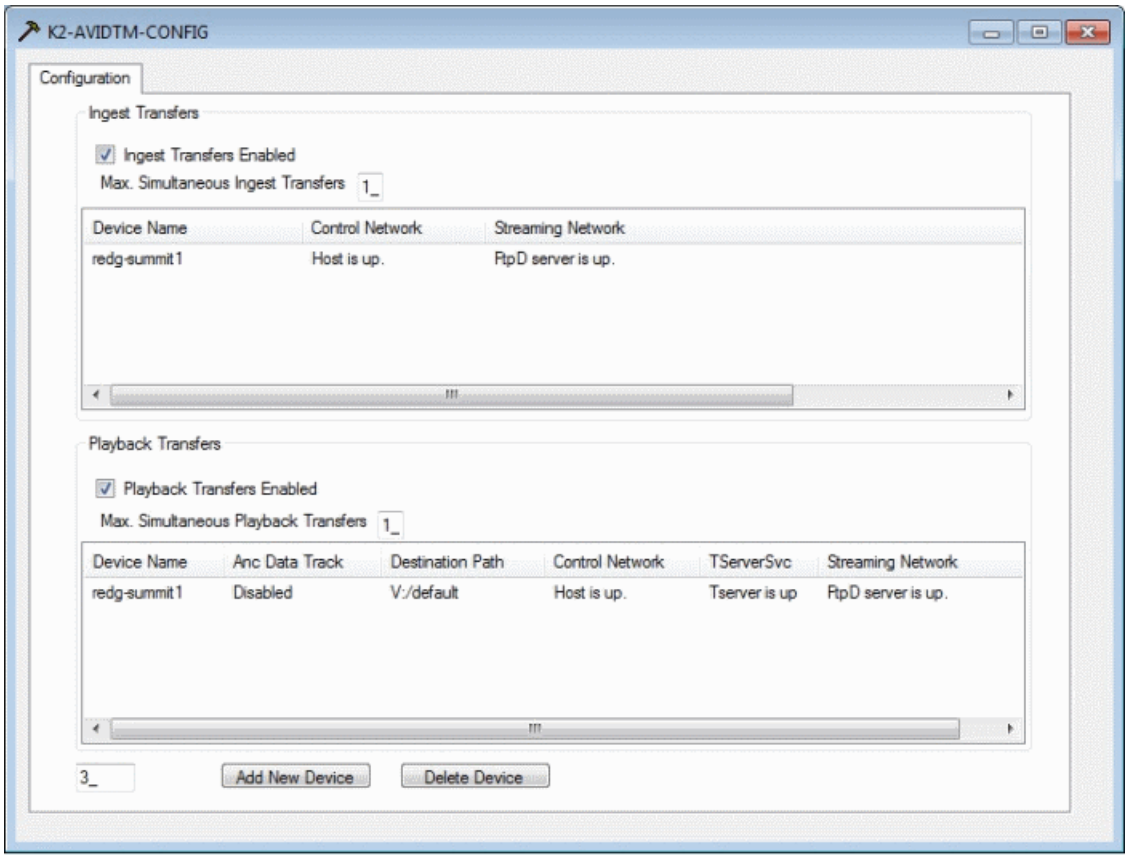
   The summary page displays.



9. Click **Finish** to exit from the Add Device Wizard.

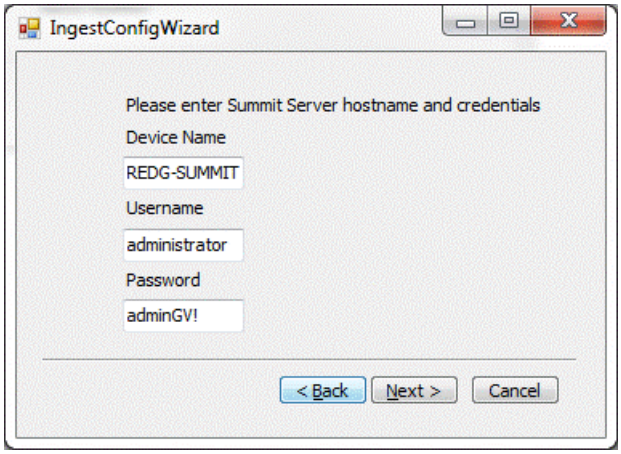
   The Configuration page displays.

   NOTE: This may take several seconds as the program verifies the network connection, if Tserver and FtpD is up.

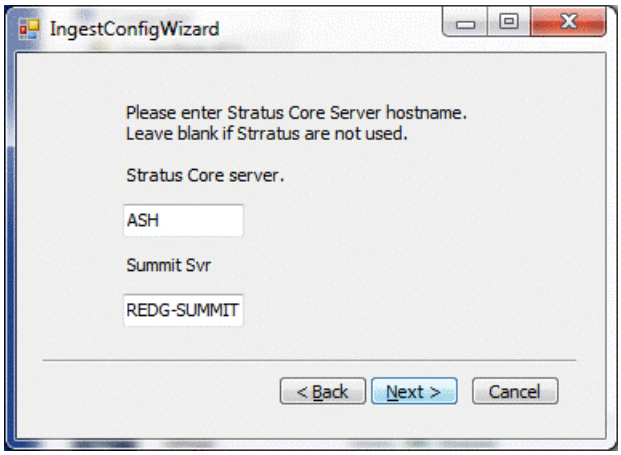


10. If GV STRATUS is used, set the GV STRATUS Core Server hostname and the hostname of the device to which the GV STRATUS K2 Summit system MDI connects.
11. Click **Next** to walk through the wizard.

12. Enter the hostname of the FSM and credentials if AMA is used, otherwise leave blank and click **Next**.

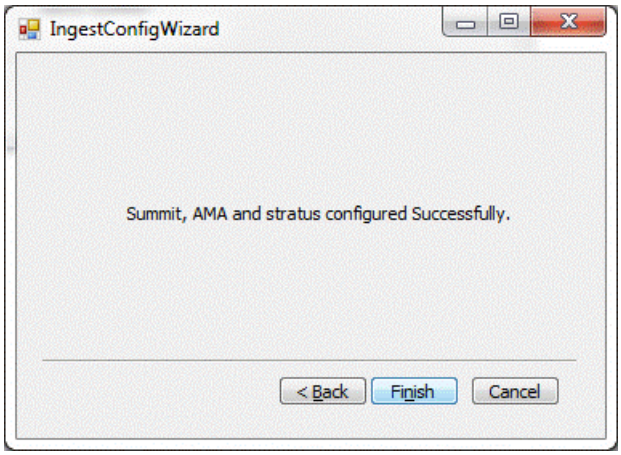


13. Enter the hostname of the Core Server and host name of the K2 Summit server used by the Grass Valley Media Server MDI.



Leave the space blank if GV STRATUS integration is not used.

14. Click **Next** to complete this Wizard.



This can be run at any time from *C:\Program Files\Avid\Avid Media Composer\IngestConfig64.exe*.

15. Click **Finish** when the install is completed.

NOTE: Default username "Administrator" and password are used by the Ingest software. You can overwrite the default credentials used by the Ingest software. This is done in the registry in the following location: HKEY_LOCAL_MACHINE\SOFTWARE\Grass Valley Group\Applications\K2-AvidTM\Setup and for the K2-AvidExplorer at HKEY_LOCAL_MACHINE\SOFTWARE\Grass Valley Group\Applications\K2-AvidTM\K2-AvidExplorer.

Using the GV AMA plug-in

Before you can link to any files, verify the following:

- Check the GV AMA plug-ins are installed. At the Editing software, select **TOOLS** and choose **Console** to call up the console window. At the bottom of the window, type AMA_ListPlugins. A report is displayed below:

  AMA PLUG-IN NAME COMPANY NAME VERSION

  - Avid MXF MSP Plug-In Avid Technology, Inc. 1.1
  - Sphere (5850 1.1.5964899) Avid Technology, Inc. 1.1
  - AS-02 Plug-In Avid Technology, Inc. 1.2
  - AS-11 Plug-In Avid Technology, Inc. 1.0
  - MSP_GrassValley for 64Bit OS Grass Valley USA, LLC. 0.3
  - MSP_MXF Plug-In Avid Technology, Inc. 1.9
  - QuickTime Plug-In Avid Technology, Inc. 1.3
  - WaveAiff Plug-In Avid Technology, Inc. 1.0

- Verify the MSP_GrassValley and MVP_GrassValley plug-ins are listed.
- Confirm the plug-ins are correctly installed and configured.

- To verify and configure the volumes, the volume must be mounted and mapped using driver letter *V:* before the GV AMA plug-ins can be used to link any files.

  If SNFS client are used: SNFS client mounting are used if K2 SAN's are used. Verify the SNFS client are installed and configured to use driver letter *V:*.

  If SMB client are used: SMB client mounts are used when working on standalone K2 Summit system. The K2 Summit system *V:* drive must be shared at root level with the Share Name **V** before this drive can be mounted using the command shown below: The volume is mounted, using the following command. net use *V: \\SummitHostname\V /USER:SummitHostname\administrator /PERSISTENT:YES*.

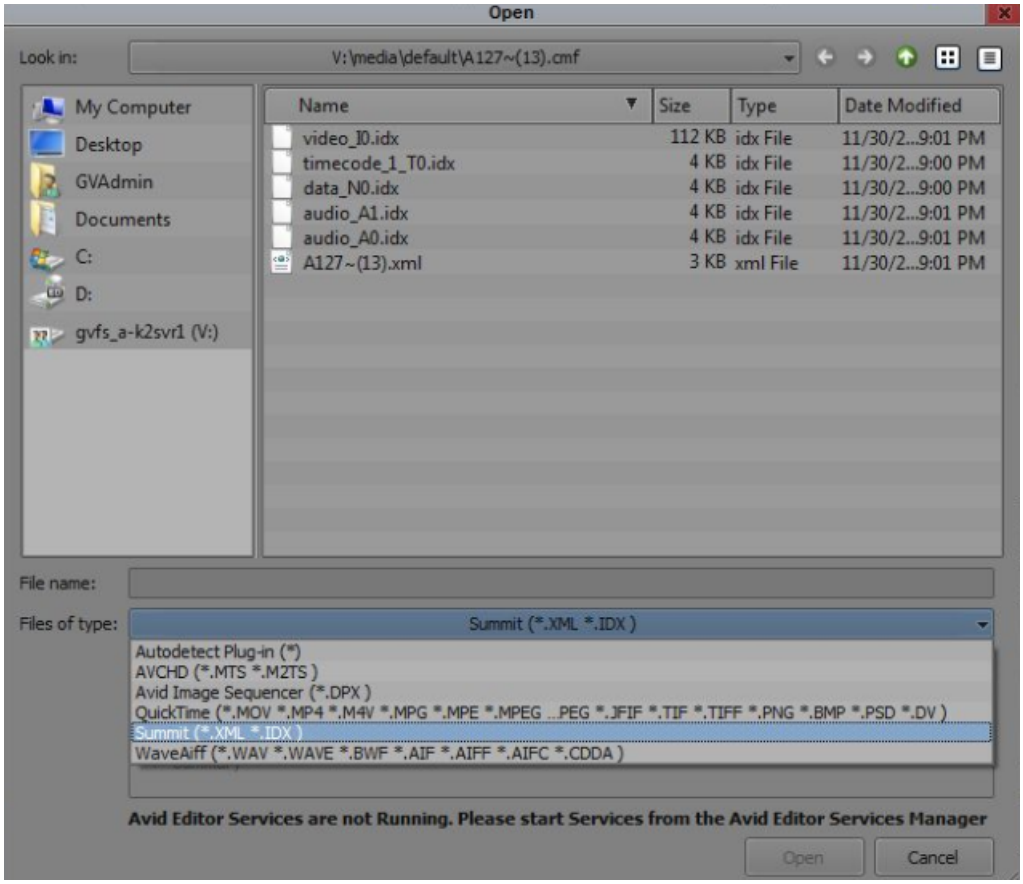
  If Removable drives are used: If the original media on the K2 Summit system existed in *V:\media\default\Myclip.cmf *, then the removable drive should have the same path *media\default\Myclip.cmf * and all the media files should reside in the *Myclip.cmf* folder.

  The GV AMA plug-in supports linking to files in two ways:

- Manually link to files using **FILE | AMA LINK**.

- Manually link to volumes (folders) **FILE | LINK TO AMA VOLUMES**.

1. To manually link to files, do the following:
   a) Open and select the bin in which you want the master clip or sequence to appear.
   b) Select **File | Input | Link to Media**, navigate to the filepath, and select the file or files for linking.



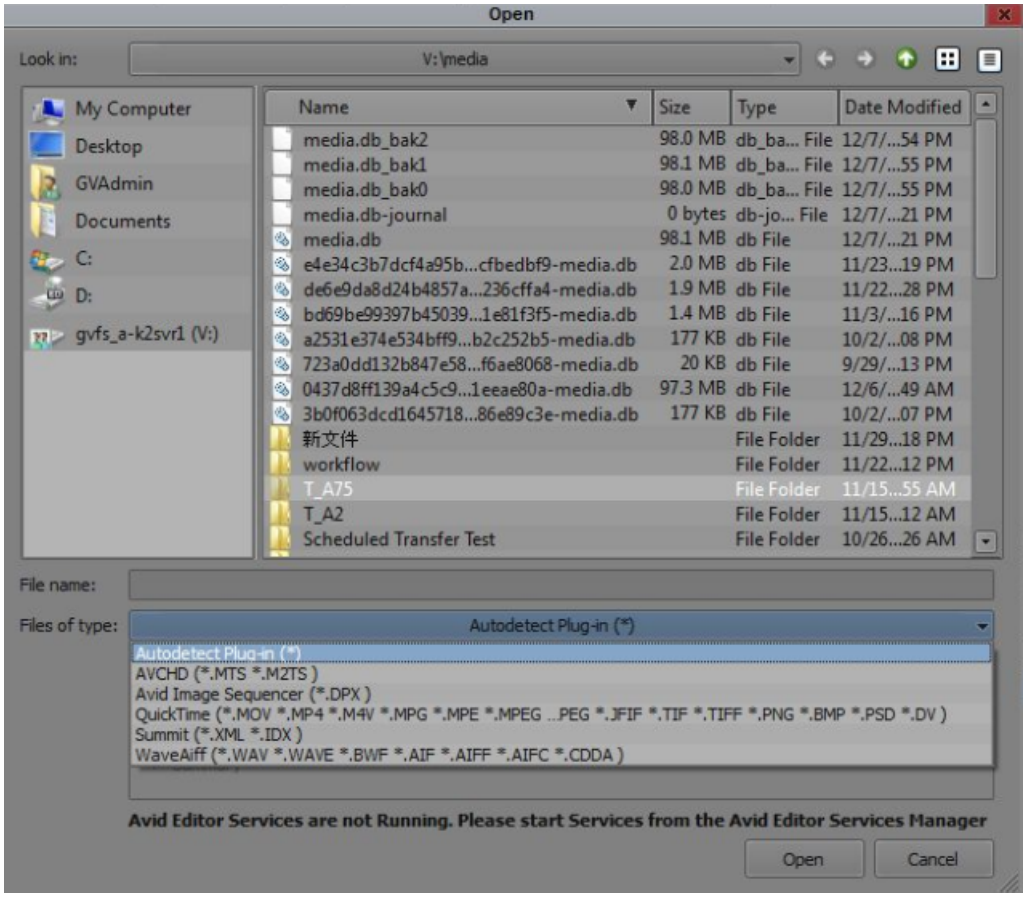
   c) Choose the file type for linking:

      - **Summit (*.XML, *.IDX)**: Creates a master clip or sequence which references all the media files and metadata as described by the XML.

   d) Click **Open**.

      The linked files appear as master clips or sequences.

2. To manually link to volumes (folders), do the following:
   a) Select **File | Input | Link to Media** and file type as below:



   - **Autodetect Plug-in (*)** for volume linking.

   b) Click **Open**.
   c) Navigate to the required folder, such as `V:\media\default`.

      A new bin is created and populated with all the assets found in the folder. The linked asset appears as master clips or sequences.

   d) To limit the number of assets in each folder, use **Link to files** and select only the files needed.

      When you link to volumes, only the content within a folder can be linked. All the assets within the selected folder are enumerated and linked. Master clips or sequences are created using all the media files and metadata as described by each of the assets XML found in the folder.

When you use AMA linked files and you are done editing the sequence, you must consolidate or transcode the sequence before this can be sent to the playout device using Avid Interplay transfer engine. Consolidate or transcode of the sequence will also share the media / sequence amongst a pool of Avid Media Composer or News Cutters sharing the same Avid storage device as the process of consolidating / transcoding checks the media into Avid Interplay.

Operational considerations

- Transfers of Mixed formats video and audio are not supported by the DHM.

- Frame chase editing (Media under construction) are reported as *In-progress* clips by the AMA plug-in. They appear in the bin with a special AMA FrameChase icon. *In-progress* clips can be refreshed using the *Refresh in-progress AMA clips* command on the Bin menu.

Using GV Connect with Final Cut Pro

Getting started

About GV Connect

GV Connect is a Grass Valley plug-in for Final Cut Pro. With the plug-in you can quickly and easily locate QuickTime files on a K2 SAN System. Then you can add the files to the current Final Cut Pro project to allow editing of the files directly over the network or after transfer locally. The capability to add files without file transfer is called Edit in Place. The plug-in also includes Final Cut Pro support for sequences, growing file support, and export/render/flattening of Final Cut Pro finished sequences on a K2 system for sharing or playout.

With GV Connect you can do the following:

Import

- Browse K2 SAN file structure to find, preview and add or transfer clips to bin
- Browse K2 file structure to find, preview and add or transfer clips to bin
- Browse K2 file structure to find and add Sequences to bin
- Browse local or network path for QuickTime files to preview and add or transfer to bin as well as adding sequences to bin.

Export

- Export one or multiple clips or sequence to a K2 SAN system
- Two presets available: Export and Quick Export

Send to Playout

- Interface with GV STRATUS Rundown placeholders.
- Create a sequence from a placeholder. GV Connect locks the placeholder on the GV STRATUS Rundown system.
- Export a finished sequence to K2 storage to be tied to a placeholder on the GV STRATUS Rundown rundown.

The GV Connect Final Cut Pro plug-in is installed in the Final Cut Pro plug-in folder and is available on the Final Cut Pro Tools menu.

Launching GV Connect

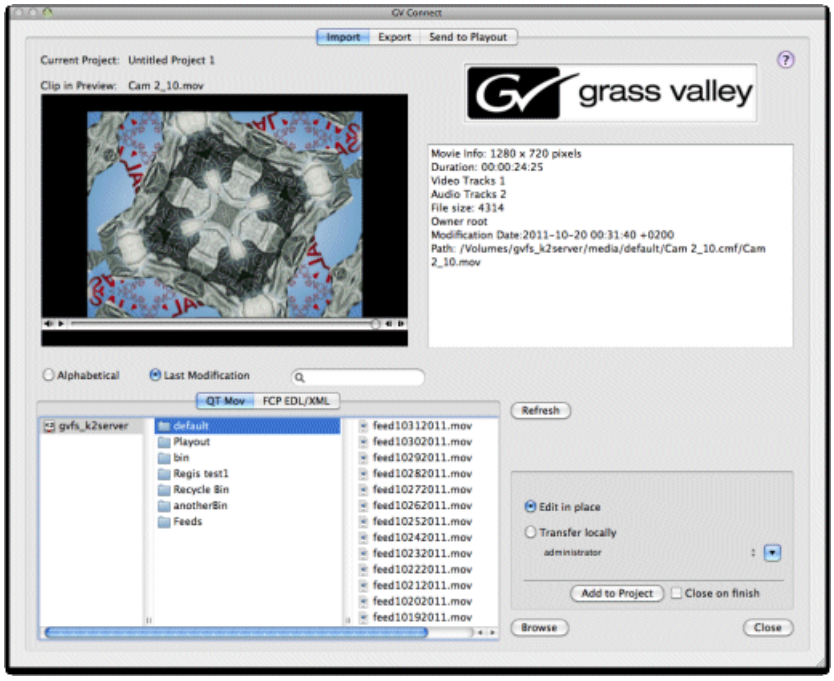
- K2 FCP Connect must be licensed
- A K2 storage volume must be mounted
- The project window (Browser) in Final Cut Pro must be active and contain a project or bin

1. In Final Cut Pro select the project or bin.

   The project must be selected to enable the GV Connect selection on the Tools menu.

2. Click **Tools | GV Connect**.

   The GV Connect window opens with the Import tab selected by default.



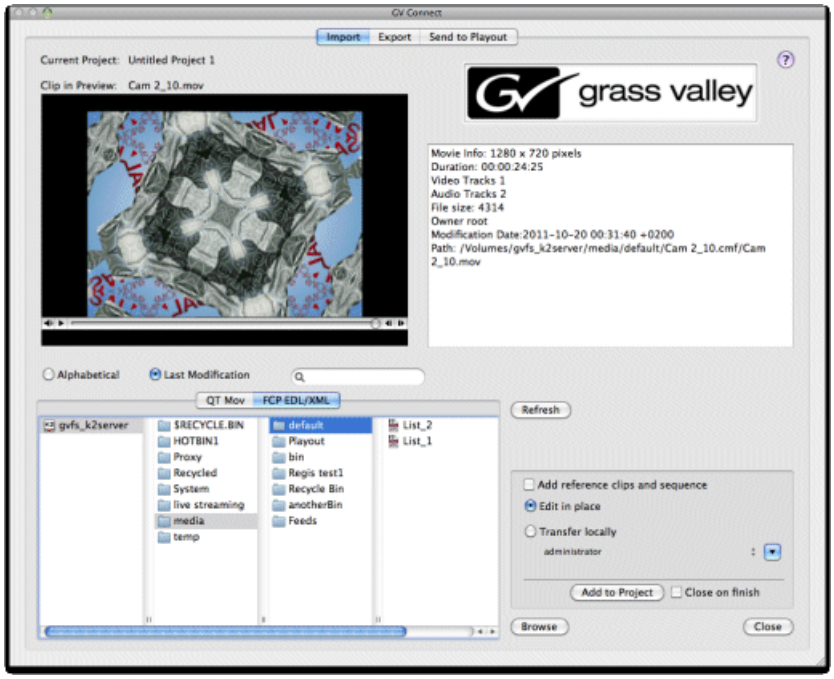
3. Switch between tabs to accomplish your tasks, as follows:

   - **Import tab**: Access media, K2 8.0 sequences, and/or Final Cut Pro XML projects and sequences.
   - **Export tab**: Export edited content to K2 storage.
   - **Send to Playout**: Access GV STRATUS Rundown placeholders/rundowns, create associated sequences, and export sequences to K2 storage.

Importing K2 media

Locating media

1. Select the **Import** tab.



   The Import tab provides a browser to locate media.

2. Select the browser tab for the type of media you are locating.

   - QT Mov – Select this tab to find QuickTime files.
   - FCP EDL/XML – Select this tab to find sequences, Final Cut Pro projects, or K2 exported XML.

3. If desired, sort or filter media as follows:

   - Alphabetical – Sort view alphabetically A to Z.
   - Last Modification – Sort by last modified date on top.
   - Search – Filter the view by typing a keyword. This is especially useful when your folder contains thousands of clips.

4. Click **Refresh** to view recently added media in the browser.

   If you add media while GV Connect is open, you must refresh in order to locate the media.

5. Double-click media to preview.

   The clip loads in the preview window and displays clip metadata.

After you have located the media to edit, add it to your Final Cut Pro project using the **Add to Project** button.

Adding media to your Final Cut Pro project

1. Locate and select the media to add to your project.
2. Select the method for adding the media to your project.
   - Add reference clips and sequence — Select to add the associated assets to the Final Cut Pro project.
   - Edit in place – Use this method to add a clip to the bin without moving the media. With this method you are playing and editing the clip over the network. This is the preferred method on a shared storage system such as a K2 SAN.
   - Transfer Locally – Use this method to transfer the media corresponding to the clip to your desired location. This is the preferred method if your editor is connected via SMB to a stand-alone K2 client. Depending on clip size, the transfer can take a significant amount of time. Wait until the cursor no longer indicates that the operation is in progress before proceeding.

     NOTE: Do not add media to a project if the transfer is still underway.
3. Click **Add to Project**.

   The media is added to your Final Cut Pro project.
4. To return to Final Cut Pro, close the GV Connect plug-in.

Edit the media as desired in Final Cut Pro. When you are finished you can export the media back to K2 storage.

Updating growing files

1. In the Final Cut Pro menu bar (in the upper right in the Mac OSX toolbar), identify the GV icon.

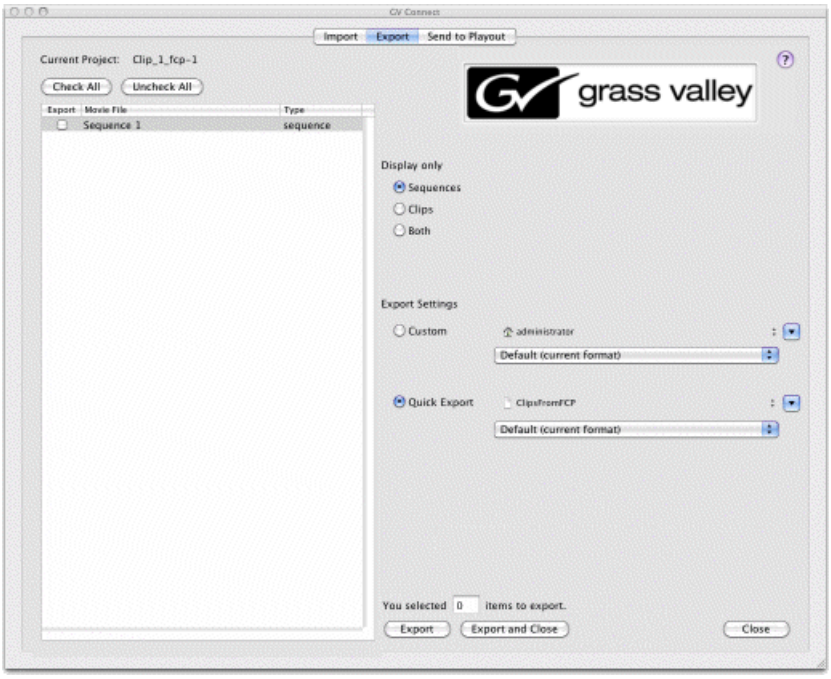
   When this icon displays a green color, it means that a clip that is in your Final Cut Pro project is currently growing in the K2 system and is ready for updating in your project.
2. When the GV icon displays a green color , click the icon and select an individual file or **Refresh All**.

   The file or files are updated in your Final Cut Pro project.

Exporting K2 media

Exporting to K2 storage

1. Select the **Export** tab.



2. Under "Display only", select whether to display Sequences, Clips, or Both.
3. In the list of media, select the media to export to K2 storage.

   You can make one selection or multiple selections.
4. Under Export Settings, select **Custom**.
5. In the drop-down list select the format in which the media is exported.
6. Click the down-arrow.

   The "Choose a Directory for Export" dialog box opens.
7. Browse to the location in K2 Storage to which the media is exported.

   Export to K2 HotBin recommended. The HotBin does the processing required so that you can play the media on the K2 system.
8. Click **Export**.

   A message box displays progress for each clip or sequence exported.

Using Quick Export

You can save and reuse export settings with the Quick Export feature. Once you have configured your Quick Export settings you can use the GV Quick Export menu entry. This bypasses the GV Connect plug-in main interface and automatically exports the selected items in the Final Cut Pro

bin to your predetermined location on K2 storage. This feature can be very useful if you export all your finished material to a K2 HotBin.

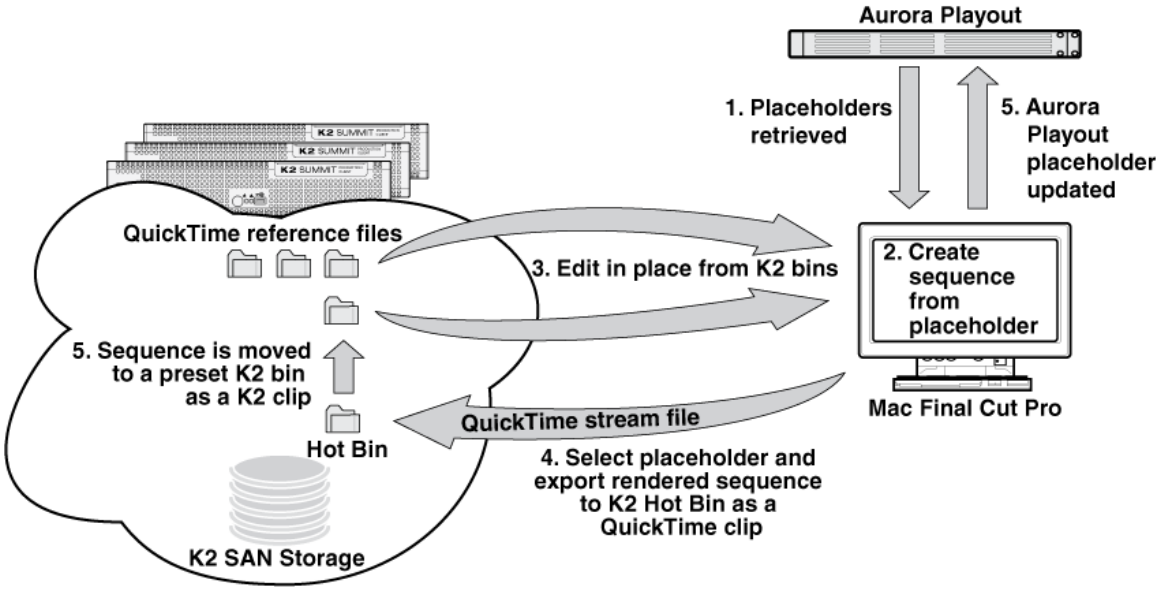
1. Configure your Quick Export settings as follows:
   a) Select the **Export** tab.
   b) Click **Quick Export**.
   c) Make export settings.
2. After your Quick Export settings are configured, you can repeatedly reuse the settings as follows:
   a) On the Final Cut Pro menu click **Tools | GV Quick Export**.

   GV Connect automatically exports the clip to K2 storage, as specified by the currently configured Quick Export settings.

Sending media to playout

About the GV STRATUS Rundown workflow

The workflow on a K2 SAN with GV STRATUS Rundown is illustrated as follows:



Before you can use GV Connect to access placeholders/rundowns and create/edit/export associated sequences, GV Connect must be configured for your site's specific systems and workflow, as follows:

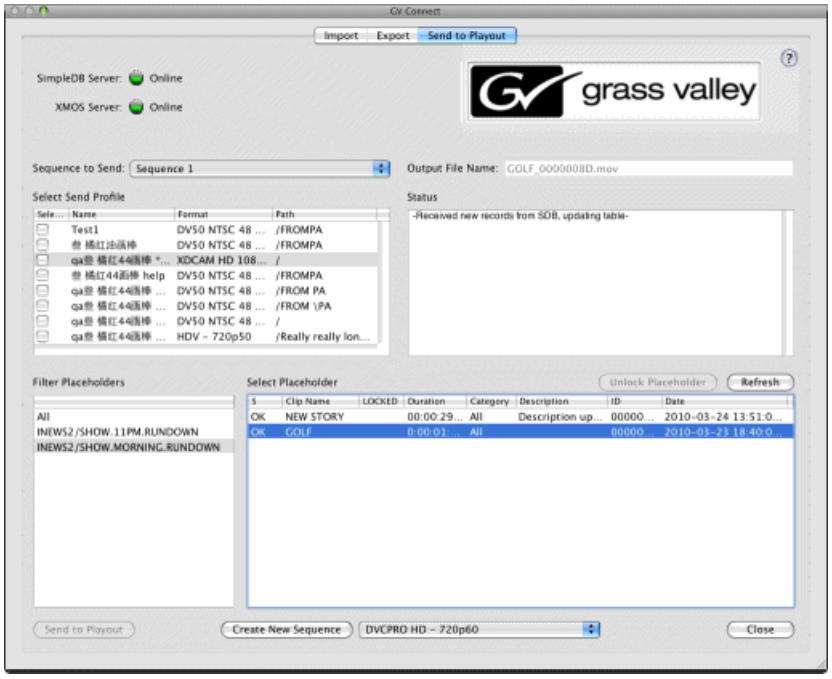
- The network address of the server and other system settings
- The formats in which sequences are exported
- The location(s) to which sequences are exported

This is configured in K2 FCP GV Connect Preferences by your system administrator. Refer to the *K2 FCP Connect Installation Manual* for more information.

Accessing placeholders/rundowns

If you are using the GV STRATUS Rundown workflow, start by choosing the placeholder or rundown on which you are working.

1. Select the **Send to Playout** tab.



   In the **Select Placeholder** list, GV Connect automatically displays all placeholders present on the GV STRATUS Rundown system.

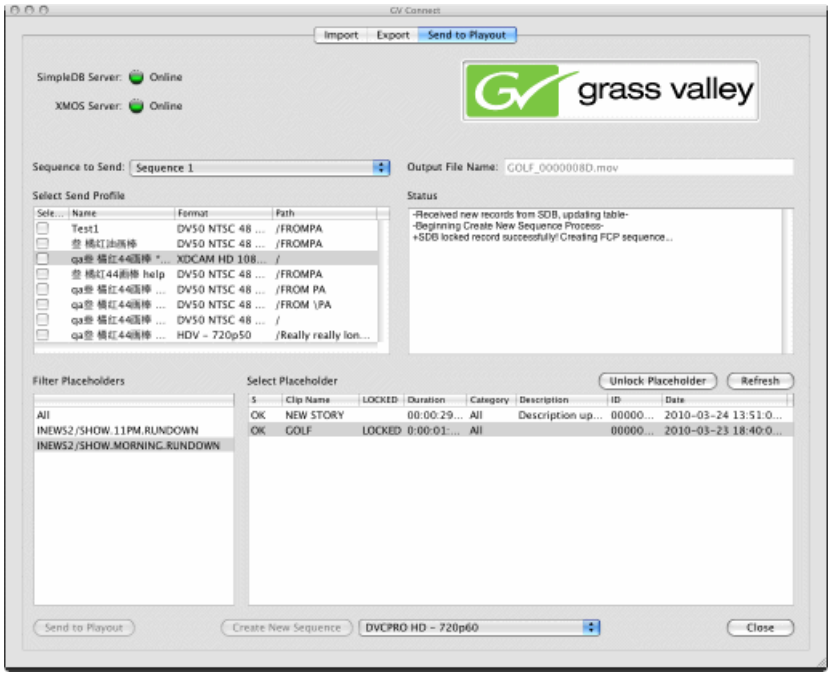
   If configured for an NRCS system, under **Filter Placeholders** GV Connect also displays rundowns.

2. To access recently added placeholder or rundowns, click **Refresh**.
3. If configured for an NRCS system, under **Filter Placeholders** do one of the following:
   - Select a rundown to display the rundown's list of placeholders.
   - Select **All** to display all placeholders.
4. Select the desired placeholder from the **Select Placeholder** list.
5. If desired, click **Unlock Placeholder** to manage the lock status of the placeholder.

Creating a sequence

If you are using the GV STRATUS Rundown workflow, you can create a sequence from a placeholder.

1. Select the **Send to Playout** tab.



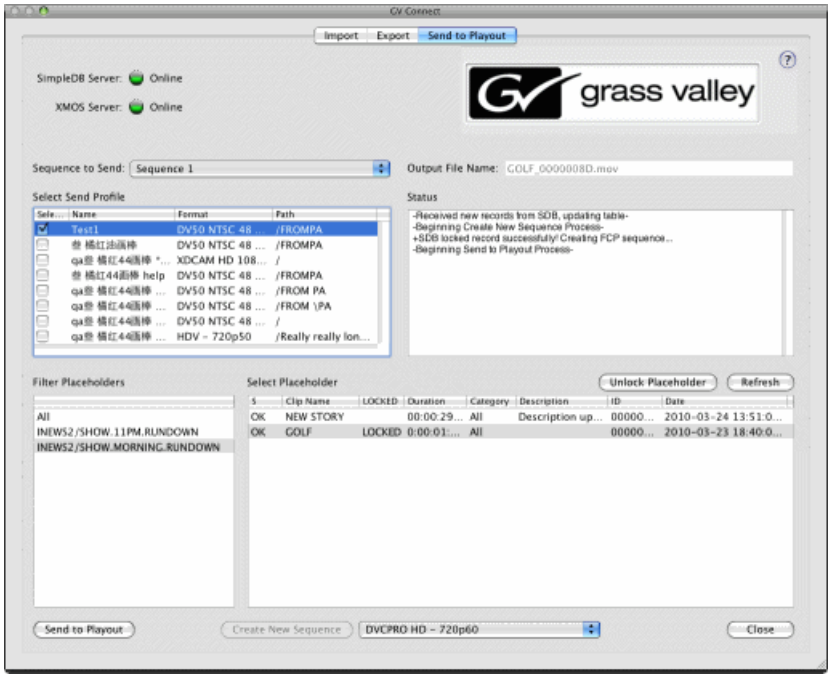
2. Access and select the placeholder from which you are creating a sequence.
3. Select the format in which the sequence is created in the Final Cut Pro project.
4. Click **Create New Sequence**.

   GV Connect attempts to the placeholder in the GV STRATUS Rundown system. If the lock is successful, GV Connect creates the sequence, names it according to the placeholder name, and adds it to the Final Cut Pro project.
5. Edit the sequence in Final Cut Pro.

Exporting a sequence and linking to GV STRATUS Rundown

Using the GV STRATUS Rundown workflow, when you export a sequence to K2 storage, GV Connect automatically links the sequence to an GV STRATUS Rundown placeholder.

1. Select the **Send to Playout** tab.



2. In the **Sequence to Send** drop-down list, select the sequence you are exporting to K2 storage.

   The sequence can be either a sequence GV Connect created from a placeholder or a sequence that you manually created in Final Cut Pro.

3. Access and select the placeholder associated with the sequence you are exporting.
4. In the **Select Send Profile** list, select the location that is configured to receive the GV STRATUS Rundown workflow sequences.

   NOTE: You must export to a HotBin that is configured to place the media in the bin that* GV STRATUS Rundown *is monitoring.

5. Click **Send to Playout**.

   GV Connect exports the sequence to K2 storage.

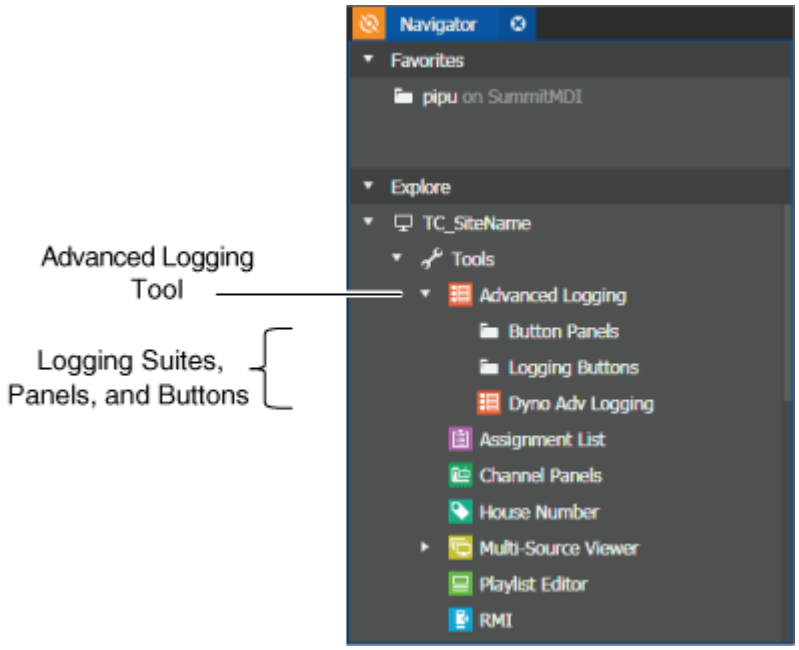
6. If desired, click **Unlock Placeholder** to manage the lock status of the placeholder.

Logging assets

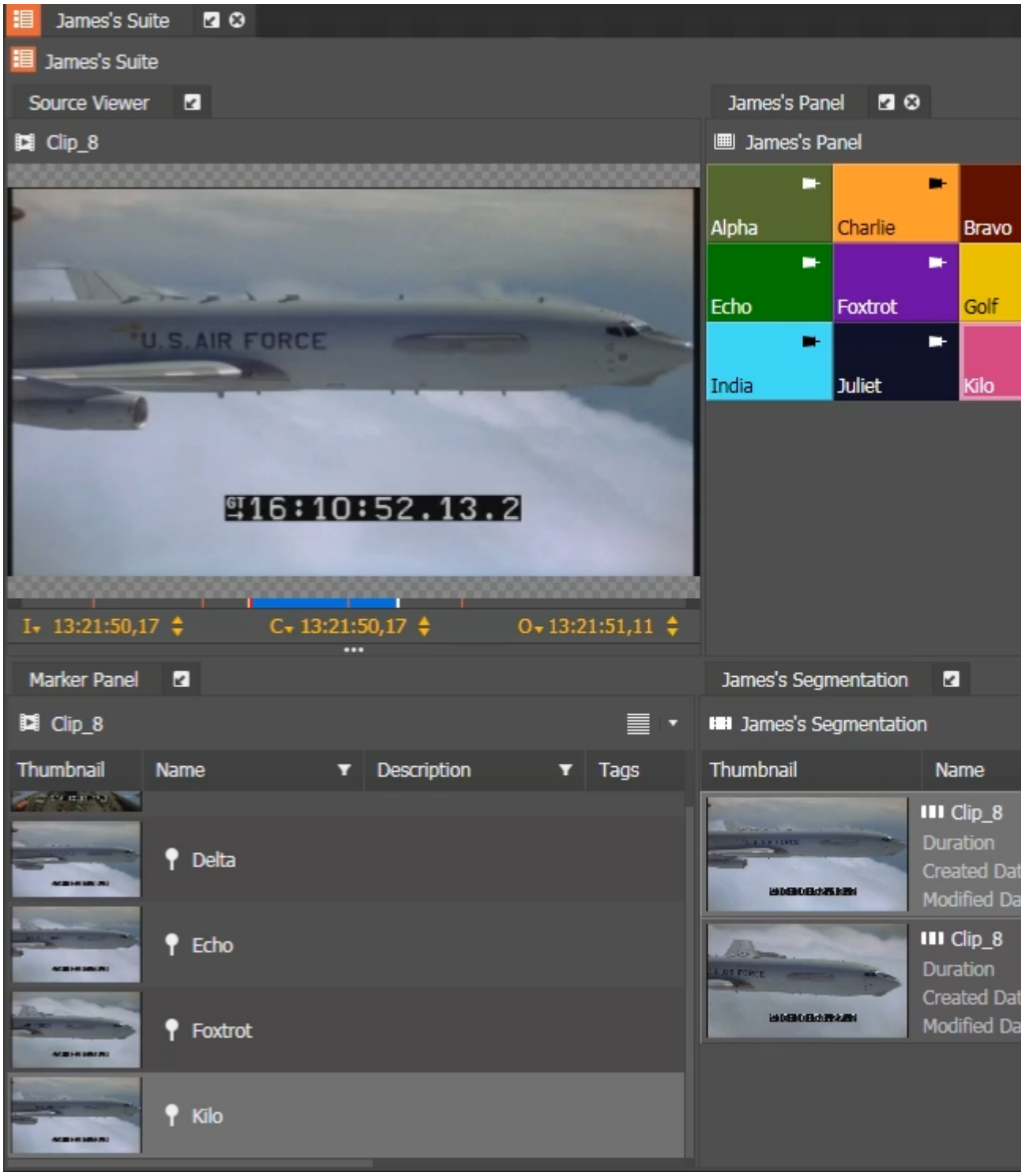
The Advanced Logging tool

The Advanced Logging tool provides users with a tool to quickly and efficiently apply metadata and marker values to assets in GV STRATUS application, via a set of pre-defined Logging buttons and Panels. It is an ideal tool for sports logging or any environment where large amounts of descriptive metadata need to be quickly applied to an asset. The markers created by the logging process greatly improve the ability to easily find and retrieve assets at a later date through a GV STRATUS Simple or Advanced Search.

The Advanced Logging tool allows you to create and assign various Logging Suites for asset logging. The Advanced Logging tool may include several Logging Suites for different logging purposes.



The Logging Suite displays as a composite panel in the GV STRATUS application. The Logging Suite includes the Source Viewer, one or more Button Panels (each of which contains buttons which create markers during the logging operation), and the Marker Panel. If assigned with the Segmentation role, you can add Segmentation Panels to the Logging Suite.



Logging Suite features are as follows:

- Source Viewer — Loads assets to be previewed.
- Button Panel — Loads a customizable set of buttons for logging.
- Marker Panel — Displays all keywords and markers that have been created.

- Segmentation Panel — Displays the list of segments created for the asset.
- **Add Button Panel**: Adds a new or existing Button Panel to the Logging Suite.
- **New Segmentation**: Creates a new segmentation panel.

If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets, and metadata that do not have read permissions are not visible. Markers and segments permissions must be set to **Allow** in order to create, update, or delete markers and segments.

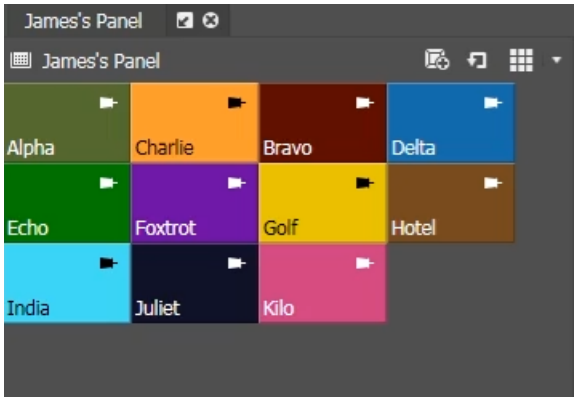
Related Topics

The Source Viewer on page 1138
Viewer buttons on page 1139
Using the Audio Overlay on page 1002
J, K, L keyboard shortcuts for transport control on page 1143

The Button Panel

The Button Panel allows you to create and load buttons for logging. In the GV STRATUS application, you can access the Button Panel when you launch the Logging Suite from the Navigator.

Each Logging suite may contain one or more Button Panels, this allows multiple panels to be created to manage buttons / marker values for different categories of metadata. For example, in sports logging, one panel may contain the names of players, another containing ‘actions’ that occur; additional panels may cater for ‘venues’, ‘tournament information’ etc.



Button Panel features are as follows:

- Toolbar — Consists of controls to manage logging buttons for the Button Panel.
- Button list — Displays all logging buttons that have been created.

Button Panel buttons

These buttons located on the Button Panel let you perform various functions.

Add Button: Adds a new or existing button to the Button Panel.

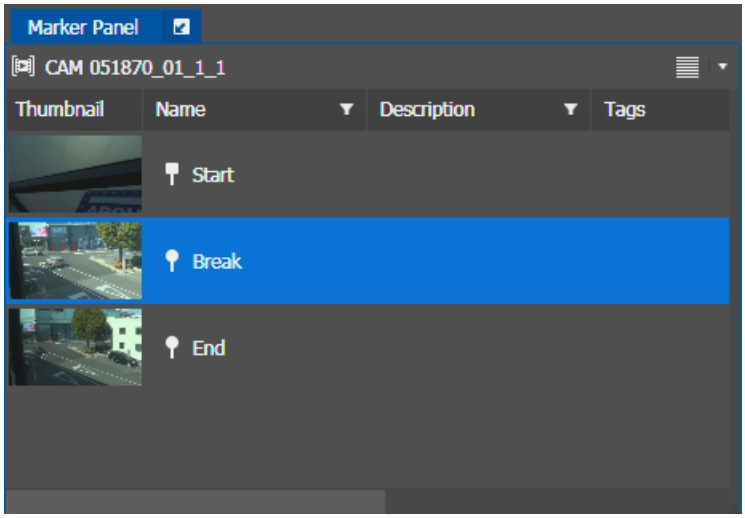
Reset Button State: Resets the pressed button state to unpressed position.

View Mode: Controls the display and size of the items in a list or panel.

Button size can be selected between 3 pre-defined sizes (in a grid layout) from the **View Mode** control, or if **Manual** is selected the button size and placing can be customized by the user.

The Marker Panel

The Marker Panel allows you to view keywords and markers that have been assigned to clips. In the GV STRATUS application, you can access the Marker Panel when you launch the Logging Suite from the Navigator.



The Marker Panel feature is as follows:

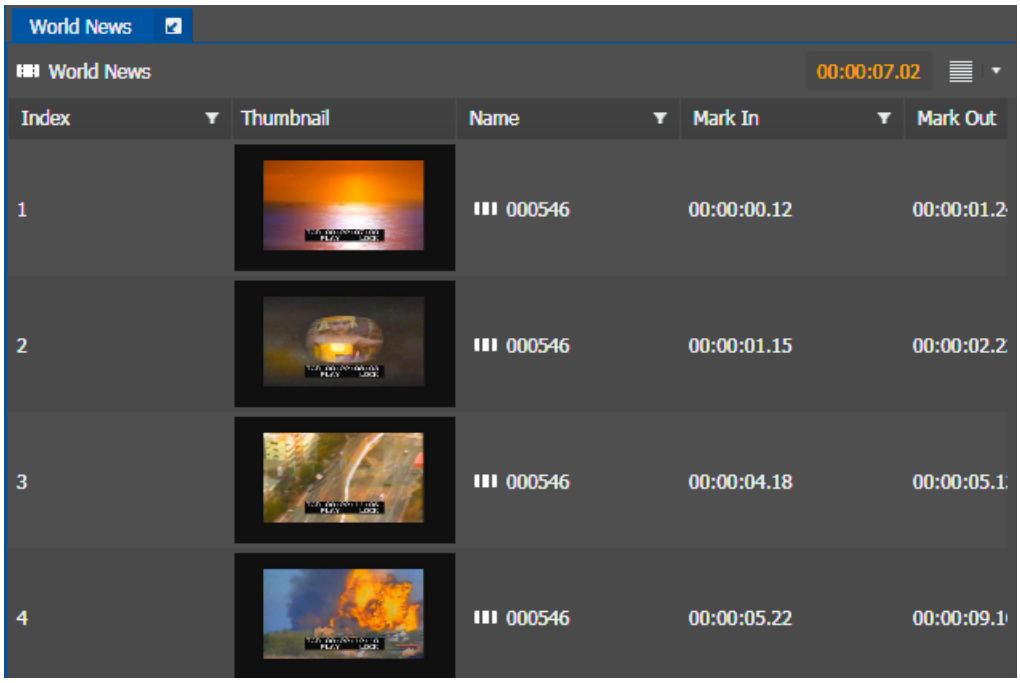
- Panel List — Displays all keywords and markers that have been created for the asset loaded into the Source Viewer within the Advanced Logging tool.

NOTE: A marker can contain multiple values if several buttons were pressed for a single logging event within the* Advanced Logging *tool.

Standard Asset List features such as filter list, sort list, and customization of the **View Mode** are available in the Marker Panel.

The Segmentation Panel

The Segmentation Panel allows you to create segments and view the list of segments created for the asset. If assigned with the segmentation role, you can set the Segmentation Panel to be displayed within the Logging Suite when you launch it from the Inspector.



The Segmentation Panel feature is as follows:

- Panel List — Displays all segments that have been created for the asset loaded in the Advanced Logging tool.
- Duration — Displays the duration timecode which sums up the duration of all the segments within the segmentation panel.

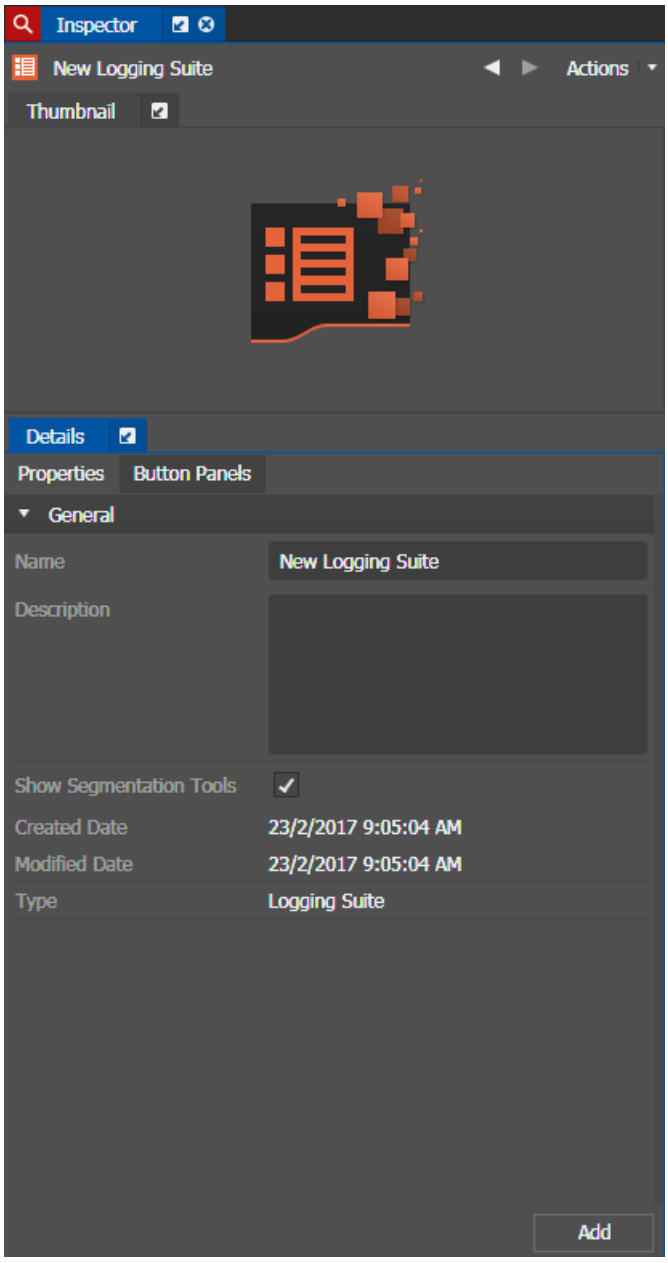
Standard Asset List features such as filter list, sort list, and customization of the **View Mode** are available in the Segmentation Panel.

Adding a Logging Suite

You can create and add Logging Suites to accommodate different kinds of logging in your operation.

1. Right-click on **Advanced Logging** from the **Tools** node in the Navigator and select **New | Logging Suite**.

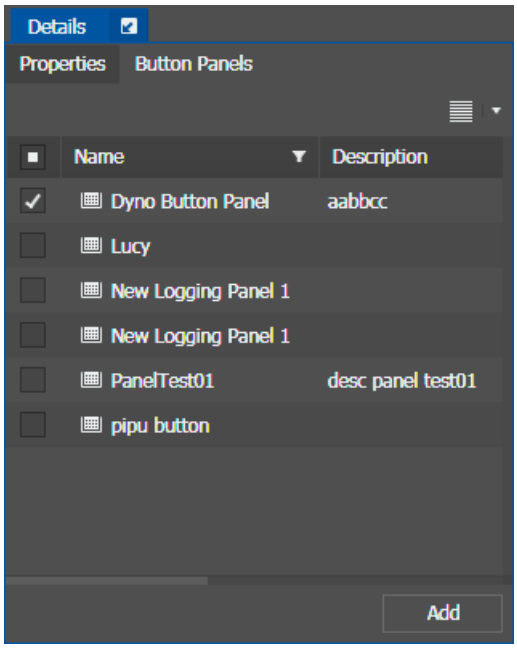
   The Inspector loads the configuration for a new Logging Suite.



2. Enter the **Name** and **Description** of the Logging Suite on the **Properties** tab.

   If assigned with the Segmentation role, the **Show Segmentation Tools** checkbox is selected by default. Deselect the checkbox if you do not want a Segmentation Panel in your Logging Suite.

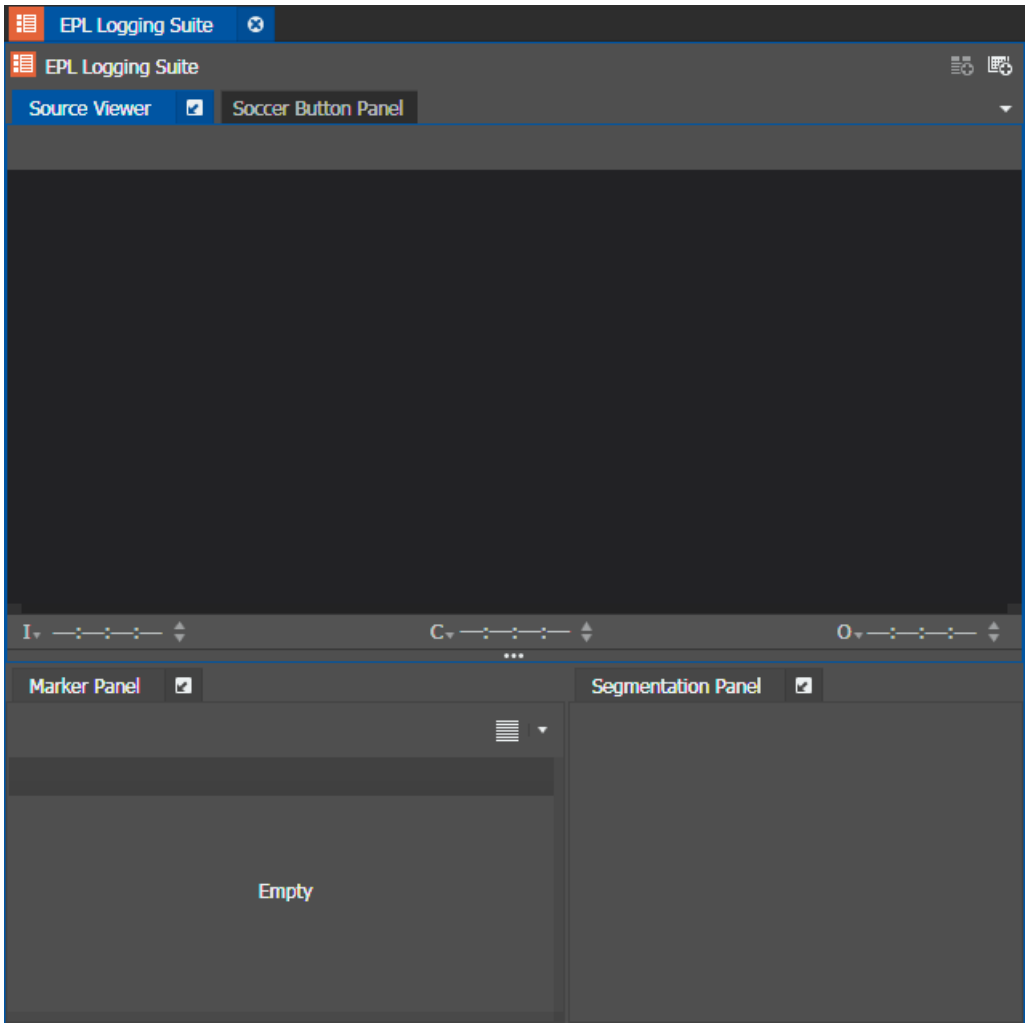
3. On the **Button Panels** tab, select Button Panel(s) for the Logging Suite.



You can customize a new Button Panel later if you don't want to use existing Button Panels.

4. Click **Add** in the Inspector panel if you want to open the new Logging Suite that you just created.

   The Source Viewer, Marker Panel, Segmentation Panel, and selected Button Panels appear in the Logging Suite. An untitled Button Panel appears if no Button Panel is selected earlier.



   The Logging Suite also appears under **Advanced Logging** tool in the Navigator.

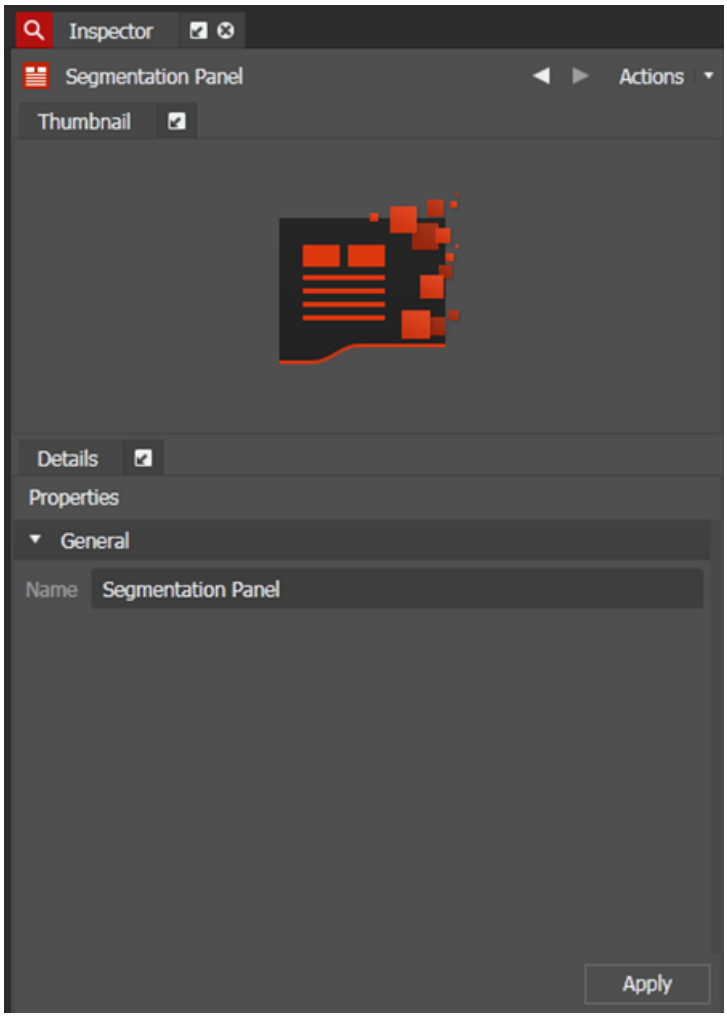
   You can drag the **Logging Suite** icon from the Logging Suite into the Inspector or you can double-click the Logging Suite name in the Navigator if you want to change properties of the Logging Suite later.

Adding a Segmentation panel

You can create and add segmentation panels to accommodate different kinds of asset segmentation in your operation.

1. Click the **New Segmentation** button on the toolbar.

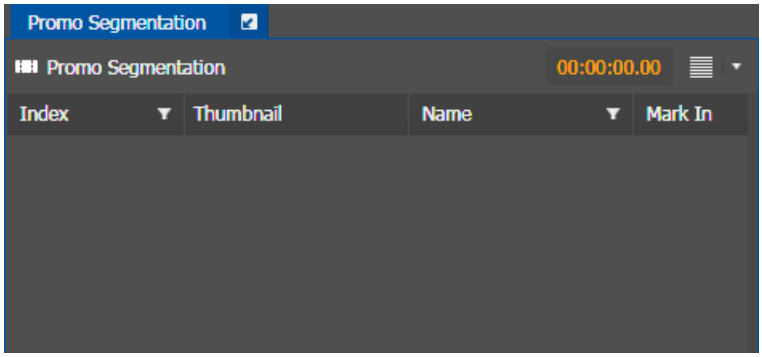
   The Inspector loads the configuration for a new segmentation panel.



2. Enter the **Name** of the segmentation panel.

3. Click **Apply** to save the segmentation panel.

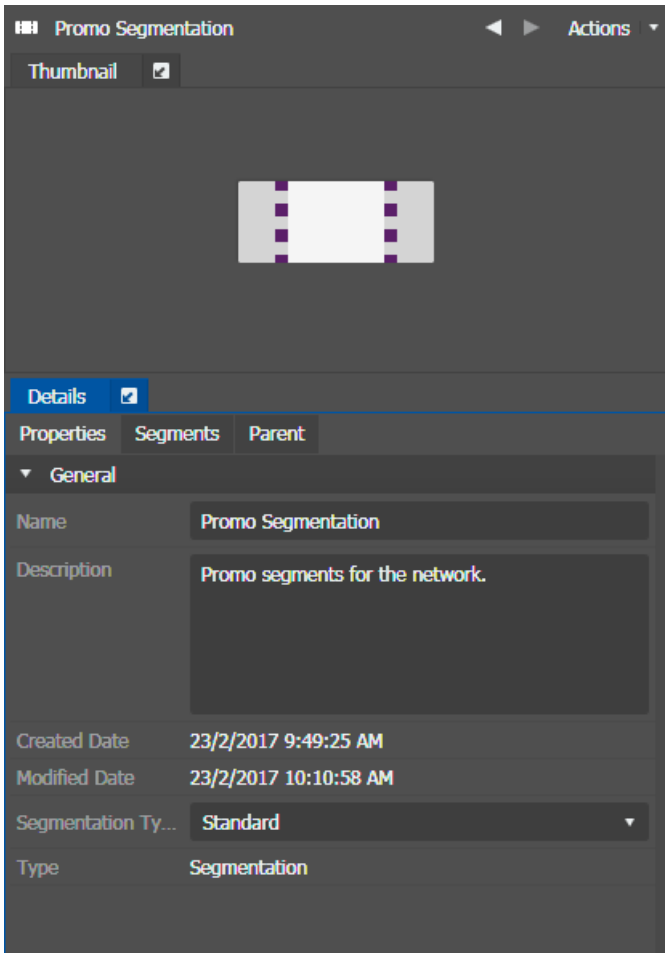
   The new segmentation panel name displays in the Segmentation panel.



4. Repeat above steps to create more segmentation panels if desired.

   You can create multiple Segmentation panels to assign different segments of an asset for different broadcast times.

   You can also drag the **Drag Source** icon on the segmentation panel into the Inspector if you want to modify the segmentation panel later.



Related Topics

Assigning segments to assets on page 1294

Assigning segments to assets

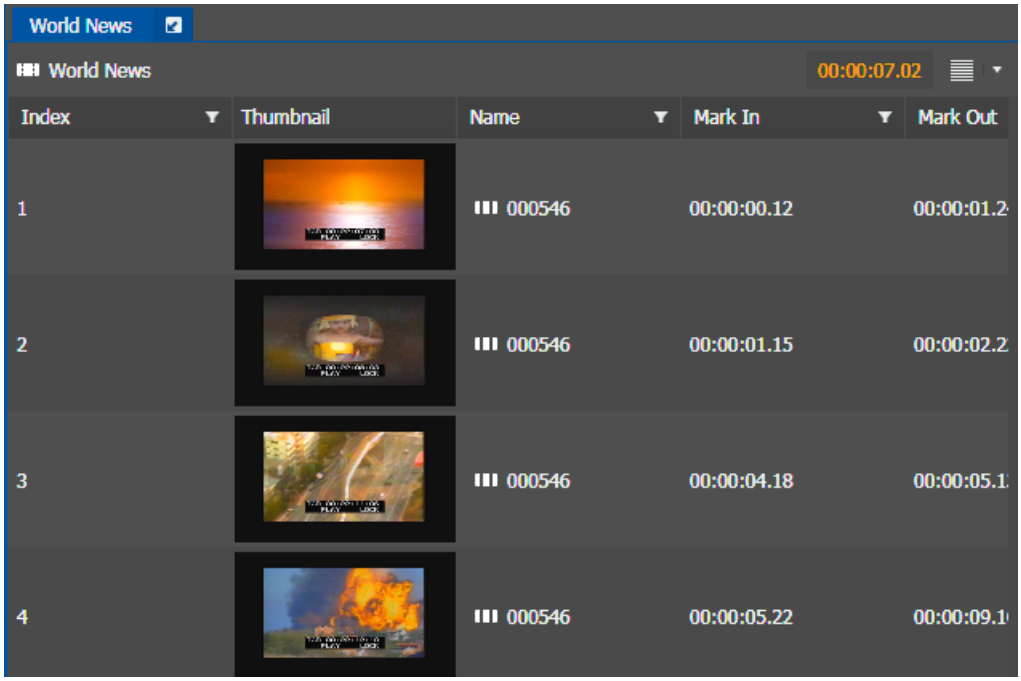
- If GV STRATUS security is enforced, your credentials must give you full read and write permissions on bins, assets, and segments. You can only view segments with read permission, and modify segments with write permission.
- Create Segment and Update Segment permissions must be set to **Allow**, for you to create and update segments.

You can assign segments to an asset in the Segmentation panel. Segments are created in the Source Viewer panel by marking in and out specific part of the asset.

1. Drag the selected asset from Asset List into the Source Viewer in the Segmentation panel.

2. If the logging controls are not shown, click the **Show/Hide Control Tray** button ... to show the controls, then the drop-down arrow at the right of the control tray and **Add/Remove** buttons if necessary.
3. Navigate to the starting point and click the **Mark In** button. (**I**)
4. Determine the end-point of your segment and click the **Mark Out** button. (**O**)
5. Click on the asset in the Source Viewer, then drag and drop the segment into the Segmentation panel. (**Alt + Ctrl + Insert**)

   The segment adds into the Segmentation panel.



6. Repeat above steps to add more segments of the asset into the Segmentation panel.

   The index number increases whenever a segment is added or duplicated.

   NOTE: Without Create Segment and Update Segment permissions, segments cannot be rearranged or dragged and dropped in the same Segmentation panel, or from one panel to another.

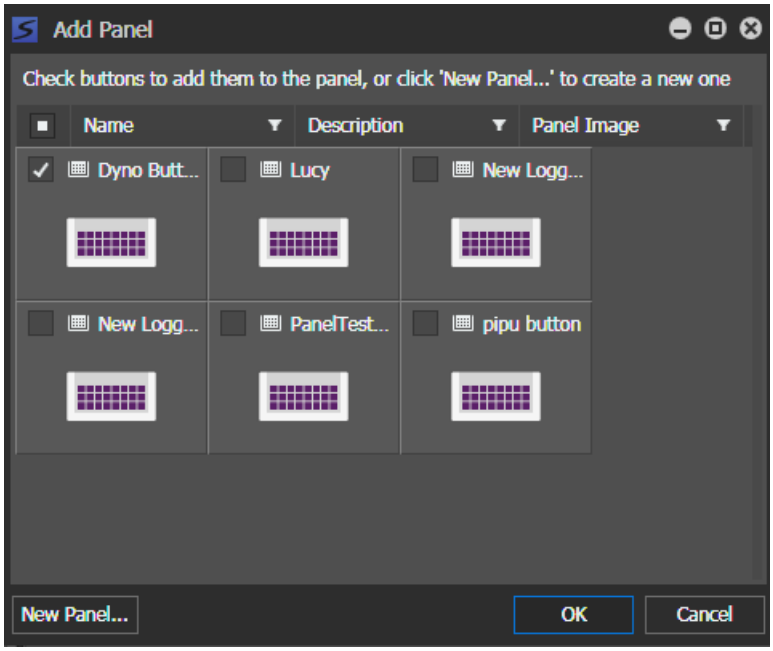
You can also create various segment lengths of an asset in multiple segmentation panels for different broadcast times. For example, a program that is scheduled for prime time has more commercial slots compared to the repeat of the same program at a later time. Therefore, several kinds of segments in multiple segmentation panels can be created for the same asset.

Adding Button Panels

You can create and add several Button Panels to customize your Logging Tool.

1. Within the Logging Suite panel, click the **Add Button Panel** button.

   The Add Panel dialog opens.

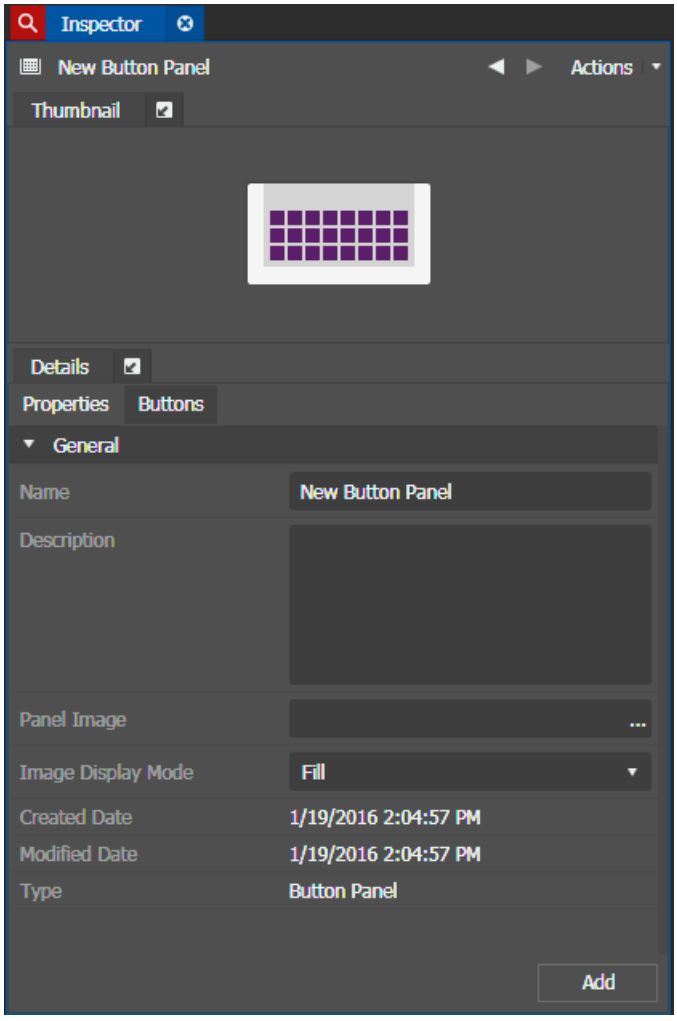


2. To choose from existing Button Panels, select the checkbox of the Button Panel to add it to the Logging Suite.

   Then, click **OK**.

3. To create a new Button Panel, click **New Panel**.

   The Inspector loads the configuration page for a new Button Panel.



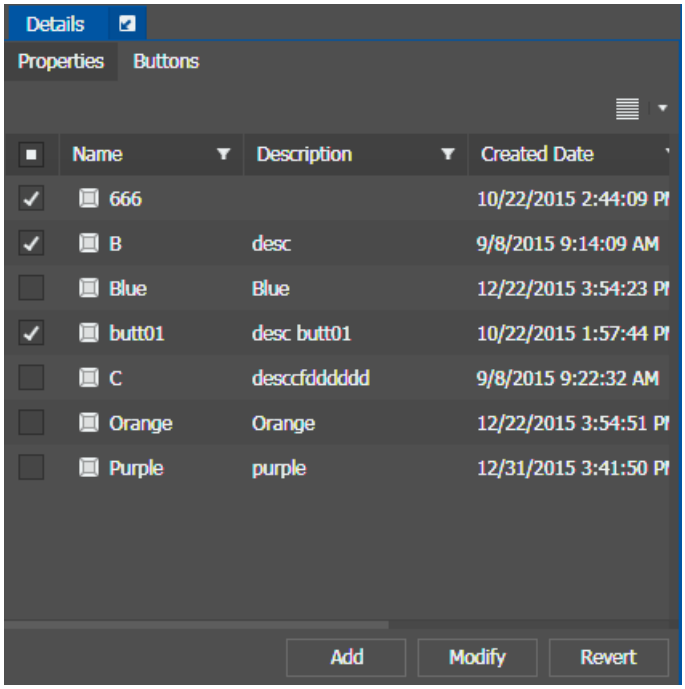
4. Enter the **Name** and **Description** of the new Button Panel.

   You can also browse and select an image to be the **Panel Image** of the Button Panel.

   The **Image Display Mode** can be selected as follows:

   - **Fill**: The image fills the entire Button Panel.
   - **Maintain Aspect Ratio**: The image maintains its aspect ratio in the Button Panel.
   - **Original Size**: The image displays according to its original size in the Button Panel.
   - **Manual**: The image size can be resized manually in the Button Panel.

5. Click on the **Buttons** tab, and select logging buttons for the panel by checking the box next to each customized button.



   You can also create new buttons later if you don't want to use existing logging buttons.

6. Click **Add** to add the Button Panel to the Logging Suite.

   ***NOTE: If you received a* Button Panel *via the* Send Message *tool, the* Button Panel *is saved automatically in your Advanced Logging tool. If the* Button Panel *already exists, it is automatically saved and updated according to the received* Button Panel.**

7. Repeat previous steps if you want to create multiple Button Panels.

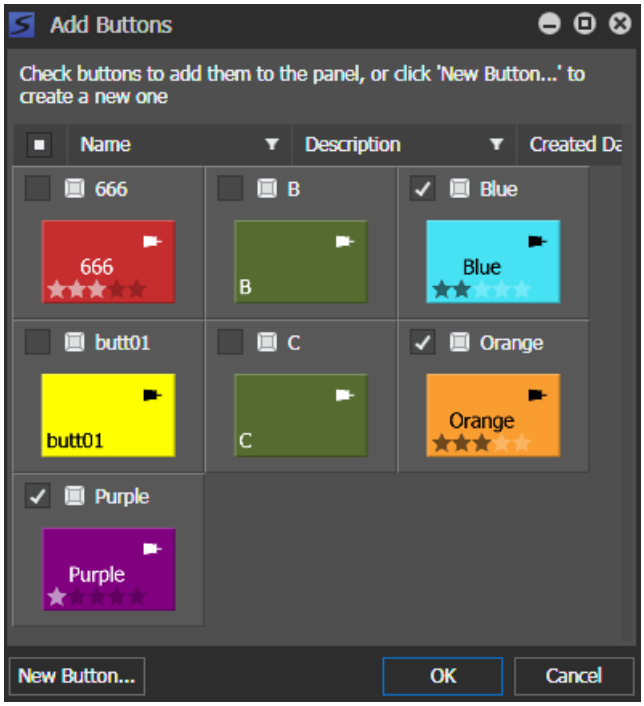
   You can also click **Revert** to undo any changes.

You can rearrange Button Panels within the Advanced Logging tool to best suit your workflow needs by dragging and dropping panels within the user interface. To customize your workspace, refer to *About customizing the application workspace* on page 970.

Creating and adding logging buttons

1. Click the **Add Button** on the Button Panel.

   The Add Buttons dialog opens.



2. To choose from existing buttons, select the checkbox of each button to add it to the Button Panel.

   Then, click **OK**.

3. To create a new logging button, click **New Button**.

   The Inspector loads the configuration page for a new button.

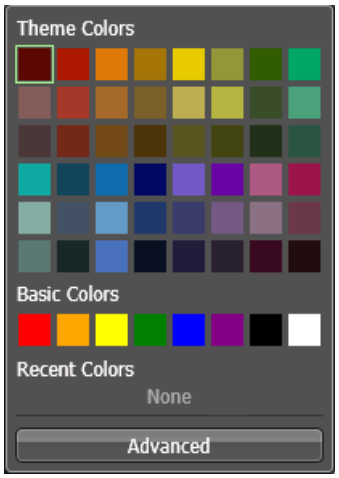
   Custom metadata for markers are also available in the Inspector if already configured in the GV STRATUS Control Panel.

4. Enter the **Name** and **Description** of the new logging button.

   The name displays in both **Name** and **Button Text** fields.

5. Enter the **Button Text** if you want to display a different name on the logging button.
6. Click the **Browse** button ··· button to browse and select the **Button Image**.
7. Select the **Rating** for the logging button.
8. Select the **Display Ratings** checkbox if you want to display the logging button rating.
9. Click the drop-down list of the **Button Color** to display the color palette, and do one of the following:

   - Select any theme or basic colors as provided.



   - Click **Advanced** to define your own custom color and RGB values.

   The color of the logging button changes according to the selected color.

10. Enter the **Tag** of the logging button if desired.

11. Enter the **Keyboard Shortcut** for the logging button by doing one of the following:

    - Press one key only.
    - Press one key and one modifier key simultaneously.

      NOTE: Tab and Alt modifier keys are not supported.

    - Press one key and two modifier keys simultaneously.

      NOTE: Pressing Alt, Shift, and one key simultaneously is not supported.

    A keyboard shortcut can be assigned to multiple logging buttons on your Button Panels.

    However, you cannot assign existing keyboard shortcuts of GV STRATUS tools for your logging button. Keyboard shortcuts of other GV STRATUS tools do not appear on the **Keyboard Shortcut** box when pressed.

12. Click **Add** to add the logging button to the Button Panel.
13. Repeat previous steps if you want to create more logging buttons.

    Logging buttons are automatically saved after they are added into the Button Panel.

NOTE: To reuse logging buttons from other* Button Panels*, you can also drag logging buttons from those* Button Panels *and drop them into your* Button Panel*.

Related Topics

All keyboard shortcuts on page 1414

Customizing of Logging Panels and Buttons using Design Mode

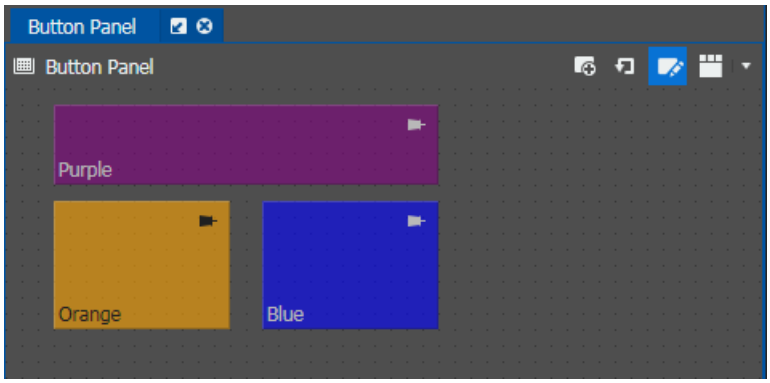
When the **Design Mode** is selected, users can customize the size and placement of buttons within a panel.

1. In the Button Panel, select **Manual** from several View Mode options within the panel toolbar.

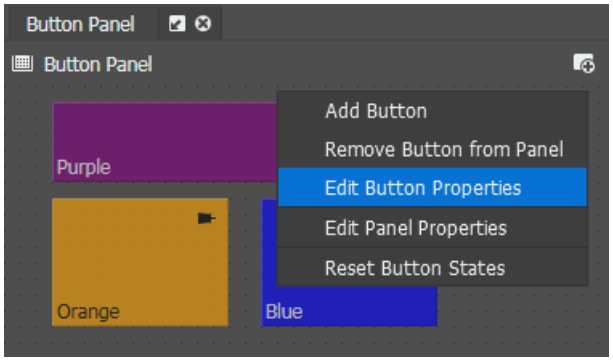
Buttons are automatically arranged in a stack, in preparation for manual placement.

2. Click the **Design Mode** button on the toolbar.

Buttons may now be freely placed within the field of the Button Panel. Buttons can also be re-sized by clicking on the button's bottom right hand corner, then scaling them using the mouse.

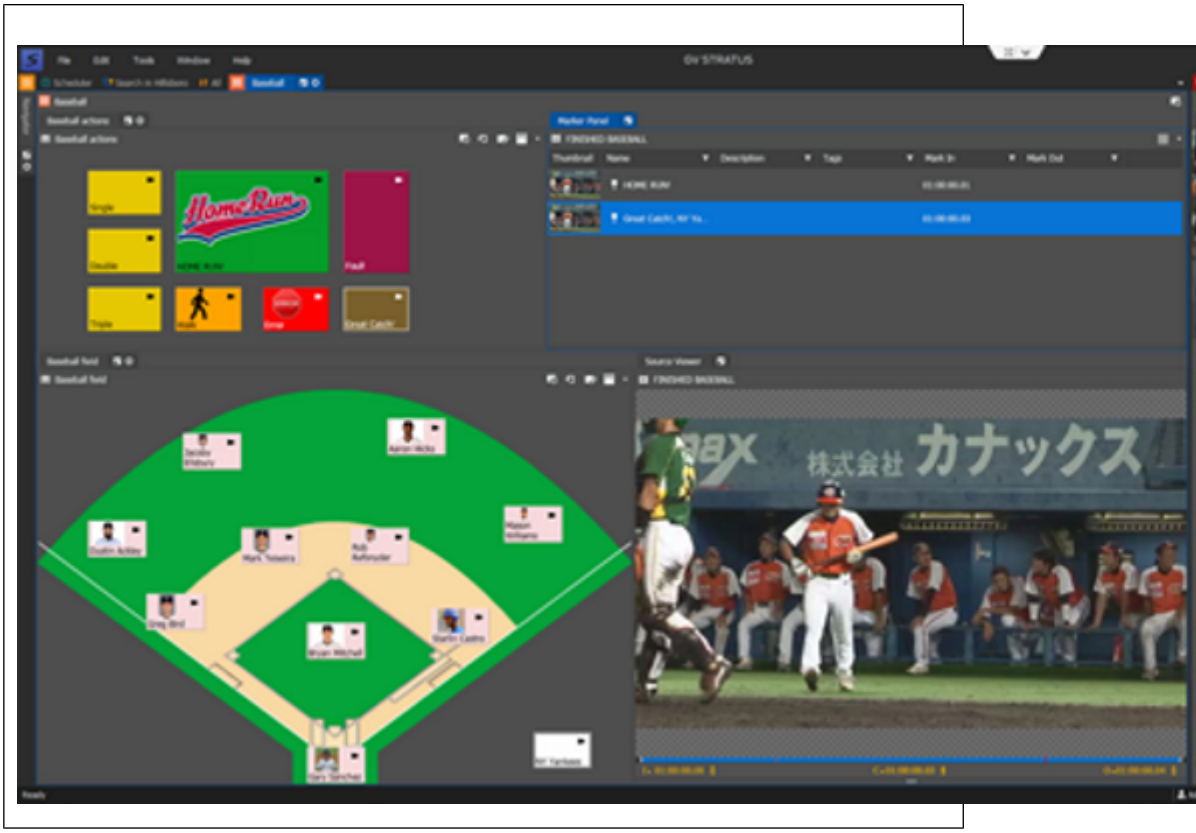


3. To change any properties of the logging button, right-click on a button and select **Edit Button Properties**.



4. Once editing is completed, click the **Design Mode** button on the toolbar to save your changes for the Button Panel.

Using this tool, it is possible to create complex graphical Button Panels and Button layouts to make the logging process simpler and more efficient for Operators.



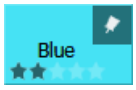
Pinning logging buttons

You can pin logging buttons to add the pinned marker to other markers during asset logging.

1. Select a logging button that you want to pin in the Button Panel.

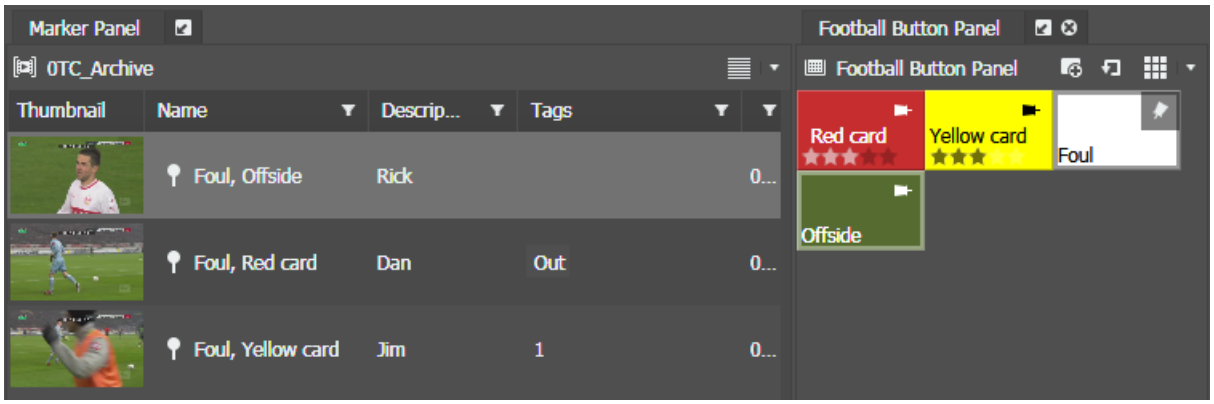
2. Click the **Pin Audio** button on the logging button.

   The pin button points downward to indicate that the logging button is pinned.



3. Start logging by selecting logging buttons on the Button Panel as you play the asset.

   Markers are displayed on the Marker Panel as logs for the asset. Each marker also has the pinned metadata added to it.



Adding markers using logging buttons

If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets, markers, keywords, and metadata that do not have read permissions are not visible. All marker permissions must be set to Allow before you can add markers to assets in the Advanced Logging tool.

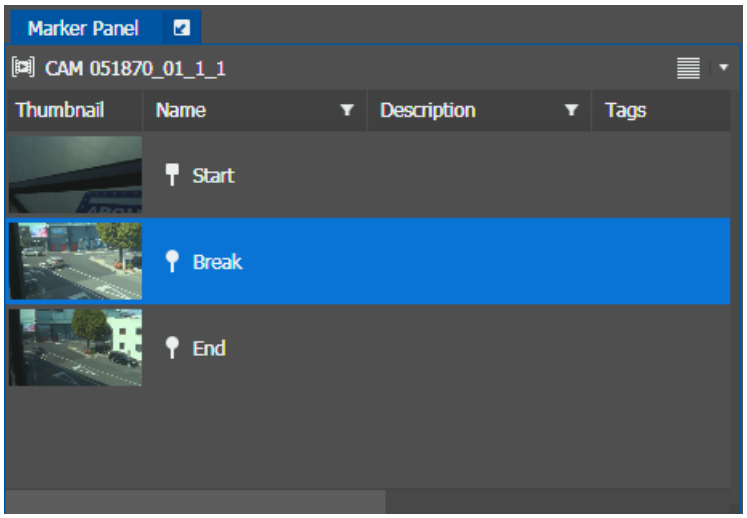
You can add markers to your assets by using logging buttons on the Button Panel.

1. Load the selected asset into the Source Viewer.
2. Click the **Play** button or use other transport controls to preview the asset.

3. Do one of the following below:

   - Click the appropriate logging button on the Button Panel.
   - Press the keyboard shortcut keys that have been set for your logging buttons.

   The marker and its metadata appear on the Marker Panel. The marker applies to a selected point in time of the asset.



4. Enter the description of the marker in the Marker Panel.

   This can be done easily if you already defined the **Set auto-focus on marker creation to** either Name, Description, or Tag in the user preferences setting for Advanced Logging.

5. If you need to click multiple buttons for a marker, set the number of seconds needed for the **Automatic Button Reset Duration** setting in the User Preferences. For more details, refer to *Changing Advanced Logging user preferences* on page 1311.

The marker is added and automatically saved to the asset. A symbol indicates its location in the Source Viewer. If you select a symbol, the thumbnail associated with that point is loaded into the Source Viewer and the slider is moved to that position.

If you need to add keywords to your assets, you can still do so in the Source Viewer.

Related Topics

Adding keywords on page 1148
Adding markers on page 1146
Changing Advanced Logging user preferences on page 1311

Logging assets in Live Mode

You can log an asset while it's still recording by adding markers via Live Mode.

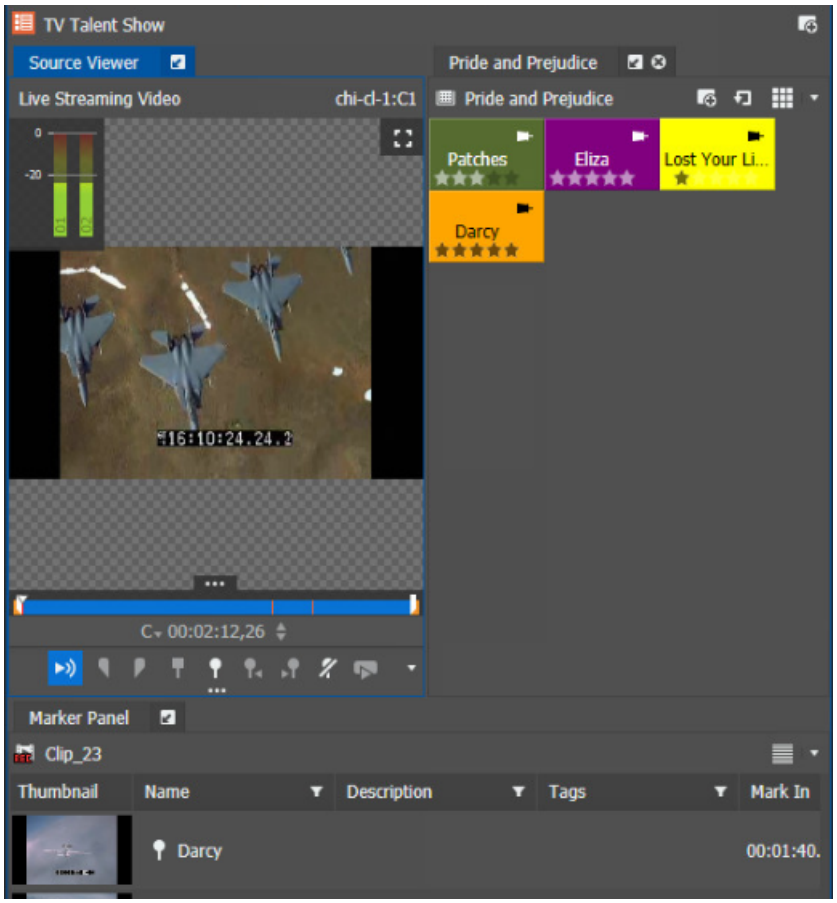
1. Load the still recording asset into the Source Viewer.

2. Click the **Live Streaming Video** button to preview the asset in Live Mode.

   The K2 Summit and channel information where the live stream is coming from is displayed on the upper right corner of the Source Viewer.

3. Click the **Play** button to play the asset.
4. To log the asset, do one of the following below:

   - Click the appropriate logging button on the Button Panel.
   - Press the keyboard shortcut keys that have been set for your logging buttons.



   The marker appears on the Marker Panel. Enter the description of the marker if desired.

   Logging is only allowed at the current timecode of the stream as displayed by the timecode control in Source Viewer. Scrubbing is disabled in Live Mode.

   Live Mode ends when the asset stops recording.

The marker is added and automatically saved to the asset. A symbol indicates its location in the Source Viewer. If you select a symbol, the thumbnail associated with that point is loaded into the Source Viewer and the slider is moved to that position.

Using a keyword or marker to add an event to a sequence

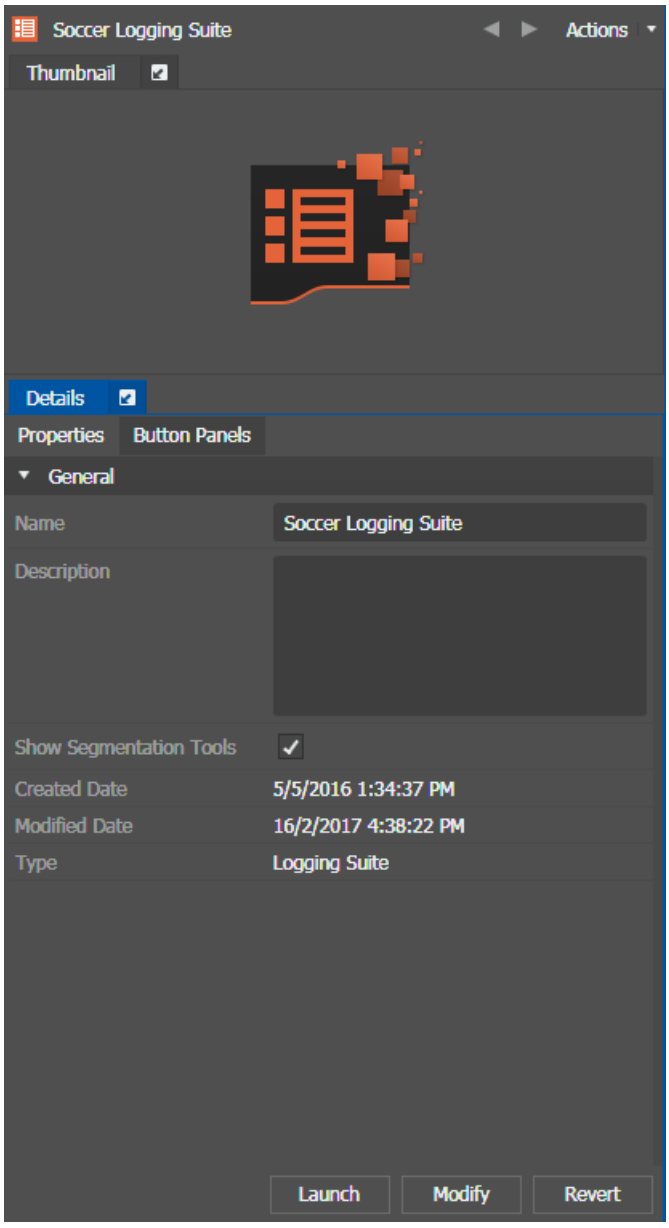
In the Source Viewer or the Inspector, drag and drop the symbol associated with the keyword or marker to the Storyboard Editor.

When dragging a keyword to the Storyboard Editor, the part of the asset between the mark-in and mark-out points is added to the sequence. When dragging a marker, the frame associated with the marker is added to sequence (plus a default duration).

Modifying Logging Suites and Button Panels

1. Do one of the following:
   - To modify the Logging Suite, drag the Logging Suite icon on the Logging Suite into the Inspector.
   - To modify the Button Panel, do one of the following:
     - Drag the Button Panel icon into the Inspector.
     - Right-click on a button in the Button Panel and select **Edit Panel Properties**.

   The properties load into the Inspector.



2. Rename the Logging Suite or the Button Panel.

   You can also change the description if desired.

3. If assigned with the Segmentation role. you can select the **Show Segmentation Tools** checkbox to add a Segmentation panel to your logging suite.

   When launched, the Segmentation panel opens in a new tab next to the Source Viewer. You can undock the panel and drag to reposition it anywhere in the GV STRATUS application.

   NOTE: Any Advanced Logging panels docked outside of the logging suite get tabbed within the suite again after closing and reopening the suite.

4. Select or deselect check boxes on the next tab to choose Button Panels for your Logging Suite, or choose logging buttons for your Button Panel.
5. Click **Modify** to save your changes.
6. Click **Revert** if you want to undo the change.
7. Click **Launch** to open the modified Logging Suite or Button Panel.

Modifying logging buttons of the Button Panel

1. Select a logging button that you want to modify on the Button Panel.
2. Do one of the following:

   - Right click and select **Edit Button Properties**.
   - Drag the logging button from the Button Panel and drop it into the Inspector.

   The button properties load into the Inspector.

3. Change any properties of the logging button.
4. Click **Modify**.

The logging button is modified.

NOTE: A button can also be dragged from the button list in the* Inspector *into the Properties panel of the* Inspector *to be modified.

Deleting logging buttons from a Button Panel

1. Right-click on the logging button that you want to delete.
2. Select **Remove Button from Panel**.

   The button is removed from the Button Panel.

Changing Advanced Logging user preferences

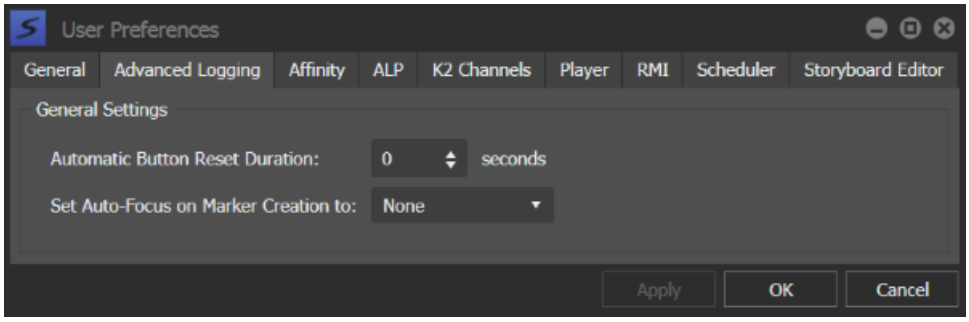
You can change a few general settings of the Advanced Logging tool within the user preferences window.

1. Select **Edit | User Preferences**.

   The User Preferences dialog box opens.

   The GV STRATUS application shows or hides sections based on the roles assigned to your GV STRATUS log on credentials.

2. Select the tab for the panel or component you are configuring and make settings accordingly.
3. To configure Advanced Logging user preferences, select the **Advanced Logging** tab.



4. To set the Automatic button reset duration, enter the number of seconds that you prefer.

   Logging buttons stay depressed according to the number of seconds that had been set, so that multiple buttons can be selected to log the marker.

5. To set auto-focus to editable fields after creating markers, click the drop-down list and select the field.

   Fields that can be selected are **Name**, **Description**, and **Tag**. The selected field is automatically focused for metadata insertion each time a marker is created.

   If you don't want to set auto-focus on any fields, select **None**.

6. To apply a change and continue editing user preferences settings, click **Apply**.
7. To accept any changes and close the dialog box, click **OK**.

   The dialog box closes.

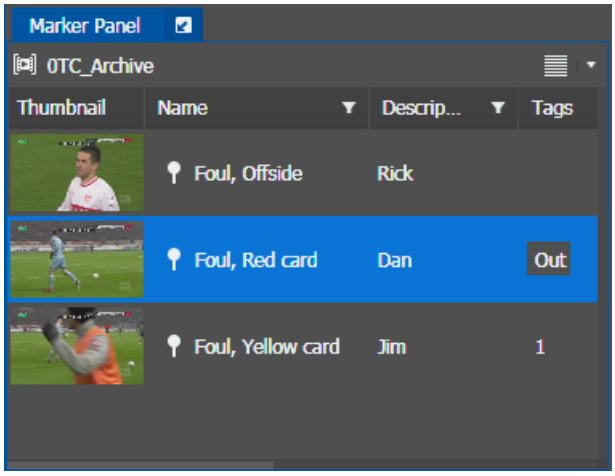
Modifying markers and keywords

- If GV STRATUS security is enforced, your credentials must give you full read and write permissions on bins, assets, metadata, and markers.

- All marker permissions must be set to Allow before you can modify or delete markers and keywords via the Advanced Logging tool. Without full marker permissions, logging buttons will be disabled.

You can view markers and keywords of an asset in the Marker Panel, Source Viewer or the Inspector panel.

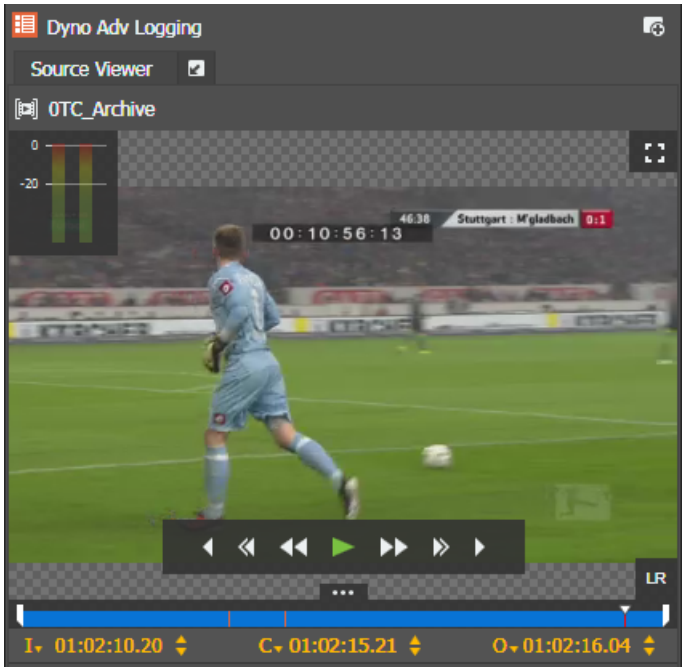
1. To view keywords and markers in the Marker Panel, scroll down the Marker Panel.



2. To view the keyword or marker in the Source Viewer or the Inspector panel, do the following:

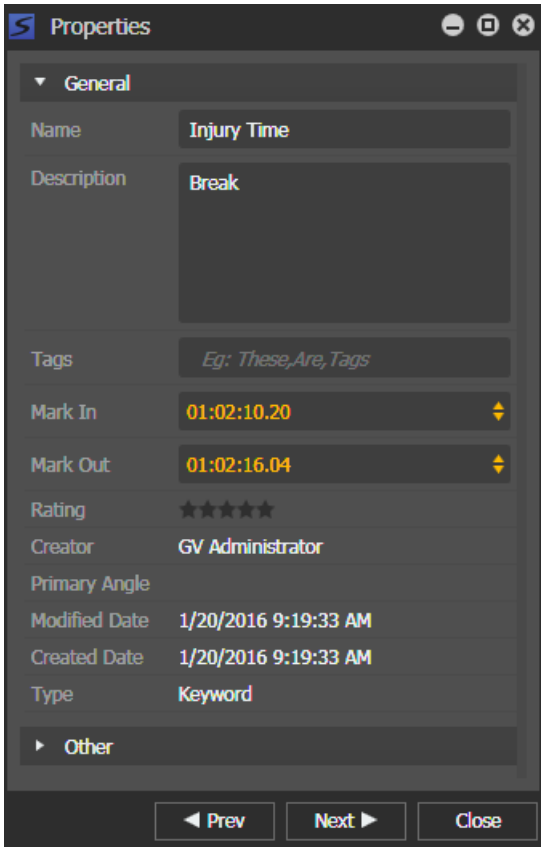
   - Click the keyword or marker in the Marker Panel to view it in the Source Viewer.
   - Drag and drop a keyword or marker from the Marker Panel into the Inspector.

   In Source Viewer, the scrub bar jumps to the keyword or marker point, and the thumbnail associated with the keyword or marker displays.



   In Inspector, the properties and thumbnail associated with the keyword or marker are displayed.

3. Double click the keyword or marker on the Marker Panel to view their properties and edit those properties in the **Properties** window.



You can see whether it's a marker or keyword from the **Type** information. For a keyword, there is an additional **Mark Out** display in the Properties window.

If you have custom metadata already defined for markers and keywords, their properties will also be displayed.

If GV STRATUS metadata access control is enforced, your credentials must give you adequate permissions. You can only view metadata with read permissions, and modify metadata with write permissions. If read or write permissions are denied, your metadata fields will be disabled.

Related Topics

Using a keyword or marker to add an event to a sequence on page 1308

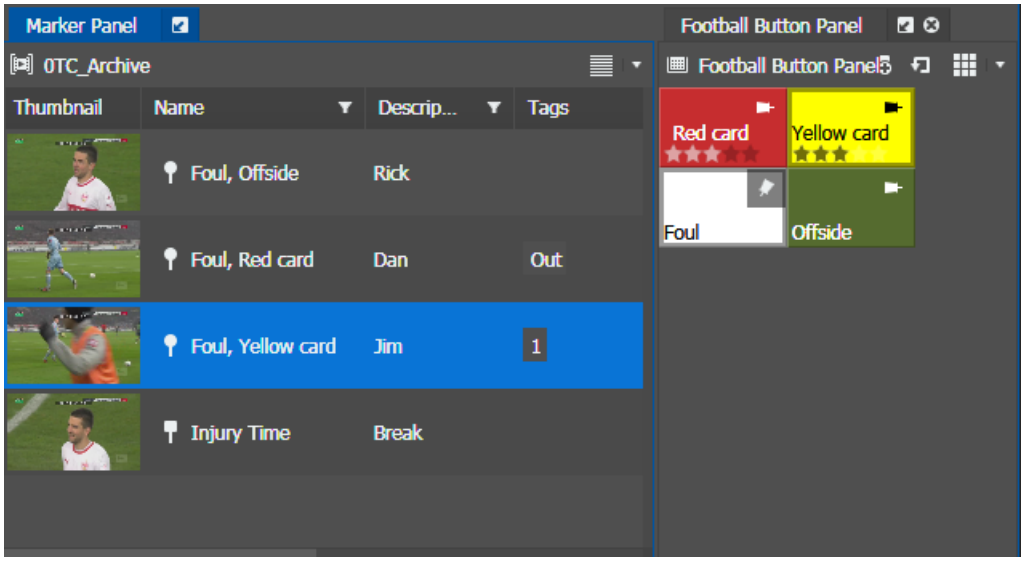
Viewing logging history of markers

You can view the logging history of markers in the Button Panel.

1. Select a marker on the Marker Panel.

   Buttons that were used to create the marker get pressed.

   Each time a marker is selected in the Marker Panel, logging buttons that made the marker are automatically pressed and highlighted in the Button Panel to indicate the logging history.



2. If you want to add more metadata to the marker, click another button in the Button Panel.

   The selected button is pressed in the Button Panel, and the metadata is added to the marker.

3. If you want to remove metadata from the marker, click a pressed button in the Button Panel.

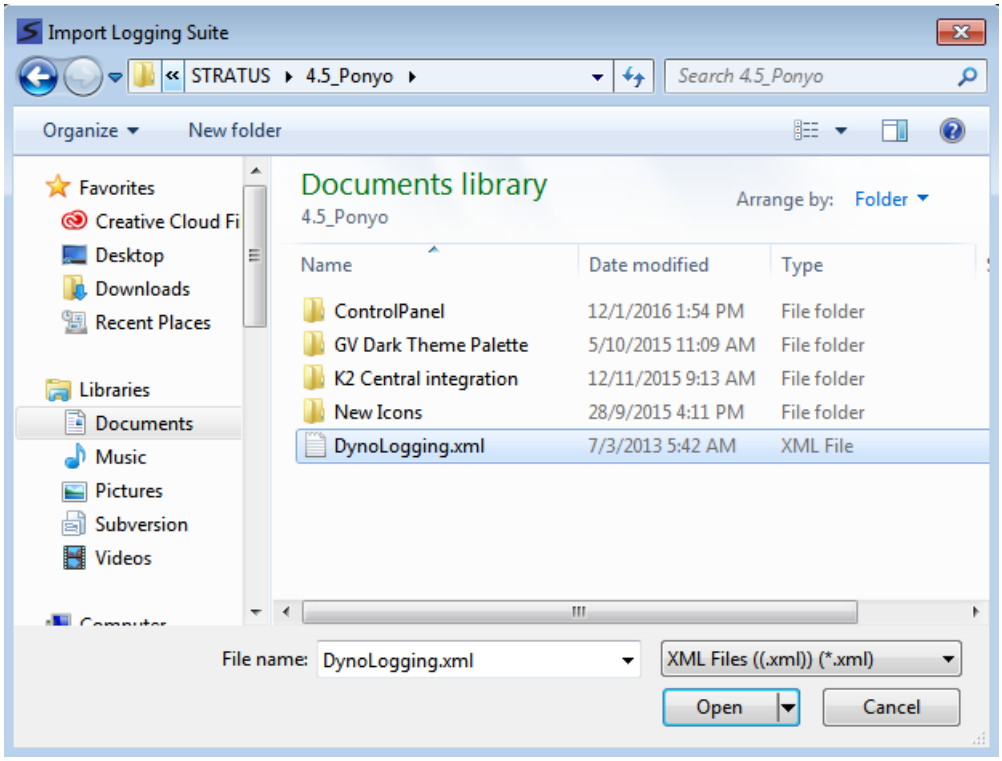
   The selected button is depressed in the Button Panel, and the metadata is removed from the marker.

Importing Logging Suite

You can import a Logging Suite configuration from an XML file into your Advanced Logging Tool.

1. Go to **Tools | Advanced Logging**, right-click and select **Import Logging Suite**.

   The **Import Logging Suite** dialog displays.



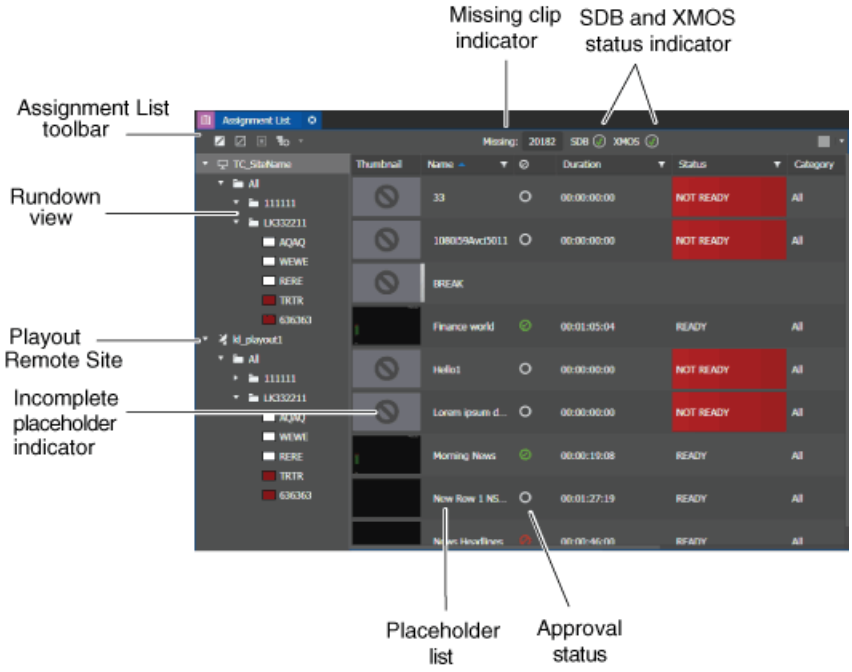
2. Browse to the location of the XML file, and select it.
3. Click **Open**.

Logging buttons and Button Panels are created in the new Logging Suite according to the imported XML file.

Using the Assignment List

The Assignment List tool

The Assignment List tool allows you to create placeholders for clips, assign those placeholders to newsroom editors, add new sequence, and link the resulting clips to rundown stories on your Newsroom Computer System. You also need GV STRATUS Rundown components such as SDB Server and XMOS Server to run the Assignment List tool. With the proper license and assigned role, Assignment List appears in the GV STRATUS application as a panel that can be accessed from the Window menu, the tool section of the Navigator panel, and the **Link to Placeholder** tab in the Inspector panel.



The Assignment List panel features are as follows:

- Toolbar — Displays buttons to add placeholders, show placeholders with missing clips, delete placeholders, and add new sequence to placeholders.
- Missing clip indicator — Displays the number of missing clips that can help you determine the number of incomplete assignments.
- Incomplete placeholder indicator — Displays blank thumbnails for incomplete placeholders. Completed placeholders are identified by the thumbnail display and **READY** status in the Status column.
- Placeholder list — Displays incomplete and completed placeholders. When you select a rundown, all placeholders in that rundown appear in the placeholder list. When you select a story in the rundown, only placeholders in that story appear in the placeholder list in the same sequence as in the story.
- Approval status — Displays the approval status of placeholders. You can only set the approval status on linked placeholders with **Ready** status in the Inspector panel.
- Playout Remote Site — Displays placeholders in the remote site. The Playout remote site must be configured in the GV STRATUS Control Panel before it can be accessed via the Assignment List.
- Rundown view — Displays rundowns and stories for each rundown. Rundowns display alphabetically in the panel, while stories appear in sequence as assigned in the Newsroom Computer System.
- SDB status indicator — Displays the connection status between Assignment List and Simple Database (SDB) Server. The SDB Server updates clip status, clip duration, and amount of missing clips for the Assignment List tool.
  - — Connected
  - — Disconnected

- XMOS status indicator — Displays the status of XMOS Server. The XMOS Server provides the communication between the Newsroom Computer System and the Assignment List tool.
  - — Connected
  - — XMOS Server is disconnected with the GV STRATUS application
  - — XMOS Server is disconnected with the Newsroom Computer System

With the Assignment List tool, you can create placeholders, monitor rundown or clip status, and view or change placeholder properties.

Standard Asset List features such as filter list, sort list, asset tooltip, and customization of **View Mode** are available in the Assignment List tool.

If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets, and metadata that do not have read permissions are not visible.

Assignment List buttons

These buttons located on the Assignment List panel let you perform various functions.

New Placeholder: Adds a new placeholder in the Assignment List tool.

Missing Placeholders Only: Shows placeholders with missing clips only in the Assignment List tool.

Delete: Deletes the selected item or items. Disabled if delete rights denied in GV STRATUS Control Panel and/or turned off in User Preferences.

New Sequence: Creates a new sequence.

New Project in EDIUS: Creates a new project in the EDIUS XS application.

Missing Clip indicator: Shows the number of placeholders with missing clips in the Assignment List tool.

Story status colors

Each story in the rundown view appears in a color that identifies its status in the Assignment List.

Story Color	Story Status
White	READY
Red	NOT READY
Dark Blue	STANDBY
Green	PLAY
Yellow	STOPPED
White	END
White	DISCONNECTED

Story Color	Story Status
Light Grey	BREAK

Changing ALP User Preferences

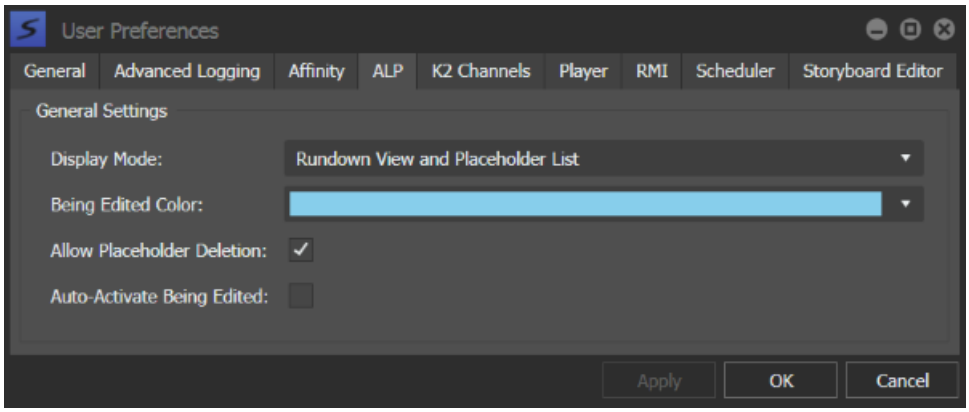
You can Assignment List options within user preference settings.

1. Select **Edit | User Preferences**.

   The User Preferences dialog box opens.

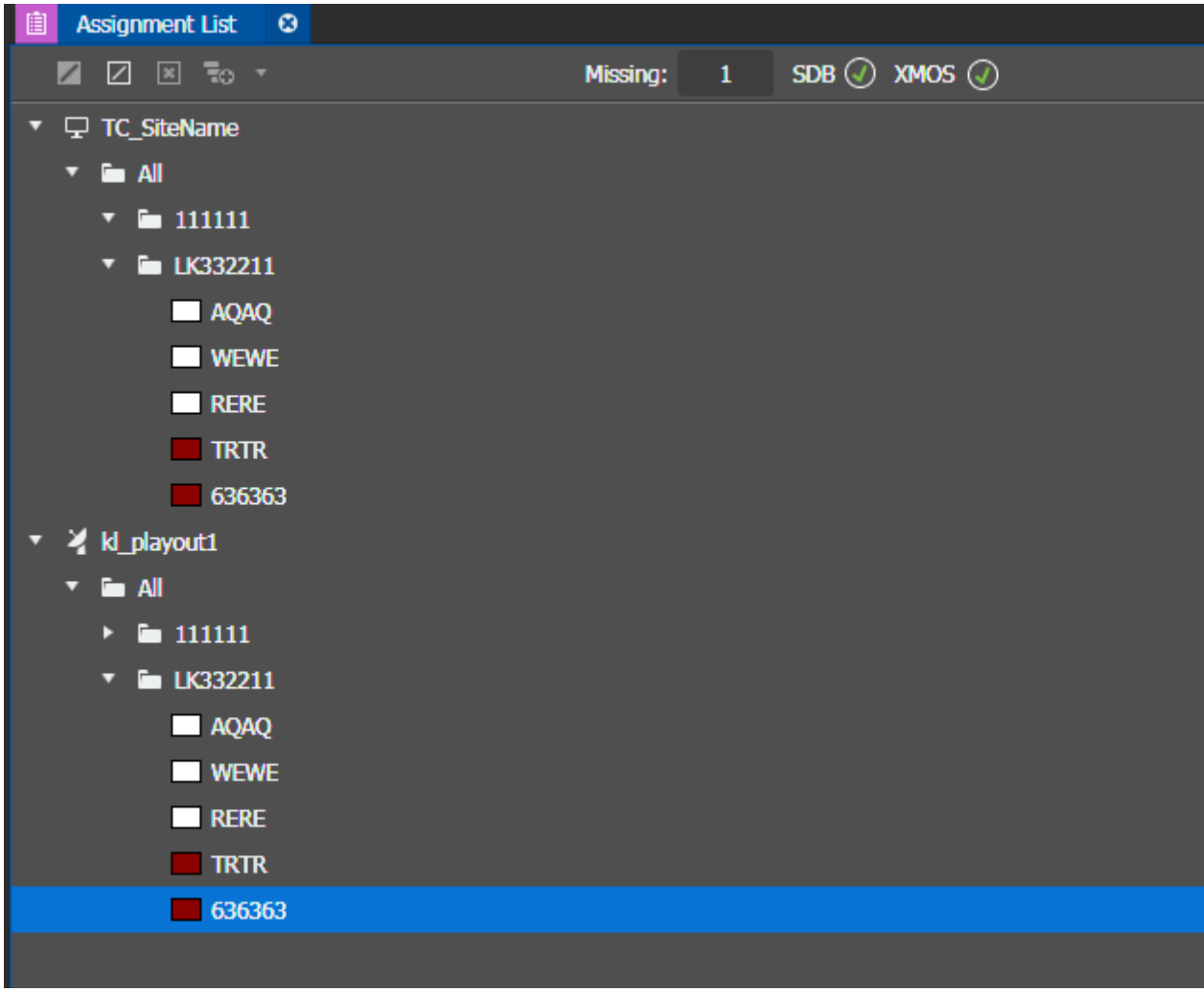
   The GV STRATUS application shows or hides sections based on the roles assigned to your GV STRATUS log on credentials.

2. Select the tab for the panel or component you are configuring and make settings accordingly.
3. To configure Assignment List user preferences, select the **ALP** tab.

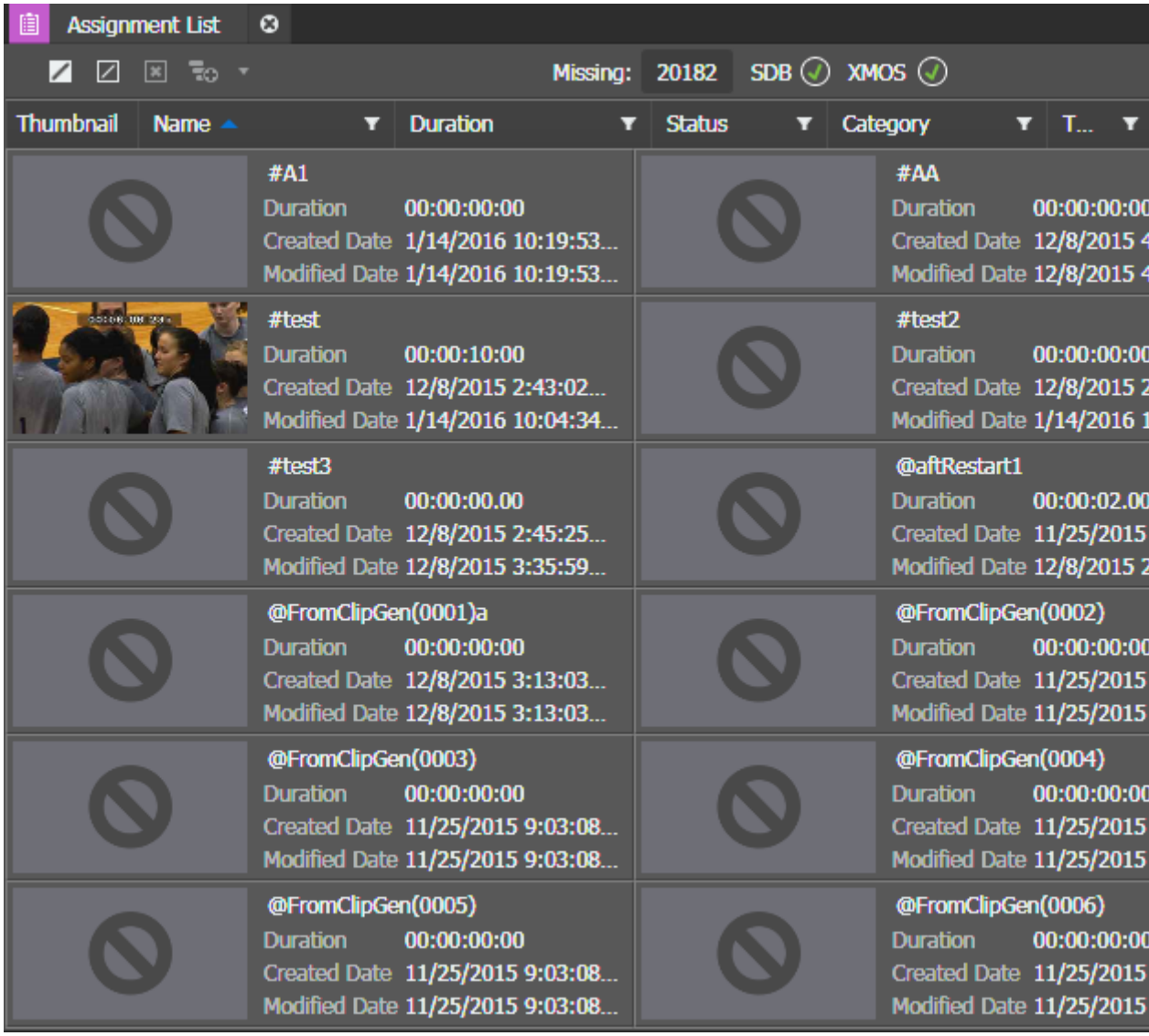


4. To select the **Display Mode** of your Assignment List tool, click the drop-down list, and choose from the following:

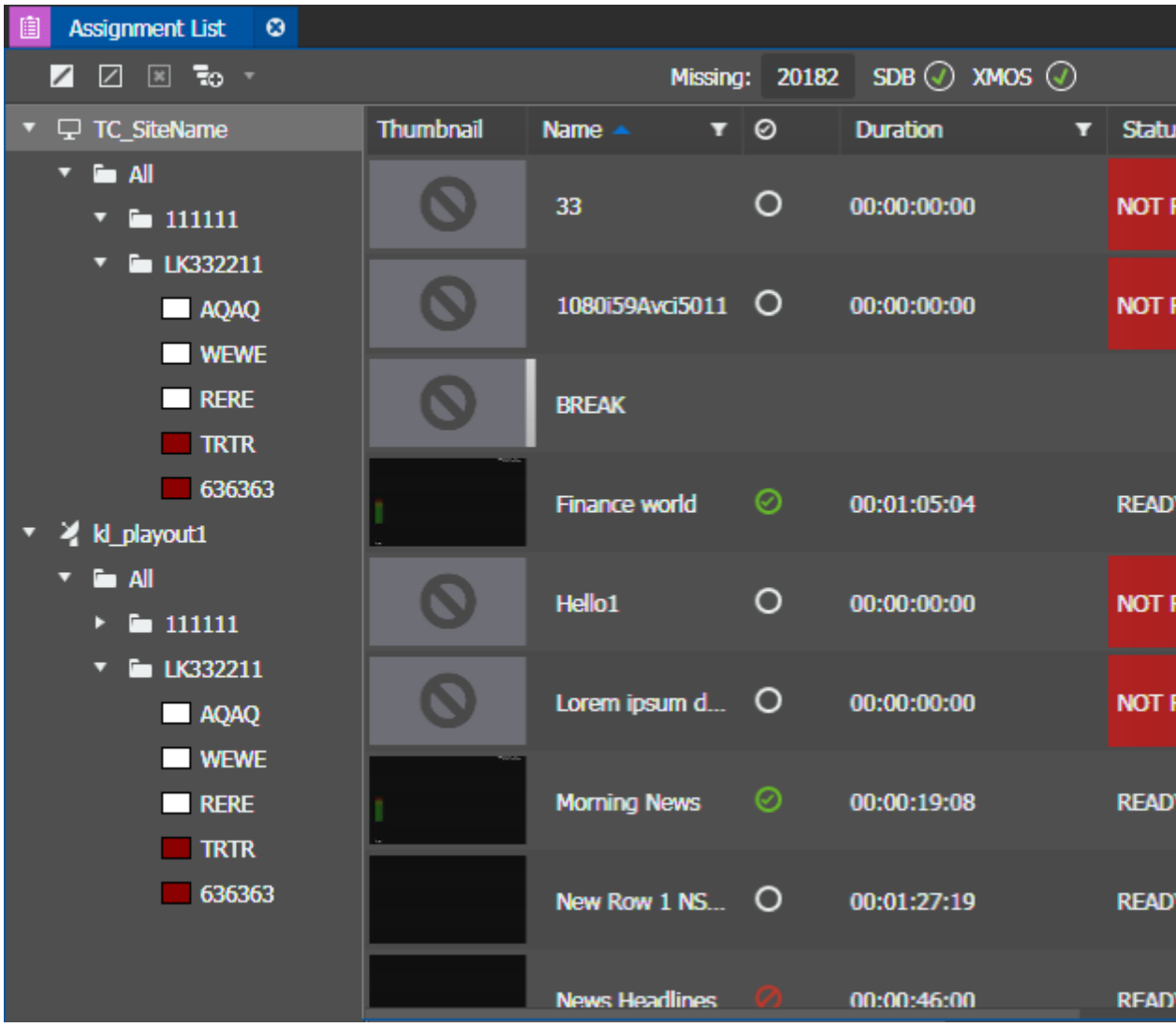
   Rundown View — Displays rundown view only.



   Placeholder List — Displays placeholder list only.

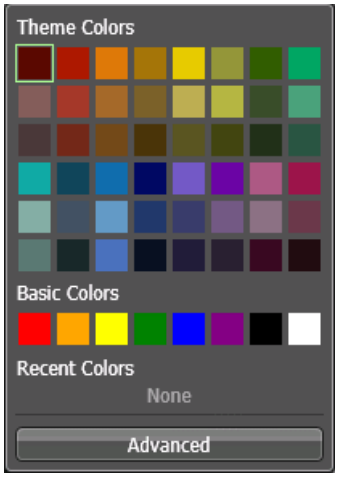

Assignment List
Missing: 20182
SDB
XMOS
Thumbnail
Name
Duration
Status
Category
T...
#A1
Duration 00:00:00:00
Created Date 1/14/2016 10:19:53...
Modified Date 1/14/2016 10:19:53...
#AA
Duration 00:00:00:00
Created Date 12/8/2015 4
Modified Date 12/8/2015 4
#test
Duration 00:00:10:00
Created Date 12/8/2015 2:43:02...
Modified Date 1/14/2016 10:04:34...
#test2
Duration 00:00:00:00
Created Date 12/8/2015 2
Modified Date 1/14/2016 1
#test3
Duration 00:00:00.00
Created Date 12/8/2015 2:45:25...
Modified Date 12/8/2015 3:35:59...
@aftRestart1
Duration 00:00:02.00
Created Date 11/25/2015
Modified Date 12/8/2015 2
@FromClipGen(0001)a
Duration 00:00:00:00
Created Date 12/8/2015 3:13:03...
Modified Date 12/8/2015 3:13:03...
@FromClipGen(0002)
Duration 00:00:00:00
Created Date 11/25/2015
Modified Date 11/25/2015
@FromClipGen(0003)
Duration 00:00:00:00
Created Date 11/25/2015 9:03:08...
Modified Date 11/25/2015 9:03:08...
@FromClipGen(0004)
Duration 00:00:00:00
Created Date 11/25/2015
Modified Date 11/25/2015
@FromClipGen(0005)
Duration 00:00:00:00
Created Date 11/25/2015 9:03:08...
Modified Date 11/25/2015 9:03:08...
@FromClipGen(0006)
Duration 00:00:00:00
Created Date 11/25/2015
Modified Date 11/25/2015

Rundown View and Placeholder List — Displays rundowns and placeholder list.

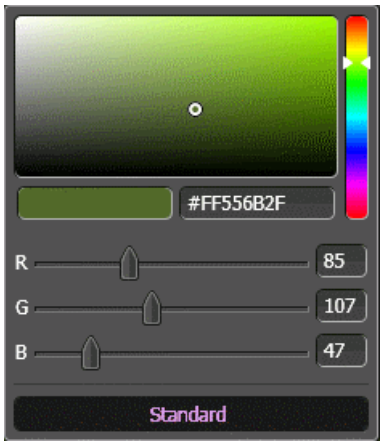


5. To change the **Being Edited Color** of placeholders, click on the drop-down list to display the color palette, and do one of the following:

   - Select any theme or basic colors as provided.



   - Click **Advanced** to define your own custom color and RGB values.



   The color of being edited placeholders is changed to the selected color.

   The status of a placeholder changes to being edited if the placeholder is linked to a scheduled event, linked to an RMI clip, or when the being edited checkbox is selected in the placeholder properties.

6. Set other options as follows:

   - **Allow Placeholder Deletion**: Allows placeholder deletion in the Assignment List tool.
   - **Auto-Activate Being Edited**: When a new sequence is added to a placeholder, the sequence is automatically set to **Being Edited**.

7. To accept any changes and close the dialog box, click **OK**.

   The dialog box closes.

Related Topics

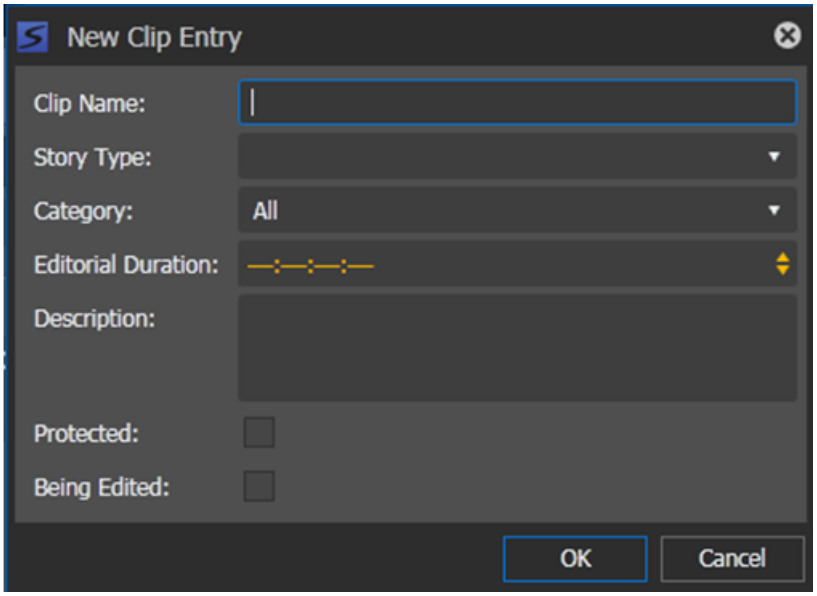
Deleting a placeholder on page 1326

Adding placeholders

Placeholders are essentially assignments for editors, who can then create clips for the story, and send them to a K2 Summit/SAN system for playback. You need to create a placeholder for each clip that you link to a rundown.

NOTE: Grass Valley recommends no more than 2,000 placeholders in the system for optimal performance.

1. In the Assignment List tool, click the **New Placeholder** button.



   The New Clip Entry dialog box opens.

2. Enter the clip name.

   The name identifies the placeholder in the Assignment List (which can also be seen in the Newsroom Computer System).

3. You can also provide additional information about the placeholder:

   - **Story Type** — Select a Story Type from the drop-down menu. Available story types are **SOT** (Sound On Tape) or **VO** (Voice Over). You can also leave this field blank.
   - **Category** — Select a category from the drop-down menu. The category determines how stories are grouped and sorted.
   - **Editorial Duration** — Enter a duration for the placeholder. The Editorial Duration is an optional value you can set for an estimated on-air duration of the clip that can be changed to a more precise value later.

     NOTE: Editorial Duration has the priority over clip duration. Once an Editorial Duration is set; it will not be adjusted to clip duration, even after clip is associated with the placeholder. The editor needs to set the final Editorial Duration before the clip is sent for playback.
   - **Description** — Enter a description for the placeholder. The description helps editors to identify the clip that they need.
   - **Protected** — Check this box to prevent the clip from being deleted by other users.
   - **Being Edited** — Check this box to indicate when the sequence for a placeholder is currently being edited.

4. Click **OK**.

The new placeholder appears on the Assignment List tool.

NOTE: The Clip ID and Date are set automatically when you create a new placeholder.

Related Topics

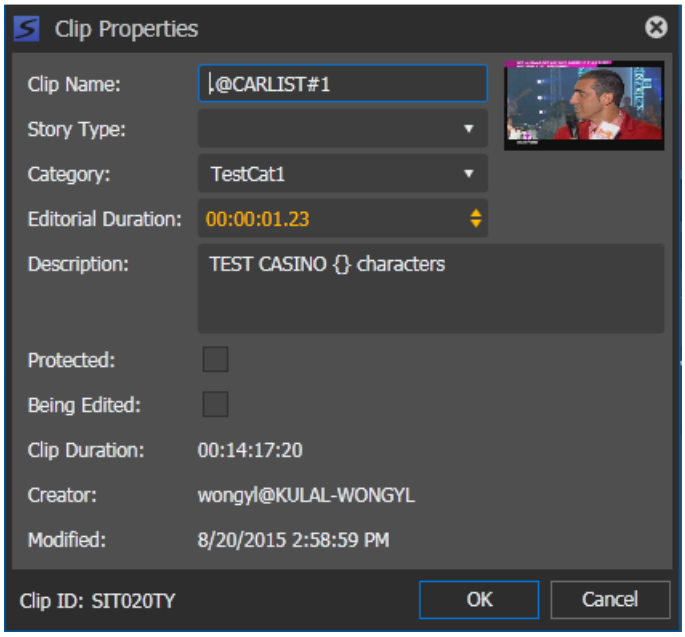
Limitations for creating and naming assets and bins on page 1428

Modifying a placeholder

If you need to, you can change or modify properties of a placeholder.

1. Right-click on the placeholder that you want to modify and select **Edit Properties**.

   The Clip Properties dialog box opens.



2. Modify any properties in the dialog box.

   NOTE: Properties that cannot be modified are creator, modified date and clip ID.

3. Click **OK**.

   The placeholder properties are modified on the Assignment List tool.

Related Topics

Limitations for creating and naming assets and bins on page 1428

Deleting a placeholder

If desired, you can delete placeholders, associated assets, and essences from the Assignment List tool.

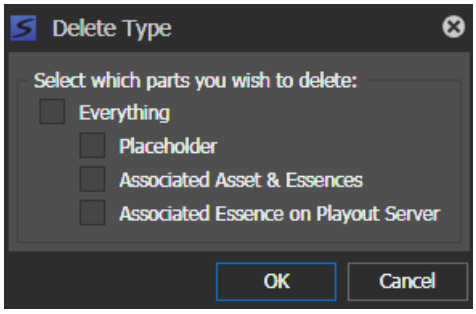
1. Do one of the following to delete a placeholder:

   - Select the placeholder that you want to delete and click the **Delete** button.
   - Right-click on the placeholder and select **Delete Placeholder**.

2. Select your options as follows:

   - Everything — Select this to delete the entire asset including placeholder, associated asset and essences, and associated essence on the managed Playout Server.
   - Placeholder — Select this to only delete the placeholder on the GV STRATUS application.
   - Associated Asset & Essences — Select this to only delete the associated asset and essences on your K2 Summit/SAN system.
   - Associated Essence on Playout Server — Select this to only delete the associated essence on the managed Playout Server if you already sent it out for playback.

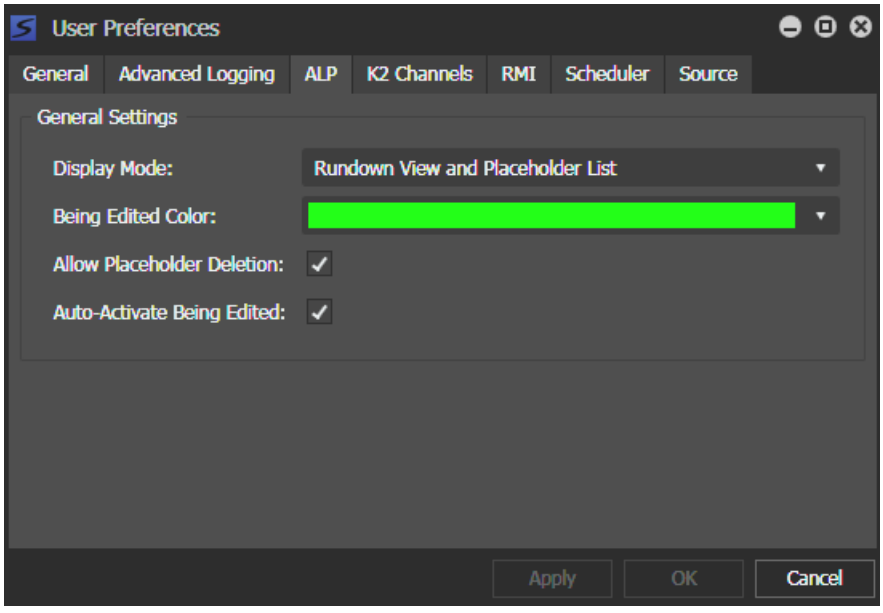
     NOTE: Deletion of essence on an unmanaged playout server is not supported. However, you can still delete via the Aurora Playout Housekeeper application or delete directly on the unmanaged playout server.



3. Click **OK**.

If the **Delete** button is not selectable or **Delete Placeholder** is grayed out in the context menu, you need to check ALP settings in the User Preferences menu.

Select **Edit | User Preferences | ALP** and check the **Allow Placeholder Deletion** box.



Related Topics

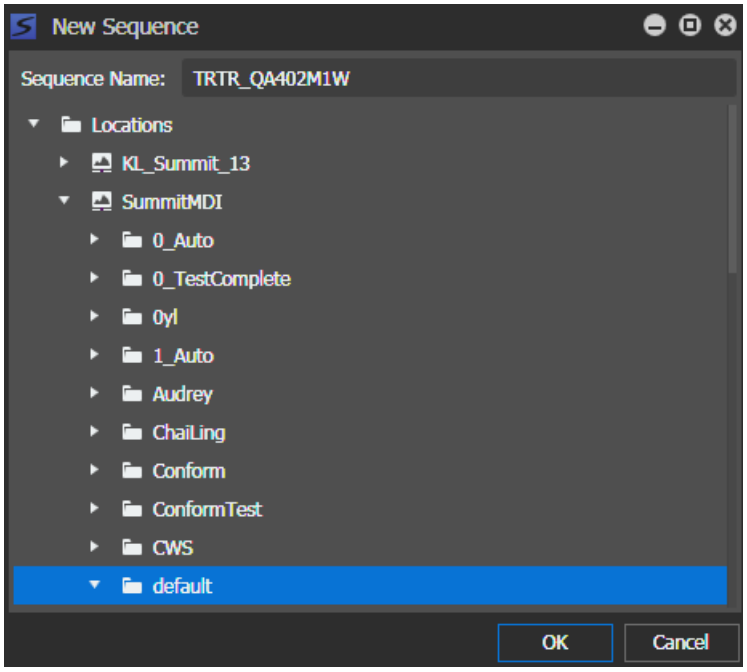
Deleting assets on page 985

Adding a new sequence

You can add a new sequence to a placeholder in the Assignment List tool.

1. Select a placeholder that you want to add a new sequence into.
2. Click the **New Sequence** button.

   The New Sequence dialog opens.



   The sequence name is automatically populated with the placeholder name and ID. You can still change the sequence name if you want to.

3. Select a location for the sequence and click **OK**.

   The Storyboard Editor tool launches automatically if it is not already opened. The sequence name can be viewed in the Sequence Viewer and Storyboard panels.

4. Add events as necessary to the sequence.

If configured in ALP user preferences settings, the placeholder row color changes to the being edited color in the Assignment List.

Checking missing clips

The Assignment List lets you see if clips are complete and ready for air.

You can only see thumbnails for placeholders with completed clips, which can also be identified by **Ready** status in the Assignment List. The thumbnail column is blank for placeholders with missing clips.

- To display placeholders with missing clips only, click the **Missing Placeholders Only** button.

  You can also see the number of placeholders with missing clips from the indicator on the toolbar.

If you want to see the entire list of placeholders, click again the **Missing Placeholders Only** button.

Viewing placeholder properties

You can view the properties of a placeholder in the Inspector panel.

Right-click on the placeholder and select **View Properties**.

The placeholder properties display in the Inspector panel.

Viewing and modifying metadata of linked placeholders

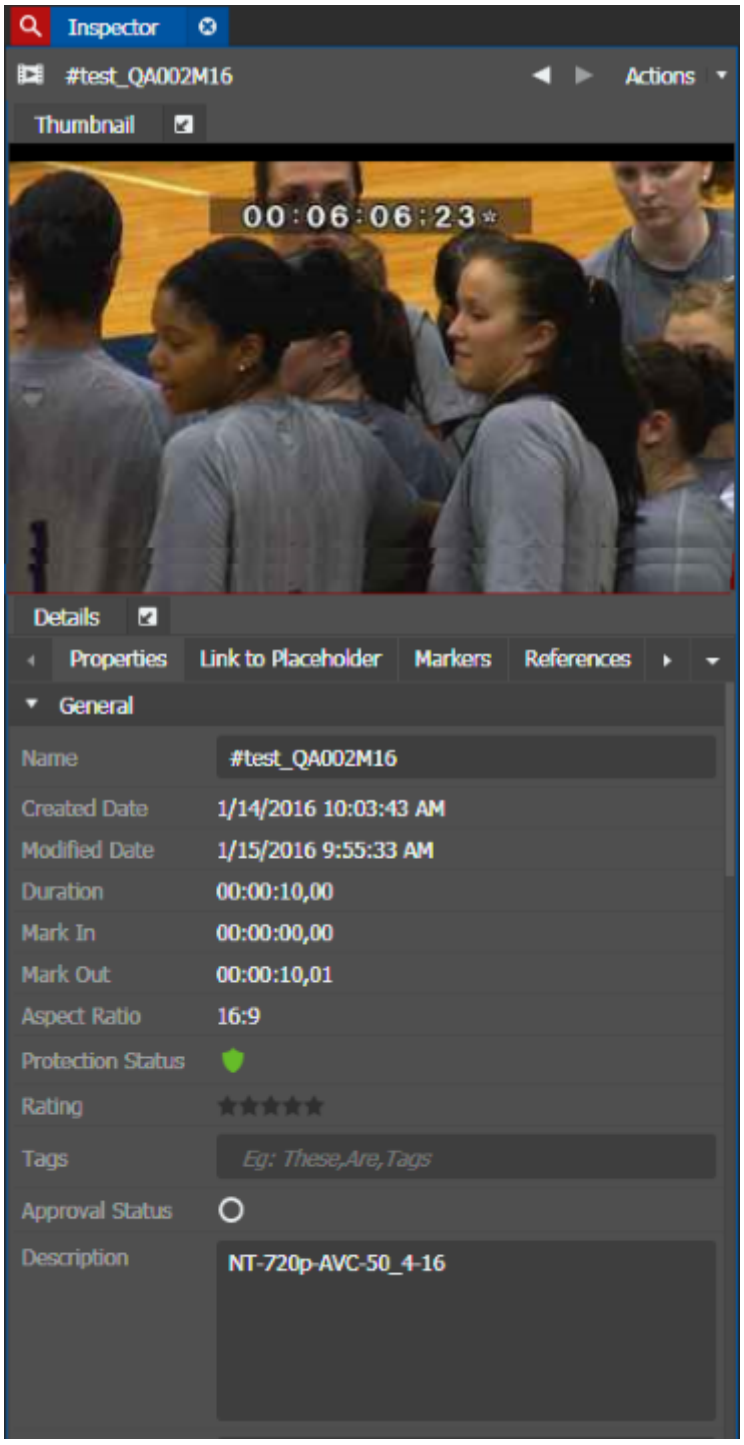
You can view and modify metadata of placeholders with **Ready** status. When you modify the metadata, you are actually modifying the metadata of the asset that is already associated with the placeholder.

The inserted metadata can then be used as the search criteria to easily search assets in the Asset List panel.

1. To view or modify the metadata, do one of the following below:

   - Drag and drop the placeholder into the Inspector panel.
   - Double-click the placeholder.

   The metadata loads into the Inspector panel.



2. On the **Properties** tab, you can view or modify metadata of placeholders.

   You can also add and customize metadata fields in the Metadata settings within the GV STRATUS Control Panel application.

3. To lock the status, click the **Unprotected** button.

   The asset is now locked. To unlock, click the **Protected** button.

4. To add a star rating, click the star or stars next to Rating.

   When you add a star, it retains the color fill even when the mouse is no longer hovering over it.

5. Click the **None** icon to change the approval status.

   The approval status changes to **Approved**.

   You can click the icon to toggle the approval status of the linked placeholder. The selected approval status displays on the Assignment List.

   - **None**: Identifies the approval status of the clip as none.
   - **Approved**: Identifies the approval status of the clip as approved.
   - **Rejected**: Identifies the approval status of the clip as rejected.

6. Set the **MetadataExpireDate** and **Source ID**, if needed.
7. To view lists of related assets and relationships, see other tabs of the Inspector panel.

Related Topics

Viewing relationships on page 1020
Verifying proxy association on page 1021

Creating a new sequence in the EDIUS application

You can create a new sequence in the EDIUS for GV STRATUS application from the Assignment List. The new sequence appears in the EDIUS as a new project. This enables further editing to be done using EDIUS before sending your sequence for playback. The sequence which is automatically linked to a placeholder can then easily be sent to the K2 system from the EDIUS application.

The **New Project in EDIUS** button is only available if you are assigned with the EDIUS XS role in the GV STRATUS Control Panel and the EDIUS application must be installed on your machine.

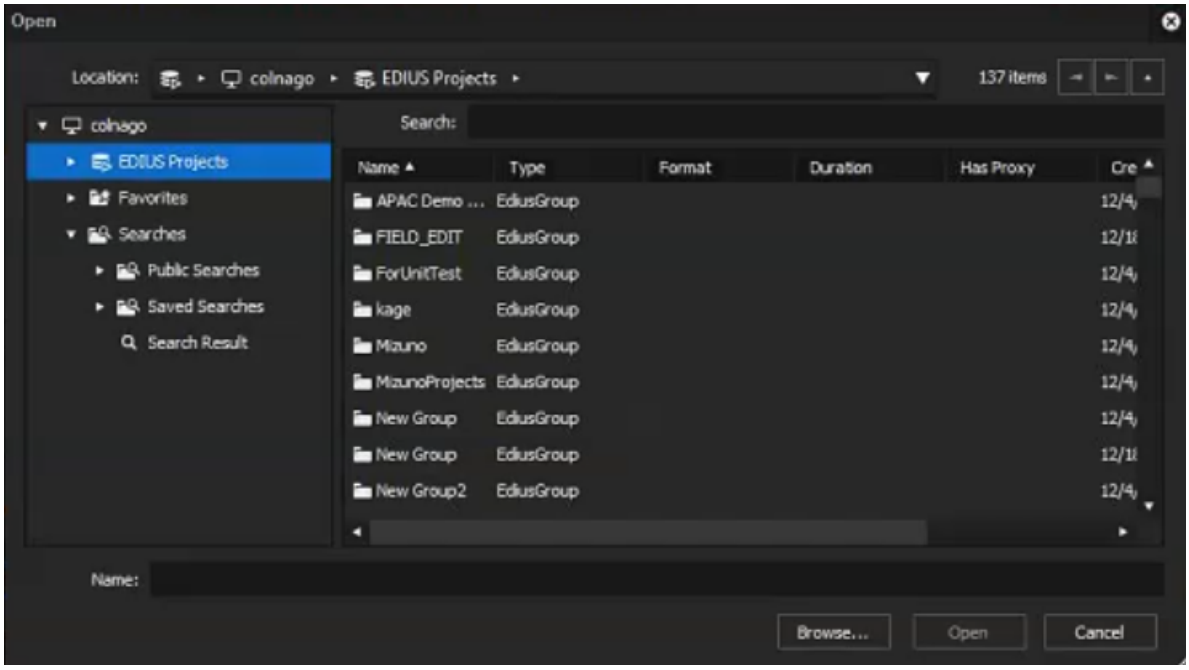
1. Select a placeholder in the Assignment List.

2. Do one of the following:

   - Click the **New Project in EDIUS** button.
   - Right-click on the placeholder and select **New Project in EDIUS**.

   NOTE: The sequence is automatically linked to a placeholder if the sequence is launched from the Assignment List panel.

   The Open dialog appears.

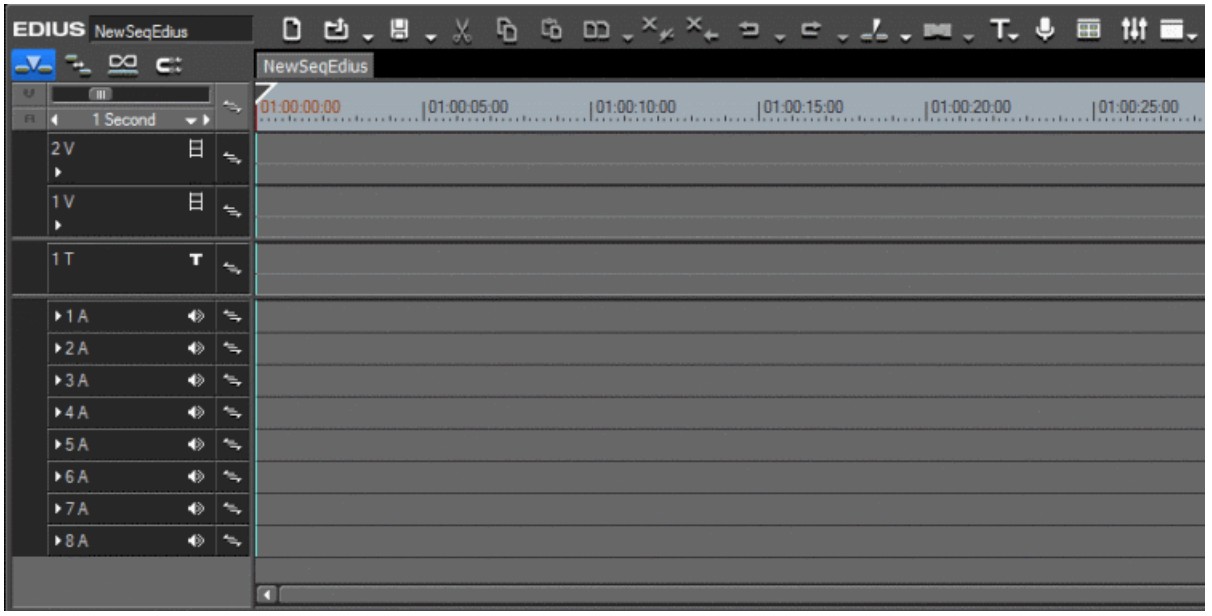


3. Select the project location.

   You can also set to other locations as long as the new location is under the default location path in EDIUS settings on the GV STRATUS Control Panel.

4. Enter the project name and click **Open**.

   The EDIUS application opens with the new project on the timeline.



After creating the project on the EDIUS timeline, you can add assets to the sequence.

Related Topics

Adding GV STRATUS assets to EDIUS timeline on page 1181
Sending EDIUS sequences to the K2 system on page 1189

Using the GV STRATUS application in a Newsroom Computer System

You can launch the GV STRATUS application as an ActiveX panel within supported MOS compliant Newsroom Computer Systems (NCS) such as ENPS, iNEWS, Octopus, OpenMedia, NIS5, Netia, and Inception. This allows you to use Assignment List, Scheduler, RMI, Inspector, Navigator, Storyboard Editor, Playlist Editor, and other panels to consolidate your entire operation into one workspace.

The Assignment List in the GV STRATUS application lets you create a placeholder for a clip and link it into the accompanying story in the NCS rundown. You can create placeholders and insert them manually into your rundown; or use the auto-create feature, to create and insert placeholders automatically.

If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, and metadata. In order to link an event to a placeholder, you must be assigned with write permission for the **Name** property in Metadata section of GV STRATUS Control Panel.

NOTE: To integrate Inception into the* GV STRATUS *system, contact Grass Valley Service.

About Newsroom Basic

The Newsroom Basic license is for journalists that work with the GV STRATUS application as an ActiveX window within a Newsroom Computer System (NCS) application. For this workflow, only the Inspector panel and the Assignment List tool are typically required. The Newsroom Basic license provides this limited functionality as an economical solution. There is no access to the full range of GV STRATUS functionality and tools, as available with other licenses.

If your license type is changed from some other license to the Newsroom Basic license, some of your previously saved workspaces might not be available. Workspaces that contain tools for which the Newsroom Basic license has no access are not allowed. Load the Default Workspace if necessary.

Related Topics

GV STRATUS roles matrix on page 37

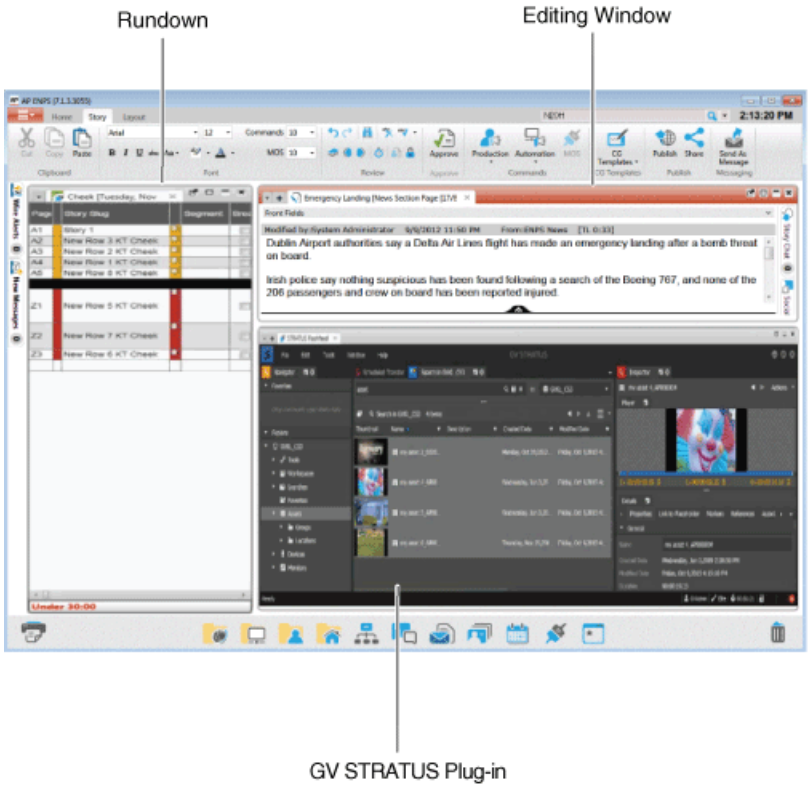
Using GV STRATUS with ENPS

The Assignment List in the GV STRATUS ActiveX panel lets you create a placeholder for a clip and insert it into the accompanying story slug in the ENPS rundown.

You can create placeholders and insert them manually into your rundown; or use the auto-create feature, to create and insert the placeholder automatically.

In addition to the placeholder workflow, GV STRATUS ActiveX panel supports the MOS Newsroom Item workflow with ENPS. Without the need to create placeholders and linking them with assets, you can just drag assets directly from GV STRATUS ActiveX panel and drop them into your ENPS stories. However, both workflows are not supported simultaneously. You must either use the placeholder workflow with Assignment List, or the MOS Newsroom Item workflow at a time.

GV STRATUS also supports the MOS Redirection workflow to transfer media between machines and locations automatically via ENPS. When MOS Redirection is triggered and stories with linked placeholders containing media are moved from one location to another, ENPS automatically transfers the media contained in those stories. This workflow supports automatic transfer of media between servers within a single newsroom, or between multiple newsrooms and servers in separate locations.



Logging on to the GV STRATUS application in ENPS

To successfully log on to the GV STRATUS application in ENPS, you need to run the ENPS client as an administrator when you launch it for the first time.

When you log on to the GV STRATUS system, the GV STRATUS application assigns GV STRATUS licenses and roles based on your user account credentials, as set by the system administrator in the GV STRATUS Control Panel application. If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins and assets that are part of your workflow. If GV STRATUS metadata access control is enforced, your credentials must give you adequate permissions on metadata fields that are part of your workflow. Your credentials must also give you access to all your K2 systems.

1. Launch and log on to your ENPS client.

   The ENPS application opens.

2. Right-click on the **MOS** icon and select GV STRATUS.

   A Log On dialog box opens.

3. Enter your user name.

   If you use domain credentials, enter in format `<domain>\<username>`. For example, if your domain is "gv" and your username is "GVuser", enter `gv\GVuser`.

   If you have successfully logged on before, select your user name from the drop-down list.

4. Enter your password.

5. Verify or enter the name of the Control Panel Host for the GV STRATUS Control Panel Service. In most systems, this is the main GV STRATUS Core server.
6. Click **Log On**.

The application opens.

GV STRATUS features are enabled according to the roles associated with your log on credentials.

When you log on to the application, the settings you make on one PC are available on other PCs when using the same user credentials, including the following:

- Settings from the User Preferences dialog box
- Workspaces
- Channel Panel configurations and Salvos
- Searches

Related Topics

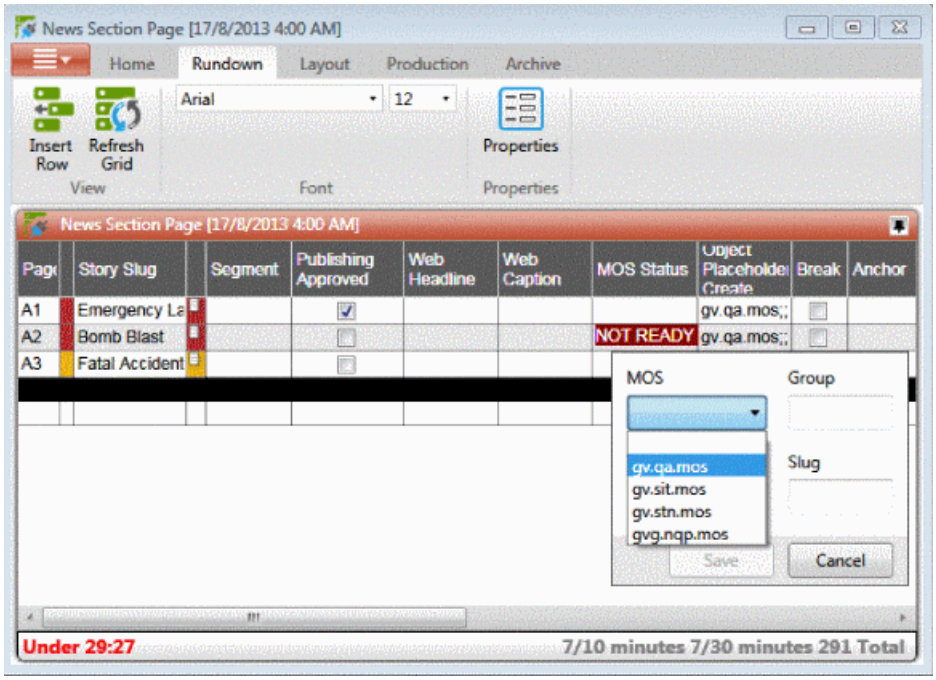
Logging off of GV STRATUS from within a NCS on page 1369

Creating placeholders automatically in ENPS

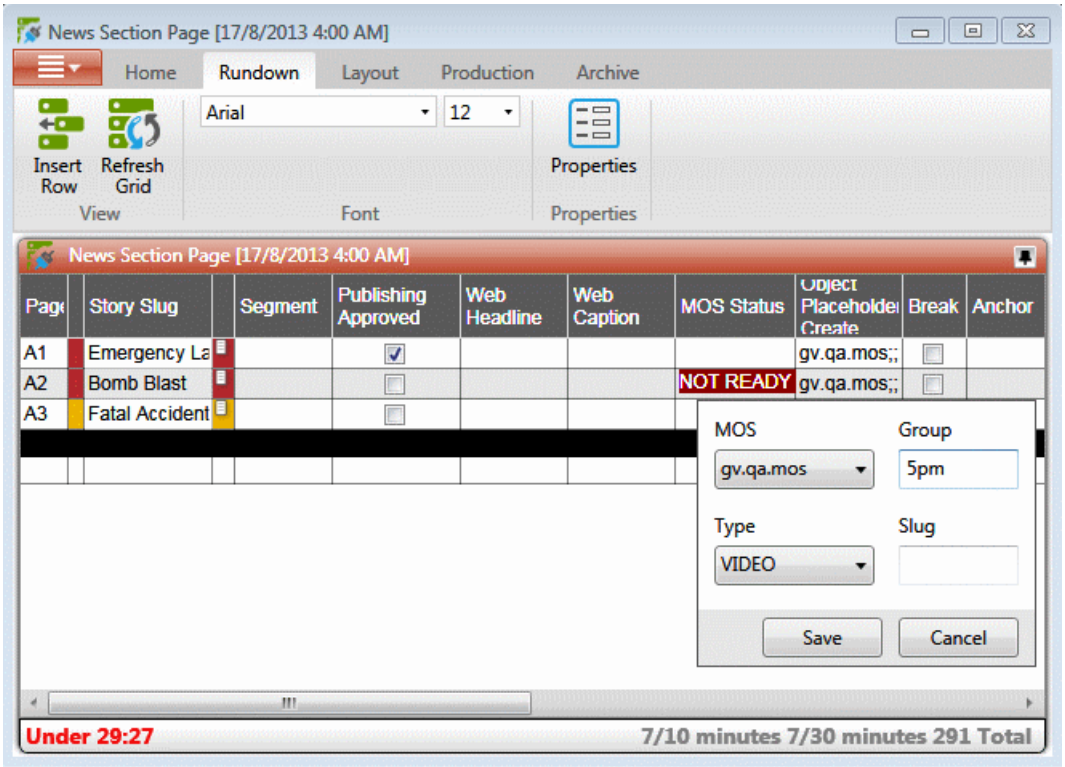
To link placeholders automatically, you need to enable the Auto Create feature in the ENPS MOS Configuration and add the Auto Create column to your ENPS rundown template.

1. Create a new rundown.

   Create a rundown as you normally would. See the ENPS documentation for details.
2. Create a new story slug in ENPS.
3. Click the **Object Placeholder Create** field, and select the MOS from the drop-down list.



4. To assign a category when you create the placeholder, select the Type from the drop-down list, and enter the Group name.



5. Click **Save**.

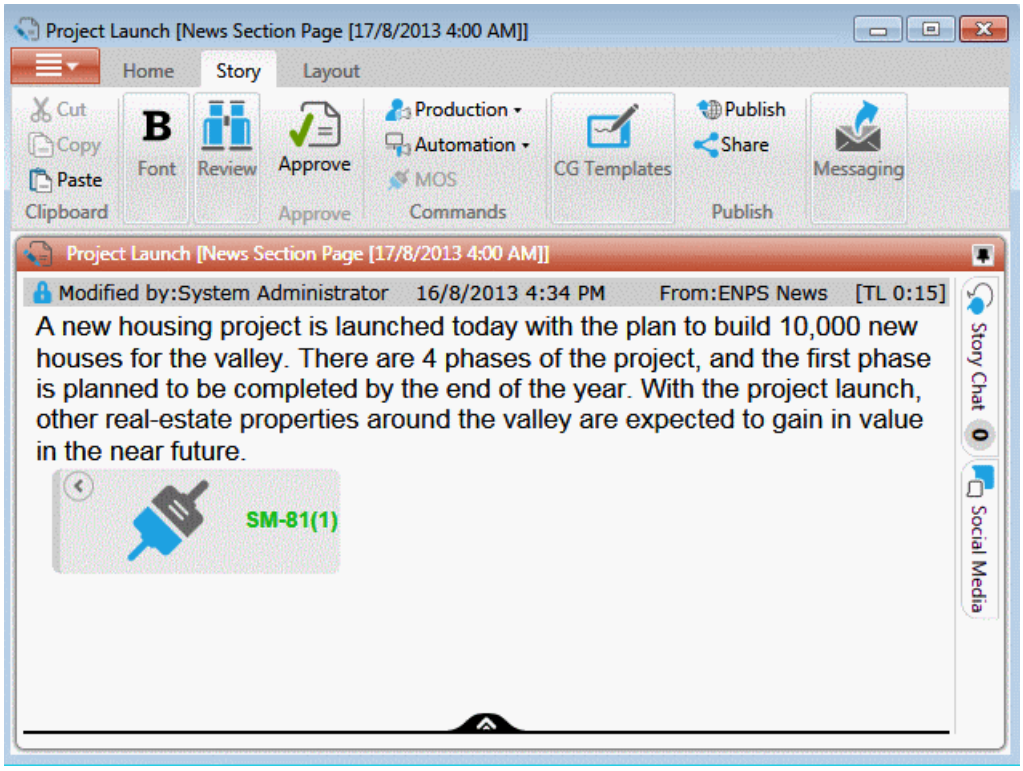
A new placeholder is created in the Assignment List of the GV STRATUS Plug-in and a MOS object is automatically linked and embedded into the script for this story.

Inserting placeholders manually into ENPS

As an alternative to using the ENPS Auto Create feature, you can manually create placeholders and add them to your story scripts.

1. Create a rundown as you normally would. See the ENPS documentation for details.
2. Create a new story in ENPS and open it.
3. Create a new placeholder using the Assignment List panel in the GV STRATUS Plug-in.

4. Drag the new placeholder from the Assignment List panel to the ENPS editing window.



The script within ENPS now shows an embedded MOS Object, which represents the on-air placeholder.

5. Save the script.

The placeholder is added to the ENPS rundown.

NOTE: You can also use this method to add an existing placeholder to your script.

Related Topics

Adding placeholders on page 1324

Inserting assets as MOS items into ENPS

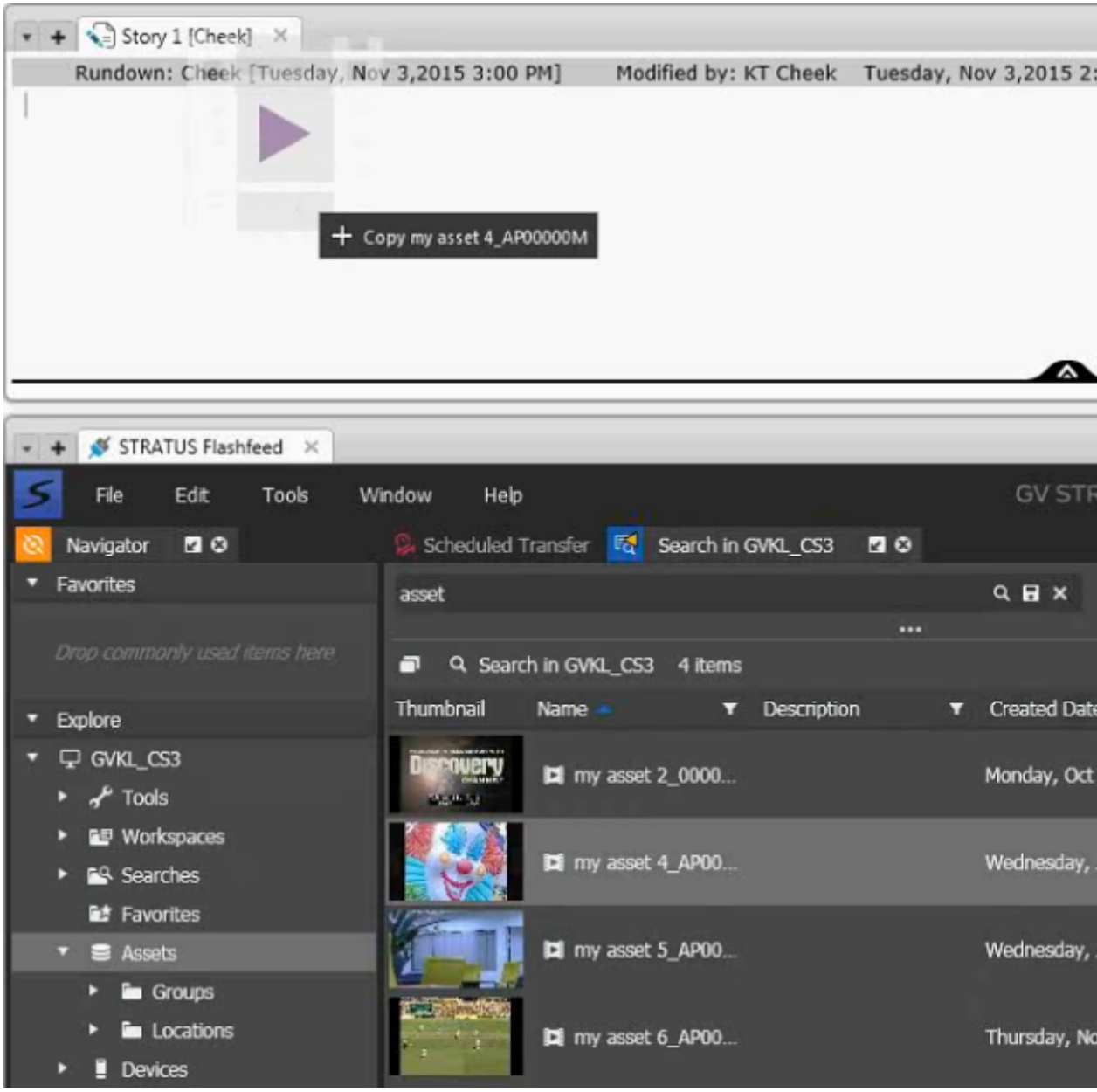
- The MOS ID must be set in **Applications | Rundown | XMOS** of GV STRATUS Control Panel and ENPS, in **ENPS | System Maintenance | MOS Configuration**.
- **ENPS** must be selected in **Applications | Rundown | XMOS | NCS Type** in GV STRATUS Control Panel if you are using ENPS version 8.2 and above.
- The **Asset Drag Content** setting must be set to **MOS Newsroom Item** in the User Preference settings of GV STRATUS application.

NOTE: Do not change this setting except under the supervision of qualified Grass Valley Support personnel. Extensive system configuration is required to achieve a working GV STRATUS system.

You can now insert GV STRATUS assets directly into your story scripts. If you are using the MOS item workflow, you must not use the linked placeholder workflow in GV STRATUS ActiveX panel at the same time. Both workflows are not supported simultaneously.

1. Create a rundown as you normally would. See the ENPS documentation for details.
2. Create a new story in ENPS and open it.
3. Launch the GV STRATUS ActiveX panel in ENPS.

4. Drag an asset from the Asset List or Search results window of GV STRATUS ActiveX panel into your ENPS story editing window.



The editing window within ENPS now shows an embedded MOS item, which represents the asset.

You can also drag and drop multiple assets into the ENPS story, if desired.

5. Save the story.
6. To preview the asset, double-click the MOS item.

   The asset displays in the Inspector of GV STRATUS ActiveX panel.

   You can trim the asset and change asset duration in the Inspector panel. However, you must re-drag the asset and drop it into the ENPS story again to update the duration of the embedded MOS item.

The asset is added as a MOS item in the ENPS story.

: Do not drag assets into ENPS if ALP and/or* GV STRATUS Rundown *is actively used.

Related Topics

Configuring User Preferences on page 1387
XMOS Server settings on page 390
Setting up GV STRATUS in ENPS on page 660

Assigning playout channels to clips in ENPS

1. Click the **MOS Channel** column for the story you want to assign.
2. Enter the channel name in the MOS Channels box and click **OK**.

   You must enter the channel label exactly as it was set up in GV STRATUS Rundown.

The story is assigned to that channel and appears on the “Assign” column of the GV STRATUS Rundown application.

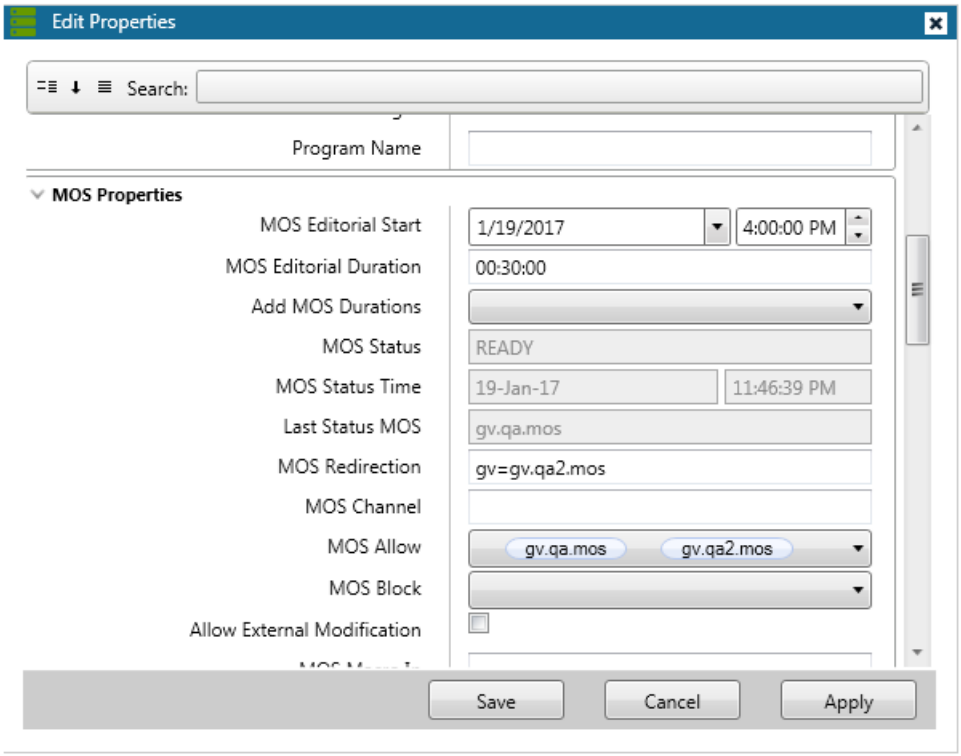
Configuring MOS Redirection workflow with ENPS

Using ENPS, you can enable the MOS Redirection workflow to automatically transfer media between different servers and locations.

1. Launch your ENPS client, and open a Rundown.

2. Click **Properties** on the ENPS toolbar.

   The Edit Properties window opens.

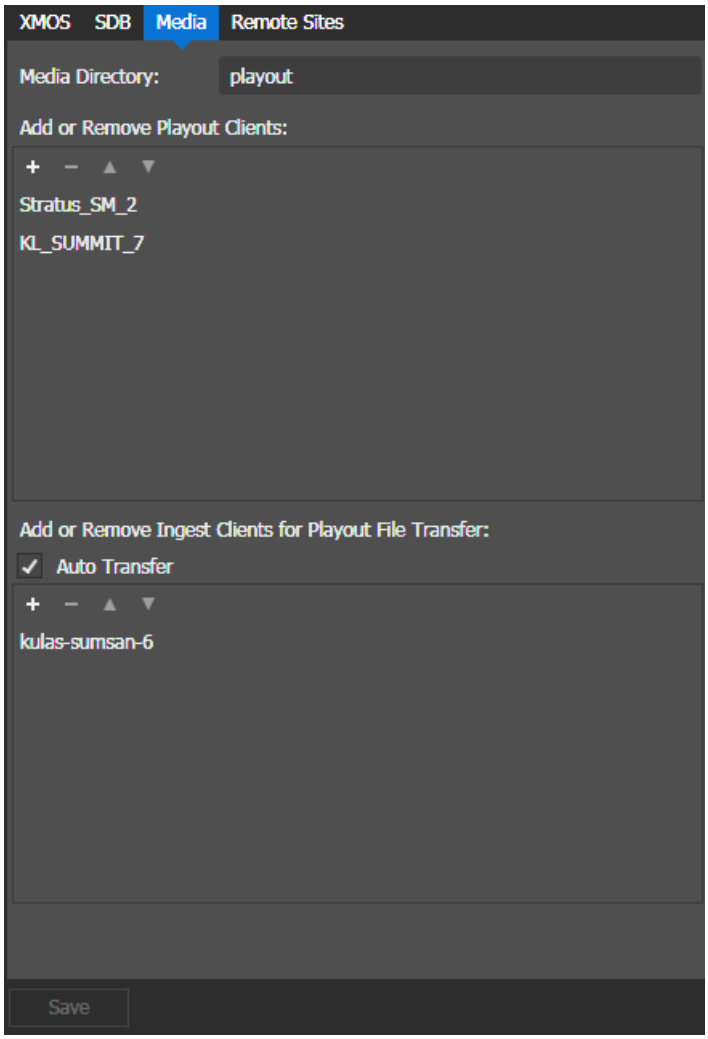


3. On the MOS Properties section, configure as follows:

MOS Redirection	Enter the following: **gv=MOS ID of destination system** (e.g., **gv=gv.qa2.mos**) ***NOTE: The setting must only be configured in lower case letters.***
MOS Allow	Enter MOS IDs of both origin and destination systems.

4. Click **Apply**, and **Save** to close the window.

5. Launch the GV STRATUS Control Panel and click **Applications | Rundown | Media**.



6. Select the **Auto Transfer** check box.
7. Click the **+** button to add destination servers for Playout File Transfer.

   The **Add Ingest Server** dialog opens.
8. Configure K2 server settings for the destination system and click **OK**.
9. Click **Save** to save the configuration.

When MOS Redirection is triggered and stories with linked placeholders containing media are moved from one location to another, ENPS automatically transfers the media contained in those stories. This workflow supports automatic transfer of media between servers within a single newsroom, or between multiple newsrooms and servers in different locations. For stories with unlinked placeholders, only the placeholder gets created at the other location.

Related Topics

Rundown Add/Modify Server settings on page 394

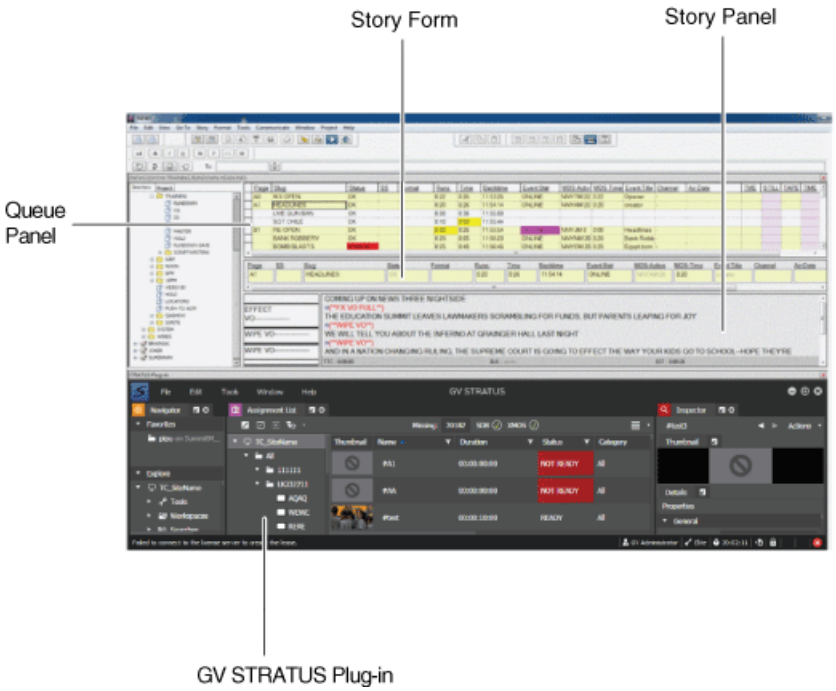
Using GV STRATUS with iNEWS

The Assignment List in the GV STRATUS ActiveX panel allows you to create placeholders for clips and link them to the accompanying story slug in the iNEWS rundown.

With the GV STRATUS panel available within iNEWS, you can easily insert placeholders into your story via drag and drop, and assign playout channels to clips.

To launch the panel, select **Tools | Plugins | STRATUS Plug-in**.

When you log on to the GV STRATUS system, the GV STRATUS application assigns GV STRATUS licenses and roles based on your user account credentials, as set by the system administrator in the GV STRATUS Control Panel application. If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins and assets that are part of your workflow. If GV STRATUS metadata access control is enforced, your credentials must give you adequate permissions on metadata fields that are part of your workflow. Your credentials must also give you access to all your K2 systems.



Related Topics

Logging on on page 953
Logging off of GV STRATUS from within a NCS on page 1369

Creating placeholders automatically in iNEWS

You can create stories, insert placeholders into those stories, and the placeholders are automatically populated into the Assignment List of GV STRATUS.

1. Create a new rundown.

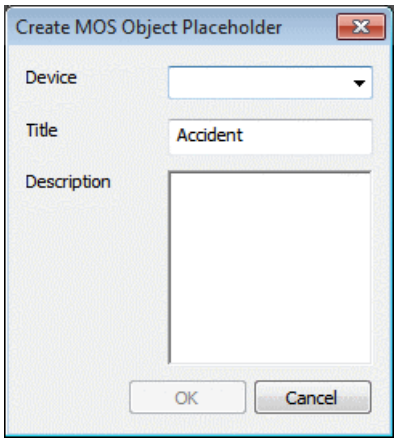
   Create a rundown as you normally would. See the iNEWS documentation for details.

2. Create a new story in your rundown.

   The Story panel opens.

3. Enter the title of the story in the Slug property field.
4. Right-click on any text property field and select **Insert Placeholder**.

   The **Create MOS Object Placeholder** dialog box opens.



5. Select your **MOS ID** from the **Device** drop-down list.
6. Click **OK**.

   The **Event Stat** column of the story shows the status as **OFFLINE**.

A placeholder is automatically created with the same name as the story in the Assignment List of GV STRATUS.

If an asset is linked to the placeholder, the **Event Stat** column of the story will change to **ONLINE**.

Creating and linking placeholders manually in iNEWS

1. Create a new rundown.

   Create a rundown as you normally would. See the iNEWS documentation for details.

2. Create a new story in iNEWS.

3. Create a new placeholder in the Assignment List panel of the GV STRATUS Plug-in.
4. Verify that the new story slug is highlighted in the Queue Panel, then drag the new placeholder from the Assignment List and drop it into the Story Form window.

   NOTE: You can also use this method to add an existing placeholder to your story.

5. Click on a different line in the Queue Panel to save your changes.

The placeholder links with the story and the clip name displays in the iNEWS Queue Panel.

Related Topics

Adding placeholders on page 1324

Assigning playout channels to clips in iNEWS

1. Select the slug you want to assign and right-click the **Ch** box.
2. Choose **Assign Channel**.
3. Enter the channel name and click **OK**.

   You must enter the channel label exactly as it was set up in GV STRATUS Rundown.

4. Save the slug.

The story is assigned to that channel and appears in the GV STRATUS Rundown application in the "Assign" column.

Setting embargo status to stories in iNEWS

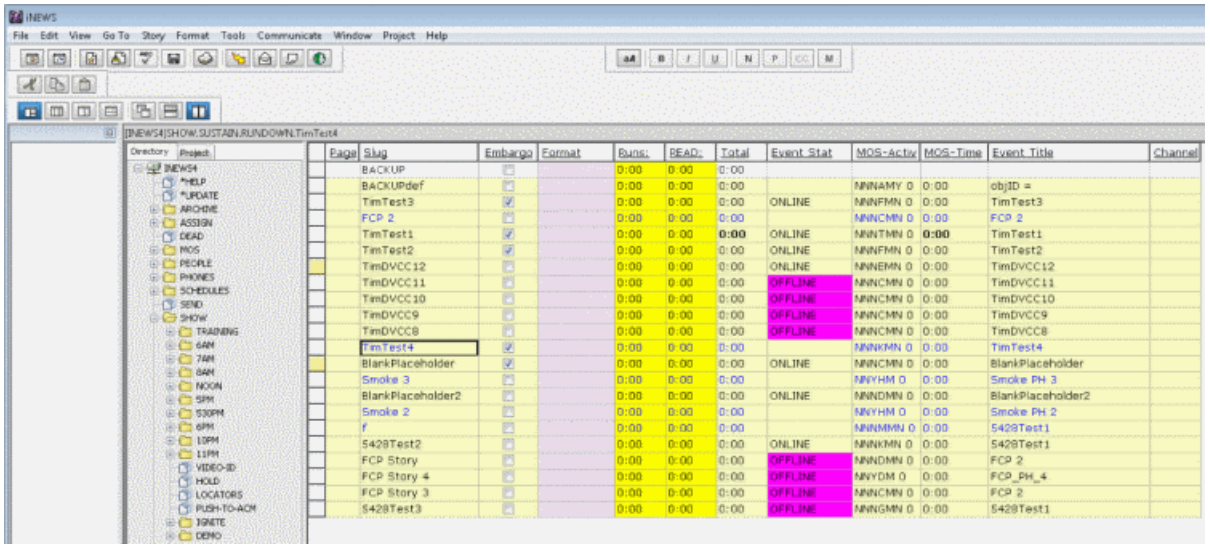
Prerequisites:

- The GPIO connection is configured between the GV STRATUS Rundown client, switcher, and streaming encoder.
- The General Purpose Output is configured for the Embargo status in the **Tools | Options | GPIO Configuration** of the GV STRATUS Rundown application.
- The **Embargo** column is configured in the iNEWS application.

Embargo status can be set to specific stories in iNEWS to prevent automatic broadcast via the internet. This is due to restrictions from news providers that some media contents are only for televised broadcasts.

1. Create a new story in iNEWS.
2. Drag a ready placeholder from the Assignment List of the GV STRATUS panel to the Story Form window.

3. Select the checkbox in the **Embargo** column for the story.



4. Click on a different line in the Queue Panel to save your changes.

When the clip is cued in the GV STRATUS Rundown channel, the **Embargo** status is sampled. Then, the embargo GPO is set to high when the clip is played.

After the **Embargo** GPO is triggered, the streaming encoder prevents the clip's broadcast via the internet. All other contents without the **Embargo** status are automatically uploaded to the news station's website.

Related Topics

Configuring General Purpose Input and Output on page 1513

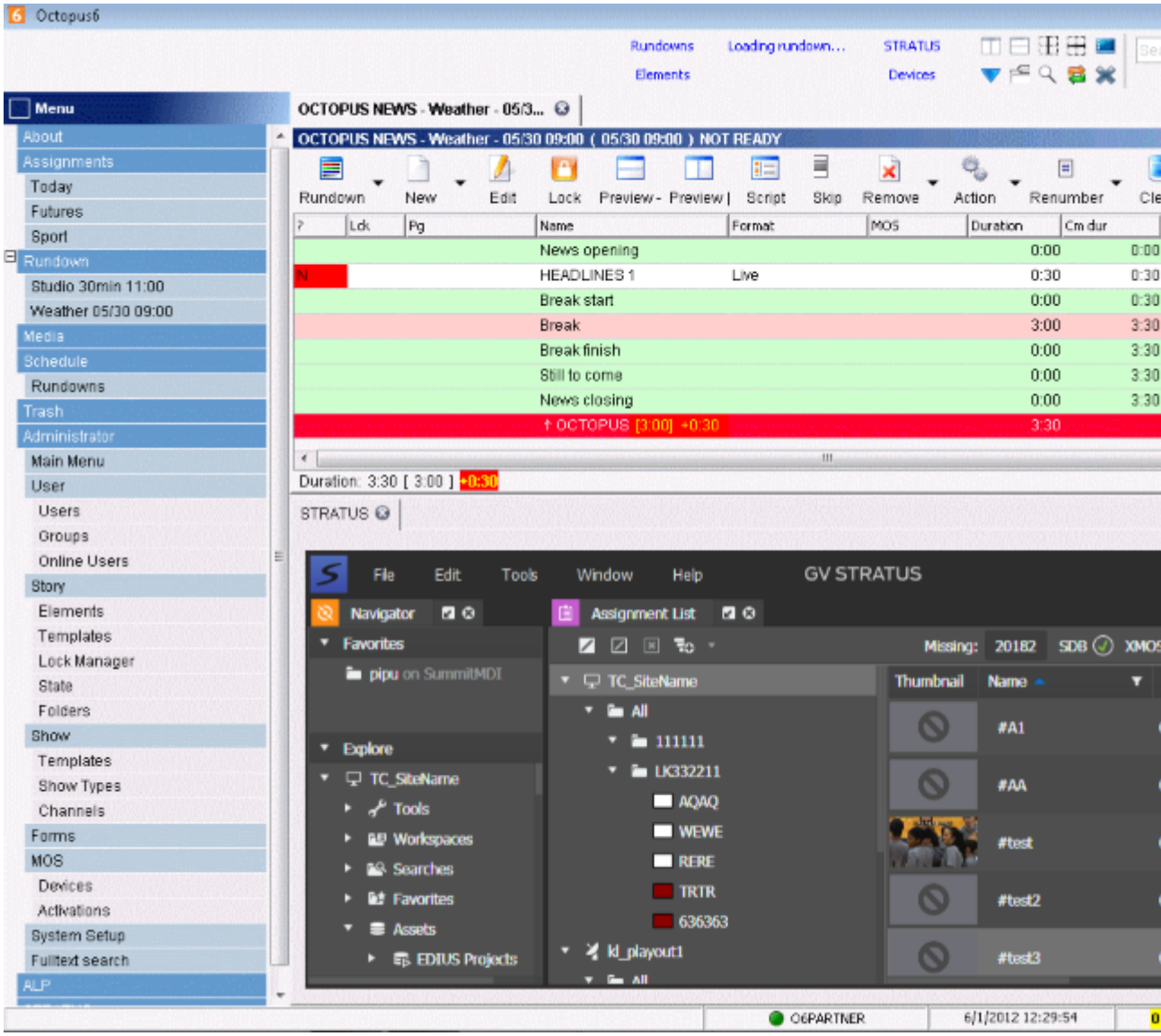
Using GV STRATUS with Octopus

The GV STRATUS ActiveX panel lets you create placeholders for clips and insert them into the accompanying story slug in the Octopus rundown.

You can create the placeholders and insert them manually into your rundown or use the auto-create feature to create and insert the placeholder automatically.

To launch the GV STRATUS panel within Octopus, click **STRATUS** on the toolbar.

When you log on to the GV STRATUS system, the GV STRATUS application assigns GV STRATUS licenses and roles based on your user account credentials, as set by the system administrator in the GV STRATUS Control Panel application. If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins and assets that are part of your workflow. If GV STRATUS metadata access control is enforced, your credentials must give you adequate permissions on metadata fields that are part of your workflow. Your credentials must also give you access to all your K2 systems.



Related Topics

Logging on on page 953
Logging off of GV STRATUS from within a NCS on page 1369

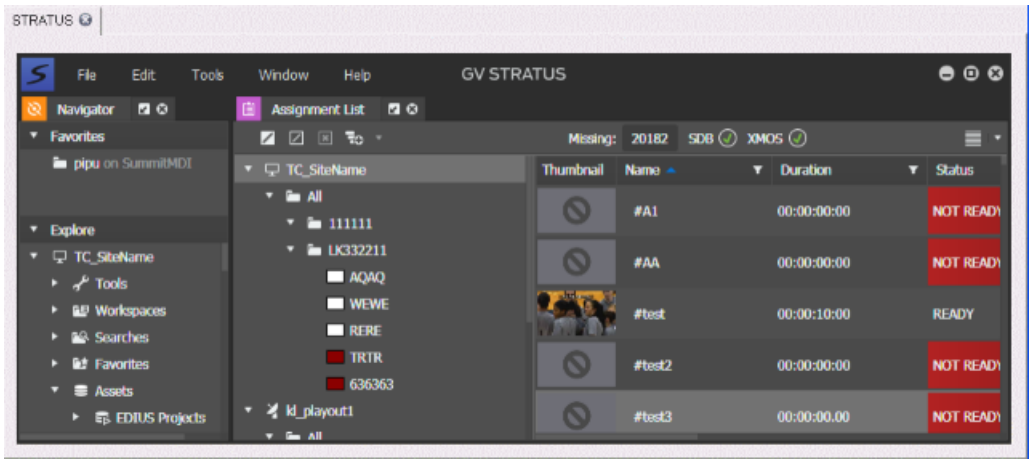
Creating placeholders automatically in Octopus

With Octopus, you can create placeholders automatically using the Auto-create feature.

1. Create a new story in Octopus.
2. Open the story.
3. Click the **Edit** button on the toolbar.
4. Right-click on the **NOT READY** status, select **MOS | Auto Create on [the name of your MOS]**.

5. Click the **Save** button on the toolbar.
6. Launch the GV STRATUS ActiveX Plug-in.

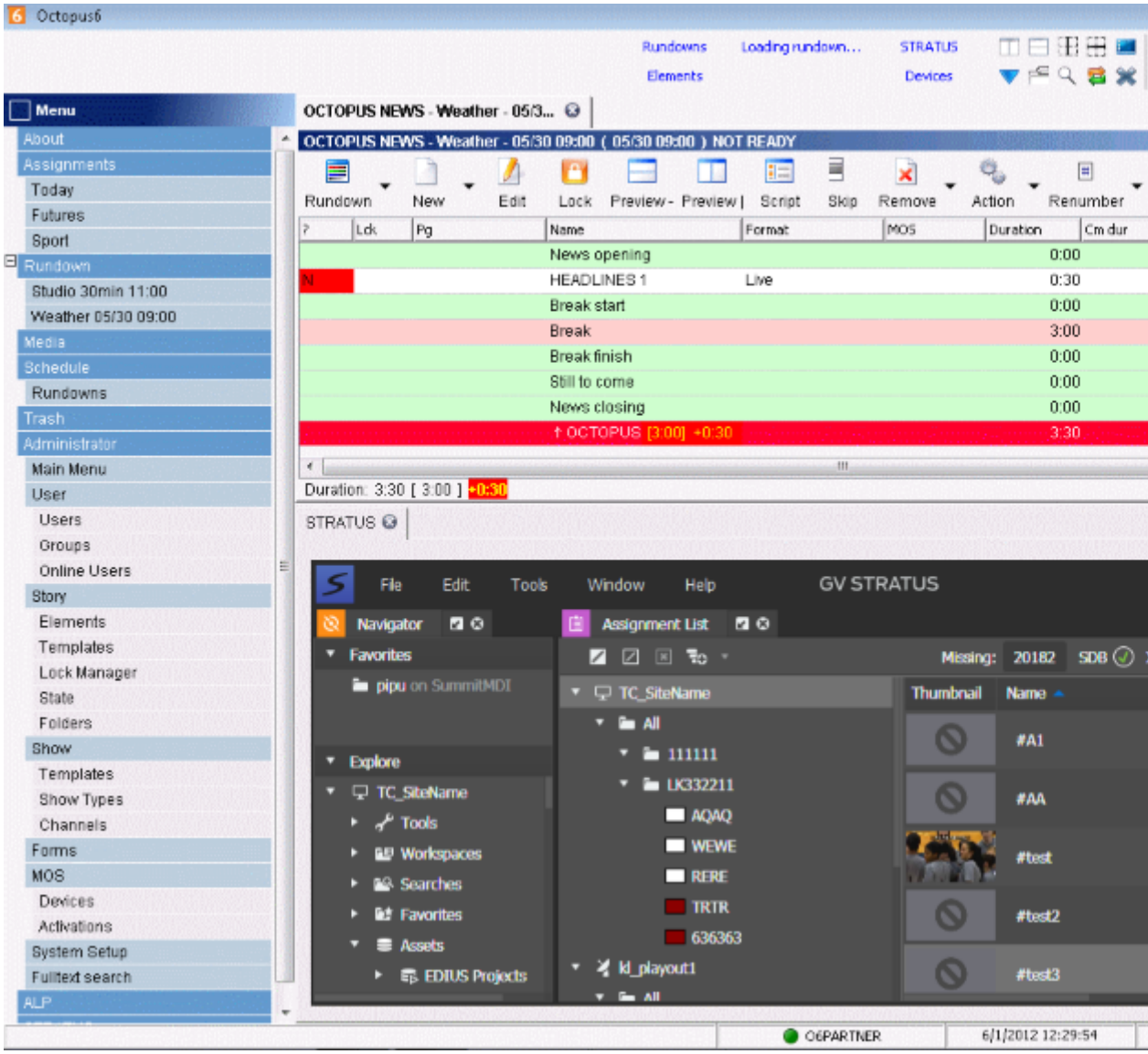
   The newly created placeholder appears on the Assignment List of GV STRATUS ActiveX Plug-in.



Inserting placeholders manually in Octopus

With Octopus, you can manually create placeholders and insert them into the Assignment List of GV STRATUS ActiveX Plug-in.

1. Split the Octopus window so you can see the Rundown View and the GV STRATUS ActiveX Plug-in.



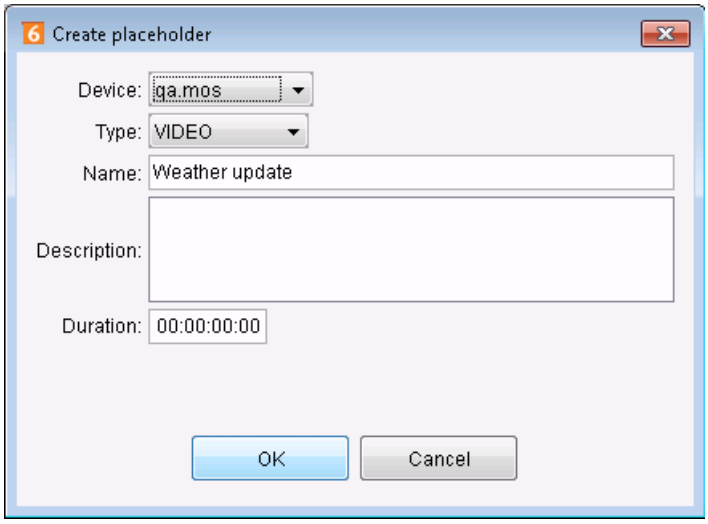
2. Double-click the story that you want to insert a placeholder into.

   The story displays on the Octopus.

3. Click the **Edit** button on the toolbar.

4. Right click on the **NOT READY** status, select **MOS | Create on [the name of your MOS]**.

   The create placeholder dialog box displays.



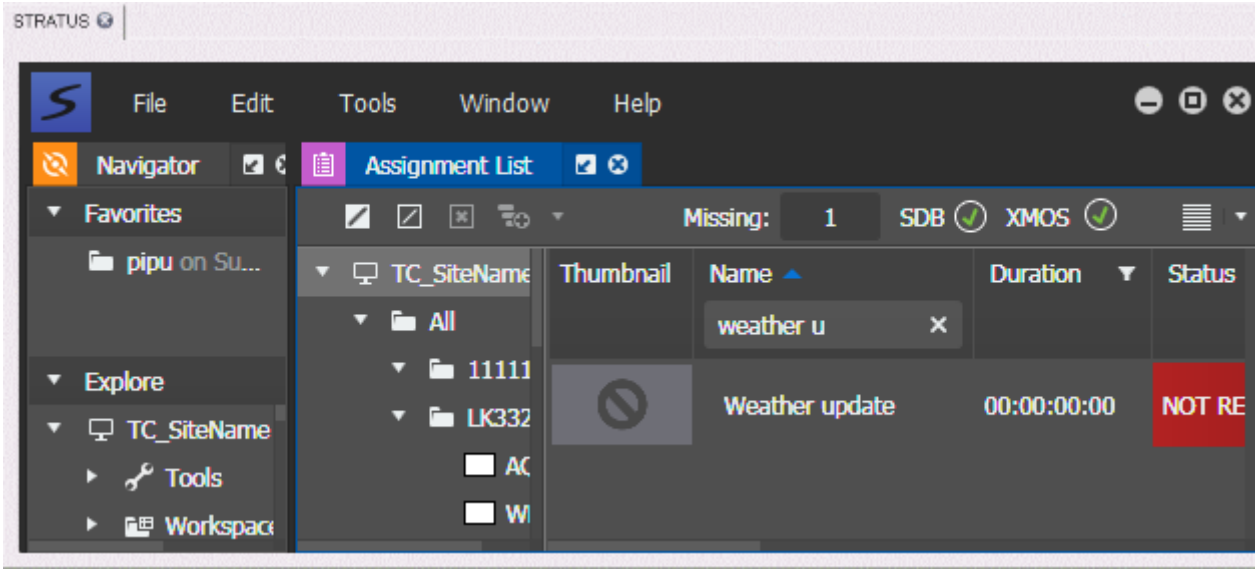
5. Select your MOS for the Device and select **VIDEO** for the Type.
6. Enter the name and duration of the placeholder.

   Enter the description, if desired.

7. Click **OK**.

8. Click the **Save** button on the toolbar.

   The placeholder appears on the Assignment List of GV STRATUS ActiveX Plug-in.



Related Topics

Adding placeholders on page 1324

Linking clips manually in Octopus

- If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, and metadata.
- In order to link to a placeholder, you must be assigned with the **Rename Asset Rights** role and write permission for the **Name** property in Metadata section of GV STRATUS Control Panel.

You can also link placeholders from the GV STRATUS ActiveX Plug-in and insert clips into your rundown manually.

1. Open the story that you want to link clips into.

   The story displays on the Octopus.

2. Click the **Edit** button on the toolbar.
3. Right click on the **NOT READY** status, select **Launch STRATUS**.

   The GV STRATUS ActiveX Plug-in displays.

   NOTE: Launching multiple GV STRATUS ActiveX Plug-ins might cause the first launched window to be blank. Click anywhere on the blank window to refocus the display of GV STRATUS ActiveX Plug-in.

4. Select a placeholder on the Assignment List of GV STRATUS ActiveX Plug-in, and click **Use** on the Octopus story.

5. Click the **Save** button on the toolbar.

   The placeholder links with the story.

6. On the GV STRATUS ActiveX Plug-in, select an asset and link it to the placeholder.

   The clip links to the story in Octopus. You can see the Clip ID in the Octopus story is the same as the Clip ID in the Assignment List of GV STRATUS ActiveX Plug-in.

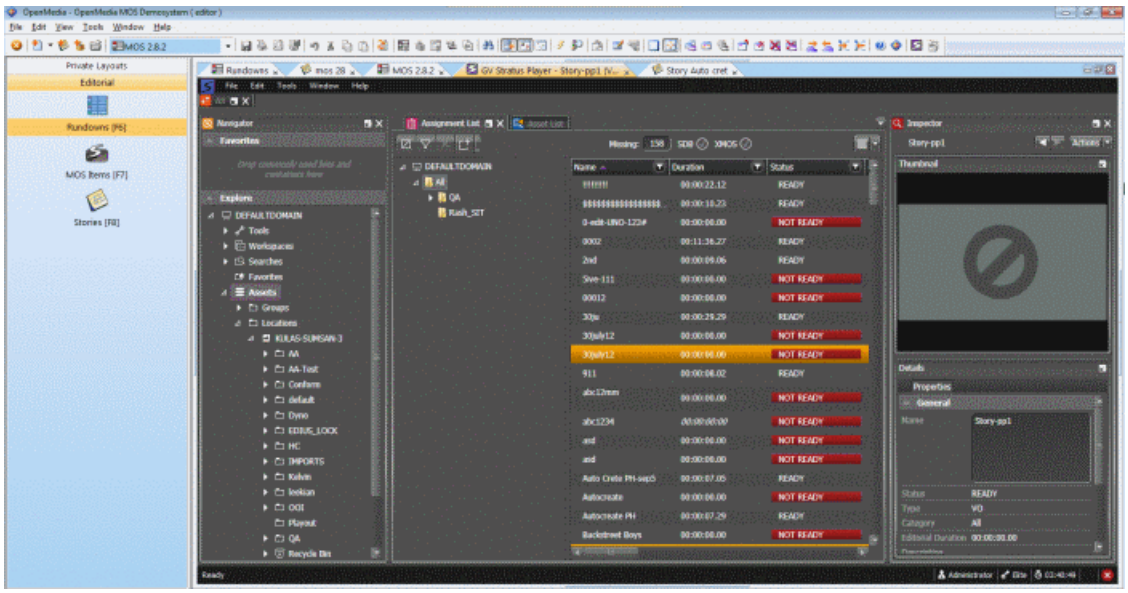
Using GV STRATUS with OpenMedia

The GV STRATUS ActiveX panel lets you create placeholders for clips and insert them into the accompanying story slug in the OpenMedia rundown.

You can create the placeholders and insert them manually into your rundown or use the auto-create feature to create and insert the placeholder automatically.

If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets, and metadata that do not have read permissions are not visible. Markers and segments permissions must be set to **Allow** in order to create, update, or delete markers and segments.

To launch the GV STRATUS panel within OpenMedia, click the **GV STRATUS** button on the toolbar.



Related Topics

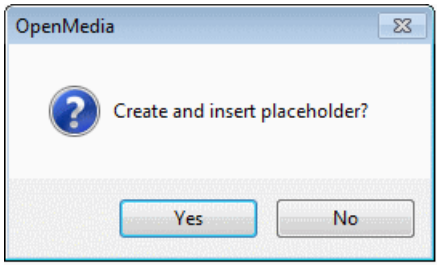
Logging on on page 953
Logging off of GV STRATUS from within a NCS on page 1369

Creating placeholders automatically in OpenMedia

You can create placeholders in OpenMedia and they are automatically populated into the Assignment List of GV STRATUS.

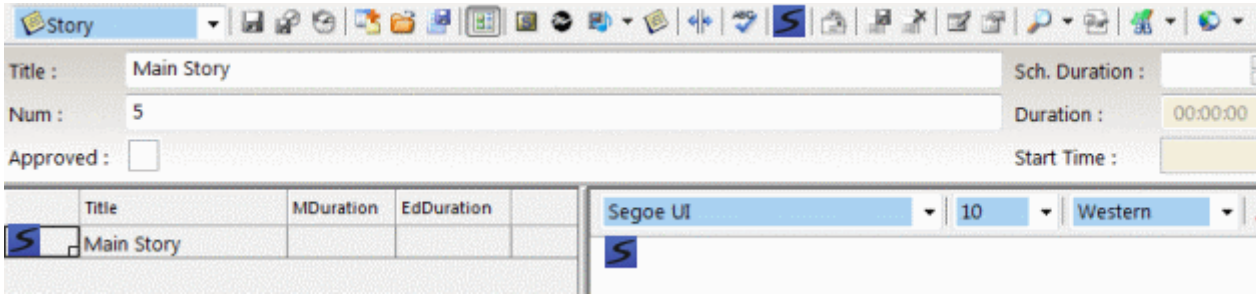
1. Create a new rundown. Create a rundown as you normally would. See the OpenMedia documentation for details.
2. Create a new story in your rundown.
3. Double-click the icon on your rundown to open the new story.
4. Click the **Create Placeholder** button on the toolbar of the story.

   A dialog box opens for you to confirm the placeholder creation.



5. Click **Yes**.

   A placeholder is created with the same name as the story.

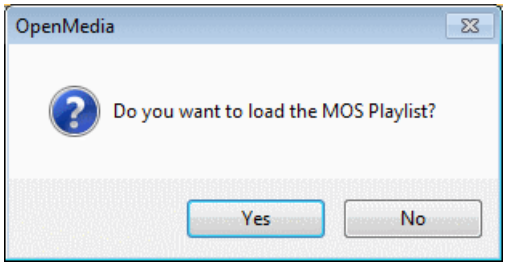


Loading rundowns in OpenMedia

You can view the newly created placeholder in the GV STRATUS Plug-in by loading your rundown.

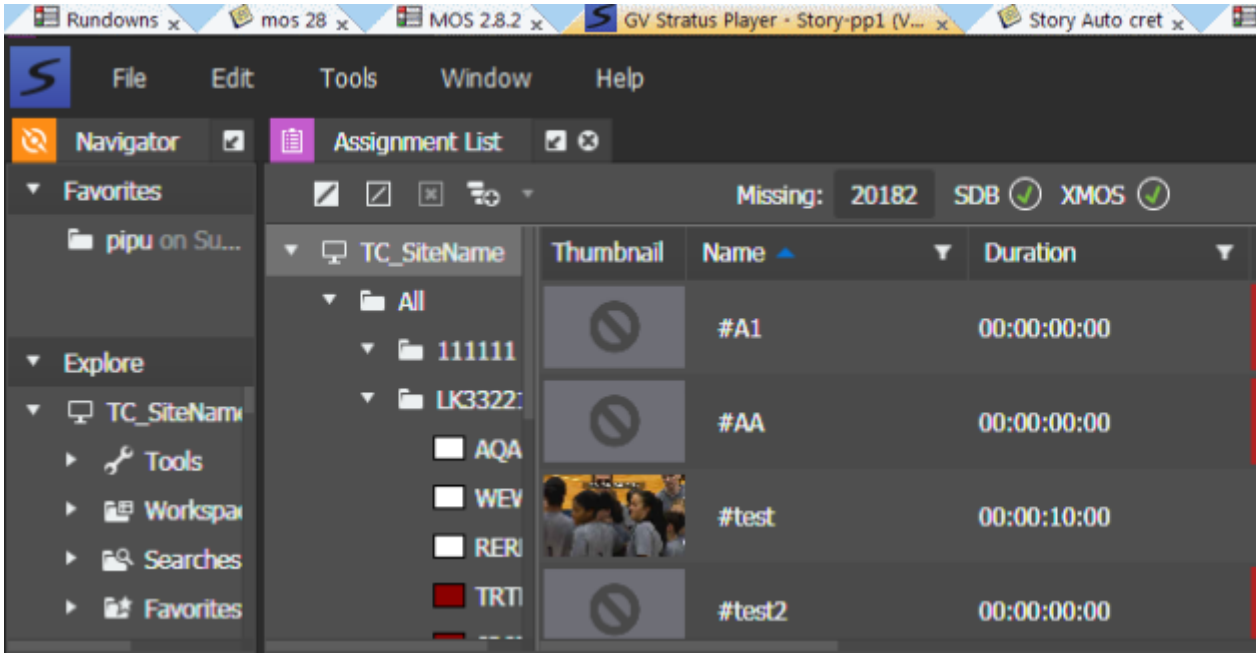
1. In OpenMedia, go to your rundown and click the **Load MOS Playlist** button on the toolbar.

   A dialog box opens for you to confirm the load of MOS playlist.



2. Click **Yes**.

   The rundown appears on the Assignment List of GV STRATUS Plug-in.



Inserting placeholders manually in OpenMedia

You can create placeholders and add them manually into your story in OpenMedia.

1. Double-click the icon on your rundown to open your story.
2. Create a new placeholder using the Assignment List in the GV STRATUS panel.

3. Drag the new placeholder from the GV STRATUS panel and drop it into your story.

   The placeholder is added to the story.

   NOTE: You can also use this step to add existing placeholders to your story.

4. Click **Save**.

Related Topics

Adding placeholders on page 1324

Linking and sending assets for playback in OpenMedia

- If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, and metadata.
- In order to link to a placeholder, you must be assigned with the **Rename Asset Rights** role and write permission for the **Name** property in Metadata section of GV STRATUS Control Panel.

You can link an asset to your placeholder, and send it to the playout server with GV STRATUS panel in OpenMedia.

1. Select an asset in the Asset List of the GV STRATUS panel.
2. Right-click on the asset and select **Send**. (**F11**)

   The Send Destinations dialog appears.

3. Click a check box to select the send destination.
4. In the **Link To Placeholder** tab, select the placeholder that you inserted in the OpenMedia story.
5. If you have adequate permissions, click **Security** and configure security options as desired, then click **OK**.

   The **Security** dialog box is available only if you have the role of Security Manager or you are the Owner.

6. Click **Send**.

   The asset links to your placeholder and copies into your selected destination.

The placeholder status changed to **READY**, and the duration is updated in the Assignment List of the GV STRATUS panel and in the rundown of OpenMedia.

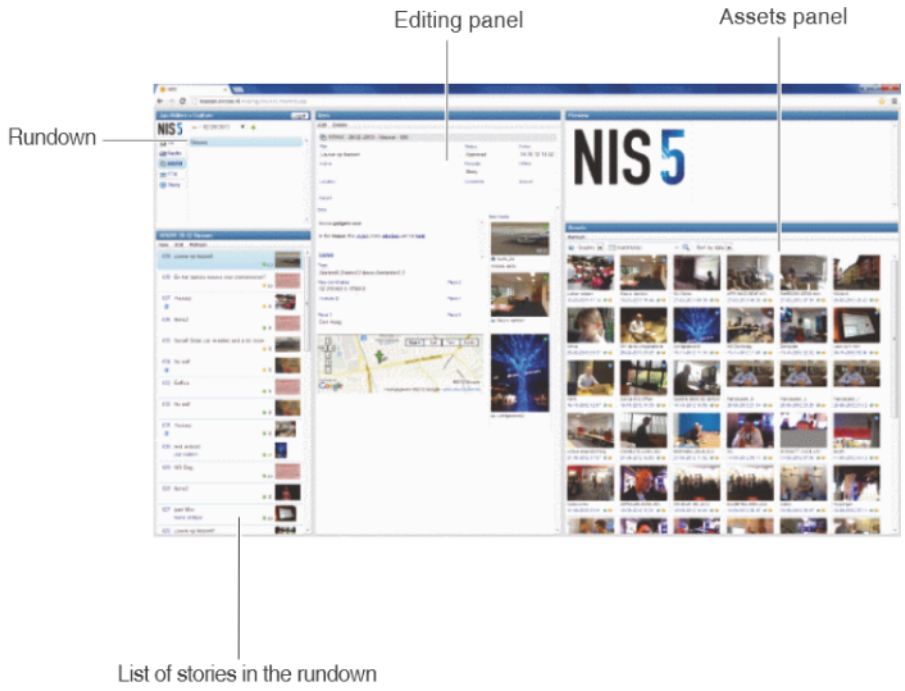
Using GV STRATUS with NIS5

The NIS5 (Newsroom Information System) web client allows you to create stories, placeholders, and link placeholders with clips in the GV STRATUS application.

You can create and insert placeholders automatically into your story in the NIS5 web client, or you can insert placeholders manually into your story via drag and drop from the GV STRATUS application.

If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets, and metadata that do not have read permissions are not visible. Markers and segments permissions must be set to **Allow** in order to create, update, or delete markers and segments.

The NIS5 workflow with GV STRATUS application is only supported via the Google Chrome™ web browser.



Creating placeholders automatically in NIS5

You can create stories, insert placeholders into those stories, and the placeholders are automatically populated into the Assignment List of GV STRATUS application.

1. Create a new rundown.

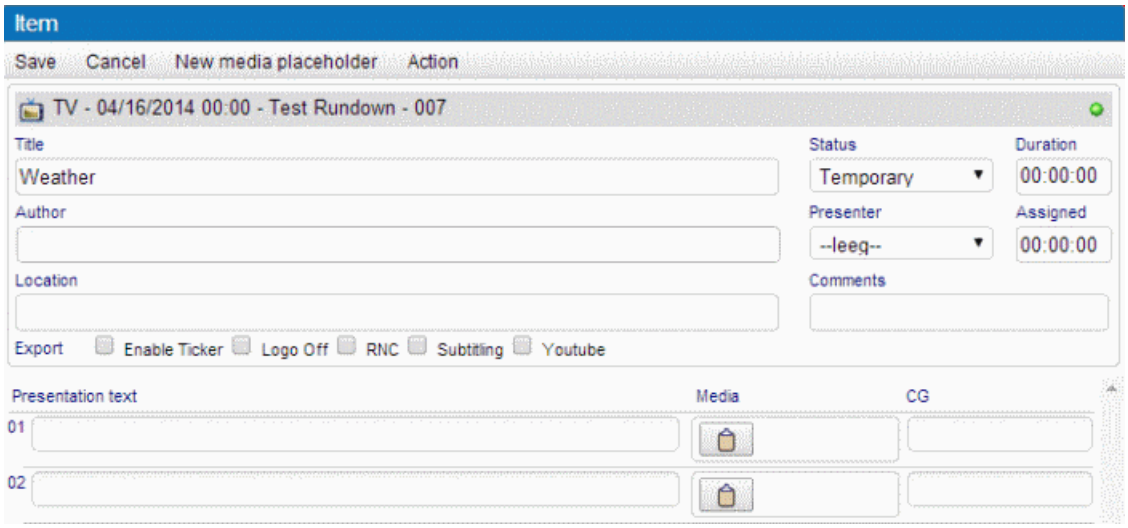
   Create a rundown as you normally would. See the NIS5 documentation for details.

2. Click **New** to create a new story in your rundown.

3. Select one of the following for the location of your story in the rundown:

   - Insert before
   - Insert after

   The story appears in the list of stories in the rundown and in the Editing panel.

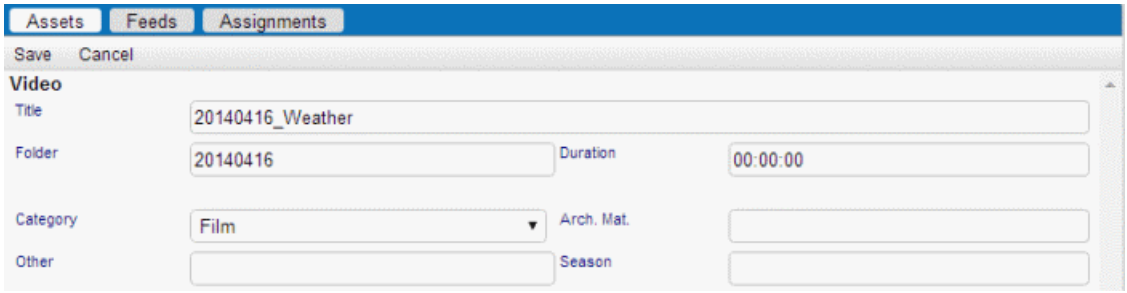


4. Enter the Title, Author, Location, and Presentation text of the story.

   The status of the story is **Temporary** by default. You can change the status of the story if desired.

5. To create a placeholder, click the **New media placeholder** button.

   The Assets panel loads the placeholder properties.

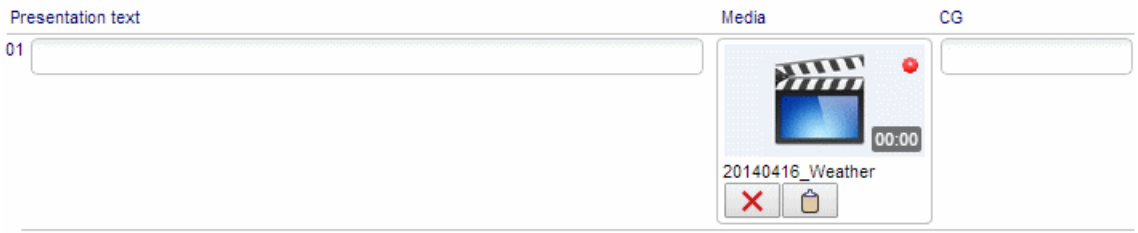


   The title of the placeholder is set to rundown and story name by default. However, you can still rename the placeholder if desired.

6. Click **Save** to save the placeholder.

   The placeholder appears in the Assets panel of the NIS5 web client.

7. Drag the placeholder from the Assets panel and drop it into the **Media** column of your story.

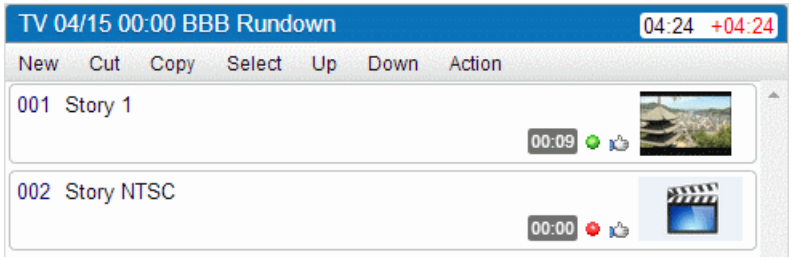


   The red dot indicates the status of the placeholder as **NOT READY**.

8. Click **Save** to save the story.

The placeholder created in the NIS5 web client is automatically populated in the Assignment List of GV STRATUS application.

If an asset is linked to the placeholder in GV STRATUS application, the red dot on the story turns to green to indicate the placeholder status as **READY**. The story duration is also updated after an asset in linked to the placeholder in the story.

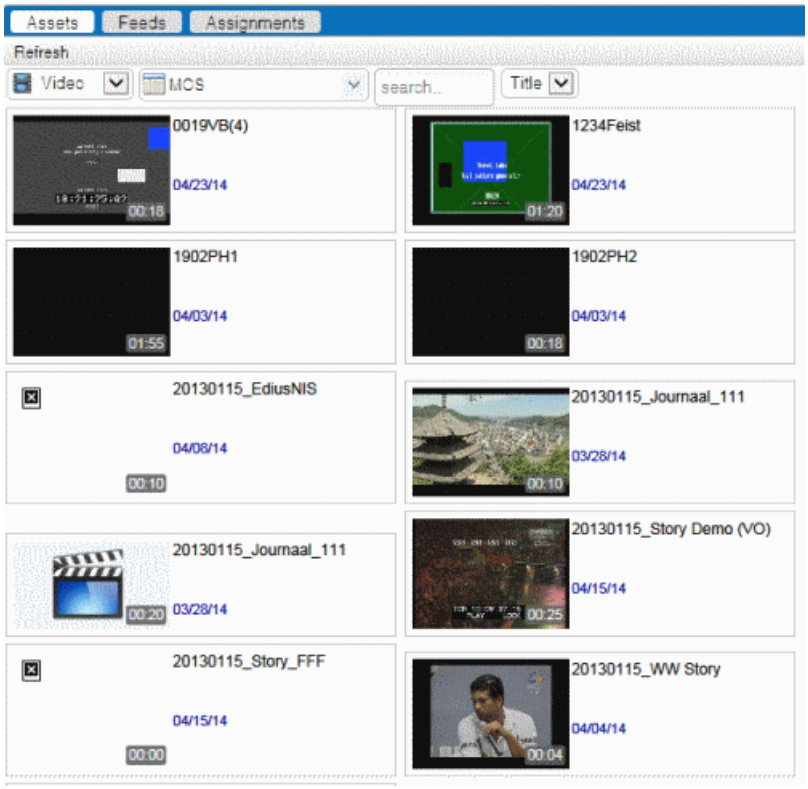


Inserting placeholders manually in NIS5

1. Create a new placeholder in the Assignment List panel of the GV STRATUS application.

   You can also use an existing placeholder in the Assignment List if desired.

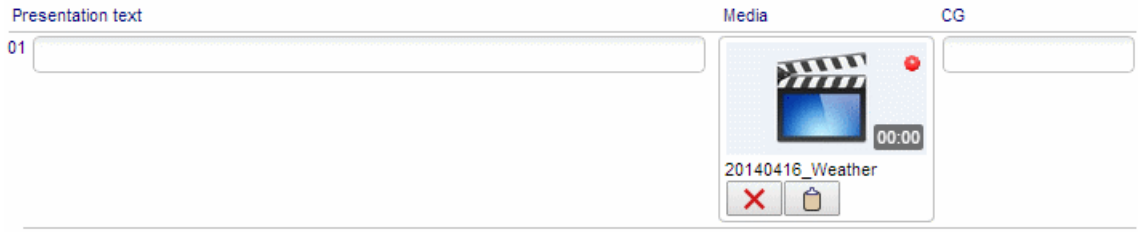
2. In the Assets panel of the NIS5 web client, select **Video** and **MOS** from the drop-down lists.



All placeholders from the Assignment List in GV STRATUS application appear in the Assets panel of the NIS5 web client.

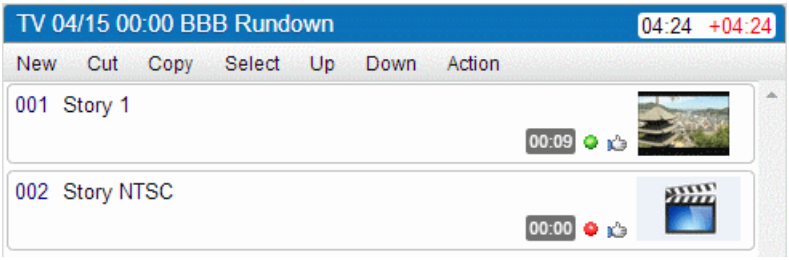
3. Open a story in the Editing panel of the NIS5 web client.
4. Drag a placeholder from the Assets panel and drop it into the **Media** column of your story.

   The placeholder is inserted into the story.



5. Click **Save** to save the story.

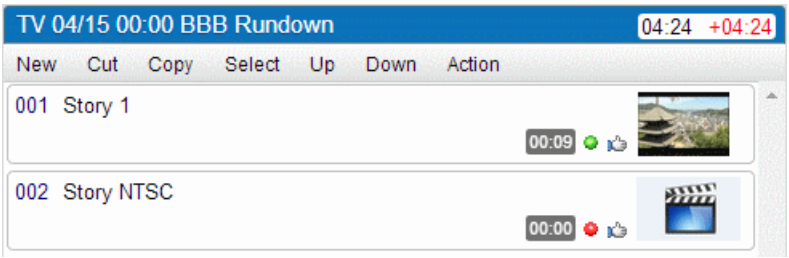
If an asset is linked to the placeholder in GV STRATUS application, the red dot on the story turns to green to indicate the placeholder status as **READY**. The story duration is also updated after an asset in linked to the placeholder in the story.



Viewing GV STRATUS assets in NIS5

You can view GV STRATUS assets that have been linked to your stories in the NIS5 web client.

1. Open your rundown to view the list of stories in the rundown.



2. Click on a story that is linked to a **READY** placeholder.

   The story opens.

3. Click on the asset in the **Media** column.

   The asset displays in the **Preview** panel.

4. Click the **Play** button to view the asset.

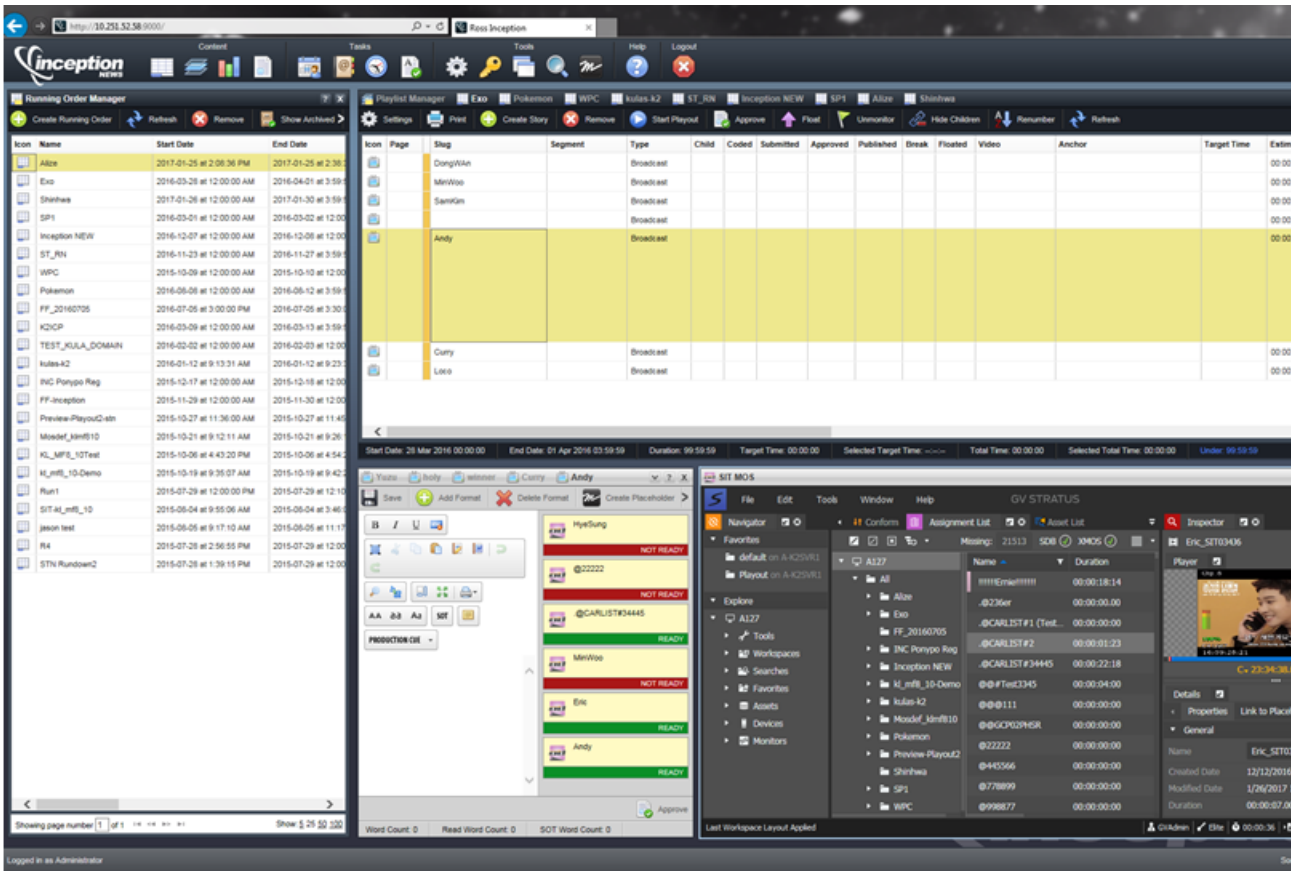
   Navigate through the asset using the appropriate transport controls.

Using GV STRATUS with Inception

The GV STRATUS workflow allows you to create placeholders for clips and insert them into the accompanying story slug in the Inception rundown.

You can create the placeholders and insert them manually into your rundown or use the auto-create feature to create and insert the placeholder automatically.

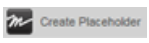
If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets, and metadata that do not have read permissions are not visible. Markers and segments permissions must be set to **Allow** in order to create, update, or delete markers and segments.



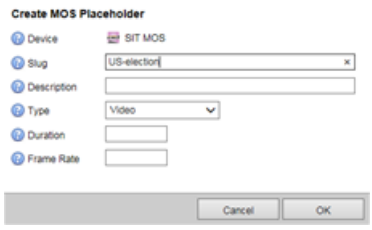
Creating placeholders automatically in Inception

You can create placeholders within Inception and they are automatically populated into the Assignment List of GV STRATUS.

1. Create a new rundown as you normally would. See the Inception documentation for details.
2. Create a new story in your rundown.

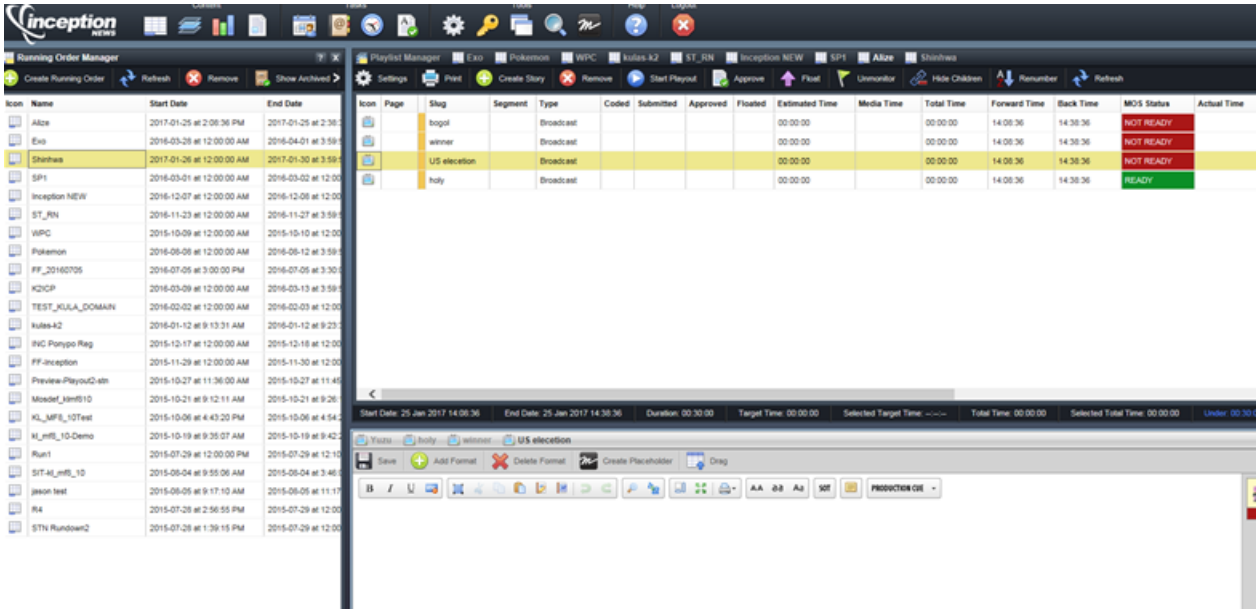
   The story opens in a new window.
3. Click the **Create MOS Placeholder** icon  on the toolbar of the story.
4. Select the MOS device configured for GV STRATUS operation.

   The **Create MOS Placeholder** dialog opens.

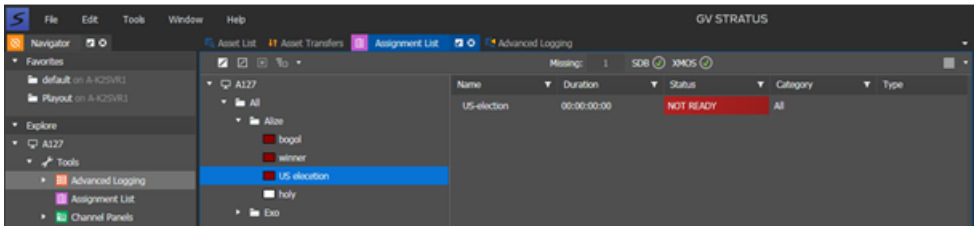


5. Enter the Slug name and click **OK**.

   A placeholder is created in the Inception story.



The same placeholder is also automatically created in the Assignment List of GV STRATUS ActiveX Plug-in.



You can double-click the placeholder to view it in the Inspector within GV STRATUS ActiveX Plug-in.

NOTE: With Inception version 11.0, double-clicking placeholders from Inception may not load in the Inspector automatically (in the case where launching the GV STRATUS ActiveX from fresh or re-launching the GV STRATUS ActiveX again after exiting/closing GV STRATUS ActiveX). You have to double-click the placeholder again to view it in the Inspector after GV STRATUS ActiveX is launched.

Inserting placeholders manually into Inception

You can create placeholders and add them manually into your stories in Inception.

1. Double-click the slug on your rundown to open your story.
2. Create a new placeholder using the Assignment List in the GV STRATUS ActiveX panel.

3. Drag the new placeholder from the GV STRATUS ActiveX panel and drop it into your story.

   The placeholder is added to the story.

   NOTE: You can also use this step to add existing placeholders to your story.

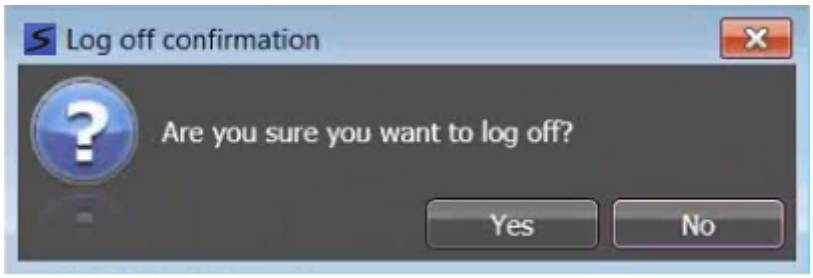
4. Click **Save**.

Logging off of GV STRATUS from within a NCS

When using GV STRATUS within ENPS, iNEWS, Octopus, and OpenMedia Newsroom Computer System applications, you can log off of GV STRATUS and log back on as a different user without shutting down the NCS application.

1. On the GV STRATUS ActiveX panel, select **File | Log Off**.

   The **Log off confirmation** dialog box opens.



2. Click **Yes**.

   The GV STRATUS ActiveX panel displays **Logging off GV STRATUS ActiveX control**.

   Then the **Log on to GV STRATUS** dialog box displays.

3. Enter the user credential if you want to log on as another user.

Related Topics

Logging on on page 953

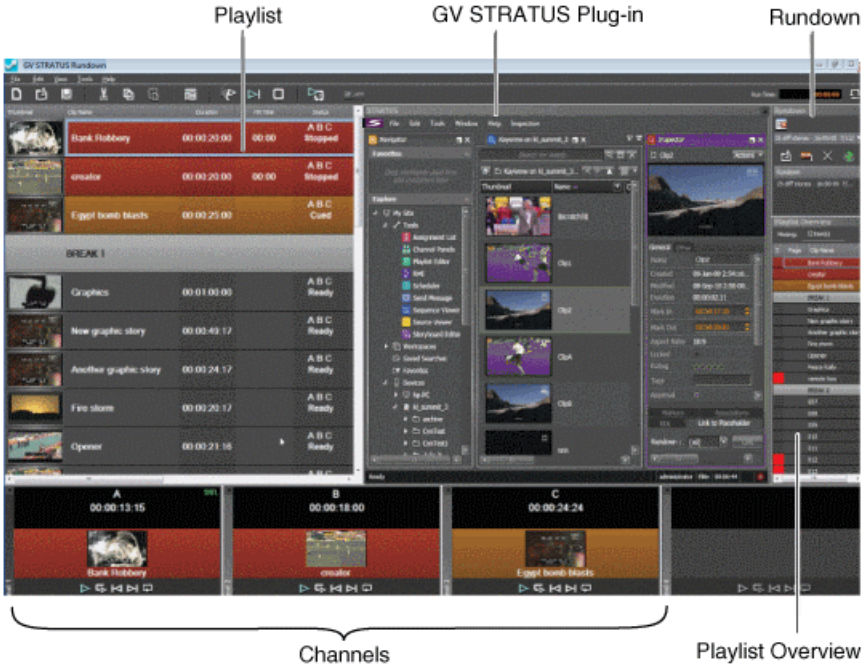
Using the GV STRATUS application in GV STRATUS Rundown

You can launch the GV STRATUS application as an ActiveX panel within the GV STRATUS Rundown application. This allows you to use all GV STRATUS tools and GV STRATUS Rundown to consolidate your entire operation including playback into one workspace.

With GV STRATUS within the GV STRATUS Rundown application, you can easily drag clips from Asset List into GV STRATUS Rundown's playlist. In addition, the Assignment List lets you create a placeholder for a clip and link it into the accompanying story in the NCS rundown. You can also assign channels for clips via the NCS for playout.

If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets, and metadata that do not have read permissions are not visible. Markers and segments permissions must be set to **Allow** in order to create, update, or delete markers and segments.

To launch the GV STRATUS panel within GV STRATUS Rundown, click **View** and select **STRATUS**.



Inserting placeholders from GV STRATUS

You can create placeholders in the GV STRATUS ActiveX plugin and insert them automatically into the playlist or any channels of GV STRATUS Rundown.

1. Select a placeholder from the Assignment List panel in the GV STRATUS ActiveX workspace.
2. Drag and drop the placeholder into GV STRATUS Rundown's playlist or channel.

   The placeholder appears in the playlist or channel.

Linking clips automatically from GV STRATUS

- If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, and metadata.
- In order to link to a placeholder, you must be assigned with the **Rename Asset Rights** role and write permission for the **Name** property in Metadata section of GV STRATUS Control Panel.

You can automatically create placeholders and link them when you drag and drop assets into the playlist.

1. Create a new playlist in the GV STRATUS Rundown application.
2. Select a clip from the Asset List in the GV STRATUS ActiveX Plug-in.
3. Drag and drop the clip into GV STRATUS Rundown's playlist.

   The clip is linked to a placeholder that is automatically generated in the Assignment List of GV STRATUS ActiveX Plug-in.

4. Click **Save** to save the playlist.

Integrating assets with traffic system and K2 Edge

Integration with traffic system and playout automation

Integration of assets with the traffic system and playout automation provides a seamless operation from program scheduling, segmentation of assets, insertion of commercials into the daily playlist, right up to automated broadcast. The integration workflow includes a traffic sytem, the GV STRATUS application, and K2 Edge for playout automation. The traffic system is responsible for scheduling daily broadcasts, while K2 Edge automates the play-to-air operation according to the traffic system's playlist.

In the GV STRATUS application, the Segmentation tool allows users to create multiple segments of an asset so that commercials can be inserted in between those segments. In the House Number list, assets are linked to house numbers and thus associated with programs on the traffic system's playlist.

The communication between the GV STRATUS application and the traffic system is via the Broadcast Exchange Format (BXF) files. The traffic system sends the list of programs and house numbers in BXF files that are dropped into the traffic watch folder. The location of the traffic watch folder must be configured in the GV STRATUS Control Panel application.

The GV STRATUS application processes those BXF files and populates house numbers automatically into the House Number List. This processing is not affected by GV STRATUS security access permissions. After assets are linked to house numbers in the House Number List, the GV STRATUS application creates another set of BXF files and sends them to the traffic system to reconcile information with the previous playlist. The traffic system's completed playlist now includes segmentation information, house numbers, duration, and asset IDs.

If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets, and metadata that do not have read permissions are not visible. Markers and segments permissions must be set to **Allow** in order to create, update, or delete markers and segments. For example, House Numbers are hidden if Read access is not granted on the linked asset.

For playback, the traffic system sends the completed playlist to K2 Edge for automated playout. The K2 Edge identifies assets from the playlist and initiates FTP transfer of assets in preparation for the broadcast. In the K2 Edge system, the Cobalt Playout Control (POC) application automates the play-to-air operation.

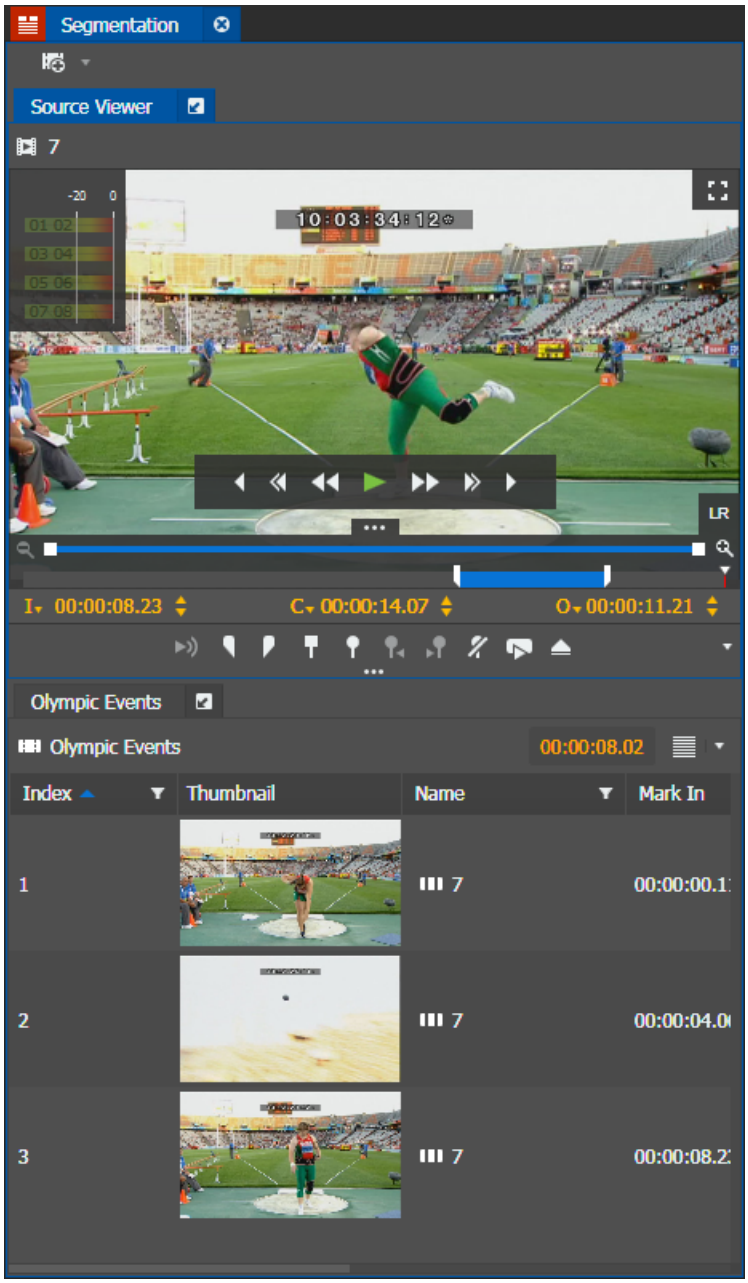
Refer to the traffic system customer documentation and "Cobalt User Manual" for more information regarding their workflows.

The Segmentation tool

The Segmentation tool allows you to assign an asset into multiple segments for insertion of commercials in between segments, and creation of diverse segments of an asset for different broadcast times. You can easily create several Segmentation panels in the tool to create multiple types of segments to suit your broadcast schedule.

The Segmentation tool displays as a composite panel in the GV STRATUS application. It includes the Source Viewer, and Segmentation panel(s).

You can create segments only if you have the Segmentation role.



Segmentation tool features are as follows:

- Source Viewer — Loads assets to be previewed.
- Segmentation Panel — Displays the list of segments of the asset.
- Toolbar — Consists of the button to create new segmentation panel.
- Duration — Displays the duration timecode which sums up the duration of all the segments within the segmentation panel.

- Index — Consists of incrementing numbers for segments. The index number increases whenever each segment is created.

If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets, and metadata that do not have read permissions are not visible. Markers and segments permissions must be set to **Allow** in order to create, update, or delete markers and segments.

Segmentation Panel button

This button located on the Segmentation Tool lets you perform the function below.

New Segmentation: Creates a new segmentation panel.

Adding a Segmentation panel

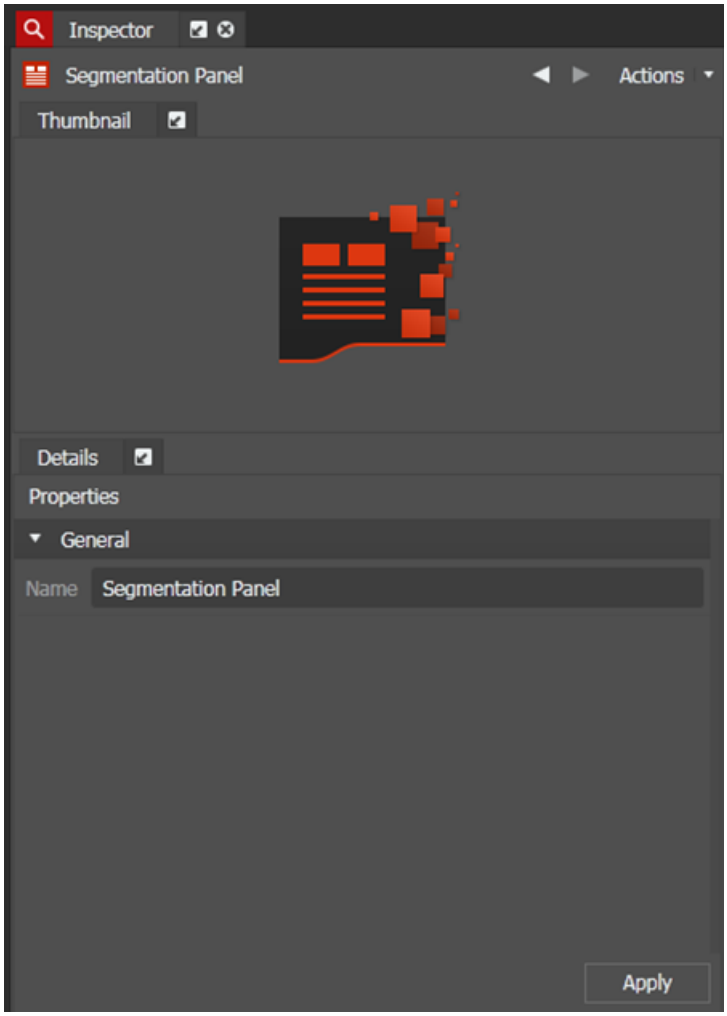
You can create and add segmentation panels to accommodate different kinds of asset segmentation in your operation.

1. Launch the Segmentation tool by doing one of the following:
   - Double-click **Segmentation** from the **Tools** section in the Navigator.
   - Right-click on **Segmentation** from the **Tools** section in the Navigator and select **Open**.

   The Segmentation tool opens.

2. Click the **New Segmentation** button on the toolbar.

   The Inspector loads the configuration for a new segmentation panel.



3. Enter the **Name** of the segmentation panel.
4. Click **Apply** to save the segmentation panel.

   The new segmentation panel name displays in the Segmentation Tool.

5. Repeat above steps to create more segmentation panels if desired.

   You can create multiple Segmentation panels to assign different segments of an asset for different broadcast times.

   You can also drag the **Drag Source** icon on the segmentation panel into the Inspector if you want to change the panel name later.

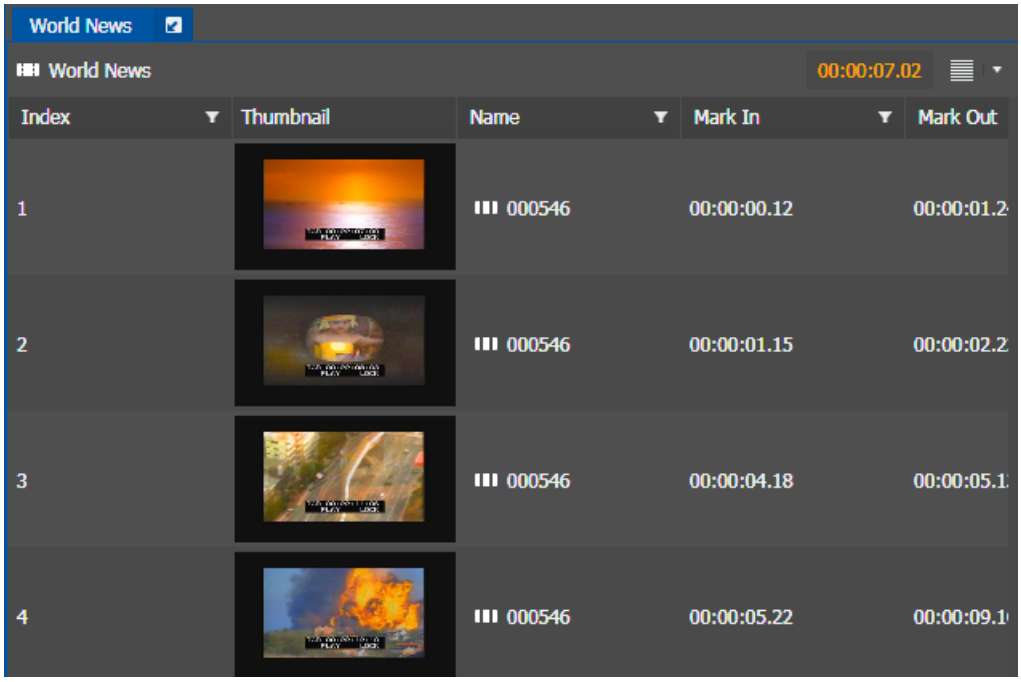
Assigning segments to assets

- If GV STRATUS security is enforced, your credentials must give you full read and write permissions on bins, assets, and segments. You can only view segments with read permission, and modify segments with write permission.
- Create Segment and Update Segment permissions must be set to **Allow**, for you to create and update segments.

You can assign segments to an asset in the Segmentation panel. Segments are created in the Source Viewer panel by marking in and out specific part of the asset.

1. Drag the selected asset from Asset List into the Source Viewer in the Segmentation panel.
2. If the logging controls are not shown, click the **Show/Hide Control Tray** button ... to show the controls, then the drop-down arrow at the right of the control tray and **Add/Remove** buttons if necessary.
3. Navigate to the starting point and click the **Mark In** button. (**I**)
4. Determine the end-point of your segment and click the **Mark Out** button. (**O**)
5. Click on the asset in the Source Viewer, then drag and drop the segment into the Segmentation panel. (**Alt + Ctrl + Insert**)

   The segment adds into the Segmentation panel.



6. Repeat above steps to add more segments of the asset into the Segmentation panel.

   The index number increases whenever a segment is added or duplicated.

   NOTE: Without Create Segment and Update Segment permissions, segments cannot be rearranged or dragged and dropped in the same Segmentation panel, or from one panel to another.

You can also create various segment lengths of an asset in multiple segmentation panels for different broadcast times. For example, a program that is scheduled for prime time has more commercial slots compared to the repeat of the same program at a later time. Therefore, several kinds of segments in multiple segmentation panels can be created for the same asset.

Editing segments

- If GV STRATUS security is enforced, your credentials must give you full read and write permissions on bins, assets, and segments. You can only view segments with read permission, and modify segments with write permission.
- Create Segment and Update Segment permissions must be set to **Allow**, for you to create and update segments.

When you edit a segment, you change the length of the viewable asset by changing the Mark In and Mark Out points of the segment.

1. Double-click on a segment in the Segmentation panel.

   The segment displays in the Source Viewer. The segment on the scrub bar appears in light blue to indicate that the segment is editable and in the **Edit Mode**.

2. Navigate to the desired starting point using the scrub bar, and click the **Mark In** button. (**I**)
3. Navigate to the desired end-point using the scrub bar, and click the **Mark Out** button. (**O**)

   Trim Asset is enabled when the asset has a mark-in or mark-out point. It is disabled if the asset does not have a mark-in or mark-out point.

   NOTE: If a clip is a part of Dyno record train sequence, Mark In and Mark Out points should not be set beyond the limit of the guard band, as configured for the record train sequence.

4. Press the **Esc** key on your keyboard to exit the **Edit Mode**.

   Your changes are saved to the segment.

   The scrub bar of the Source Viewer turns back to dark blue to indicate that the segment is no longer in the **Edit Mode**.

The Segmentation panel displays the new duration, mark in, and mark out points for the segment.

You can also change Mark In and Mark Out points on the Inspector panel.

If you set a segment in the **Edit Mode** by double-clicking the segment, you can play the segment from Mark In point and it will automatically stop at the Mark Out point. Then you can click the **Play** button or press spacebar to continue playing the clip until the end, if desired.

If the **Loop Playback** button is clicked, the segment plays from Mark In point to the Mark Out point repeatedly in a loop playback.

Renaming a segment

- Update Segment permission must be set to **Allow**, for you to rename segments.

You can rename segments to differentiate multiple segments for an asset.

1. Select a segment that you want to rename.
2. Right-click and select **Rename**. (**F2** or **Alt + Click**)

   The segment name becomes editable.
3. Enter the new name for the segment.
4. Repeat above steps to rename other segments.

   Segments are renamed on the segmentation panel.

   Segments can also be renamed by dragging the segment into the Inspector.

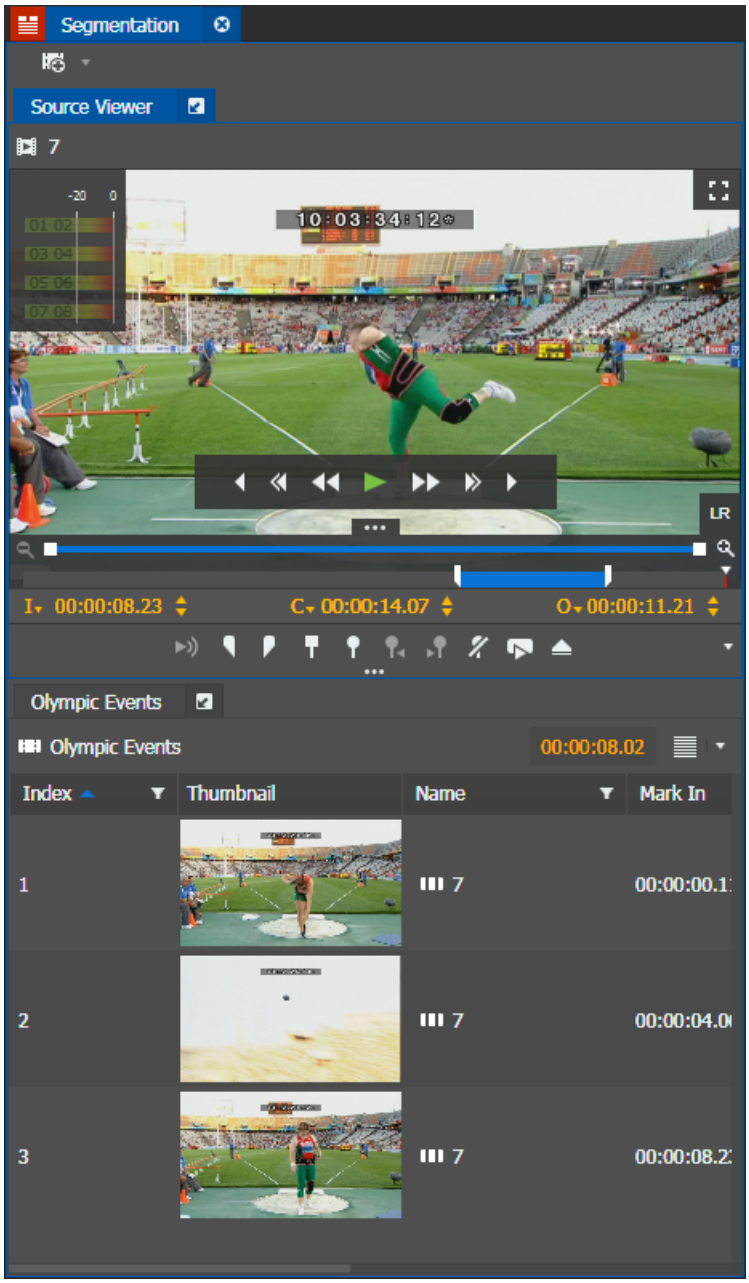
Previewing a segment

- If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, metadata, markers, keywords, and segments.

You can preview segments using the Inspector or Source Viewer in the Segmentation tool.

1. Select a segment that you want to preview from the list of segments in the Segmentation panel.

2. Press the spacebar or click the **Play** button.



The segment plays from the Mark In point to the Mark Out point. Then you can click the **Play** button or press spacebar to continue playing the clip until the end, if desired.

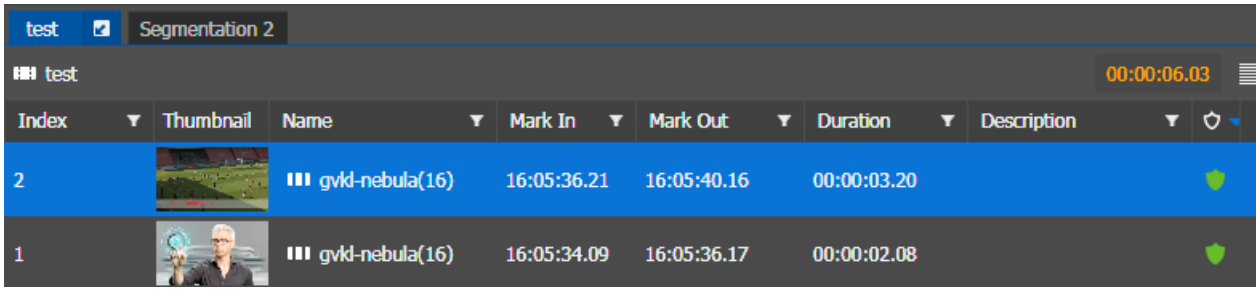
If the **Loop Playback** button is clicked, the segment plays from Mark In point to the Mark Out point repeatedly in a loop playback.

Protecting a segment

If it is not already displayed, display the Protection Status column.

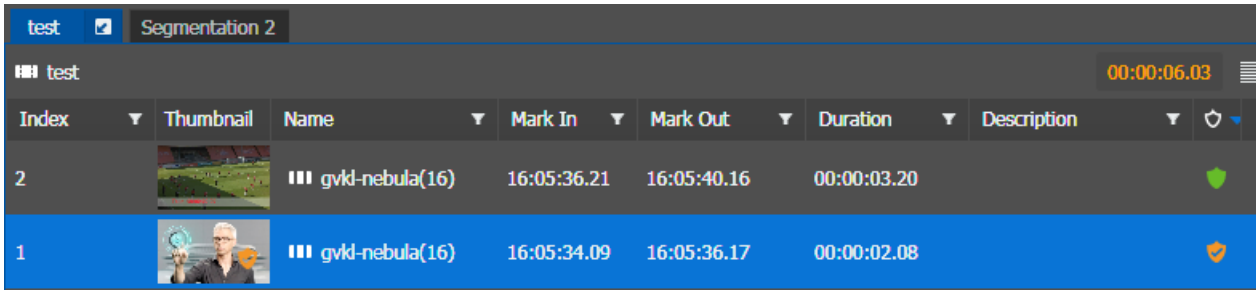
1. In the Segmentation Panel, right-click and select **Columns | Protection Status**.

   The Protection Status column displays.



2. Select a segment to be protected and click the **Unprotected** button.

   The segment status toggled from unprotected to protected.



A protected segment cannot be modified, deleted, or moved. However, it can be copied into another Segmentation Panel.

When it is protected, the Edit mode is not allowed and you can only be in the Preview mode.

Merging segments

- Create Segment and Update Segment permissions must be set to **Allow**, for you to merge segments.

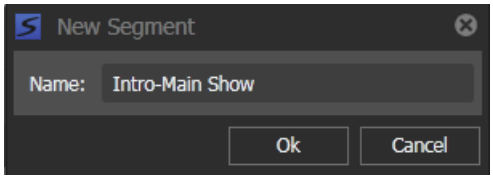
You can merge multiple segments into a single segment in the Segmentation tool. This allows you to combine segments later in post-production if multiple segments were automatically created during a live show.

1. In the desired order, select segments of the same type that you want to merge into one segment.

   NOTE: Protected assets cannot be merged.

2. Right-click and select **Merge**.

   The New Segment dialog box appears.

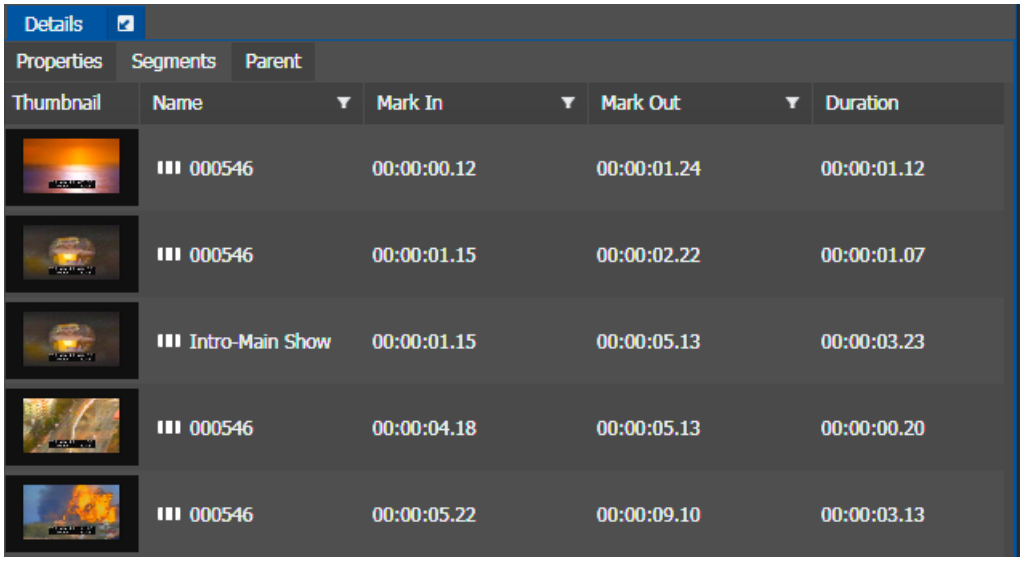


   By default, the merged segment name displays according to the order of segments that you selected earlier.

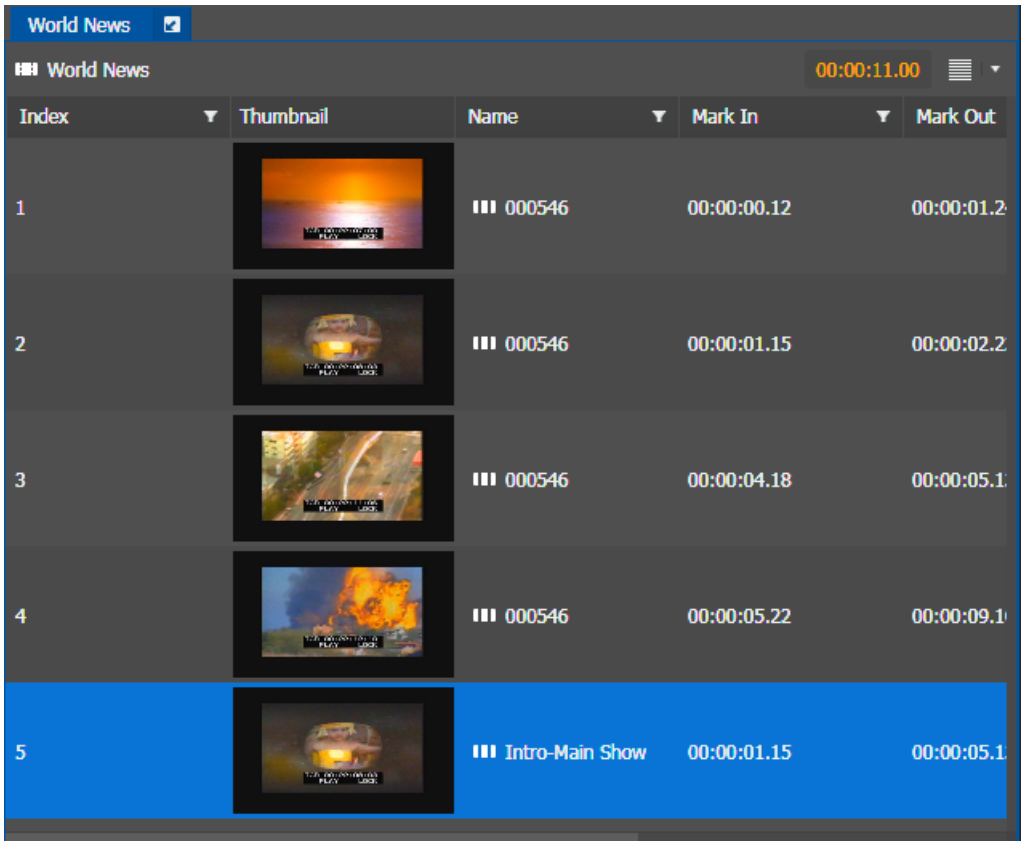
   You can insert a new name or use the combined name from those merged segments.

3. Click **OK**.

   Those segments are merged into one segment in the Segmentation Panel according to the order of the timecode in clips. You can also view the merged segment on the **Segments** tab of the Inspector.



   The merged segment is also assigned with the next available index number in the segmentation panel.



The merged segment has the core properties and custom metadata of the first selected segment.

NOTE: Merging segments of different Segment Types is not allowed. You can only merge segments with the same Segment Type.

Moving and copying a segment

- Create Segment and Update Segment permissions must be set to **Allow**, for you to copy or move segments.

You can move or copy a segment from one segmentation panel into another. This saves time in your operation as you don't have to create new segments for each segmentation panel.

1. Select the segment you want to move in a segmentation panel.
2. Drag the segment to another segmentation panel.

   Once you drag the segment, a tooltip appears to describe your action.
3. Drop the segment into the other segmentation panel.

   The segment moves from one segmentation panel into another.

To copy a segment into another segmentation panel, drag and drop the segment while pressing the **Ctrl** button.

Multiple segments can also be copied at the same time.

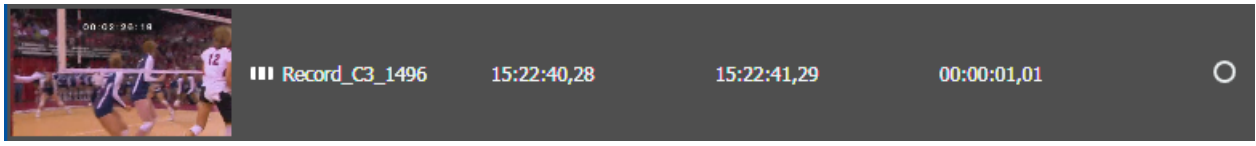
Approving a segment

- Update Segment permission must be set to **Allow**, for you to approve segments.

You can set the approval status if you want to use it in your workflow.

1. Select a segment in the Segmentation panel.

   The approval status of a segment is set to **None** by default.



2. Click the **None** icon to change the approval status.

   The approval status changes to **Approved**.

   You can click the icon to toggle the approval status of each segment.

   None: Identifies the approval status of the clip as none.

   Approved: Identifies the approval status of the clip as approved.

   Rejected: Identifies the approval status of the clip as rejected.

Deleting a segment

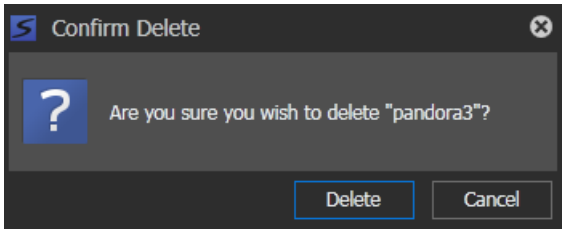
- Delete Segment permission must be set to **Allow**, for you to delete segments.

1. Select a segment or multiple segments that you want to delete.

   To select multiple segments, hold the **Shift** key down and select all segments between two selected segments; or hold the **Ctrl** key down and select segments randomly.

2. Right-click and select **Delete**. (**Delete**)

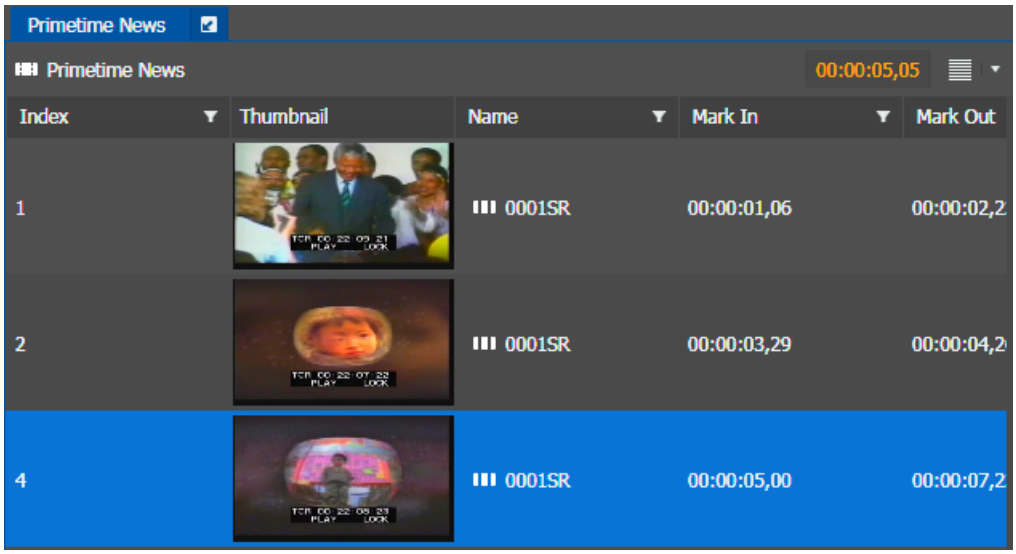
   The Confirm Delete dialog opens.



3. Click **Delete**.

The selected segment is deleted from the segmentation panel.

The index number is also deleted and not replaced in the segmentation panel.



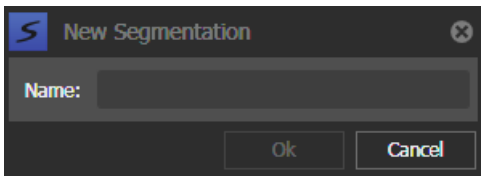
Duplicating a Segmentation Panel

- Write permission must be set to **Allow**, for you to duplicate segmentation panels.

1. Right-click on the **Drag Source** icon in the segmentation panel that you want to duplicate.

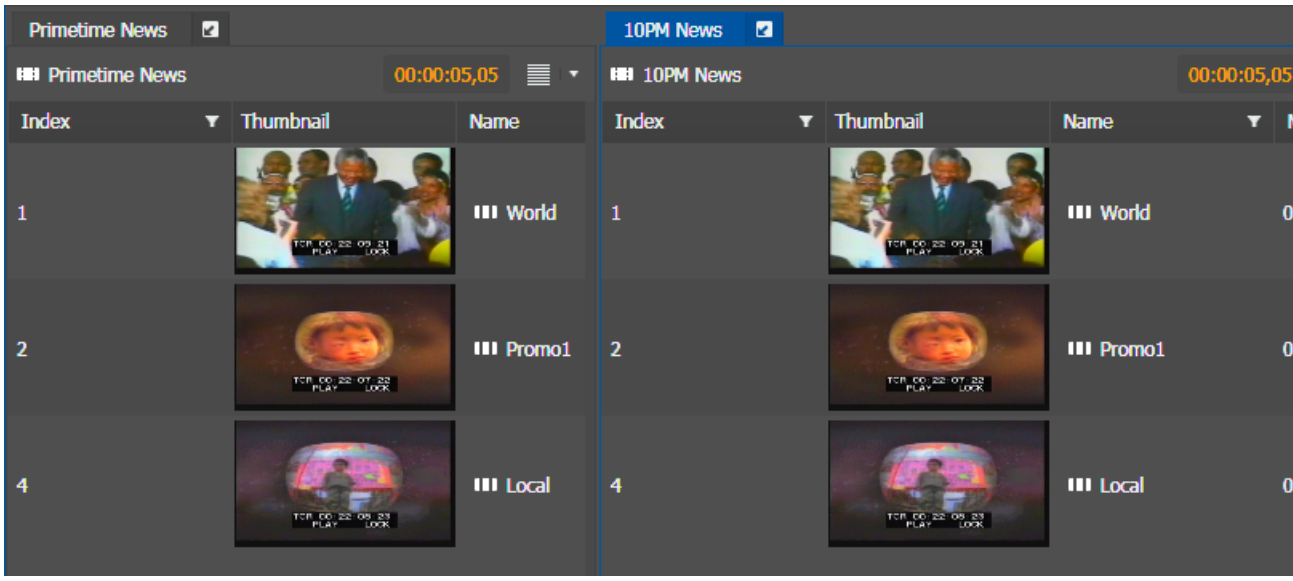
2. Select **Duplicate**.

   The New Segmentation dialog appears.



3. Enter the name of the new segmentation panel and click **OK**.

The segmentation panel is duplicated and added to Segmentation Tool with the new name. The content, index, and order of segments are the same with the original segmentation panel. You can also dock the panel to another location if desired.



Deleting a Segmentation Panel

- Delete permission must be set to **Allow**, for you to delete segmentation panels.

1. Right-click on the **Drag Source** icon in the segmentation panel that you want to delete.
2. Select **Delete**.

   A dialog opens for you to confirm the segmentation panel deletion.

3. Select **Yes**.

   The segmentation panel is deleted from the Segmentation Tool.

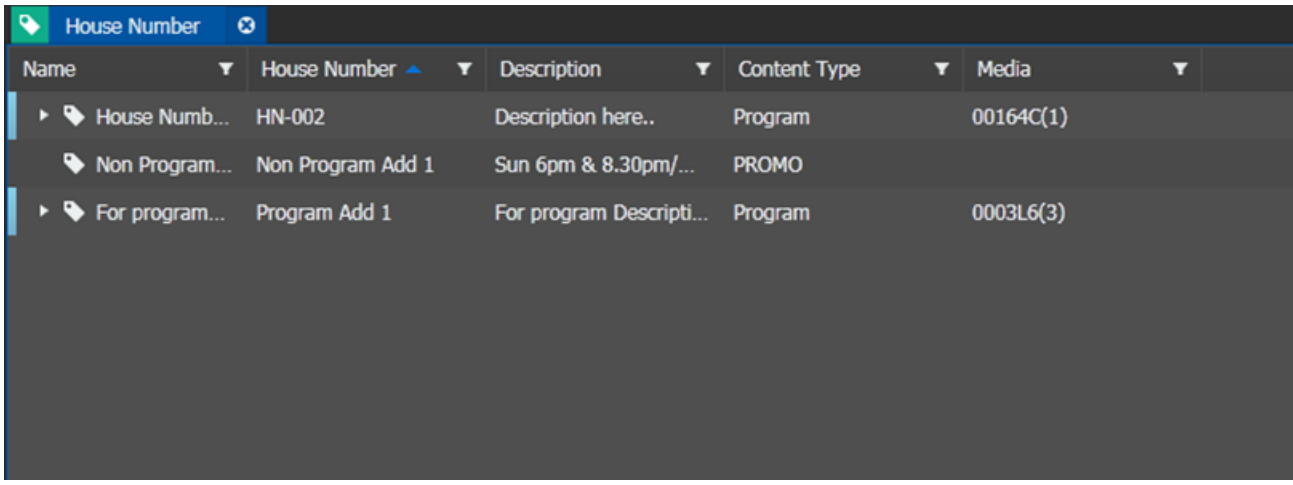
The House Number panel

The House Number panel displays house numbers that are sent from the traffic system. The traffic system sends house numbers to the GV STRATUS application by dropping BXF files into a traffic watch folder. You can link these house numbers to GV STRATUS assets in this panel. If you have

created multiple segments for an asset associated with a house number, you can also view those segmentations in the panel.

You can only access the House Number panel if you have the Segmentation role.

NOTE: The 4K video format is not currently supported in House Number/ Traffic Gateway system.



House Number panel features are as follows:

- List — Populates the House Number List after BXF files are dropped into the traffic watch folder. The list consists of program name, house number, content type, description, and media.
- Sortable columns — Sorts the list when you click the column head.
- Filter tool — Filters the list based on criteria you enter. The Filter tool opens when you click the **Enable Filter** button.

If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets, and metadata that do not have read permissions are not visible. Markers and segments permissions must be set to **Allow** in order to create, update, or delete markers and segments. For example, House Numbers are hidden if Read access is not granted on the linked asset.

Configuring custom metadata for House Number List

For the integration between traffic system and the House Number List, you need to add below custom fields manually in the Metadata settings of GV STRATUS Control Panel application.

If GV STRATUS security is enforced, your credentials must give you read and write permissions for all 5 custom metadata fields below:

Field name	Type
House Number	Text - 256 Characters
Program	Boolean
Content Name	Text - 256 Characters

Field name	Type
Content Description	Text - 256 Characters
Content Type	Text - 256 Characters

Related Topics

Custom Metadata settings on page 318

Linking asset to a house number

House numbers are automatically populated in the House Number List when the traffic system drops BXF files inclusive of list of programs and house numbers into the traffic watch folder. Users can then browse for assets related to those programs and link them to the respective house numbers. The link between assets and house numbers provide an easy workflow for playout automation later.

If GV STRATUS security is enforced, your credentials must give you full permissions for all 5 custom metadata fields of House Numbers.

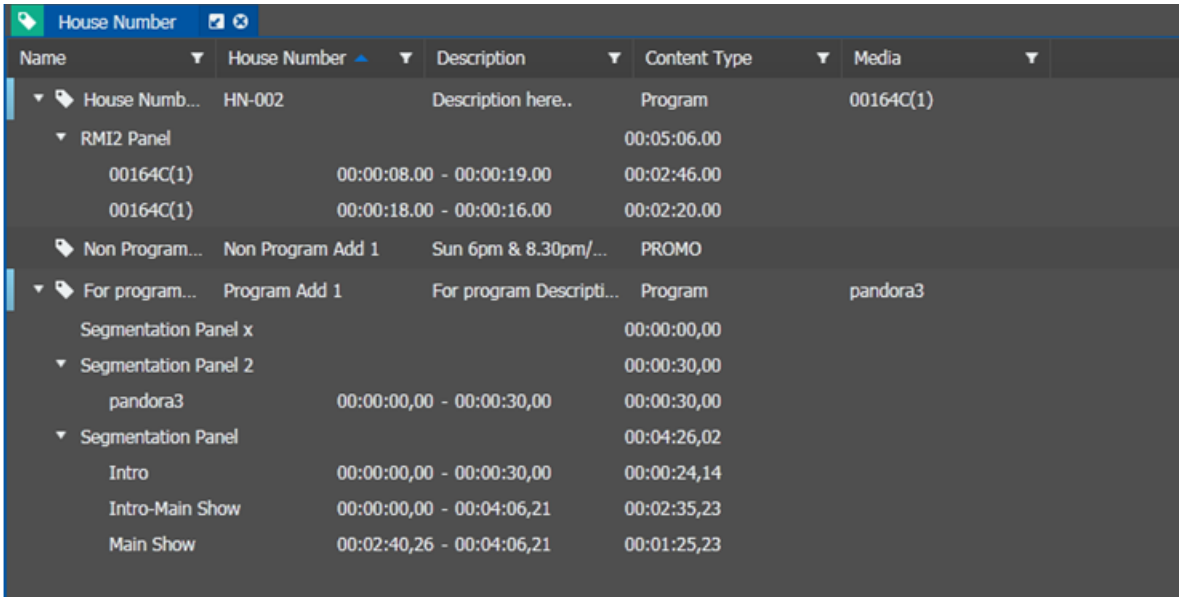
1. Select an asset in the Asset List.
2. Drag the asset into the House Number List.

   A tooltip appears and each row in the House Number List highlights when your cursor selects a row.

   NOTE: Without Write permissions on all 5 custom metadata fields, the Not Allowed icon displays and the process to link/unlink asset to a house number is not permitted.

3. Drop the asset into the selected row of House Number.

   The asset links to the house number and the asset name appears in the **Media** column of the house number.



   The beginning for each row of linked house number displays in blue.

4. If you linked an asset to a wrong house number, right-click on the house number and select **Unlink**.
5. Repeat above steps to link more assets to other house numbers.

After an asset is linked to a house number, a BXF file is generated and sent to the traffic system for notification of the new association.

When an asset with multiple segmentations is linked to a house number, those segmentations can also be viewed in the House Number List.

Configuring the GV STRATUS application

Configuring User Preferences

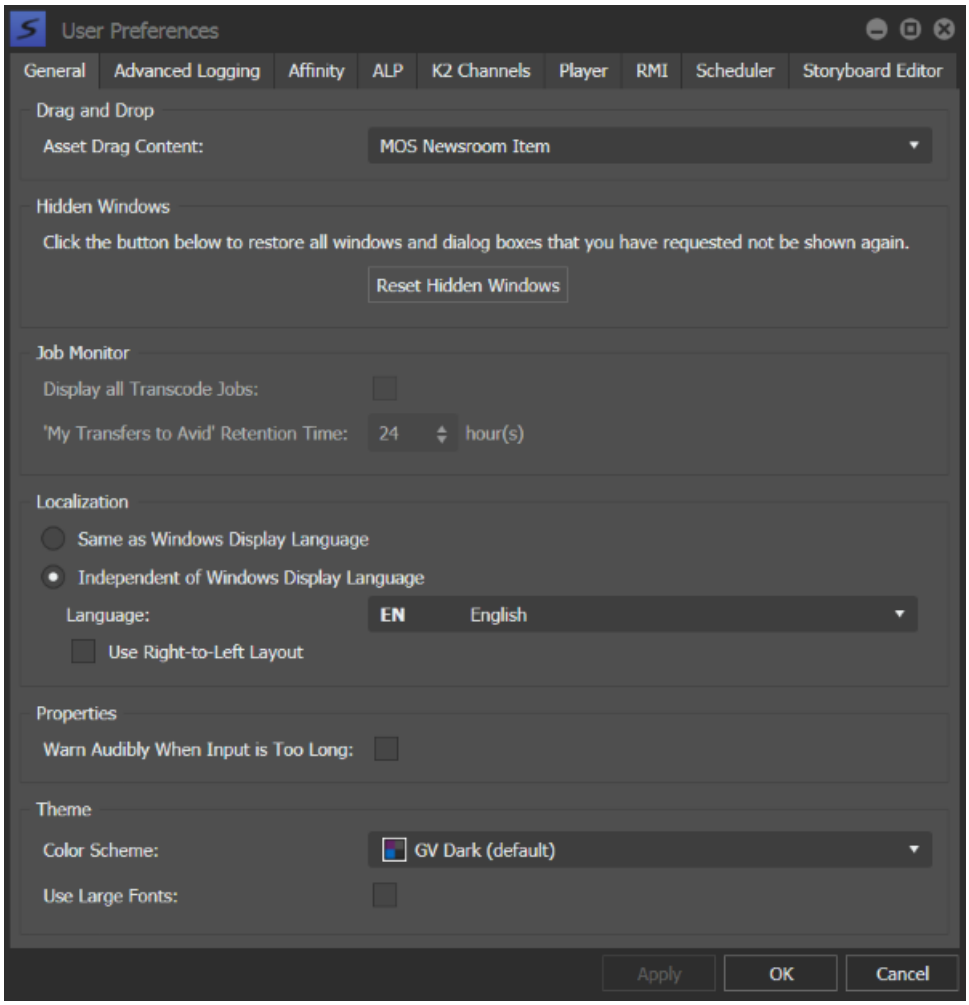
1. Select **Edit | User Preferences**.

   The User Preferences dialog box opens.

   The GV STRATUS application shows or hides sections based on the roles assigned to your GV STRATUS log on credentials.

2. Select the tab for the panel or component you are configuring and make settings accordingly.

3. To configure general user preferences, select the **General** tab.



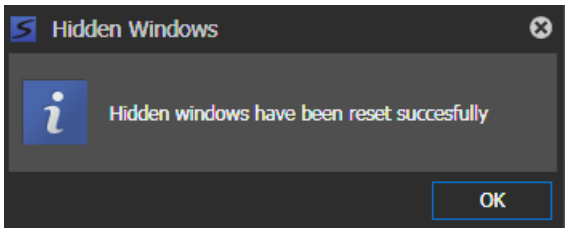
4. To configure the **Asset Drag Content** setting for Drag and Drop workflow in GV STRATUS application, select one from the following:

   - **STROB File** - This is the default setting, as STROB file is the file format used to drag and drop all assets in the GV STRATUS application.
   - **MOS Newsroom Item** - All GV STRATUS assets can be dragged and dropped as MOS items into the ENPS application.
   - **Legacy Avid DHM Ingest** - All GV STRATUS assets can be dragged and dropped into the Avid application.

   NOTE: Do not change this setting except under supervision of qualified Grass Valley Support personnel. Extensive system configuration is required to achieve a working GV STRATUS system.

5. To display windows and dialog boxes that you have set to "Do not ask again", click **Reset Hidden Windows**.

   The **Hidden Windows** dialog appears to confirm the reset, so click **OK**.



6. To configure Job Monitor settings, do the following:
   a) To display detailed transcode jobs in Jobs Monitor, select **Display all Transcode Jobs**.

      When not selected, only hi-res transcoding and proxy encoding jobs are displayed. When selected, the associated thumbnail, closed caption, and metadata jobs are also displayed.

      By default, this setting is not selected. You must have the **Media Manager** role to change this setting.

   b) To set the display duration of Transfer to Avid jobs in Jobs Monitor, set the retention time in **My Transfers to Avid** setting.

      By default, this setting is set to 24 hours.

7. To configure Localization settings, do the following:
   a) Make sure the GV STRATUS language pack for the language you are configuring is installed on the GV STRATUS client PC.

      This is required for any GV STRATUS localization.

   b) Select the localization option as follows:

      - To localize the GV STRATUS application with the language currently configured in the Windows operating system, select **Same as Windows Display Language**.

        The GV STRATUS language pack that corresponds to the Windows display language must be installed.
      - To localize the GV STRATUS application with a language different than that currently configured in the Windows operating system, select **Independent of Windows Display Language**, then in the **Language** list select one of the GV STRATUS language packs currently installed. Also configure the **Use Right-to-Left Layout** check box to suit the selected language.

   c) Restart the GV STRATUS application to put the localization setting into effect.

8. To configure Inspector properties, do the following:
   a) To set an audible alarm when reached the maximum text limit, select **Warn Audibly When Input is Too Long**.

      By default this is not selected, so you need to select this setting to have the audible alarm in your operation.

      The alarm will only be activated when the maximum text limit is reached, if the custom metadata text limit had been configured in the GV STRATUS Control Panel.
9. To set the theme of the application, configure the **Color Scheme** drop-down list and **Use Large Fonts** as desired.
10. To apply a change and continue editing user preferences settings, click **Apply**.
11. To accept any changes and close the dialog box, click **OK**.

    The dialog box closes.

Related Topics

Installing a GV STRATUS language pack on page 1392
Loading an application window workspace on page 1398
Changing Advanced Logging user preferences on page 1311
Changing ALP User Preferences on page 1319
Configuring K2 Channels User Preferences on page 1073
Configuring RMI User Preferences on page 1060
Configuring Scheduler User Preferences on page 1055
Inserting assets as MOS items into ENPS on page 1342

Configuring Affinity User Preferences

You can configure Affinity settings to limit your displayed Assets Locations and Associations to specific storage or device locations using the user settings preferences window.

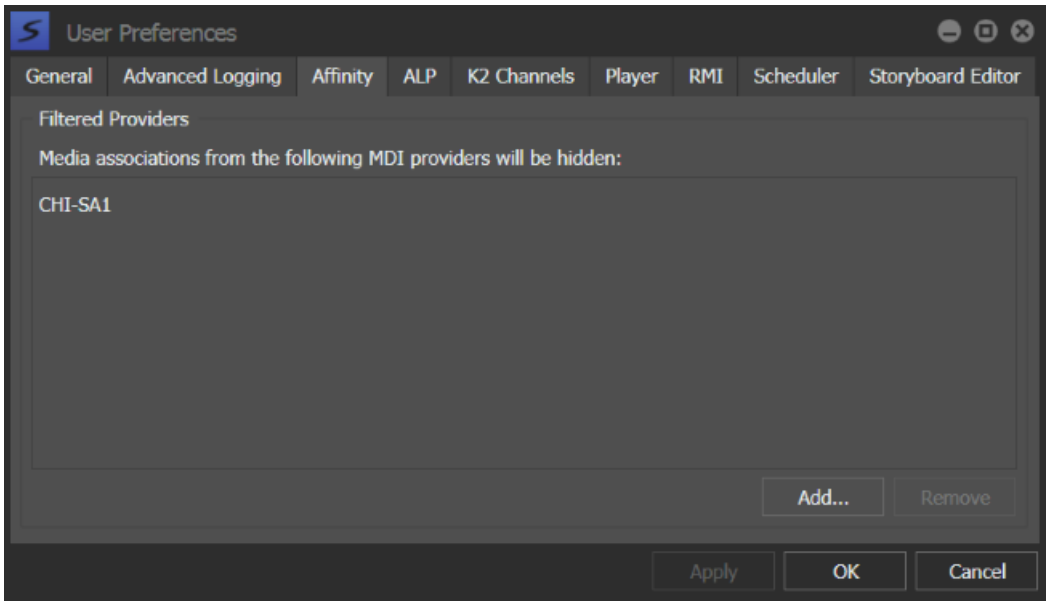
NOTE: Users with the Media Manager role do not have access to the Affinity tab in the User Preferences settings.

1. Select **Edit | User Preferences**.

   The User Preferences dialog box opens.

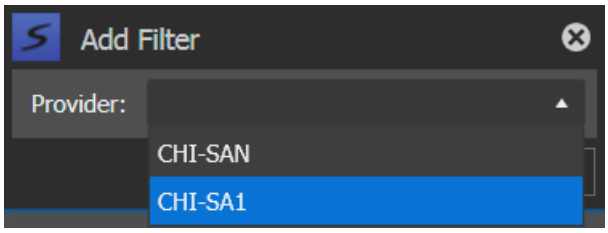
   The GV STRATUS application shows or hides sections based on the roles assigned to your GV STRATUS log on credentials.

2. To configure Affinity user preferences, select the **Affinity** tab.



3. To add a storage or device location to hide, do the following:
   a) Click **Add**.

      The Add Filter dialog box opens.



   b) Select the storage or device location you would like to filter out from the drop-down list.
4. To unhide a storage or device location, do the following:
   a) Click to highlight its row on the **Affinity** tab.
   b) Click **Remove**.
5. To apply a change and continue editing user preferences settings, click **Apply**.
6. To accept any changes and close the dialog box, click **OK**.

   The dialog box closes.
7. Restart the GV STRATUS application for these changes to take effect.

After specific storage or device location had been hidden, take note of the following:

- The selected storage or device location is now filtered out and not displayed in the GV STRATUS application.
- Assets whose only online association is now filtered out will have no online association. Those assets display with the red X icon and red indicator in the asset status column.
- Assets who have multiple online associations, and the primary physical association is filtered out will use the next online association as primary association.

- Searches are not affected as it is still possible to search for assets that have an association on a particular device, even if the returned asset appears to have no online association.

Installing a GV STRATUS language pack

1. Download one or more GV STRATUS language packs.
   Each downloaded language pack is a zip file.
2. Unzip a downloaded file.
   The unzipped file is a directory, named for the language.
3. Put the directory in your GV STRATUS install location.
   By default, the GV STRATUS install location is `C:\Program Files\Grass Valley\STRATUS`.

You can now select the language in GV STRATUS User Preferences.

Related Topics

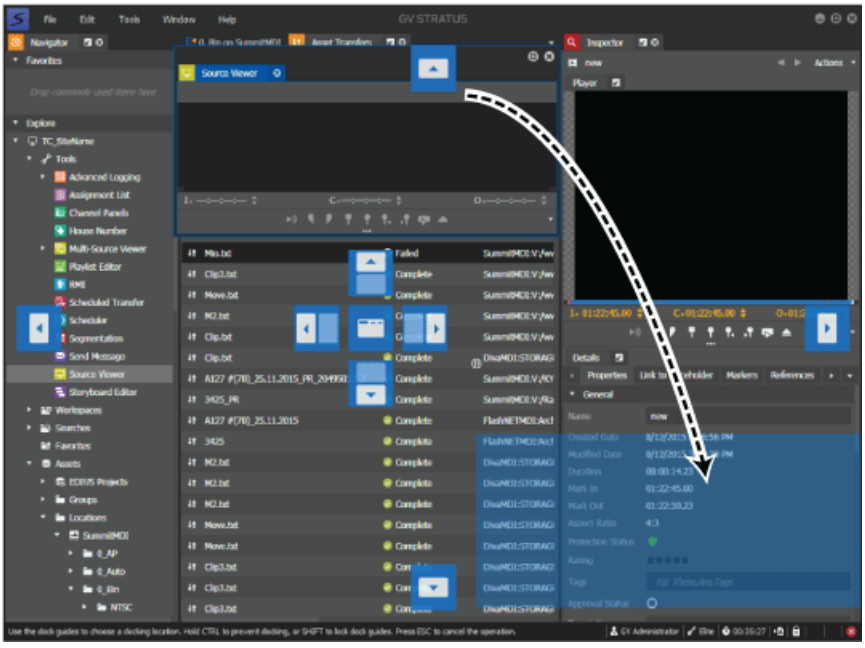
Configuring User Preferences on page 1387
Loading an application window workspace on page 1398

Customizing the application workspace

Use the topics in this section to customize the application workspace.

About customizing the application workspace

You can rearrange the panels of the application to best suit your workflow needs.



Features for customizing the workspace are as follows:

- Undock panels and move them to another location within the application window, within another panel, or to their own location on the Windows desktop.
- Hide panels so that they show only as a tab.
- Close panels.
- Resize panels.
- Save an arrangement of docked and undocked panels as a uniquely named workspace.
- Load a workspace to automatically arrange panels.

Related Topics

Customizing the application workspace on page 1392

Showing a panel

If a panel is not currently visible in the user interface, the way you make the panel visible depends on whether the panel is currently closed, showing as a tab, or open yet obscured by another panel or application. If you are not sure of the current state of the panel, you should find it and determine its state before attempting to make it visible.

Finding a panel

If you are not sure of the location or current state of a panel, use the following procedure to find it.

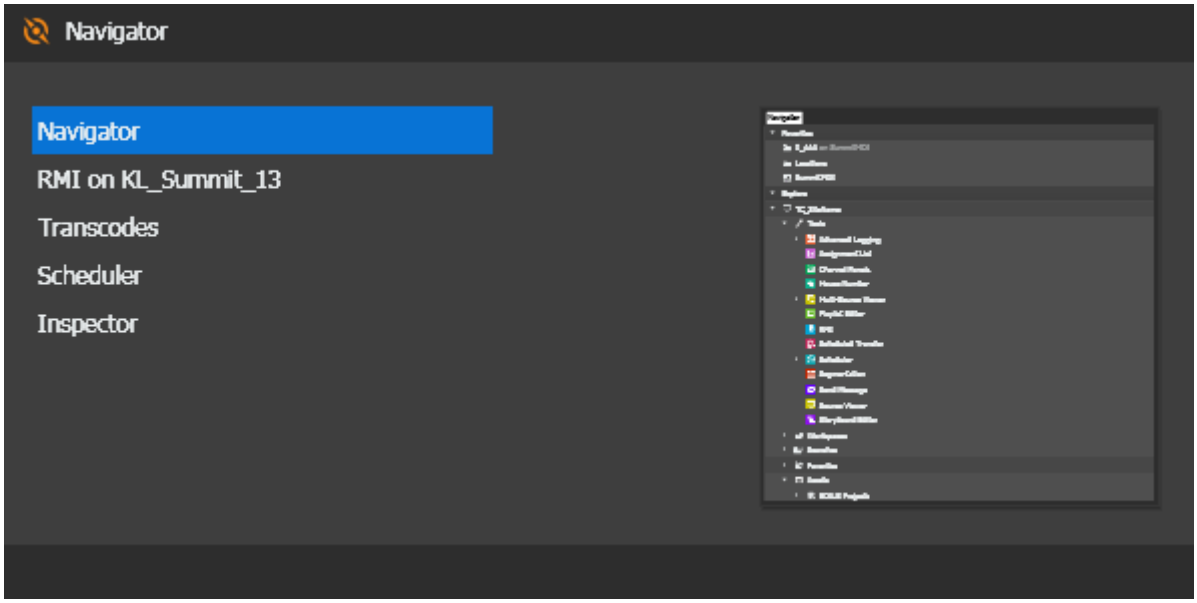
1. Click **Window | Panels**.
2. Identify the name of the panel on the menu list and determine its current state as follows:
   - If the panel name does not have a checkmark next to it, the panel is currently closed. You can select the panel name to open the panel in its last location.
   - If the panel name has a checkmark next to it, the panel is already showing. If you select the panel name, the panel closes, rather than opens.

3. If the panel is already showing, find your panel as follows:

   - Use keyboard shortcuts either **Ctrl + Tab** or **Alt + F7** to view and select from a list of panels with thumbnails. Then, press **Tab** or **F7** key repeatedly to move down the list, and release the **Ctrl** or **Alt** key to select a panel.

   In addition, you can also press **Shift** together with keyboard shortcuts above to move up the list. Then, release the hold on all shortcut keys to select a tool from the list.

   When selected, the tool is given focus. If the tool includes a player or viewer such as the Inspector, Advanced Logging Suite, Segmentation, or Storyboard Editor, then the primary viewer of the tool is in focus.



   - Check the edges of the application window to find your panel showing as a Show/Hide tab.
   - In other panels check the area under the title bar to find your panel showing as a panel tab.
   - Check the Windows taskbar and/or desktop to find your panel as an undocked panel. Your panel might be obscured by another panel or application window.
   - If you are having difficulty finding your panel, close and then reopen the panel from **Window | View**. This causes the panel to open in front of any other panels that could be obscuring it.
   - Click **Window | View** and reload a workspace.

Related Topics

Loading an application window workspace on page 1398
Configuring User Preferences on page 1387
Installing a GV STRATUS language pack on page 1392

Showing a closed panel

If a panel is currently closed and its tab is not showing, you can open the panel as follows:

1. Click **Window | Panels**.

2. Identify the name of the panel on the menu list, then do one of the following:
   - If the panel name does not have a checkmark next to it, select the panel name. The panel opens in its last location.
   - If the panel name already has a checkmark next to it. The panel is already showing as a fully open panel or as a tab at the edge of the application . If you select the panel name, the panel closes, rather than opens.

Showing a panel from its Show/Hide tab

If the panel is currently displayed as a Show/Hide tab at the edge of the application window, you can open the panel temporarily or permanently.

1. Hover the cursor over the panel's Show/Hide tab.

   The panel opens.

2. Proceed as follows:
   - If you want the panel to stay open temporarily, use the panel as desired, then click outside of the panel. This returns the panel to show as a Show/Hide tab only.
   - If you want the panel to stay open permanently, click the **Pin** button in the upper-right corner of the panel. The panel opens and docks in its last location in the application window.

Hiding a panel

You can hide or close a panel to make room in the application window.

Do one of the following to hide or close a panel:

- If you want to hide the panel as a Show/Hide tab, click the **Pin** button in the upper-right corner of the panel. The panel collapses into a Show/Hide tab, which is displayed at the nearest edge of the application window. The tab shows the location of the hidden panel.
- If you want to close the panel completely, click the **X** button in the upper-right corner of the panel. The panel closes. No visible indicator of its location remains.

Undocking a panel

You can undock a panel from the application window so that it becomes an independent, floating panel. You can then move the panel to another location to suit your workflow needs.

To undock a panel do one of the following:

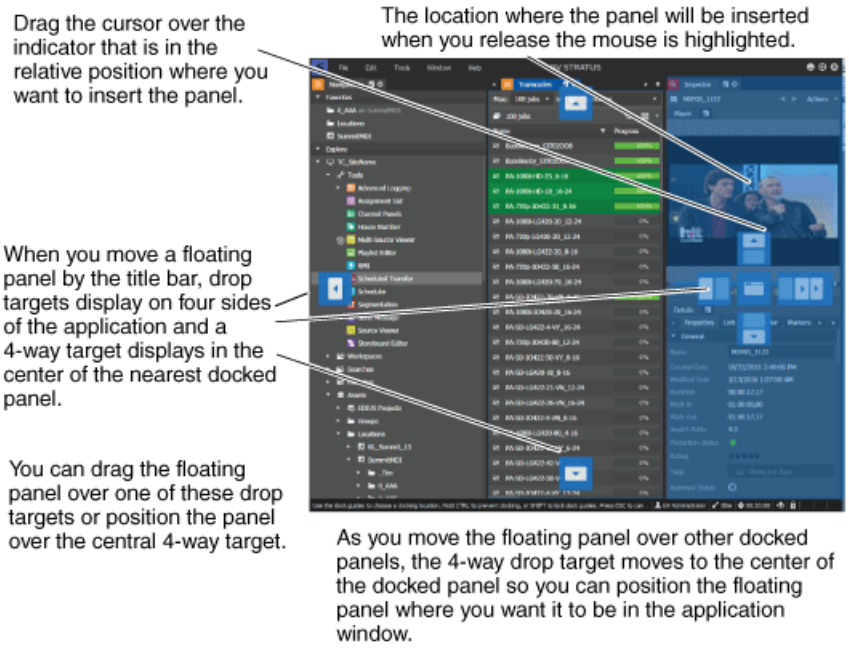
- Double-click the panel's title bar. This automatically undocks the window and moves it to its last location.
- Drag the panel by its title bar to another location. This can be one of the following locations:
  - Within another panel.
  - Within the application window.
  - Outside the application window on your Windows desktop.

If you want to move the panel to new location within another panel or within the application window, you must dock it in the new location.

Docking a panel

Once you have undocked a panel so that it is independent, you can then dock the panel.

1. To dock a panel do one of the following:
   - Double-click the panel's title bar. This automatically docks the panel in its last location. If you do this you can skip the remainder of this procedure.
   - Drag the panel by its title bar as a floating panel and move it to a location within another panel or within the application window, then continue with the remainder of this procedure.
2. Move the cursor over the panel that is closest to your target area for docking the floating panel.
3. Identify the drop target direction arrows that are displayed in the center of the target panel and on each side of the screen.



4. When the desired drop target appears, press and hold the **Shift** key to retain drop target positions.

   This prevents your drop target from shifting or disappearing as you move the cursor.
5. Move the cursor until it is over the drop target nearest the location where you want the panel docked, as follows:
   - Choose the drop target up, down, right, or left arrows to dock as a fully open panel.
   - Choose the indicator in the center of the drop target square that is surrounded by a 4-way arrow to dock as a tab within the target panel.

   A drop preview (a highlighted area) appears.
6. Verify that the drop preview is the location where you want the panel docked.
7. Release the mouse button to dock the panel.
8. Resize the panel as necessary.

Saving an application workspace

Once you have the application workspace, including both docked and undocked panels, arranged according to your workflow needs, you can save the workspace with a unique name. You can then load the saved workspace to return automatically to the same arrangement.

1. To save a workspace, click **Window | Workspace | Save Workspace**.

   The Save Workspace dialog box opens.

2. Enter a name for the workspace and click **OK**.

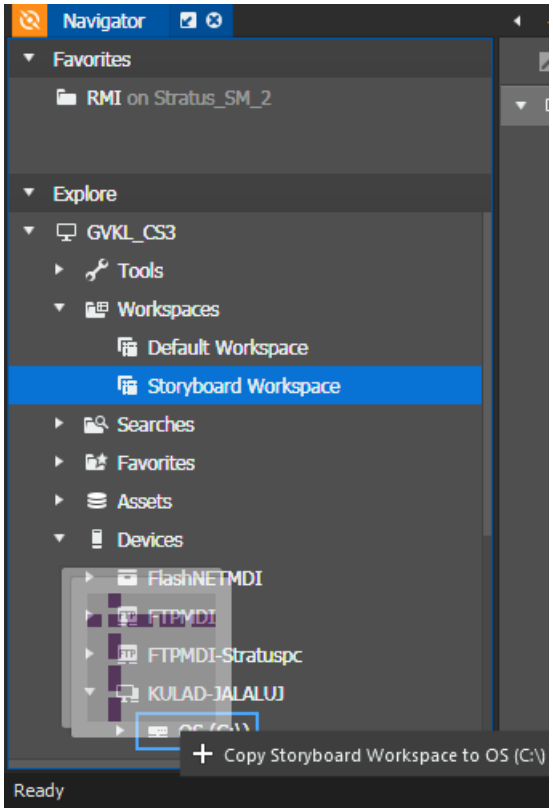
   If you enter the same name as a previously saved workspace, the new workspace overwrites the previously saved workspace.

   The workspace is saved and added to the **Window | Workspace** list.

Copying an application workspace

Once you have saved an application workspace, you can copy it to a drive or directory on the GV STRATUS client PC.

1. To use drag-and-drop, in the Navigator panel, drag a saved workspace to a drive or directory on the local GV STRATUS client PC.



2. To use **Copy To**, in the Navigator panel, right-click the workspace, select **Copy To**, and in the **Copy To** dialog box navigate to a drive or directory on the local GV STRATUS client PC.

The workspace is saved as a file on the local GV STRATUS client PC.

Opening a closed panel

If a panel is currently closed, you can open the panel as follows:

1. Click **Window | Panels**.
2. Verify that the name of the panel on the menu list does not have a checkmark next to it.

   If the panel name has a checkmark next to it, the panel is already showing as a fully open panel or as a tab. If you select the panel name, the panel closes, rather than opens.
3. Select the panel name.

   The panel opens in its last location.

Loading an application window workspace

Do one of the following:

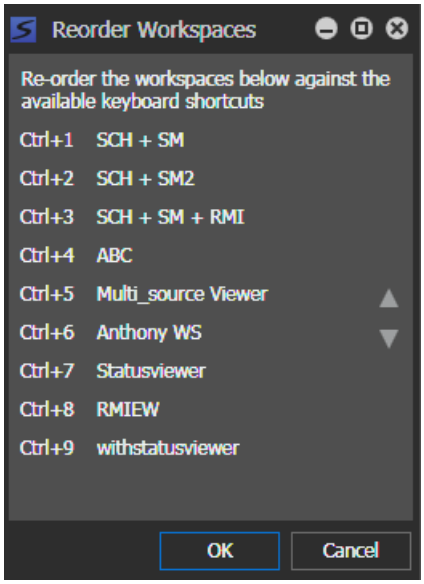
- Click **Window | Workspace** and select a workspace from the list.
- Use keyboard shortcut **Ctrl + 1**, **Ctrl + 2**, **Ctrl + 3**, etc to switch between workspaces.

The application window workspace is automatically arranged, including both docked and undocked panels.

Reordering an application workspace

1. Click **Window | Workspace | Reorder Workspaces**.

   The Reorder Workspaces dialog box opens and lists saved workspaces.



2. Select a workspace from the list.
3. Click the **Move Up** button ▲ or **Move Down** button ▼ to move the workspace and reorder it against other available keyboard shortcuts.

4. Click **OK**.
   The workspace list is rearranged on the **Window | Workspace** menu.

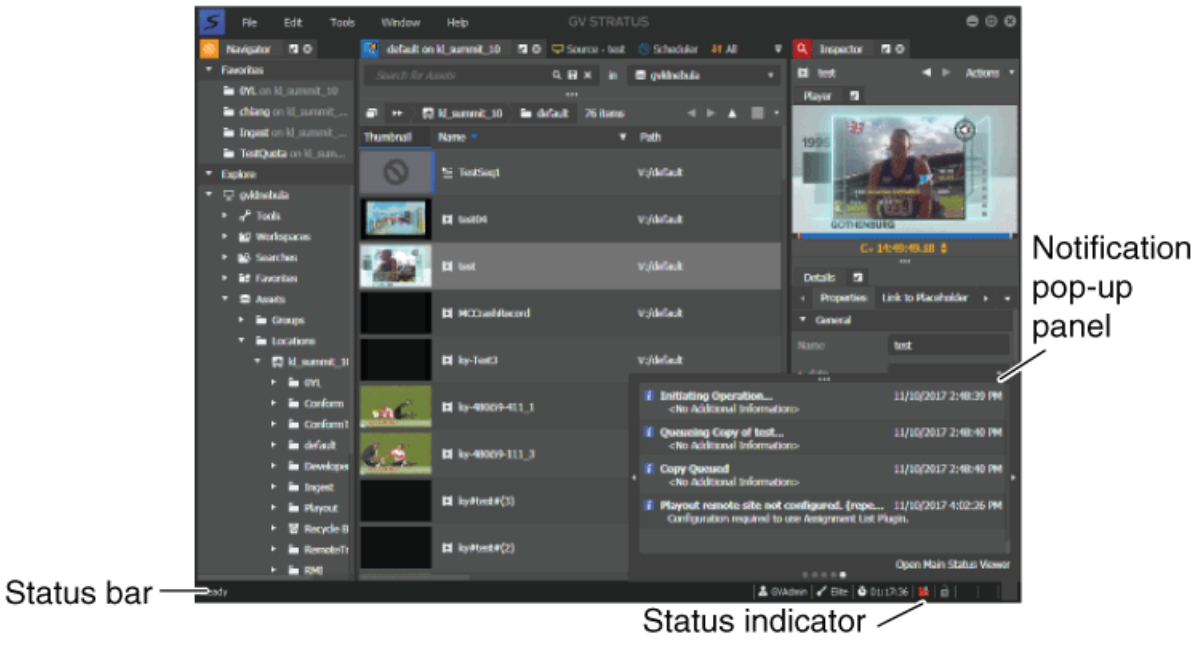
Deleting an application workspace

1. Click **Window | Workspace | Delete Workspace**.
   The Delete Workspace dialog box opens and lists saved workspaces.
2. Select a workspace from the list.
   You can press Ctrl + Click to select multiple workspaces.
3. Click **Delete**.
   The workspace is removed from the **Window | Workspace** list.

Troubleshooting the GV STRATUS application

About application status

You can view the status of the application as follows:



Status Bar

Indicates whether the application is ready or not, the user account currently logged on, and license information.

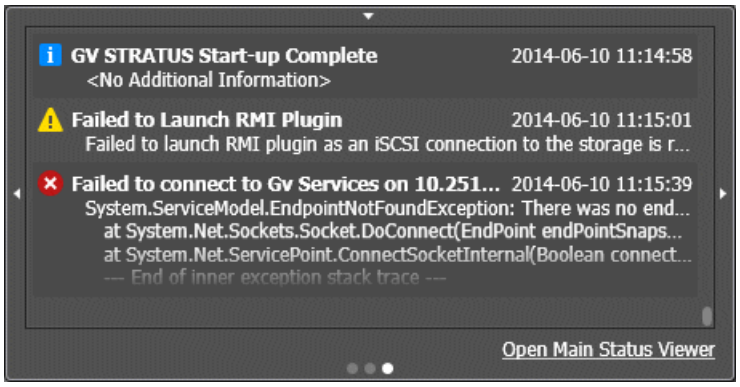
Status Indicator

Displays an alert when a problem occurs that requires your attention.

Notification pop-up panel

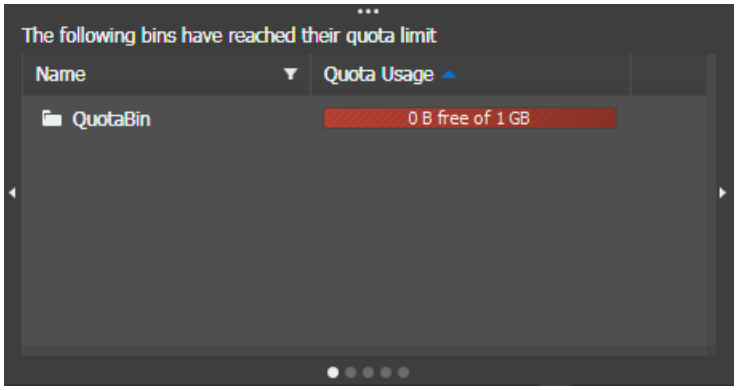
Provides a condensed view of status.

To open the Notification pop-up panel to the Status page, in the lower-right GV STRATUS application Status bar, click the Status indicator. The Status indicator can display the **Error** message icon.



To open the Status Viewer panel for an expanded view, click **Open Main Status Viewer**.

To view other notifications, click the arrow on the right of the pane. You can view security notification, background tasks, job status, system status, and bin quota limit, if reached.



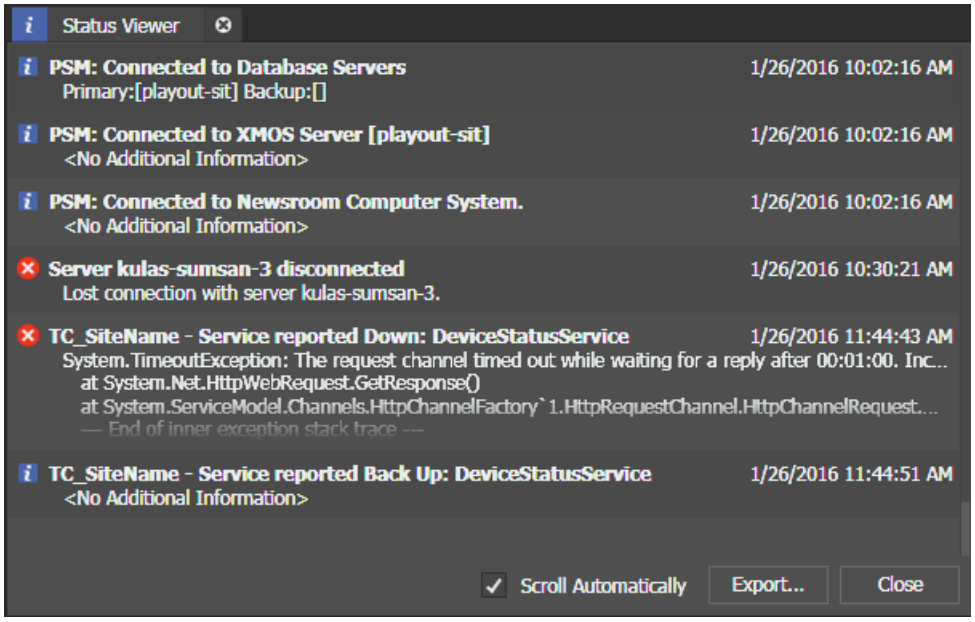
To close the Notification pop-up panel, click the down-arrow on the top edge of the panel or click the Status indicator again.

Status Viewer panel

Allows you to view the status of the application, its components, workspace layout, and any services associated with the application.

To open the main Status Viewer panel, do one of the following:

- Click the Status indicator then click **Open Main Status Viewer**.
- Click **Help | Status**.



The Status Viewer panel gives a complete view of information. You can quickly evaluate the system status information by scanning the display icons:

- **Information**: Indicates an information message.
- **Warning**: Indicates a warning message.
- **Error**: Indicates an error message.

By default, the **Scroll Automatically** box is checked.

Viewing and copying version and status information

You can view version information and status information. If necessary, you can also copy the information and send it to Grass Valley support.

- To access version information do the following:
  a) Click **Help | About**.
     The About dialog box opens.
  b) To copy the detailed system information, click the **Copy Details** button.
  c) When finished viewing or copying the information, click **Close**.
     The dialog box closes.
  d) Paste the copied information into a text file or email, and send it to Grass Valley support.

- To access status information do the following:
  a) Click **Help | Status**.
     The Status Viewer panel opens.
  b) To copy status information, double-click a status message.
     A message box opens.
  c) Highlight the message information and press **Ctrl + C**.
  d) Paste the copied information into a text file or email, and send it to Grass Valley support.

If you have trouble launching EDIUS XS

Confusion about EDIUS for GV STRATUS licensing can cause problems.

The following is required in order to launch the EDIUS for GV STRATUS as a low-resolution editor (EDIUS XS) correctly:

- Your GV STRATUS system must have a Flex, Pro, or Elite license.
- You must be logged on with the EDIUS XS role assigned.
- The client PC on which you are launching EDIUS must not be licensed for EDIUS Workgroup. This is an EDIUS license, intstalled on the client PC and managed by EDIUS license management. It is not a Sabretooth license.

The EDIUS for GV STRATUS application can launch and operate as follows:

- A high resolution editor, identified as EDIUS Workgroup, which can operate in STRATUS mode or in standalone mode. In STRATUS mode, the EDIUS for GV STRATUS application can access GV STRATUS high resolution assets. In standalone mode, the EDIUS for GV STRATUS application cannot access GV STRATUS high resolution assets.
- A low resolution proxy editor, identified as EDIUS XS, which operates in a single mode that must access GV STRATUS proxy assets.

Both of these applications can launch from the **EDIUS** icon .

The same EDIUS software installation package is used to install both types of EDIUS for GV STRATUS applications, so there can be confusion about which application is being launched. This is especially true if licenses for both applications apply to the same client PC, which is not supported. When you launch an EDIUS for GV STRATUS application, it detects the licensing on the client PC. If licensed for EDIUS Workgroup, you are prompted to logon and the EDIUS Workgroup application always launches. You cannot launch EDIUS XS. If not licensed for EDIUS Workgroup you are prompted to logon. Based on your logon, the application checks licensing and roles on the GV STRATUS Core server. If the license includes EDIUS XS and your logon account is assigned the EDIUS XS role, EDIUS XS launches. Therefore, if you have ever licensed the client PC for EDIUS Workgroup, do not use that PC for EDIUS XS.

Troubleshooting tips

Symptom	Solution
No video appears when you click the Live Streaming Video button.	Check networking and connection to the K2 Summit/SAN system V:\ drive. To test, navigate on the K2 Summit/SAN system to the V:\live streaming directory. Open the corresponding *.sdp file in Quicktime and verify that video is available.
Problem with Live Streaming when the K2 Summit system's IP address is changed.	On the K2 Summit system navigate to `V:\live streaming` and use Notepad or a similar text editor to open a `*.sdp` file. Check the first IP address listed in the file, on the `o=` line. If it is not the K2 Summit system's Control Connection IP address, delete the `*.sdp` files in the directory and restart the K2 Summit system.
When running GV STRATUS on a virtual machine or connecting with a Remote Desktop session to a PC running GV STRATUS, there is no video or graphic display in the GV STRATUS application.	Use the GV STRATUS application directly on an actual GV STRATUS client PC. Remote Desktop and virtual machines do not provide the graphics support required by the GV STRATUS application.
The GV STRATUS application takes a long time to open or does not open.	This can happen when the application attempts to load the last used workspace when it opens and there is a problem with that workspace. To open with the default workspace, hold down the left-hand **Alt** key while the application opens. To open with all user settings disabled, open the application from the command prompt using the failsafe switch, as in `STRATUS /failsafe`.
A "Windows could not start the GV STRATUS ... service" Error 1069 message appears.	This can happen when a password is changed using an improper procedure. Refer to related topics in this Topic Library.

Keyboard shortcuts

Inspector keyboard shortcuts

Function	Key	Comment
-1 Frame	**A**	
-10 Frames	**D**	
+1 Frame	**S**	
+10 Frames	**F**	

Function	Key	Comment
Add Keyword	**Ctrl + Insert**	
Add Marker	**Insert**	
Clear Mark In	**Shift + I**	
Clear Mark Out	**Shift + O**	
Clear Marks	**Shift + P**	
Create Subclip	**F4**	In Inspector
Eject	**Ctrl + E**	In Source Viewer, Inspector, Channel Panel, Playlist Editor.
Enable Editable Field	**Alt + Click**	
Fast Forward	**R**	Fast forward with 8X speed.
Forward by Frame	**K (press and hold) + L**	Play video forward by one frame with each press of L.
Send	**F11**	In Inspector, Asset List, Storyboard Editor, Sequence Viewer.
Go to Beginning	**Home**	
Go to End	**End**	
Go to Mark In	**Ctrl + I**	
Go to Mark Out	**Ctrl + O**	
Go to Next Marker	**H**	
Go to Previous Marker	**G**	In Inspector
Toggle visibility of Markers and Keywords	**Ctrl + ?**	
Mark In	**I**	In Channel Panel, trims material before Mark In. In Inspector and Source Viewer, does not affect material before Mark In.
Mark Out	**O**	In Channel Panel, trims material after Mark Out. In Inspector and Source Viewer, does not affect material after Mark Out.
Navigate Back	**Alt + Left Arrow**	
Navigate Forward	**Alt + Right Arrow**	
Pause	**K**	In Inspector, Channel Panel, Source Viewer, Storyboard Editor.
Play/Pause	**Spacebar**	Toggles between play and pause.

Function	Key	Comment
Play from Start	**Q**	
Forward	**L**	In Inspector, Channel Panel, Source Viewer, Storyboard Editor.
Play speed increase	**L (press repeatedly)**	Play video forward, increasing speed with each press (1X, 1.5X, 2X, 5X, 8X, 16X).
Play speed increase	**Shift + (F1 through F9)**	Play video forward, increasing speed with each press of function key: F1 = 0.1X F2 = 0.3X F3 = 0.5X F4 = 1X F5 = 1.5X F6 = 2X F7 = 4X F8 = 8X F9 = 16X
Play Slo-Mo	**K + L (hold down both)**	Play video forward, increasing by 1/10 speed.
Forward by Frame	**K (press and hold) + L**	Play video forward by one frame with each press of L.
Play	**W**	
Reverse	**J**	Play video in reverse.
Reverse speed increase	**J (press repeatedly)**	Play video in reverse, increasing speed with each press (1X, 1.5X, 2X, 5X, 8X, 16X).

Function	Key	Comment
Reverse speed increase	**Ctrl + (F1 through F9)**	Play video in reverse, increasing speed with each press of function key: F1 = 0.1X F2 = 0.3X F3 = 0.5X F4 = 1X F5 = 1.5X F6 = 2X F7 = 4X F8 = 8X F9 = 16X
Reverse Slo-Mo	**K + J (hold down both)**	Play video in reverse, increasing by 1/10 speed.
Reverse by Frame	**K (press and hold) + J**	Play video in reverse by one frame with each press of J.
Rewind	**E**	Rewind with 8X speed.
Solo Audio (for mono tracks)	**Alt + (Corresponding audio track number)**	Only 8 sets of shortcut keys for mono audio tracks are supported. Therefore, only (Alt + 1) through (Alt + 8) shortcut keys are available.
Solo Audio (for stereo pairs)	**Alt + (Corresponding audio pair number)**	Only 8 sets of shortcut keys for stereo audio pairs are supported. Therefore, only (Alt + 1) through (Alt + 8) shortcut keys are available.
Mute Audio	**Shift + Alt + (The number of audio track / audio pair)**	Applicable to mono audio tracks and stereo audio pairs.
Restore all audio tracks	**Alt + 0**	
Toggle Audio between Mono and Stereo	**Shift + Alt + G**	
Trim	**F3**	In Inspector

Channel Panel keyboard shortcuts

Function	Key	Comment
Cue Start	**Home**	
Cue End	**End**	
Eject	**Ctrl + E**	In Source Viewer, Inspector, Channel Panel, Playlist Editor.
Fast Forward	**R**	Fast forward with 8X speed.
Rewind	**E**	Rewind with 8X speed.
Add Marker	**Insert**	In Inspector, Channel Panel, Source Viewer, Sequence Viewer, Storyboard Editor.
Go to Next Marker	**H**	In Inspector, Channel Panel, Source Viewer, Sequence Viewer, Storyboard Editor.
Go to Previous Marker	**G**	In Inspector, Channel Panel, Source Viewer, Sequence Viewer, Storyboard Editor.
Toggle visibility of Markers and Keywords	**Ctrl + ?**	
Mark In	**I**	In Channel Panel, trims material before Mark In. In Inspector and Source Viewer, does not affect material before Mark In.
Mark Out	**O**	In Channel Panel, trims material after Mark Out. In Inspector and Source Viewer, does not affect material after Mark Out.
Play/Pause	**Spacebar**	Toggles between play and pause. Can be disabled in User Preferences for Channel Panel and Playlist Editor.
Play	**W**	
Forward	**L**	In Inspector, Channel Panel, Source Viewer, Storyboard Editor.
Play speed increase	**L (press repeatedly)**	Play video forward, increasing speed with each press (1X, 1.5X, 2X, 5X, 8X, 16X).
Pause	**K**	In Inspector, Channel Panel, Source Viewer, Storyboard Editor.

Function	Key	Comment
Reverse	**J**	Play video in reverse.
Reverse speed increase	**J (press repeatedly)**	Play video in reverse, increasing speed with each press (1X, 1.5X, 2X, 5X, 8X, 16X).
Record	**F12**	
Stop Record	**F11**	In Channel Panel
Enable Editable Field	**Alt + Click**	

Related Topics

About keyboard shortcuts and input focus in a Channel Panel on page 1093

Playlist Editor keyboard shortcuts

Function	Key	Comment
Delete	**Delete**	
Eject	**Ctrl + E**	In Source Viewer, Inspector, Channel Panel, Playlist Editor.
Go to Beginning	**Home**	
Go to End	**End**	
Go to Next	**H**	
Go to Previous	**G**	
Toggle visibility of Markers and Keywords	**Ctrl + ?**	
Play/Pause	**Spacebar**	Toggles between play and pause. Can be disabled in User Preferences for Channel Panel and Playlist Editor.
Play	**W**	
Select All	**Ctrl + A**	
Enable Editable Field	**Alt + Click**	

Scheduler keyboard shortcuts

Function	Key	Comment
Add Event	**A**	
Delete Event	**Delete**	Disabled for deleting bins and assets if delete rights are denied.

Function	Key	Comment
Go to Date	**D**	In Scheduler
Go to Next Day	**H**	In Scheduler
Go to Previous Day	**G**	In Scheduler
Modify Event	**M**	
Properties	**P**	
Quick Schedule	**Q**	
Rename Event	**F2**	
Stop Event	**S**	
Zoom In	**Up Arrow**	In Scheduler
Zoom Out	**Down Arrow**	In Scheduler
Enable Editable Field	**Alt + Click**	

Segmentation keyboard shortcuts

Function	Key	Comment
Delete segment	**Delete**	Disabled for deleting bins and assets if delete rights are denied.
Add Segment	**Alt + Ctrl + Insert**	In Segmentation Panel
Select All	**Ctrl + A**	
Enable Editable Field	**Alt + Click**	

Sequence Viewer keyboard shortcuts

Function	Key	Comment
-1 Frame	**A**	
-10 Frames	**D**	
+1 Frame	**S**	
+10 Frames	**F**	
Add Keyword	**Ctrl + Insert**	
Add Marker	**Insert**	In Inspector, Channel Panel, Source Viewer, Sequence Viewer, Storyboard Editor.
Fast Forward	**R**	Fast forward with 8X speed.
Go to Beginning	**Home**	

Function	Key	Comment
Go to End	**End**	
Go to Next Marker	**H**	In Inspector, Channel Panel, Source Viewer, Sequence Viewer, Storyboard Editor.
Go to Next Page	**Page Down**	
Go to Previous Marker	**G**	In Inspector, Channel Panel, Source Viewer, Sequence Viewer, Storyboard Editor.
Toggle visibility of Markers and Keywords	**Ctrl + ?**	
Play	**W**	
Play/Pause	**Spacebar**	Toggles between play and pause.
Play from Start	**Q**	
Rewind	**E**	Rewind with 8X speed.
Split	****	
Trim In	**F5**	
Trim Out	**F6**	

Source Viewer keyboard shortcuts

Function	Key	Comment
-1 Frame	**A**	
-10 Frames	**D**	
+1 Frame	**S**	
+10 Frames	**F**	
Add Keyword	**Ctrl + Insert**	
Add Marker	**Insert**	In Inspector, Channel Panel, Source Viewer, Sequence Viewer, Storyboard Editor.
Clear Mark In	**Shift + I**	
Clear Mark Out	**Shift + O**	
Clear Marks	**Shift + P**	
Copy Clip	**C**	Copy clip in Source viewer from user-defined mark-in/mark-out values and paste to Storyboard Editor.

Function	Key	Comment
Eject	**Ctrl + E**	In Source Viewer, Inspector, Channel Panel, Playlist Editor.
Fast Forward	**R**	Fast forward with 8X speed.
Forward by Frame	**K (press and hold) + L**	Play video forward by one frame with each press of L.
Go to Beginning	**Home**	
Go to End	**End**	
Go to Mark In	**Ctrl + I**	
Go to Mark Out	**Ctrl + O**	
Go to Next Marker	**H**	In Inspector, Channel Panel, Source Viewer, Sequence Viewer, Storyboard Editor.
Go to Previous Marker	**G**	In Inspector, Channel Panel, Source Viewer, Sequence Viewer, Storyboard Editor.
Toggle visibility of Markers and Keywords	**Ctrl + ?**	
Mark In	**I**	In Channel Panel, trims material before Mark In. In Inspector and Source Viewer, does not affect material before Mark In.
Mark Out	**O**	In Channel Panel, trims material after Mark Out. In Inspector and Source Viewer, does not affect material after Mark Out.
Pause	**K**	In Inspector, Channel Panel, Source Viewer, Storyboard Editor.
Play	**W**	
Play/Pause	**Spacebar**	Toggles between play and pause.
Play from Start	**Q**	
Forward	**L**	In Inspector, Channel Panel, Source Viewer, Storyboard Editor.
Play speed increase	**L (press repeatedly)**	Play video forward, increasing speed with each press (1X, 1.5X, 2X, 5X, 8X, 16X).

Function	Key	Comment
Play speed increase	**Shift + (F1 through F9)**	Play video forward, increasing speed with each press of function key: F1 = 0.1X F2 = 0.3X F3 = 0.5X F4 = 1X F5 = 1.5X F6 = 2X F7 = 4X F8 = 8X F9 = 16X
Play Slo-Mo	**K + L (hold down both)**	Play video forward, increasing by 1/10 speed.
Reverse	**J**	Play video in reverse.
Reverse speed increase	**J (press repeatedly)**	Play video in reverse, increasing speed with each press (1X, 1.5X, 2X, 5X, 8X, 16X).
Reverse speed increase	**Ctrl + (F1 through F9)**	Play video in reverse, increasing speed with each press of function key: F1 = 0.1X F2 = 0.3X F3 = 0.5X F4 = 1X F5 = 1.5X F6 = 2X F7 = 4X F8 = 8X F9 = 16X
Reverse Slo-Mo	**K + J (hold down both)**	Play video in reverse, increasing by 1/10 speed.
Reverse by Frame	**K (press and hold) + J**	Play video in reverse by one frame with each press of J.
Rewind	**E**	Rewind with 8X speed.

Function	Key	Comment
Solo Audio (for mono tracks)	**Alt + (Corresponding audio track number)**	Only 8 sets of shortcut keys for mono audio tracks are supported. Therefore, only (Alt + 1) through (Alt + 8) shortcut keys are available.
Solo Audio (for stereo pairs)	**Alt + (Corresponding audio pair number)**	Only 8 sets of shortcut keys for stereo audio pairs are supported. Therefore, only (Alt + 1) through (Alt + 8) shortcut keys are available.
Mute Audio	**Shift + Alt + (The number of audio track / audio pair)**	Applicable to mono audio tracks and stereo audio pairs.
Toggle Audio between Mono and Stereo	**Shift + Alt + G**	
Restore all audio tracks	**Alt + 0**	

Storyboard keyboard shortcuts

Function	Key	Comment
Add Marker	**Insert**	In Inspector, Channel Panel, Source Viewer, Sequence Viewer, Storyboard Editor.
Delete Event	**Delete** **Ctrl + D**	Both keyboard shortcut keys are supported to delete events in the list.
Forward by Frame	**K (press and hold) + L**	Play video forward by one frame with each press of L.
Go to Next Marker	**H**	In Inspector, Channel Panel, Source Viewer, Sequence Viewer, Storyboard Editor.
Go to Previous Marker	**G**	In Inspector, Channel Panel, Source Viewer, Sequence Viewer, Storyboard Editor.
Toggle visibility of Markers and Keywords	**Ctrl + ?**	
New Sequence	**Ctrl + Shift + N**	
Pause	**K**	In Inspector, Channel Panel, Source Viewer, Storyboard Editor.
Forward	**L**	In Inspector, Channel Panel, Source Viewer, Storyboard Editor.

Function	Key	Comment
Play speed increase	**L (press repeatedly)**	Play video forward, increasing speed with each press (1X, 1.5X, 2X, 5X, 8X, 16X).
Play Slo-Mo	**K + L (hold down both)**	Play video forward, increasing by 1/10 speed.
Reverse	**J**	Play video in reverse.
Reverse speed increase	**J (press repeatedly)**	Play video in reverse, increasing speed with each press (1X, 1.5X, 2X, 5X, 8X, 16X).
Reverse Slo-Mo	**K + J (hold down both)**	Play video in reverse, increasing by 1/10 speed.
Reverse by Frame	**K (press and hold) + J**	Play video in reverse by one frame with each press of J.
Save	**Ctrl + S**	
Split	****	
Trim In	**F5**	
Trim Out	**F6**	
Send	**F11**	In Inspector, Asset List, Storyboard Editor, Sequence Viewer.

All keyboard shortcuts

Key	Function	Comment
A	Add Event	
A	-1 Frame	
Alt + 0	Restore all audio tracks	
Alt + Ctrl + Insert	Add Segment	In Segmentation Panel
Alt + Click	Enable Editable Field	
Alt + (Corresponding audio track number)	Solo Audio (for mono tracks)	Only 8 sets of shortcut keys for mono audio tracks are supported. Therefore, only (Alt + 1) through (Alt + 8) shortcut keys are available.
Alt + (Corresponding audio pair number)	Solo Audio (for stereo pairs)	Only 8 sets of shortcut keys for stereo audio pairs are supported. Therefore, only (Alt + 1) through (Alt + 8) shortcut keys are available.

Key	Function	Comment
Ctrl + C	Copy	Copy clip in Source viewer from user-defined mark-in/mark-out values and paste to Storyboard Editor.
Ctrl + E	Eject	In Source Viewer, Inspector, Channel Panel, Playlist Editor.
Ctrl + (F1 through F9)	Reverse speed increase	Play video in reverse, increasing speed with each press of function key: F1 = 0.1X F2 = 0.3X F3 = 0.5X F4 = 1X F5 = 1.5X F6 = 2X F7 = 4X F8 = 8X F9 = 16X
Ctrl + Insert	Add Keyword	
Ctrl + ?	Toggle visibility of Markers and Keywords	
D	-10 Frames	
D	Go to Date	In Scheduler
Delete	Delete	Disabled for deleting bins and assets if delete rights are denied.
Down Arrow	Zoom Out	In Scheduler
E	Rewind	Rewind with 8X speed.
End	Cue End	
End	Go to End	
F	+10 Frames	
F2	Rename	
F3	Trim	In Inspector
F4	Create Subclip	In Inspector
F5	Trim In	
F6	Trim Out	
F11	Stop Record	In Channel Panel

Key	Function	Comment
F11	Send	In Inspector, Asset List, Storyboard Editor, Sequence Viewer.
F12	Record	
G	Go to Previous Marker	In Inspector, Channel Panel, Source Viewer, Sequence Viewer, Storyboard Editor.
G	Go to Previous Day	In Scheduler
H	Go to Next Marker	In Inspector, Channel Panel, Source Viewer, Sequence Viewer, Storyboard Editor.
H	Go to Next Day	In Scheduler
Home	Cue Start	
Home	Go to Beginning	
I	Mark In	In Channel Panel, trims material before Mark In. In Inspector and Source Viewer, does not affect material before Mark In.
Ctrl + I	Go to Mark In	
Shift + I	Clear Mark In	
Insert	Add Marker	In Inspector, Channel Panel, Source Viewer, Sequence Viewer, Storyboard Editor.
J	Reverse	Play video in reverse.
J (press repeatedly)	Reverse speed increase	Play video in reverse, increasing speed with each press (1X, 1.5X, 2X, 5X, 8X, 16X).
K + J (hold down both)	Reverse Slo-Mo	Play video in reverse, increasing by 1/10 speed.
K (press and hold) + J	Reverse by Frame	Play video in reverse by one frame with each press of J.
K	Pause	In Inspector, Channel Panel, Source Viewer, Storyboard Editor.
L	Forward	In Inspector, Channel Panel, Source Viewer, Storyboard Editor.
L (press repeatedly)	Play speed increase	Play video forward, increasing speed with each press (1X, 1.5X, 2X, 5X, 8X, 16X).

Key	Function	Comment
K + L (hold down both)	Play Slo-Mo	Play video forward, increasing by 1/10 speed.
K (press and hold) + L	Forward by Frame	Play video forward by one frame with each press of L.
Alt + Left Arrow	Navigate Back	
M	Modify Event	
Ctrl + Shift + N	New Sequence	
O	Mark Out	In Channel Panel, trims material after Mark Out. In Inspector and Source Viewer, does not affect material after Mark Out.
Ctrl + O	Go to Mark Out	
Shift + O	Clear Mark Out	
Ctrl + Alt + 0	Full Screen	
P	Properties	
Shift + (F1 through F9)	Play speed increase	Play video forward, increasing speed with each press of function key: F1 = 0.1X F2 = 0.3X F3 = 0.5X F4 = 1X F5 = 1.5X F6 = 2X F7 = 4X F8 = 8X F9 = 16X
Shift + P	Clear Marks	
Shift + Alt + (The number of audio track / audio pair)	Mute Audio	Applicable to mono audio tracks and stereo audio pairs.
Shift + Alt + G	Toggle Audio between Mono and Stereo	In Inspector and Source Viewer
Page Down	Go to Next Keyword/Marker/Page	
Page Up	Go to Previous Keyword/Marker/Page	
Q	Quick Schedule	

Key	Function	Comment
Q	Play from Start	
R	Fast Forward	Fast forward with 8X speed.
Alt + Right Arrow	Navigate Forward	
S	Stop Event	
S	+1 Frame	
Ctrl + S	Save	
Spacebar	Play/Pause	Toggles between play and pause. In Inspector, Source Viewer, Sequence Viewer, Playlist Editor, Channel Panel. Can be disabled in User Preferences for Channel Panel and Playlist Editor.
Up Arrow	Zoom In	In Scheduler
W	Play	
****	Split	

Specifications

System requirements for GV STRATUS client PC

All systems require one or more GV STRATUS client PCs. Verify that all GV STRATUS client PCs meet system requirements.

Virtual Machines, Remote Desktop, and other modes of remote access are not supported. Lack of robust video/graphic support can cause video display problems.

It is also recommended not to run multiple GV STRATUS desktop clients at a time logged in as the same user.

GV STRATUS Web client

These minimum requirements apply to a device running the following:

- The GV STRATUS Web Client

Characteristic	Specification
Web Browser	Recommended: Google Chrome
Frame accurate Streaming	Browser must support webRTC GV STRATUS system must be licensed with GV STRATUS Streaming Server.

GV STRATUS Laptop, and low-resolution Client workstation

These minimum requirements apply to a PC running one or more of the following:

- The GV STRATUS application with a proxy media workflow.
- The GV STRATUS Control Panel application.
- The SiteConfig application.

Characteristic	Specification
Processor	Minimum: Intel Core i3 mid-range processors and above Recommended: Intel Core i5 processor and above
Memory	Minimum: 4GB RAM Recommended: 8GB RAM (Especially when shared with 3rd party applications)
Graphics	Direct 3D 9+ support
System drive	Minimum: 80GB 7200RPM hard drive
Network	Single Ethernet 1000 Base-T network interface
Operating system	Microsoft Windows 7 SP1 32-bit (supported) or 64-bit (preferred) Microsoft Windows 10 64 bit
Microsoft .NET Framework	Version 4.7.1
Web Browser	Recommended: Google Chrome
Other support	DirectX 9 compatible

GV STRATUS/EDIUS XS Laptop, and low-resolution Client workstation

These minimum requirements apply to a PC running the following:

- The GV STRATUS application and the EDIUS XS application, with a proxy media workflow.

Characteristic	Specification
Processor	Intel Core i5 4 core processor and above
Memory	8GB RAM
Graphics	Integrated or discrete graphics with Direct 3D 9 or better
System drive	Minimum: 80GB 7200RPM hard drive Recommended: 128GB SSD drive or larger
Network	Single Ethernet 1000 Base-T network interface

Characteristic	Specification
Operating system	Microsoft Windows 7 SP1 32-bit (supported) or 64-bit (preferred) Microsoft Windows 10 64-bit ***NOTE: 64-bit required for EDIUS XS***
Microsoft .NET Framework	Version 4.7.1
Web Browser	Recommended: Google Chrome
Other support	DirectX 9 compatible

GV STRATUS high-resolution workstation

These requirements apply to a PC running the following:

- The GV STRATUS application with a high-resolution media workflow. This requires access to high-resolution assets.
- The EDIUS Workgroup application with a high-resolution media workflow. This requires access to high-resolution assets.

Characteristic	Specification
Processor	Recommended: Intel Core i7 4 Core 4GHz (For desktop grade machines) OR Recommended: Intel Xeon E5-2630 Quad Core 2.4 GHz (For workstation grade machines)
Memory	Minimum: 8GB RAM Recommended: 16GB RAM
Graphics	Integrated or discrete graphics with Direct 3D 9 or better
System drive	256GB SSD drive recommended OR 1TB 7200RPM hard drive (if SSD not available)
Network	Dual Ethernet 1000 Base-T network interface
Operating system	Microsoft Windows 7 SP1 64-bit Microsoft Windows 10 64-bit (on systems with SNFS 6.0.6 installed) ***NOTE: 64-bit required for EDIUS Workgroup.***
Microsoft .NET Framework	Version 4.7.1
Other support	DirectX 9 compatible

4K (QFHD) and 1080p supported formats

GV STRATUS supports operations with 4K and 1080p assets as follows:

Formats	Compression	Inspector, Source Viewer, RMI, & EDIUS	Storyboard & Playlist Editor	Transfer, Scavenge, & GVRE Transcoder	Conform	Archive, Restore & Partial File Restore (PFR)
2160p - 4K (QFHD) (STRATUS QFHD license is required to be installed on the ExpressCore server)	XAVCI 300 VBR	Supported.	Not supported.	Supported.	Supported for single location only. Conform to multiple (GXF) location is not supported.	Supported. (For MXF files only) ***NOTE: Masstech and GFTP do not support Partial File Restore (PFR) of 4K assets.***
	XAVCI 480 VBR	Supported.	Not supported.	Supported.	Supported for single location only. Conform to multiple (GXF) location is not supported.	Supported. (For MXF files only) ***NOTE: Masstech and GFTP do not support Partial File Restore (PFR) of 4K assets.***
1080p	AVC-Intra Class 100 (AVC-Long GOP is not supported)	Supported.	Supported.	Supported.	Supported.	Supported. (For MXF files only) ***NOTE: GFTP does not support Partial File Restore (PFR) of 1080p assets.***

Notes:

- 4K is not supported on K2 SAN systems with clients that are connected via iSCSI. A 4K client must be connected via fibre channel.
- K2 SAN clients with iSCSI connections can only support a maximum of two 1080p records per client.
- RMI supports the import of 4K (QFHD) assets of single essence AVCI and playback as MXF file.
- EDIUS Workgroup supports 4K (QFHD) direct write as CMF file. (Provided that K2 XAVC Clip exporter is added to EDIUS Exporter dialog)
- GV Render Engine supports the proxy creation of 4K (QFHD) and 1080p assets.

- GVRE Transcoder supports the export of 4K (QFHD) assets via iSCSI/SMB and FTP connections.
- GVRE Transcoder supports the import of 4K (QFHD) assets via iSCSI/SMB connection only. If K2 Summit Access Protocols were configured to FTP, 4K (QFHD) import will fail since 4K GXF format is not supported.
- DIVA and FlashNet archive systems support archive, restore, and partial file restore (PFR) operations of 4K (QFHD) and 1080p assets.
- Masstech and Generic FTP archive systems support archive and restore operations of 4K (QFHD) and 1080p assets.
- Masstech supports the partial file restore (PFR) operation of 1080p assets, but not 4K (QFHD) assets.
- Generic FTP archive system does not support the partial file restore (PFR) operation of any assets.

K2 system specifications

This section contains specifications for K2 systems.

Video codec description K2 Summit system

K2 Summit 3G Production Client, and K2 Solo Media Server specifications are shown in the following tables. Licenses and/or hardware options are required to enable the full range of specifications.

DV formats

Format	Sampling	Frame Rate	Data Rate	Other
DVCAM 720x480i 720x576i	4:1:1/4:2:0	29.97, 25	28.8 Mbps	Conforms to IEC 61834
DVCPRO25 720x480i 720x576i	4:1:1	29.97, 25	28.8 Mbps	Conforms to SMPTE 314M
DVCPRO50 720x487.5i 720x585i	4:2:2	29.97, 25	57.6 Mbps	Conforms to SMPTE 314M
DVCPRO HD 1280x1080i 1440x1080i	4:2:2	29.97, 25	100 Mbps	Conforms to SMPTE 370M
DVCPRO HD 960x720p	4:2:2	59.94, 50	100 Mbps	Conforms to SMPTE 370M

MPEG-2 formats

Format	Sampling	Frame Rate	Data Rate (Mbps)	Other
720x480i	4:2:0	29.97	2-15	I-frame and long GoP
720x480i	4:2:2	29.97	4-50	I-frame and long GoP
720x512i	4:2:2	29.97	4-50	I-frame and long GoP
720x576i	4:2:0	25	2-15	I-frame and long GoP
720x576i	4:2:2	25	4-50	I-frame and long GoP
720x608i	4:2:2	25	4-50	I-frame and long GoP
D10/IMX 720x512i	4:2:2	29.97	30, 40, 50 CBR	I-frame only
1280x720p	4:2:0	59.94, 50	20-80	I-frame and long GoP
1280x720p	4:2:2	59.94, 50	20-100	I-frame and long GoP
D10/IMX 720x608i	4:2:2	25	30, 40, 50 CBR	I-frame only
1920x1080i	4:2:0	29.97, 25	20-80	I-frame and long GoP[1]
1920x1080i	4:2:2	29.97, 25	20-100	I-frame and long GoP
XDCAM-HD 1440x1080i	4:2:0	29.97, 25	18 VBR, 25 CBR, 35 VBR	Long GoP
XDCAM-HD422 1920x1080i	4:2:2	29.97, 25	50 CBR	Long GoP
XDCAM-HD422 1280x720p	4:2:2	59.94, 50	50 CBR	Long GoP
XDCAM-EX 1920x1080i	4:2:0	29.97, 25	35 VBR	Long GoP
XDCAM-EX 1280x720p	4:2:0	59.94, 50	25 CBR, 35 VBR	Long GoP

K2 systems record closed GoP structure. If an open GoP clip is imported, it is fully supported, including trimming the clip, playout of the clip, using the clip in playlists, and exporting the clip.

[1] Decode of lower bit rate is possible

AVC-Intra formats

Format	Sampling	Frame Rate	Data Rate	Other
AVC-Intra Class 50 1440x1080i	4:2:0	29.97, 25	50 Mbps	Requires licenses or hardware for support on different K2 Summit system models.
AVC-Intra Class 50 960x720p	4:2:0	59.94, 50	50 Mbps	
AVC-Intra Class 100 1920 x 1080i	4:2:2	29.97, 25	100 Mbps	
AVC-Intra Class 100 1280 x 720p	4:2:2	59.94, 50	100 Mbps	
AVC-Intra Class 100 1920 x 1080p	4:2:2	59.94, 50	200 Mbps	

AVCHD/H.264 formats

The following formats are for AVCHD and PitchBlue content. These are only supported for play output (decode) on AVCHD. A license is required. Record input (encode) is not supported.

Format	Sampling	Frame Rate	Data Rate	Other
720x480i	4:2:0	29.97	4-50	H.264-style open GoP. GoP length up to 30 frames. Up to 4 B-frames between anchor frames.
	4:2:2	29.97	4-50	
720x512i	4:2:2	29.97	4-50	
720x576i	4:2:0	25	4-50	
	4:2:2	25	4-50	
720x608i	4:2:2	25	4-50	
1920x1080i	4:2:0	29.97, 25	24 Mbps max.	
	4:2:2	29.97, 25	24 Mbps max.	
1440x1080i	4:2:0	29.97, 25	24 Mbps max.	
	4:2:2	29.97, 25	24 Mbps max.	
1280x720p	4:2:0	59.94, 50	24 Mbps max.	
	4:2:2	59.94, 50	24 Mbps max.	

AVC-LongG formats

The following formats are for AVC-LongG content. These are only supported for play output (decode). A license is required. Record input (encode) is not supported.

Format	Sampling	Frame Rate	Data Rate	Other
AVC-LongG6 1920x1080i	4:2:0	29.97, 25	6 Mbps	LongG
AVC-LongG6 1280x720p	4:2:0	59.94, 50	6 Mbps	
AVC-LongG12 1920x1080i	4:2:0	29.97, 25	12 Mbps	
AVC-LongG12 1280x720p	4:2:0	59.94, 50	12 Mbps	
AVC-LongG25 1920x1080i	4:2:2	29.97, 25	25 Mbps	
AVC-LongG25 1280x720p	4:2:2	59.94, 50	25 Mbps	
AVC-LongG50 1920x1080i	4:2:2	29.97, 25	50 Mbps	
AVC-LongG50 1280x720p	4:2:2	59.94, 50	50 Mbps	

Avid DNxHD formats

The following formats are for Avid DNxHD content. These are supported for record input (encode) and play output (decode). A Summit 3G Codec board with a K2-XDP2-DNX-2CH license is required.

Format	Frame Rate	Data Rate	Bits	Other
1920x1080i	29.97	220 Mbps	10	Avid DNxHD 220x
	29.97	220 Mbps	8	Avid DNxHD 220
	29.97	145 Mbps	8	Avid DNxHD 145
	25	184 Mbps	10	Avid DNxHD 185x
	25	184 Mbps	8	Avid DNxHD 185
	25	121 Mbps	8	Avid DNxHD 120
1280x720p	59.94	220 Mbps	10	Avid DNxHD 220x

Format	Frame Rate	Data Rate	Bits	Other
	59.94	220 Mbps	8	Avid DNxHD 220
	59.94	145 Mbps	8	Avid DNxHD 145
	50	175 Mbps	10	Avid DNxHD 175x
	50	175 Mbps	8	Avid DNxHD 175
	50	116 Mbps	8	Avid DNxHD 115

Playout of multiple formats

The K2 Summit system automatically handles material of various types and formats as specified in the following sections:

Playout on K2 Summit system

For a given frame rate, you can play SD clips of any format back-to-back on the same timeline. Both 16:9 and 4:3 SD aspect ratio formats can be played on the same timeline. Refer to video codec description earlier in this section for a list of the supported formats.

On channels with the XDP (HD) license, for similar frame rates (25/50 fps or 29.97/59.95 fps), SD material transferred or recorded into the K2 Summit system along with its audio is up-converted when played on a HD output channel. Likewise, HD material is down-converted along with its audio when played on an SD output channel. HD and SD clips can be played back-to-back on the same timeline, and aspect ratio conversion is user configurable.

The K2 Summit system supports mixed clips with uncompressed and compressed (PCM, AC3, and Dolby) audio on the same timeline.

25/50 fps conversions on HD K2 Summit system models

The following specifications apply to K2 Summit system channels with the XDP (HD) license.

		Converted SD format	**Converted HD format**	**Converted HD format**
		625 at 25 fps	**1080i at 25 fps**	**720p at 50 fps**
Source SD format	**625 at 25 fps**	No conversion	Up-convert SD to HD	Up-convert SD to HD
Source HD format	**1080i at 25 fps**	Down-convert HD to SD	No conversion	Cross-convert from 1080i to 720p
	720p at 50 fps	Down-convert HD to SD	Cross-convert from 720p to 1080i	No conversion

29.97/59.95 fps conversions on HD K2 Summit system models

The following specifications apply to K2 Summit system channels with the XDP (HD) license.

		Converted SD format	Converted HD format	Converted HD format
		525 at 29.97 fps	**1080i at 29.97 fps**	**720p at 59.94 fps**
Source SD format	**525 at 29.97 fps**	No conversion	Up-convert SD to HD	Up-convert SD to HD
Source HD format	**1080i at 29.97 fps**	Down-convert HD to SD	No conversion	Cross-convert HD to HD
	720p at 59.94 fps	Down-convert HD to SD	Convert HD to HD	No conversion

Internationalization

When you enable internationalization on a K2 Summit system, you can name your media assets in a local language. The K2 Summit system supports the local language name as specified in the following table.

System	Internationalization support
Keyboard input and display	• English • Chinese • Japanese • French • German • Spanish • Cyrillic (Russian) • Portuguese • Korean
Media database	• All external views of movie assets can be represented as wide-file names. • AppCenter runs in Unicode. • Only movie assets and searchable User Data keys are Unicode.
Media file system	• Support for Kanji and wide-character file and folder names. • File-folder representation of movie are internationalized, as well as the QuickTime reference file it contains. • Key names (V:\media) remain unchanged, but are Unicode.
K2 Summit system applications	• Movie assets are described in Unicode. • Application user interfaces are Unicode compliant.
Protocols	Refer to "Remote control protocols" in the "Configuring the K2 System" section of the K2 Topic Library.

System	Internationalization support
FTP transfers	Refer to "FTP internationalization" in the "Configuring the K2 System" section of the K2 Topic Library.

Names of media assets and bins must conform to the naming specifications for assets and bins.

Limitations for creating and naming assets and bins

Media assets and bins must conform to the following specifications.

Characters not allowed in asset and bin names

Position	Character	Description
Anywhere in name	\	backward slash
	/	forward slash
	:	colon
	*	asterisk
	?	question mark
	<	less than
	>	greater than
	%	percent sign
	|	pipe
	"	double quote
At beginning of name	~	tilde
		space
At the end of name		space

Asset and bin name limitations

The maximum number of characters in an asset path name, including the bin name, is 259 characters. This includes separators such as "\" and parts of the path name that are not visible in AppCenter. The file system limits the number of bytes in a name as well as the number of characters. The values in this table apply to names in English and other languages referred to in ISO 8859-1. The full count of 259 characters might not be available with some other character sets.

	Asset name, bin name, and path			
Sections of an asset/path name	**The rest of the path name** (i.e. everything apart from the bin and asset names)	Bin name	Asset media directory and extension	Asset name and extension
Naming limitation	This part of the path name is not visible in AppCenter.	The bin name can be up to 227 characters (which would leave room for only a 1-character asset name)	This part of the path name is not visible in AppCenter. The directory name is the same as the asset name. 4 characters are reserved for the extension.	The extension is not visible in AppCenter. At least 25 characters are reserved for the asset name and extension, even if they are not all used.
Example	*\media*	*\mybin1\mybin2*	*\MyVideo.cmf*	*\MyVideo.xml*

The following examples show how a path name would appear in AppCenter and in the file system.

In AppCenter:

V:\mybin1\mybin2\MyVideo

In the file system:

V:\media\mybin1\mybin2\MyVideo.cmf\MyVideo.xml

Bin nesting limitations

The K2 media database supports nine levels of nested bins. This includes the top level (first) bin. Exceeding this specification results in a database error. When creating a bin do not create a bin at level ten or deeper.

For example:

- The following is supported:
  ```
  default\en\fr\es\de\it\be\dk\cn
  ```
- The following is not supported:
  ```
  default\en\fr\es\de\it\be\dk\cn\jp
  ```

Formats supported for import and export

When you import or export files using the GV STRATUS application, your K2 Summit/SAN system does the actual import/export. Therefore, if a format is supported for import/export in the GV STRATUS application, it must be supported on the K2 Summit/SAN system.

The following formats are supported for import/export using the GV STRATUS application:

- GXF
- MXF

- QuickTime
- MPG (for import only); including support for both MPG Transport Stream files (TS) and Programme Stream files (PS)

In addition, the following formats are supported for import/export on K2 Summit/SAN systems. By using the K2 AppCenter application or other file interchange mechanisms supported on K2 Summit/SAN systems, these formats can be used to make assets available to the GV STRATUS system:

- AVI
- MPEG
- P2
- WAV

Refer to topics in this section for detailed information about file interchange with these formats.

About file interchange mechanisms on K2 systems

K2 Summit, Solo, and SAN systems can send and receive files as follows:

- File based import/export — This is based on a file that is visible from the operating system. For example, AppCenter import/export features are file based.
- HotBin import/export — This is file based import/export, with automated features that are triggered when a clip is placed in a bin. Some HotBin functionality requires licensing.
- FTP stream — This is file interchange via File Transfer Protocol (FTP).

GXF interchange specification

This specification applies to GXF file transfer, import, and export on K2 Summit, Solo, and SAN systems.

Streaming between online K2 systems supports complex movies and agile playlists of mixed format.

Formats are supported are as follows:

Supported formats		Notes
Video	DVCPRO25	—
	DVCPRO50	—
	DVCPRO HD	Super Slo-Mo requires software version 7.1.x or higher
	DVCAM	—
	MPEG-2	Includes all MPEG-2 formats (IMX, XDCAM, etc.) that can be stored on a K2 system
	AVC-Intra	—
	H.264	Playable on K2 Summit 3G system only. Can transfer to systems with K2 software version 8.x and higher.

Supported formats		Notes
	Avid DNxHD	Playable on K2 Summit 3G system only. Can transfer to systems with K2 software version 8.x and higher.
	Apple ProRes	Supported systems: K2 Summit 3G system, K2 Summit IP client SDI I/O and K2 Summit IP client IP I/O. Can transfer to systems with K2 version 9.8 and higher.
Audio	48 kHz	—
	16 bit, 24 bit	—
	PCM, Dolby-E, AC-3	—
Data	VBI	—
	Ancillary	—

Interchange mechanisms are supported as follows:

Mechanism		Support
File based	Import	Yes
	Export	Yes
FTP stream	Import	Yes
	Export	Yes

MXF interchange specification

This specification applies to MXF file transfer, import, and export on K2 Summit, Solo, and SAN systems.

MXF supports simple clips with a single video track only.

Formats are supported are as follows:

Supported formats		Notes
Video	DVCPRO25	—
	DVCPRO50	—
	DVCPRO HD	Super Slo-Mo requires software version 7.1.x or higher
	DVCAM	—
	D10	See MXF export behavior for eVTR style D10AES3.
	MPEG-2	Includes all MPEG-2 formats (IMX, XDCAM, etc.) that can be stored on a K2 system

Supported formats		Notes
	AVC-Intra	—
	Avid DNxHD	Playable on K2 Summit 3G system only. Can transfer to systems with K2 software version 8.x and higher.
	Apple ProRes	Supported systems: K2 Summit 3G system, K2 Summit IP client SDI I/O and K2 Summit IP client IP I/O. Can transfer to systems with K2 version 9.8 and higher.
Audio	48 kHz	—
	16 bit, 24 bit	—
	PCM, Dolby-E, AC-3	—
Data	VBI	MXF supports either ancillary data packets or VBI lines in the data track but not both, so if ancillary data packets and VBI lines have been recorded into the K2 clip's data track, then the VBI lines will be dropped from the MXF data track on an MXF export.
	Ancillary	—

Interchange mechanisms are supported as follows:

Mechanism		Support
File based	Import	Yes
	Export	Yes
FTP stream	Import	Yes
	Export	Yes

With a special export option, you can export a completed continuous (loop) record clip as MXF or QuickTime, with the result being a flattened stream file. Recording must be complete before you export the clip, however you can make subclips while record is underway and export the subclips. For this feature, MPEG-2 long GoP is not supported.

MXF export behavior on K2 systems

Upon MXF export the K2 system checks clip structure for specifications as they apply to industry standard formats such as Sony XDCAM (SMPTE RDD-09) and Sony eVTR style (SMPTE ST 386). If specifications match, the media is exported as the appropriate format.

The K2 system allows you to override the MXF export behavior so that the exported MXF file no longer match the specifications for the industry-standard format. For example, you can export a clip containing more audio tracks than constrained by the specific MXF standard for the maximum number of audio tracks in a D10AES3 channel. If you export a clip with such an override, the K2 will generate a generic MXF op1a file (instead of the default D10 or XDCAM constrained MXF file).

About MXF with DIDs and SDIDs

You can import and export MXF containing ANC packets and VBI lines as specified in SMPTE ST 436. The K2 system extracts the ANC packets or VBI lines to the K2 clip's data track.

MXF Export Type

When importing and exporting MXF the K2 system behaves as follows, in relation to the MXF Export Type setting in K2Config or in K2 AppCenter:

- The MXF Export Type setting applies to all MXF exports on the K2 system. There is one setting for one K2 system. The K2 system can be a K2 Summit system system or a K2 SAN. If a K2 SAN, the one setting applies to the K2 Media Server with role of FTP server that handles exports for all SAN-attached K2 Summit systems.
- For export, the K2 system must be set to one of the following MXF Export Types:
  - **377M**: SMPTE ST 377:2004 compliant. Ensures compatibility with older products.
  - **377-1**: SMPTE ST 377-1:2009 compliant.
  - **ARD and 377-1**: ARD is only for AVC-Intra Class 100 (720p and 1080i PAL only) and XDCAMHD-422 (1080i PAL only).
- By default the K2 system is set to SMPTE ST 377:2004. This setting is only applicable to the MXF op1a import and export.
- The SMPTE ST 377:2004 setting is recommended for compatibility with older systems which do not support SMPTE ST 377-1:2009.
- The following format does not support SMPTE ST 377-1:2009 export. Therefore the format is always exported as SMPTE ST 377:2004, regardless of the MXF Export Type setting:
  - D10 media
- ARD profile is the MXF profile based only on AVC-Intra Class 100 and XDCAMHD-422 formats for compliance with ARD consortium.
- The following format does not support ARD export. Therefore the format is always exported as SMPTE ST 377-1:2009, when **ARD and 377-1** option is selected:
  - DV media
  - Avid DNxHD media
  - Media in NTSC format
- For import, both SMPTE ST 377:2004 and SMPTE ST 377-1:2009 are supported, regardless of the MXF Export Type setting. The MXF Export Type setting affects export only.

AMWA AS-02 interchange

The K2 system behaves as follows in relation to the Advanced Media Workflow Association (AMWA) AS-02 version 1.0: 2011 MXF Versioning Specification:

- The K2 system supports the AS-02 specification with no customizations
- Supports import of AS-02 content
- Plays media imported with AS-02

- Exports media to AS-02 content
- Requires license K2-ExtendedFileServices.

QuickTime interchange specification

This specification applies to QuickTime file transfer, import, and export on K2 Summit, Solo, and SAN systems.

The following are not supported:

- Sequences and lists
- Lists of mixed formats or containing empty tracks, such as tracks that do not contain recorded media

Formats are supported are as follows:

Supported formats		Notes
Video	DVCPRO25	—
	DVCPRO50	—
	DVCPRO HD	Super Slo-Mo requires software version 7.1.x or higher
	DVCAM	—
	AVC-Intra	—
	D10/IMX	—
	XDCAM-HD	—
	XDCAM-EX	—
	XDCAM-HD422	—
	H.264	Playable on K2 Summit 3G system only. Can transfer to systems with K2 software version 8.x and higher.
	Avid DNxHD	—
	Apple ProRes	—
Audio	48 kHz	
	16 bit, 24 bit PCM	
Data	None	—

Interchange mechanisms are supported as follows:

Mechanism		Support
File based	Import	Yes
	Export	Yes

Mechanism		Support	
FTP stream	Import	Yes	FTP import (FTP put) of a QuickTime file is internally handled in two stages. The FTP put will result in the QuickTime file being internally copied and the FTP status will reflect the status of this copy. When the entire QuickTime file is copied, the K2 will internally import the copied QuickTime file and the imported file will then become available as a K2 clip.
	Export	Yes	***NOTE: FTP get of a growing K2 clip (a K2 clip being recorded or imported) is not supported.***

With a special export option, you can export a completed continuous (loop) record clip as MXF or QuickTime, with the result being a flattened stream file. Recording must be complete before you export the clip, however you can make subclips while record is underway and export the subclips. For this feature, MPEG-2 long GoP is not supported.

QuickTime video and key import specification

This specification applies to importing a QuickTime file with an alpha channel. This is a licensed feature.

The imported file must be QuickTime 32 with alpha RLE 32-bit raster encoding, as produced by the Apple Animation Codec.

Supported video formats for import are as follows:

Format		Scan	Frame Rate
SD video	720 x 480	Interlaced	29.97
	720 x 512	Interlaced	29.97
	720 x 576	Interlaced	25
	720 x 608	Progressive	25
HD video	1920 x 1080	Interlaced	29.97, 25
	1280 x 720	Progressive	59.94, 50

Supported audio formats for import are as follows:

Format		
Audio tracks (if present)	48 kHz	Mono or stereo
	16 bit, 24 bit	
	PCM	

Interchange mechanisms are supported as follows:

Mechanism		Support	
File based	Import	Yes	
	Export	No	
FTP stream	Import	Yes	FTP import (FTP put) of a QuickTime file is internally handled in two stages. The FTP put will result in the QuickTime file being internally copied and the FTP status will reflect the status of this copy. When the entire QuickTime file is copied, the K2 will internally import the copied QuickTime file and the imported file will then become available as a K2 clip.
	Export	Yes	***NOTE: FTP get of a growing K2 clip (a K2 clip being recorded or imported) is not supported.***

When K2 software imports a file that meets the above requirements, it creates a K2 clip with two video tracks, in formats as follows:

Format			Frame Rate	Data Rate
SD video	D10/IMX	720 x 512	29.97	50 CBR
	D10/IMX	720 x 608	25	50 CBR
HD video	AVC-Intra Class 100	1920 x 1080	29.97, 25	100 Mbps
	AVC-Intra Class 100	1280 x 720	29.97, 25	100 Mbps

Audio tracks, if present are imported.

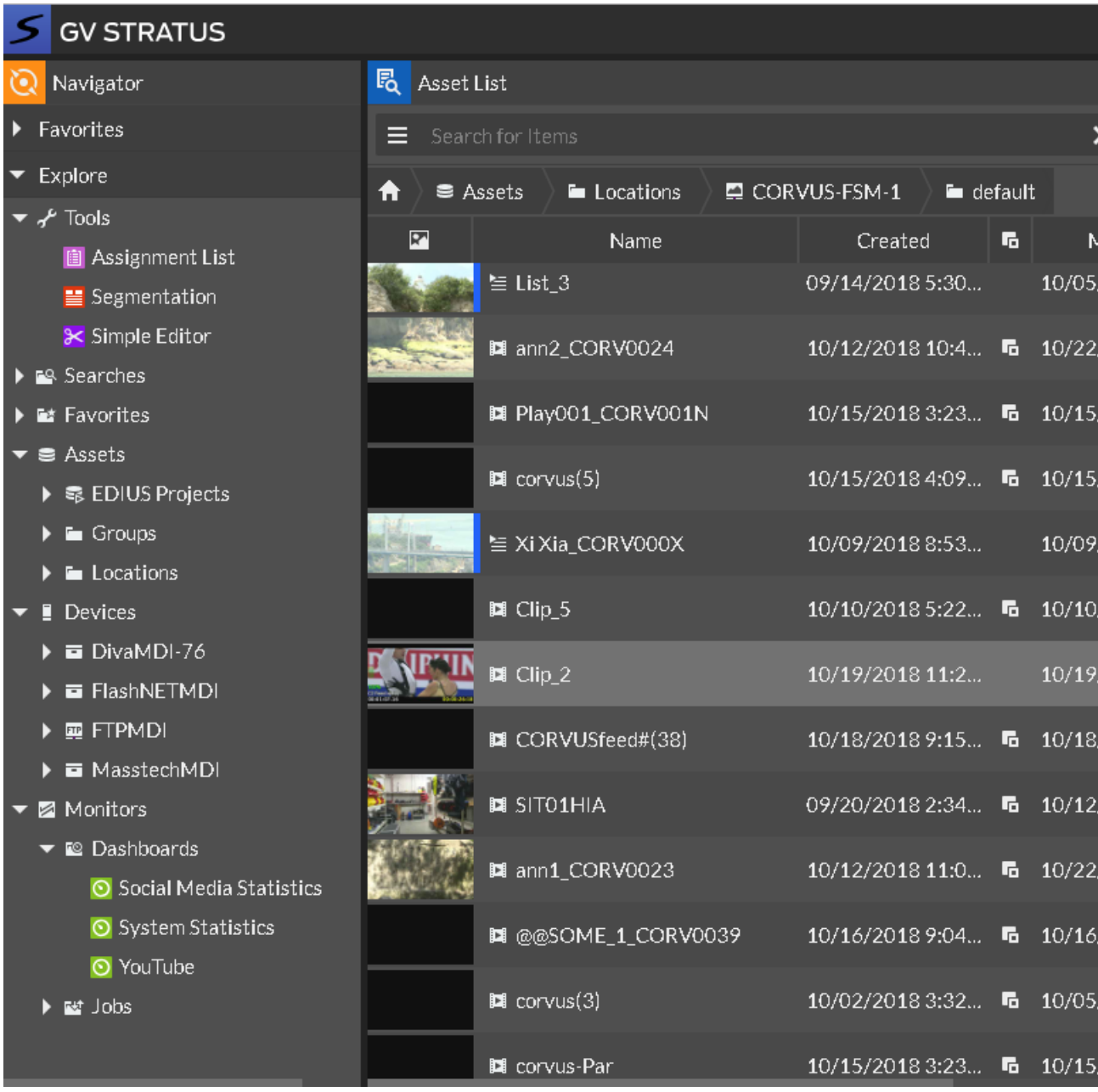
Timecode data is imported as K2 striped timecode. The first timecode value is the starting value and subsequent timecode is continuous.

The import process consumes system resource since this involves video transcoding. Be aware of this if running other resource intensive processes during import.

GV STRATUS Web Client

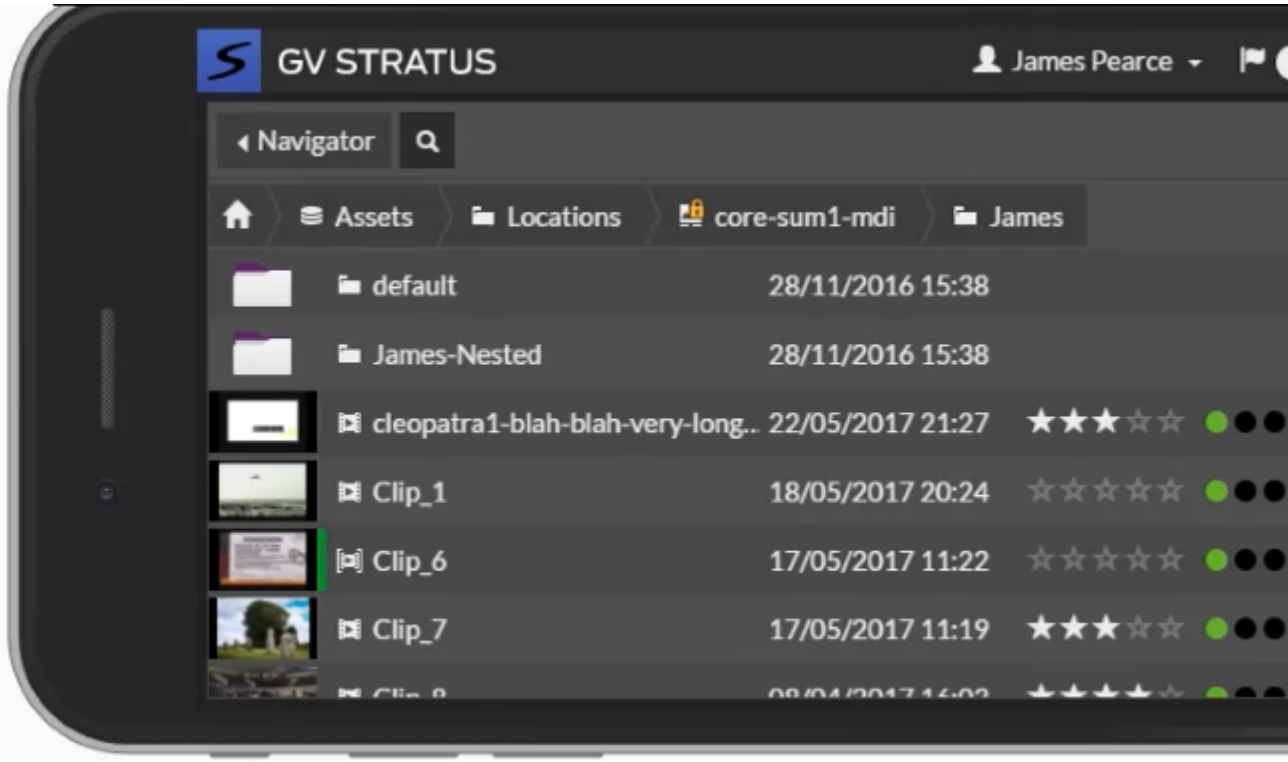
Using the GV STRATUS Web Client

The GV STRATUS Web Client consists of the Navigator, Asset List, Inspector, Assignment List, Segmentation tool, and the Simple Editor tool. You can search assets, navigate to assets, view assets in the video player, modify asset properties, insert markers/keywords into assets, archive assets, and use the Simple Editor tool to edit assets. The Assignment List allows you to create placeholders for assets, assign those placeholders to newsroom editors, and link the resulting assets to rundown stories on your Newsroom Computer System. The Segmentation tool allows you to create multiple segments of the asset for diverse broadcast schedules, and arrange segments for insertion of commercials in between. With this workflow, you can easily view your high resolution media, insert markers or keywords, edit assets, and regenerate proxy in just one workspace.



If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. You can only view metadata with read permissions, and modify metadata with write permissions. If read or write permissions are denied, your metadata fields will be disabled.

The GV STRATUS Web Client is also supported on mobile devices as shown below.



Logging on to the GV STRATUS Web Client

- These SiteConfig roles must be assigned in the Express/Core server:
  - GV STRATUS Web Apps
  - GV STRATUS Web Client
  - GV STRATUS Proxy Streaming Service
- These licenses must be installed in the Express/Core server via SabreTooth:
  - STRATUS-WEB-CLIENT
  - STRATUS-PROXYSTREAMING

When you log on to the GV STRATUS system, the GV STRATUS application assigns GV STRATUS licenses and roles based on your user account credentials, as set by the system administrator in the GV STRATUS Control Panel application. If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins and assets that are part of your workflow. If GV STRATUS metadata access control is enforced, your credentials must give you adequate permissions on metadata fields that are part of your workflow. Your credentials must also give you access to all your K2 systems.

You can open the GV STRATUS Web Client in a supported web browser, such as Chrome, using the following web address template: **http://<core_server_name>/webclient**

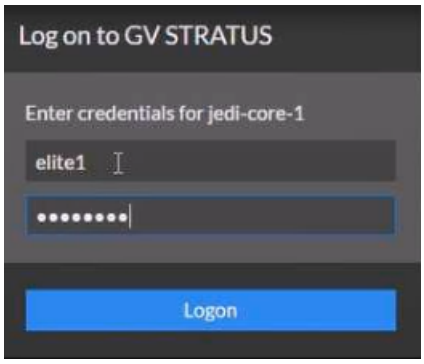
If you have a certificate from a genuine, trusted, authority installed, you can also access the web client at: **https://<core_server_name>/webclient**

The web page (the origin) may be served unencrypted over HTTP, but all communication with the GV STRATUS core services, including log on credentials, occurs over HTTPS and is fully encrypted. In order for the browser to trust the server and begin an HTTPS connection, it needs to validate a

certificate. These certificates must come from a known organization called a certificate authority – one that the browser trusts to verify the server is who it says it is.

1. Launch the GV STRATUS Web Client using your web browser.

   A GV STRATUS Log On dialog opens.



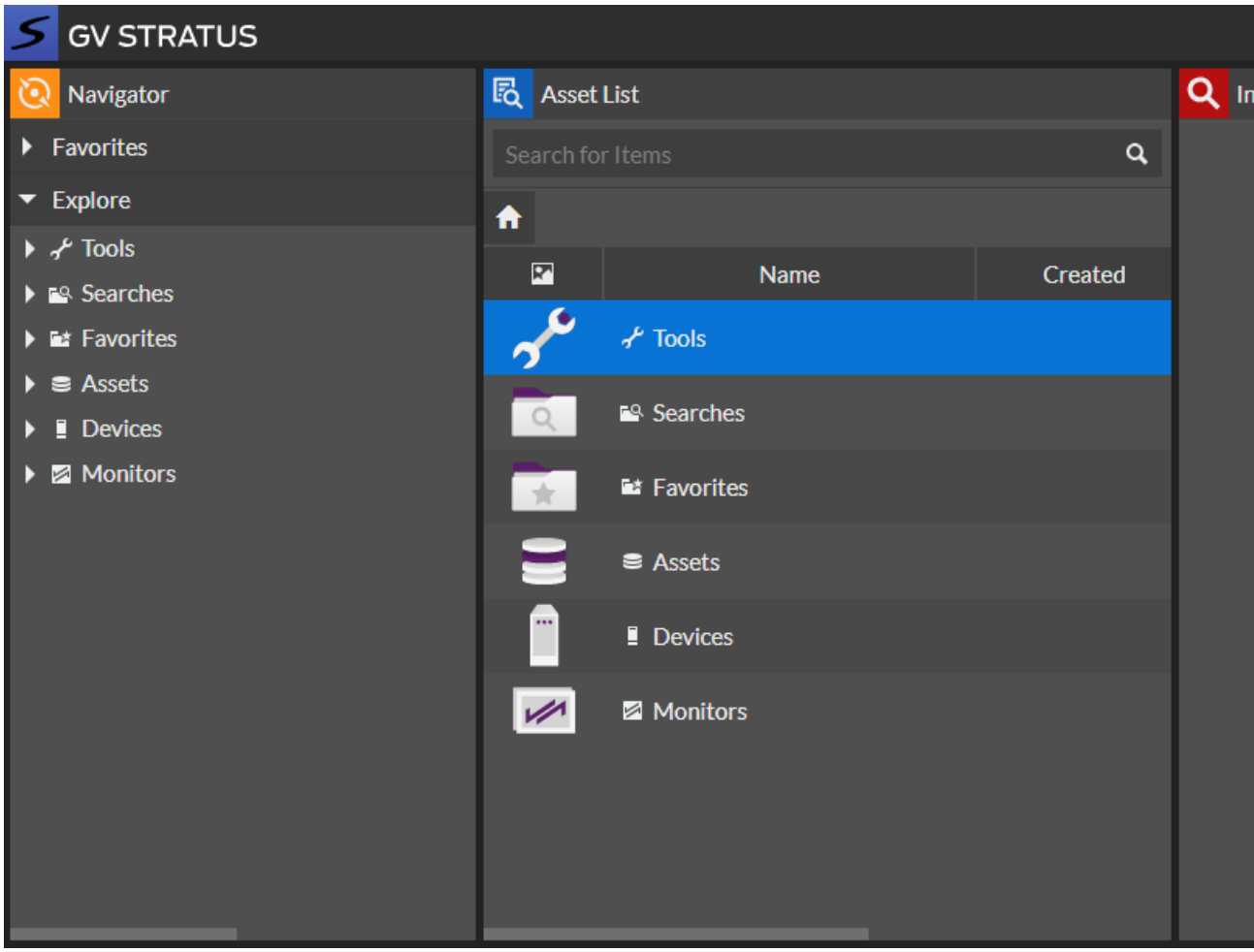
2. Enter your user name.

   If you use domain credentials, enter in format `<domain>\<username>`. For example, if your domain is "gv" and your username is "GVuser", enter `gv\GVuser`.

   If you have successfully logged on before, select your user name from the drop-down list.

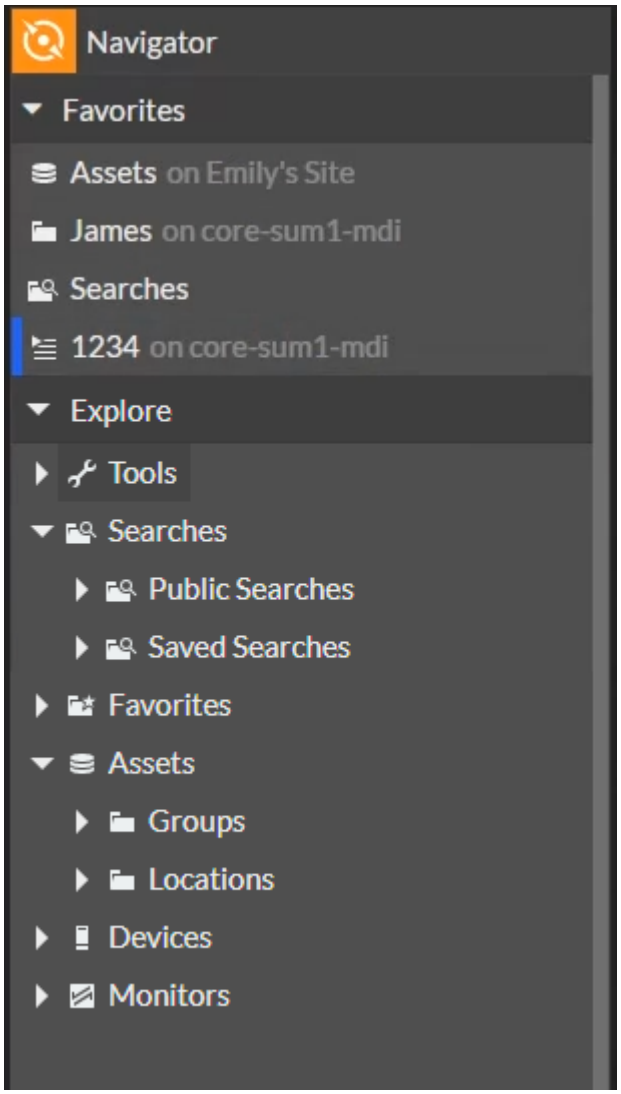
3. Enter your password.
4. Click **Log On**.

The GV STRATUS Web Client opens.



The Navigator panel

The Navigator panel functions as the starting point for workflows using the GV STRATUS Web Client. When you select an item in the Navigator, it displays in the Asset List panel.



The Navigator panel contains the following section:

- **Favorites** — A list of shortcuts to GV STRATUS items.
- **Explore** — A tree-based hierarchy with which you can browse your system.

From the Explore section, you can access the following:

Tools: Expands to display the Simple Editor tool for editing workflow in the GV STRATUS Web Client application.

Searches: Expands to display searches that can be reused and shared.

Favorites: Expands to display a list of favorites.

Assets: Expands to display a view of groups and assets based on the information available in the STRATUS database. Any assets can be grouped together, regardless of their actual location in K2 system storage.

Devices: Expands to display the devices that the STRATUS application accesses or controls.

Monitors: Expands to display tools for monitoring transfers and web pages. The status of **Jobs** can be accessed from here.

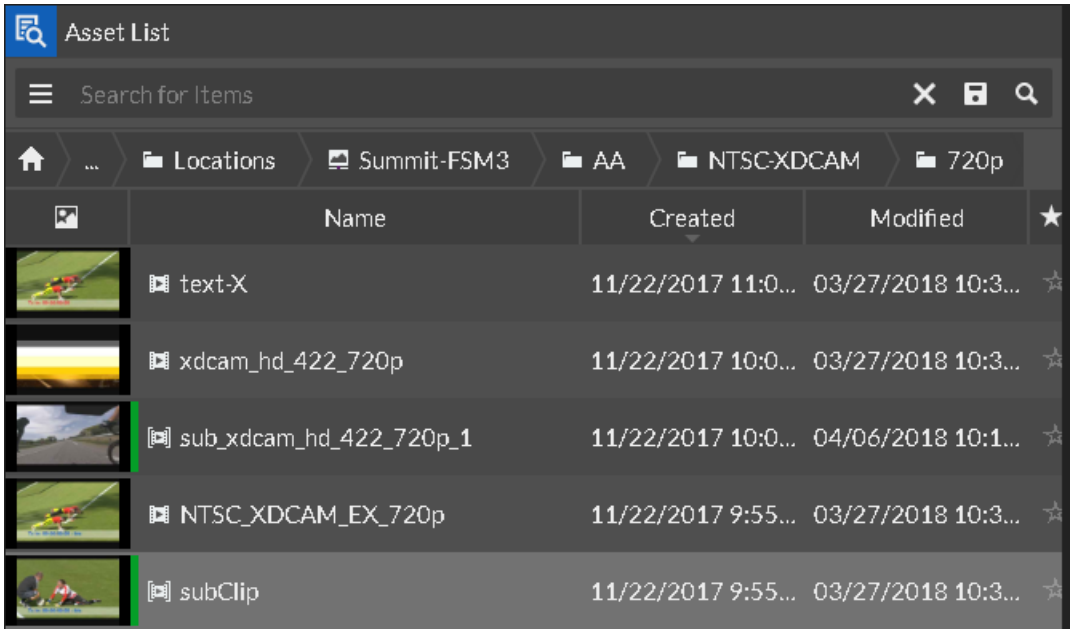
The Navigator panel displays all items under the node for your local site.

The Navigator panel is also customizable. To resize, drag the sides of the panel to suit your operation.

If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets, and metadata that do not have read permissions are not visible. Marker permissions must be set to **Allow** in order to create, update, or delete markers.

The Asset List panel

The Asset List panel displays the contents of the item selected in the Navigator panel, such as a group, bin, or sub-bin. Each time you select an item in the Navigator panel, an updated view of its contents is displayed. You can also search for assets or groups and save your searches, then select them later in the Navigator panel. The Asset List panel appears in the middle of the GV STRATUS Web Client.



The Asset List panel features are as follows:

- Asset location — Displays the location of the asset, relative to the Navigator hierarchy. The breadcrumb trail of the selected bin displays. To navigate up the breadcrumb trail, click a bin on the toolbar.
- Asset properties — The selected item in the Navigator has its contents displayed in the Asset List panel. Properties are displayed by Thumbnail, Name, Created Date, Modified Date, Ratings, High-Res Status, and Has Proxy Status.
- Sortable columns — Sorts the list when you click the column head.
- Search tool — Searches on asset names, descriptions, tags, comments, custom text fields, and customizable search conditions.

The Asset List panel is customizable. To resize, drag the sides of the panel to suit your operation.

If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, assets, metadata, and other controls can be disabled or hidden.

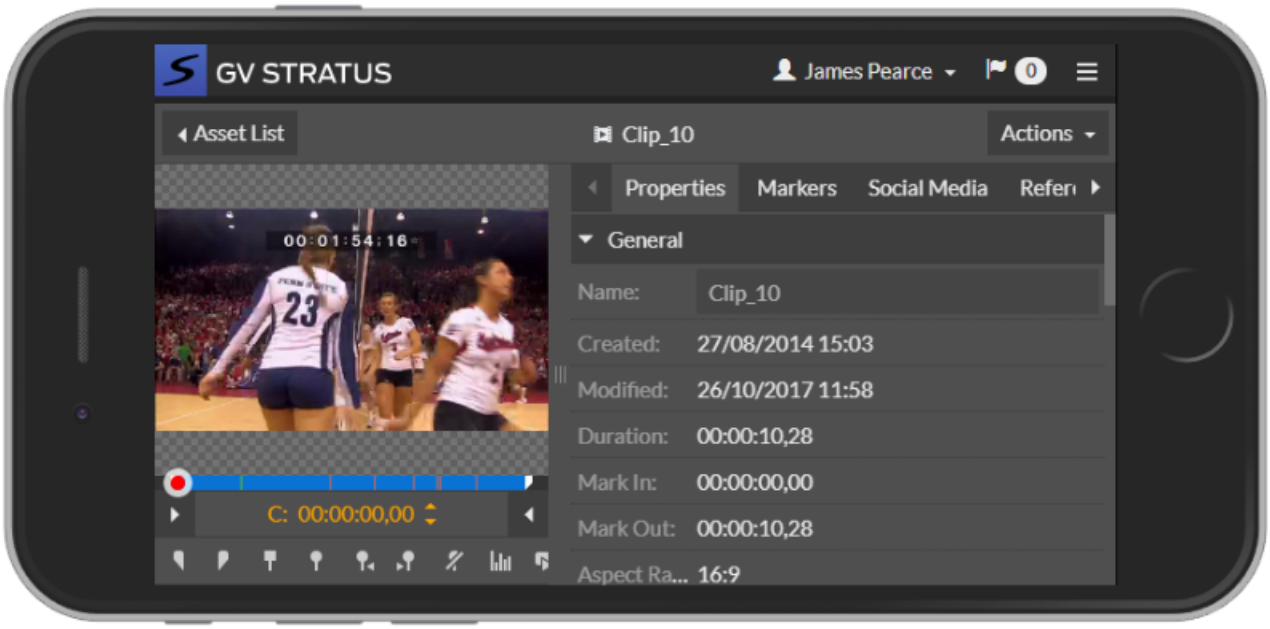
The Inspector panel

The Inspector panel allows you to view, mark up, and edit properties of an asset. The Inspector panel appears on the right side of the GV STRATUS Web Client.

The Inspector panel features are as follows:

- Viewer — Allows you to view and mark up an asset. You can show and hide viewer controls to accommodate resizing the Inspector panel.
- Actions drop-down list — Allows you to mark up the asset, delete, rename, add to favorites, send, copy, transfer, archive, create sub-clip, upload thumbnail, regenerate proxy of the asset, apply rules to the asset, and open the asset via the Simple Editor tool.
- Overlay Controls — Transport controls navigate through the asset. Visible when you hover the mouse pointer over the asset.
- Viewer controls — Allows you to mark in/out the asset, insert markers/keywords, toggle hide markers, and eject the clip.
- Timecode Controls — Allows you to select the mark in/out and other timecode types to display. Also lets you navigate through the clip to a specific timecode.
- Tabs — Provides sections for viewing properties and details of an asset. On the Properties tab you can make changes, such as editing clip names, setting ratings, inserting tags, and adding description or comments for the asset. On the Markers tab, you can view the list of markers and keywords added to the asset. You can also view references and associations of the asset on other tabs.

The Inspector panel is customizable anywhere whether in a desktop application or mobile devices. To resize, drag the sides of the panel to suit your operation.



Inspector keyboard shortcuts

Function	Key	Comment
-1 Frame	**A**	
-10 Frames	**D**	

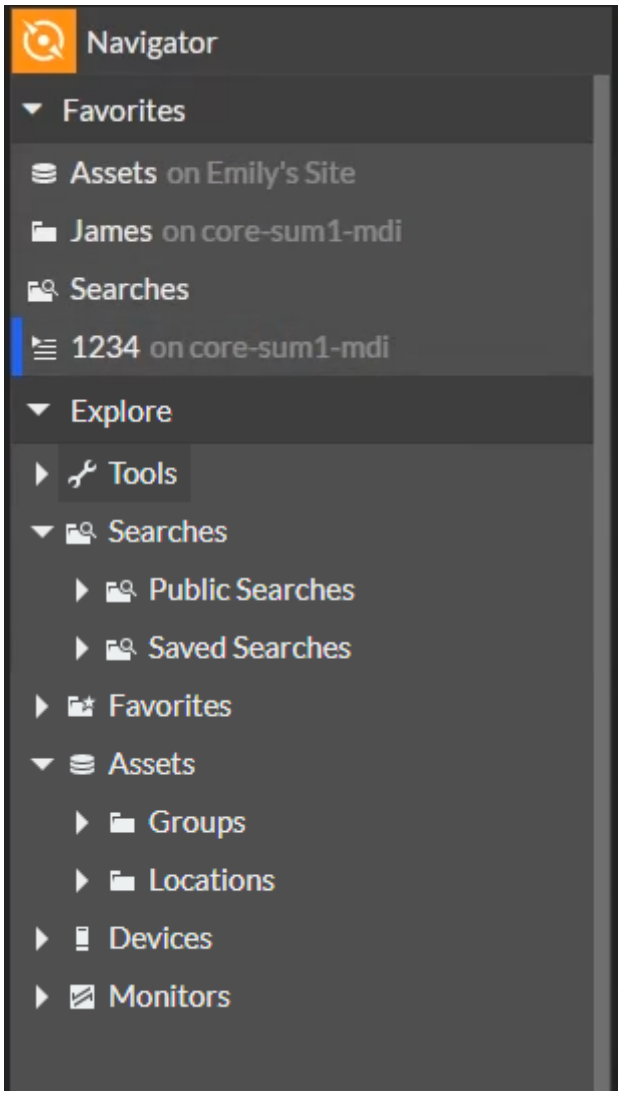
Function	Key	Comment
+1 Frame	**S**	
+10 Frames	**F**	
Create Keyword	**Ctrl + Insert**	
Create Marker	**Insert**	
Clear Mark In	**Shift + I**	
Clear Mark Out	**Shift + O**	
Clear Marks	**Shift + P**	
Create Subclip	**F4**	
Eject	**Ctrl + E**	
Fast Forward	**R**	Fast forward with 8X speed.
Send	**F11**	
Go to Beginning	**Home**	
Go to End	**End**	
Go to Mark In	**Ctrl + I**	
Go to Mark Out	**Ctrl + O**	
Go to Next Event	**H**	
Go to Previous Event	**G**	
Mark In	**I**	
Mark Out	**O**	
Pause	**K**	
Play/Pause	**Spacebar**	Toggles between play and pause.
Play from Start	**Q**	
Forward	**L**	
Reverse	**J**	Play video in reverse.
Rewind	**E**	Rewind with 8X speed.
Trim	**F3**	

Browsing assets

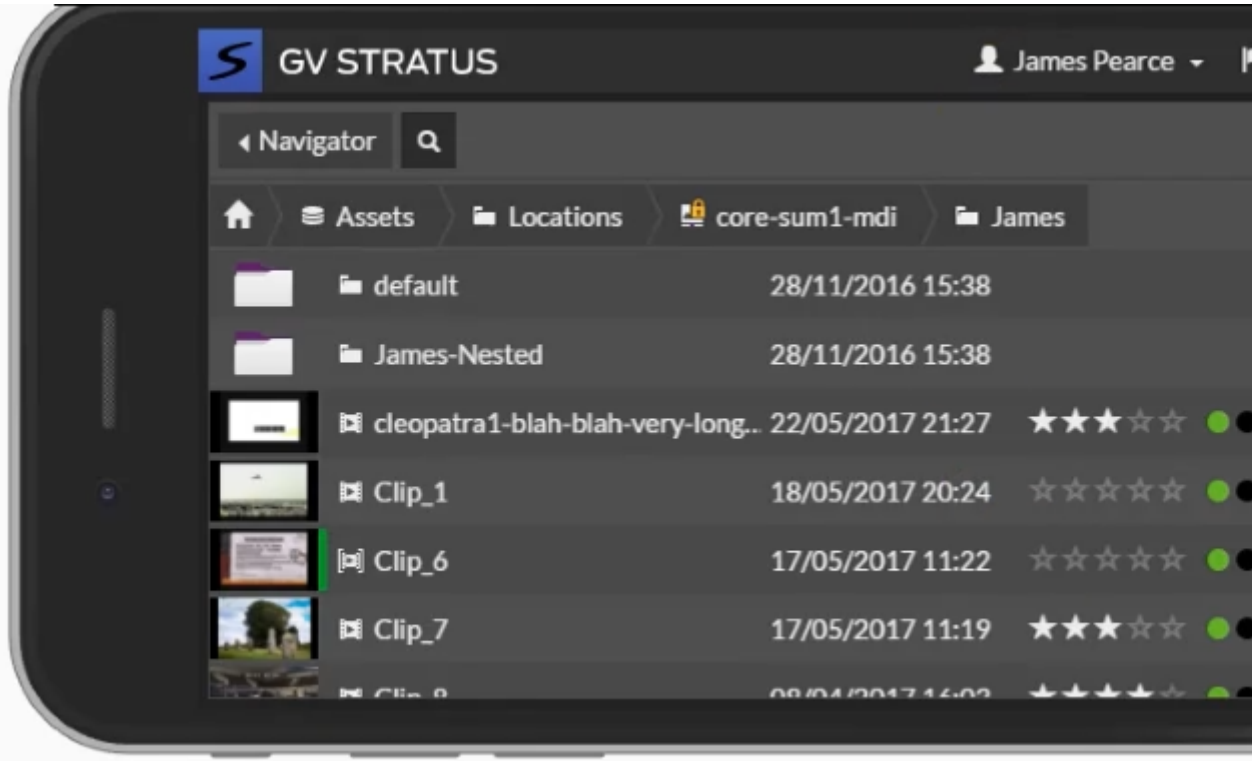
You can browse and navigate into bins and sub-bins of the GV STRATUS system.

1. Click the **Assets** node on the Navigator panel to start browsing.
2. To expand a bin, click the arrow next to the bin name.
3. To minimize the bin, click the arrow next to the bin name a second time.

4. To browse for assets, click on bins or sub-bins in the Navigator panel.



Assets in the selected bin display in the Asset List panel.



Viewing assets

If GV STRATUS security is enforced, your credentials must give you adequate permissions. You can only view assets with read permissions, and edit assets with write permissions. If read permissions are denied on specific assets, those assets will not be available for viewing.

1. Locate the desired asset by browsing or using the Search tool.

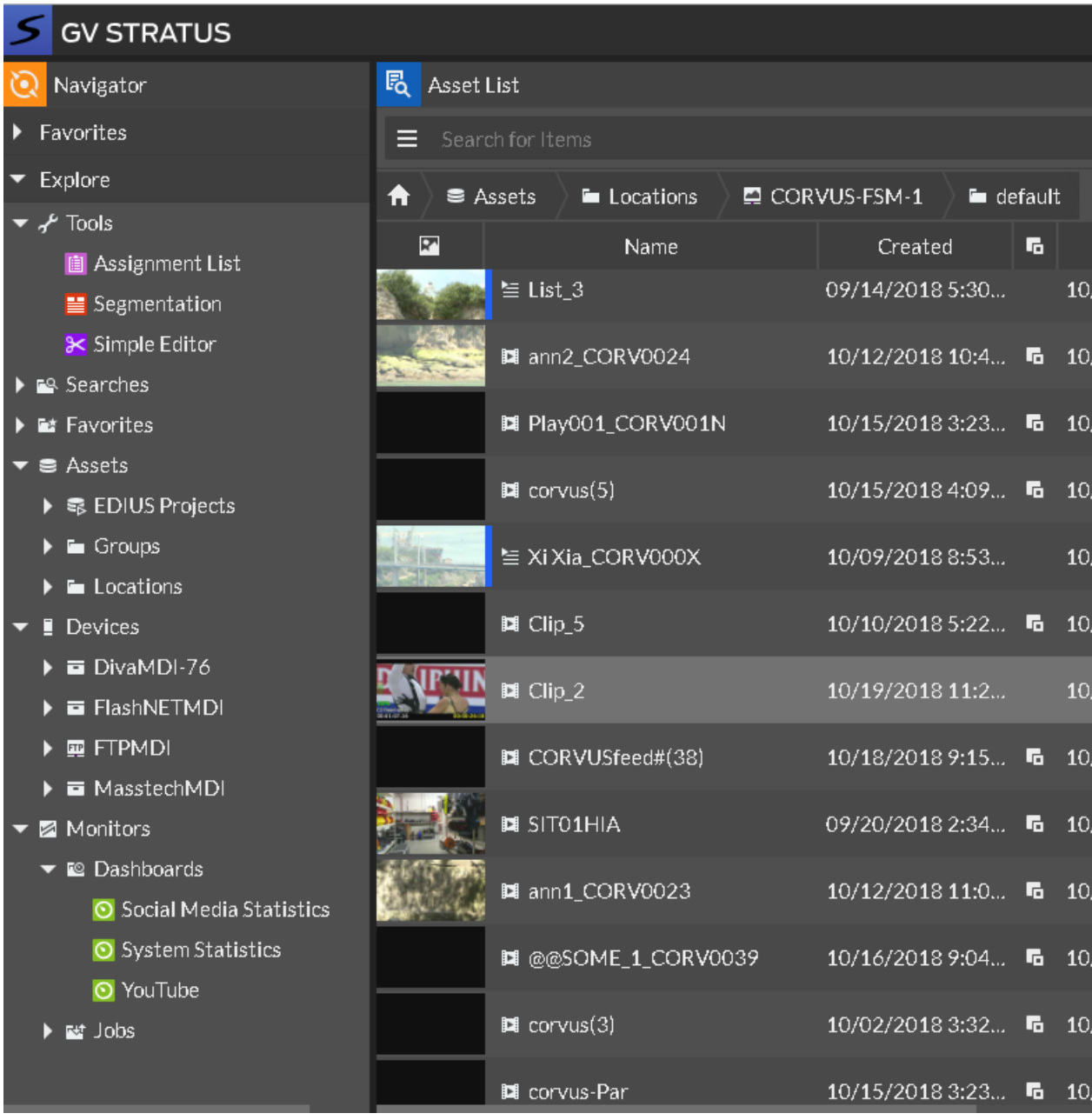
2. To view the asset, do one of the following:

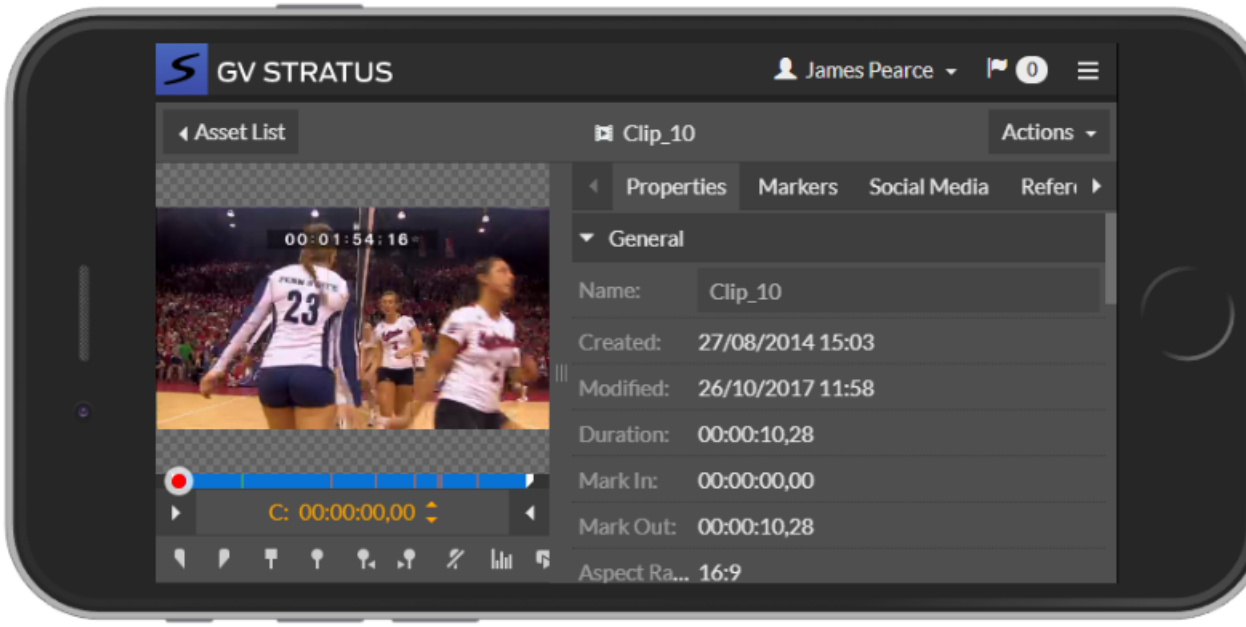
   - Double-click the asset in the Asset List panel.
   - Drag and drop the asset into the Inspector panel.
   - Right-click on the asset and select **Open With | Inspector**.

   The asset displays in the Inspector panel.

   You can play the asset, set markers and keywords, trim the asset, create segmentation, view asset properties, link the asset to a placeholder, copy, transfer, or archive the asset.

   To copy asset properties, right-click on each property and select **Copy 'Property' Value**.



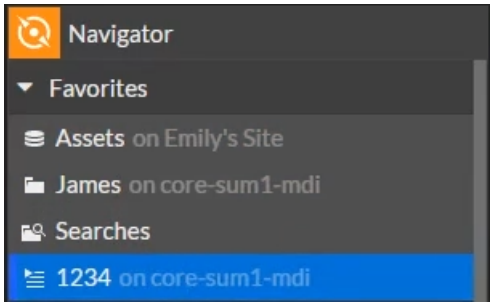


Adding a favorite

You can drag and drop any type of GV STRATUS item to the Navigator panel and save it there as a shortcut.

1. In the Navigator panel, expand the Favorites section by clicking on the **Favorites** Show/Hide control.

   The Favorites section expands.



2. Identify the item that you want to make a favorite.
3. Do one of the following:

   - Right-click on the item and select **Add to Favorites**.
   - Drag and drop the item into the Favorites section.

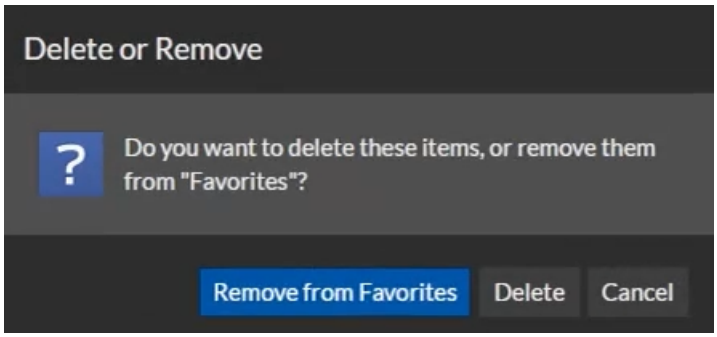
A shortcut to the item displays in the Favorites section.

NOTE: Renaming a bin removes it from the Favorites node. You must add the bin to the Favorites node again after renaming it.

Removing or deleting a favorite

1. To remove a favorite from the Favorites section, right-click on the favorite and select **Delete**.

   The **Delete or Remove** dialog box opens.



2. Select **Remove from Favorites**.

   The item is removed from the Favorites section. The item itself is not deleted from its original location.

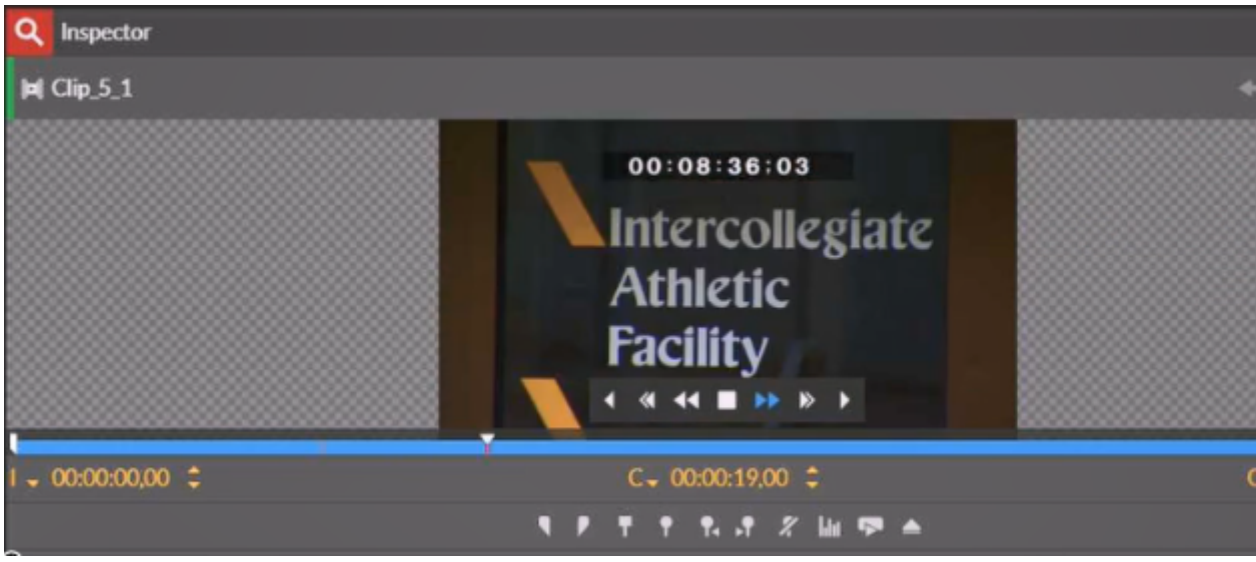
3. To delete the item itself, select **Delete** in the **Delete or Remove** dialog box.

   The item is deleted from its original location.

Using mark-in and mark-out points

- If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, metadata, markers, keywords, and segments.
- Create Marker and Update Marker permissions must be set to **Allow** for you to create and update markers.

1. Navigate to the desired starting point using the scrub bar, and click the **Mark In** button. (**I**)



2. Navigate to the desired end-point using the scrub bar, and click the **Mark Out** button. (**O**)

   Trim Asset is enabled when the asset has a mark-in or mark-out point. It is disabled if the asset does not have a mark-in or mark-out point.

3. To navigate to a mark-in or mark-out point, select keyboard shortcuts for **Goto Mark In** (**Ctrl + I**) or **Goto Mark Out**. (**Ctrl + O**)
4. To clear a mark-in or mark-out point, select keyboard shortcuts for **Clear Mark In** (**Shift + I**) or **Clear Mark Out**. (**Shift + O**)

Trimming a clip in Inspector

If GV STRATUS security is enforced, your credentials must give you adequate permissions. You can only view assets with read permissions, and edit assets with write permissions. If read permissions are denied on specific assets, those assets will not be available for viewing.

When you trim an asset, you change the length of the viewable asset, restricting it to the material between the Trim In and Trim Out points. The material outside the trim marks is not deleted. It remains on disk but is not viewable. To use the Trim Asset operation, you must be logged on with a user account to which the Trim Rights role is assigned. If the role is not assigned, the Trim Asset operation is not available.

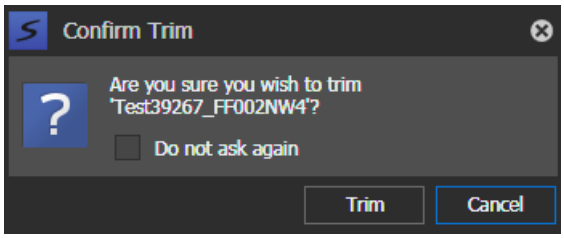
1. Load the asset into the Inspector.
2. Navigate to the desired starting point using the scrub bar, and click the **Mark In** button. (**I**)
3. Navigate to the desired end-point using the scrub bar, and click the **Mark Out** button. (**O**)

   Trim Asset is enabled when the asset has a mark-in or mark-out point. It is disabled if the asset does not have a mark-in or mark-out point.

   NOTE: If a clip is a part of Dyno record train sequence, Mark In and Mark Out points should not be set beyond the limit of the guard band, as configured for the record train sequence.

4. Click on the **Actions** drop-down arrow, and select **Trim Asset**.

   The **Confirm Trim** dialog box appears.



5. Select the **Do not ask again** checkbox to prevent recurring display of the **Confirm Trim** dialog box.
6. Click **Trim** to confirm the trimming of the asset.

Adding markers

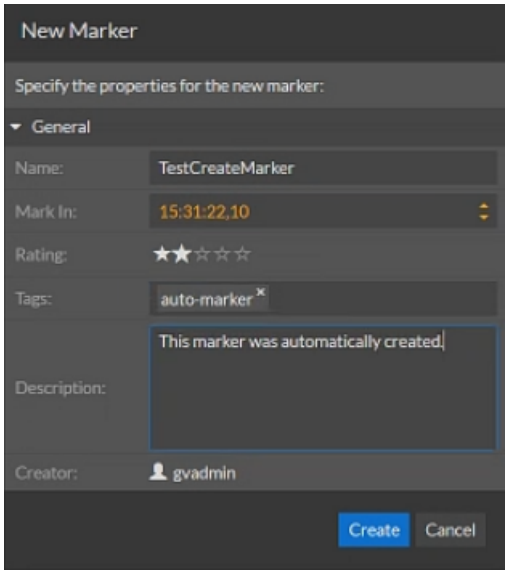
- If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, metadata, markers, keywords, and segments.

- Create Marker, Update Marker, and Write permissions must be set to **Allow** for you to create and update markers.

1. Load an asset into the viewer of the Inspector.
2. Click the **Create Marker** button. (◇)

   The New Marker dialog box opens.
3. Enter the name of the marker.

   You can also add the description, tags, and rating if needed.



4. Click **Create**.

The marker is added to the asset. A symbol indicates its location. If you select a symbol the thumbnail associated with that point is loaded into the Viewer, and the slider is moved to that position.

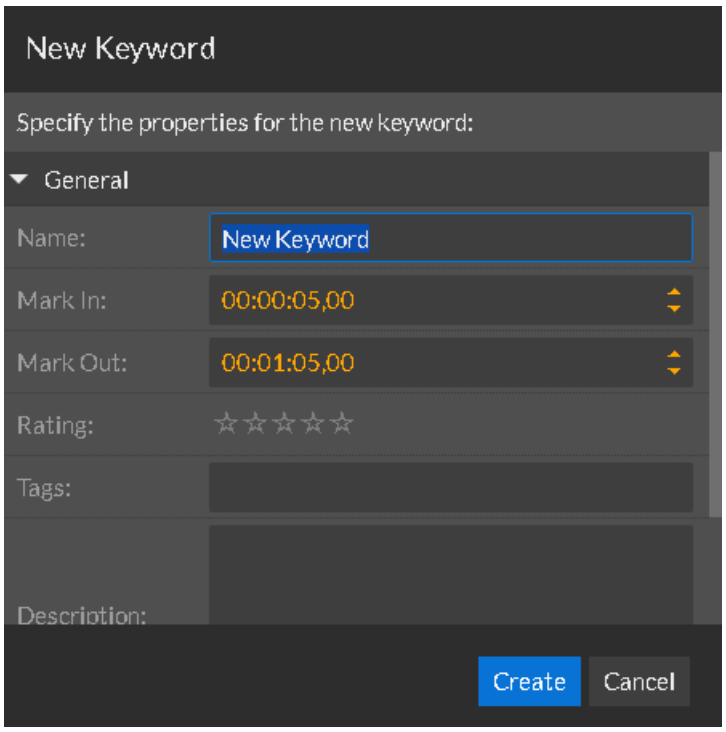
Adding keywords

- If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, metadata, markers, keywords, and segments.
- Create Marker, Update Marker, and Write permissions must be set to **Allow** for you to create and update keywords.

1. Load the selected asset into the Inspector.
2. Navigate to the desired starting point using the scrub bar, and click the **Mark In** button. (◇ **I**)
3. Navigate to the desired end-point using the scrub bar, and click the **Mark Out** button. (◇ **O**)

4. Click the **Create Keyword** button. ( )

   The New Keyword dialog box opens.



5. Enter the name of the keyword.

   You can also add the description, tags, and rating if needed.

6. Click **Create**.

The keyword is added to the asset. A symbol indicates its location. If you select a symbol the thumbnail associated with that point is loaded into the Viewer, and the slider is moved to that position.

Deleting a marker

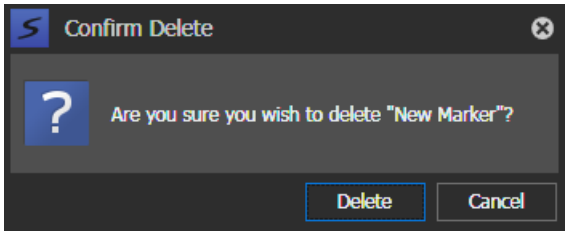
- Delete Marker permission must be set to **Allow** for you to delete markers.

1. Select a marker or multiple markers that you want to delete.

   To select multiple markers on the **Markers** tab of the Inspector, hold the **Shift** key down and select all markers between two selected markers; or hold the **Ctrl** key down and select markers randomly.

2. Right-click and select **Delete**. (**Delete**)

   The Confirm Delete dialog opens.



3. Click **Delete**.

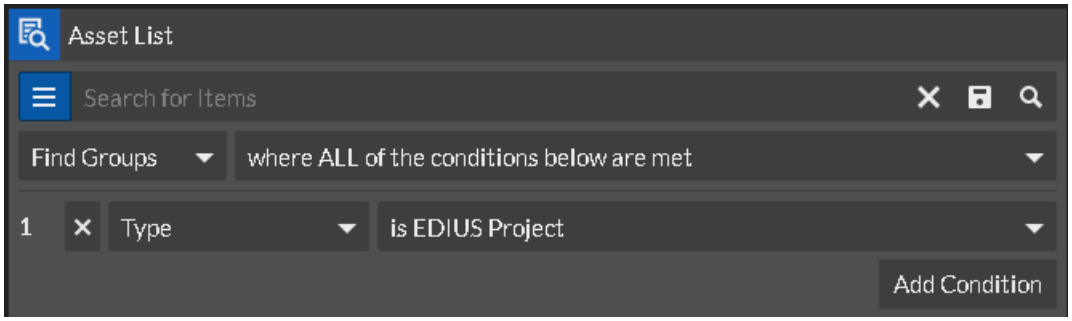
Selected marker or markers are deleted from the **Markers** tab.

Searching assets

1. In the Search tool, enter the text for your search.

   For a simple search you can enter text with advanced query syntax. Assets with names, tags, descriptions, comments, marker text, or custom text data that match the search are returned.

2. Click this button to display the Advanced Search section.



3. Select either **Find Assets** or **Find Groups** from the left drop-down list.

   - **Find Assets** — The search returns assets only such as clip, sub-clip, list, sequence, edl, and EDIUS sequence.
   - **Find Groups** — The search returns groups such as STRATUS Group, EDIUS Group, EDIUS Project, EDIUS Template, and Device Bin.

4. For the drop-down list on the right, select the type of search you are doing:
   - **where ALL of the conditions below are met** — The search returns results that match all conditions.
   - **where ANY of the conditions below are met** — The search returns results that match any condition.
   - **where a Custom expression is satisfied** — A Custom Expression field opens in which you can enter a custom search expression.
5. Configure search conditions as follows:
   - For each condition (1, 2, 3, 4, etc) select from lists or enter text to define the condition.

     A **Marker** search includes marker name, marker description, and marker tags. While a custom metadata field search also allows you to search for an empty field.
   - Click the **Add Condition** button or the **X** button to add or remove conditions from the list.
   - When you create a "contains" condition that searches a text field, you can enter text with advanced query syntax to search that field.
   - When you create an "is between" condition, you can enter dates and times to specify a time range for the search.
   - When you create the "is Empty" condition, you can search for empty fields including rating, tags, and Boolean custom metadata.
6. To start the search, click the **Search** button.

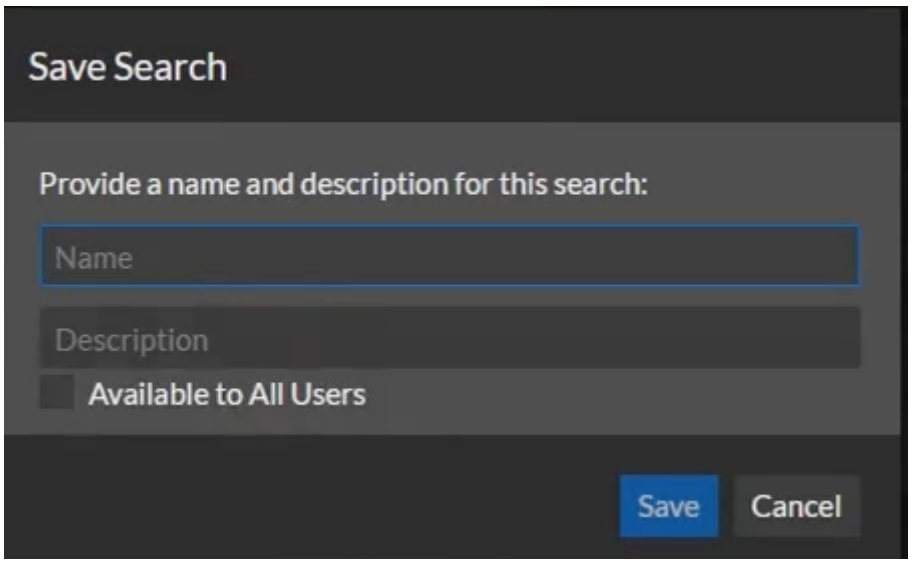
   Results matching the search criteria are displayed in the Asset List.

Saving searches

Searches that you create can be saved in the Navigator panel under the Favorites node.

1. To save a search, click the the **Save** button next to the **Search** text field.

   The Save Search dialog box displays.



2. Enter the name of the search and, if desired, a description.
3. If the **Available to All Users** check-box is selected, you can make the search available to all GV STRATUS system users.
4. Click **OK**.

The saved search appears under **Searches | Saved Searches** in the Navigator panel.

If you selected the **Available to All Users** check-box, the saved search appears under **Searches | Public Searches** and it is available to all GV STRATUS users.

Using a saved search

1. In the Navigator panel, expand the **Searches** node.
2. Find saved searches, organized as follows:
   - Public Searches: Searches saved as public by GV STRATUS system users with the role of Media Manager.
   - Saved Searches: Searches saved by you.
3. Select a saved search.

   The search is re-run. The Asset List panel displays the latest results.

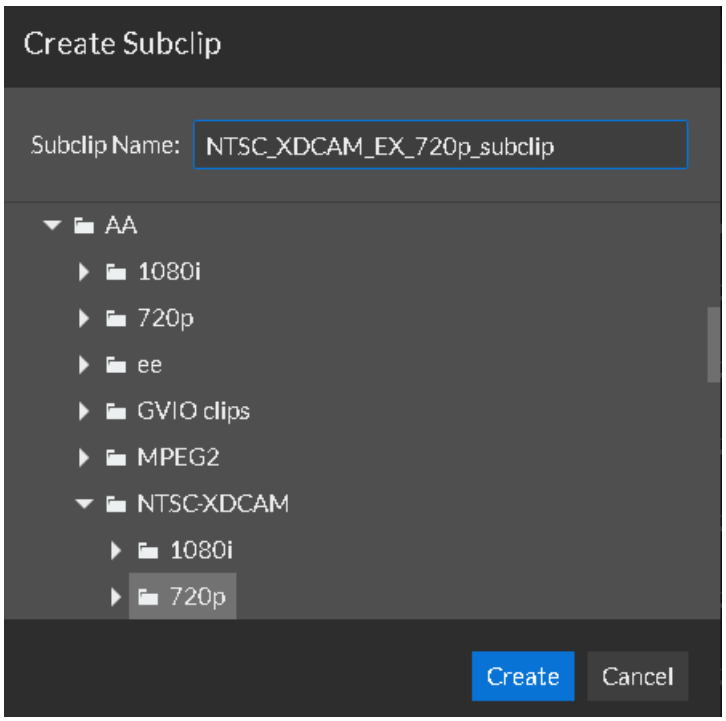
Creating a subclip

1. Load an asset into the Inspector.
2. Navigate to the desired starting point using the scrub bar, and click the **Mark In** button. (**I**)
3. Navigate to the desired end-point using the scrub bar, and click the **Mark Out** button. (**O**)

   NOTE: If a clip is a part of Dyno record train sequence, Mark In and Mark Out points should not be set beyond the limit of the guard band, as configured for the record train sequence.

4. Click on the **Actions** button and select **Media | Create Subclip**.

   The **Create Subclip** dialog box opens.



5. Enter a name for the subclip. If not, **subclip** is appended to the asset name by default.
6. Navigate and select a location to save the subclip.

   NOTE: The last path from the previous subclip operation is automatically remembered as the starting point to save subsequent subclips. If there was no prior subclip operation, the starting path is automatically the same with the loaded asset.

7. Click **Create**.

The subclip is created in the specified location. The following is inherited from the parent clip:

- Rating
- Tags
- Description
- Markers and keywords that are between mark in and mark out

The following is not inherited:

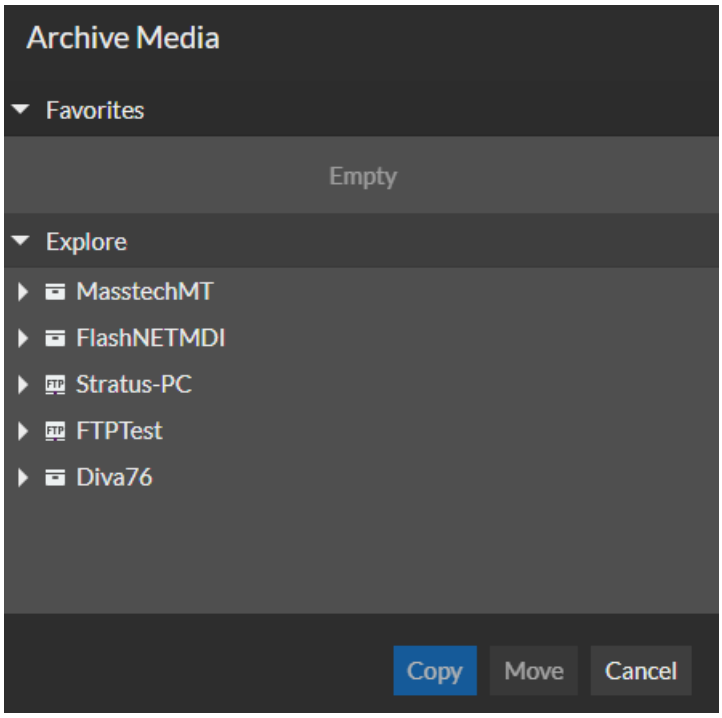
- Approval Status
- Protection Status

Archiving an asset

You can only archive an asset if you are assigned with the archive role. When you want to archive an asset, you can choose whether to copy or move the asset to an archive location.

1. In the Asset List panel, select an asset.
2. Right-click and select **Transfer | Archive Media**.

3. Select the archive destination.



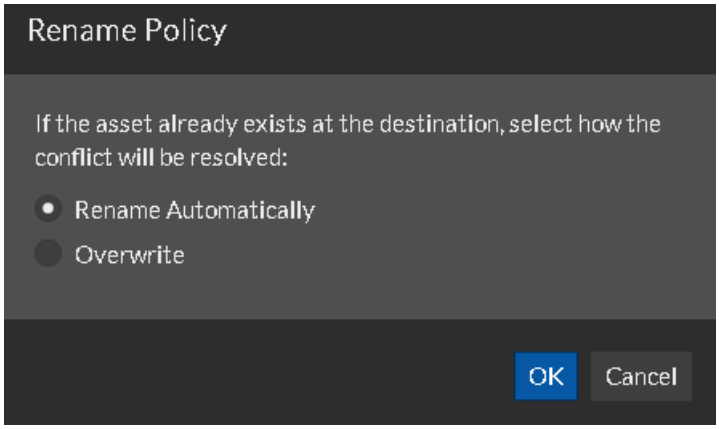
Tip: If you plan to archive or transfer assets frequently to the same folder, add that folder to your favorites. This allows you to select that folder directly from the Favorites menu instead of browsing to the archive location.

4. Click **Copy** or **Move**.

   NOTE: A copy operation archives a copy of the asset to the archive location. A move operation archives the asset and deletes it from its online location.

   You can also archive an asset via copy and paste, or drag and drop assets directly into a bin in your archive directory.

   The **Rename Policy** dialog box opens.



   You cannot archive two assets with the same name at the same archive location. So, you can either select **Rename Automatically** or **Overwrite** in the Rename Policy dialog box.

5. From the Navigator, select **Monitors | Jobs | Asset Transfers** to track the progress of the archive operation.

A protected asset can be archived via the copy operation, but a move operation is not allowed as the high resolution media cannot be deleted.

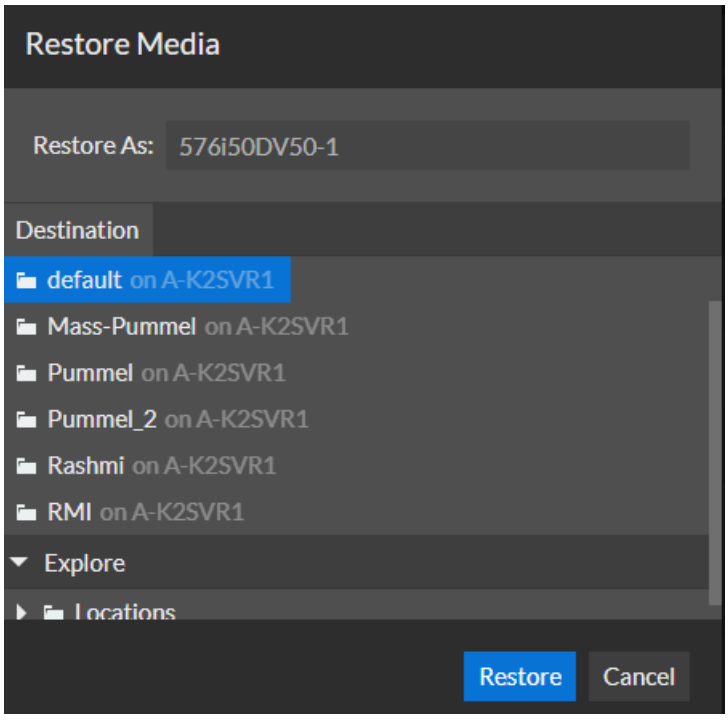
Restoring archived assets

You can restore assets if you are assigned with the restore role. Only archived assets can have their high resolution material restored into the K2 Summit/SAN system. However, you cannot restore or partial restore an asset if the high resolution material for that asset already exists in the K2 Summit/SAN system.

If you are logged on with the Media Manager role assigned, permission is granted to move assets from an archive system to the GV STRATUS system. Without this permission, assets may be copied but not moved.

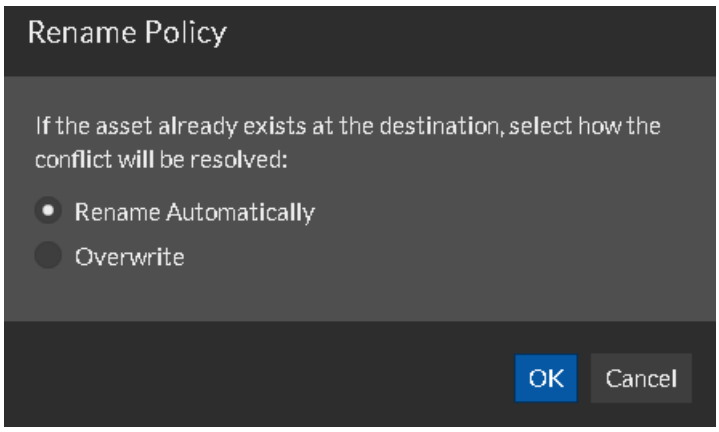
1. In the Asset List panel, select the asset or assets you want to restore as follows:
   - Right-click a single asset to open a context menu.
   - Use **Ctrl + Click** to select multiple assets, then right-click to open a context menu.
2. In the context menu, select **Transfer | Restore Media**.

   The Restore Media dialog opens.



3. Select the restore destination and click **Restore**.

   The **Rename Policy** dialog box opens.



   You cannot restore two assets with the same name at the same location. So, you can either select **Rename Automatically** or **Overwrite** in the Rename Policy dialog box.

4. Click **OK** to restore the media.
5. From the Navigator, select **Monitors | Jobs** to track the progress of the restore operation.

Upon completion of the restore operation, the Asset List displays a High-Res Status indicator.

Applying rules via the GV STRATUS UI

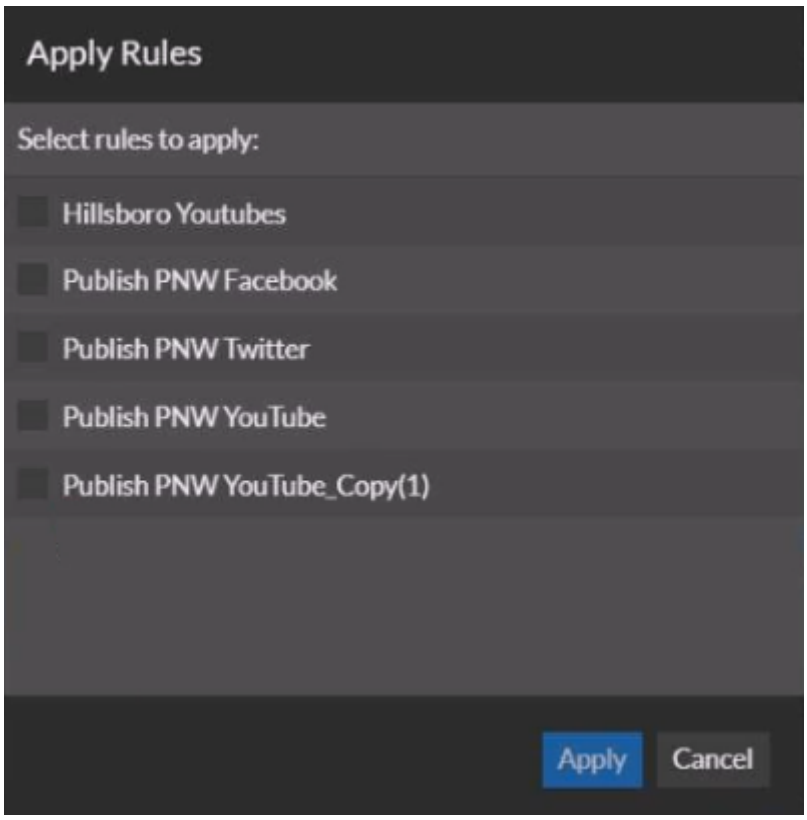
- The **Visible in STRATUS UI** check-box must be selected under **Rule Options** section in **General | Rules | Rule Editor** of GV STRATUS Control Panel. If permissions settings had been configured, only specific users and groups are allowed to apply the rules via GV STRATUS UI.
- Optionally, select **STRATUS UI only** option under **Frequency** section when configuring the rule in **Rule Editor** tab to only trigger the rule from the UI.
- The rule must be enabled in GV STRATUS Control Panel.

You can trigger rules to be applied on assets via context menu in the Asset List. This is applicable to Export, Transfer, Archive, Custom, and Publish Social Media rules.

1. In the Asset List panel, select an asset to be applied with the rule.

2. Right-click on the asset and select **Media | Apply Rules**.

   The Apply Rules dialog box opens.



3. Select a rule or multiple rules to be applied to the asset, and click **Apply**.

The rule is automatically triggered and applied on the asset.

***NOTE: Triggering a rule via Asset List will ignore whatever Rule Conditions that have been set up for the rule in* GV STRATUS Control Panel.**

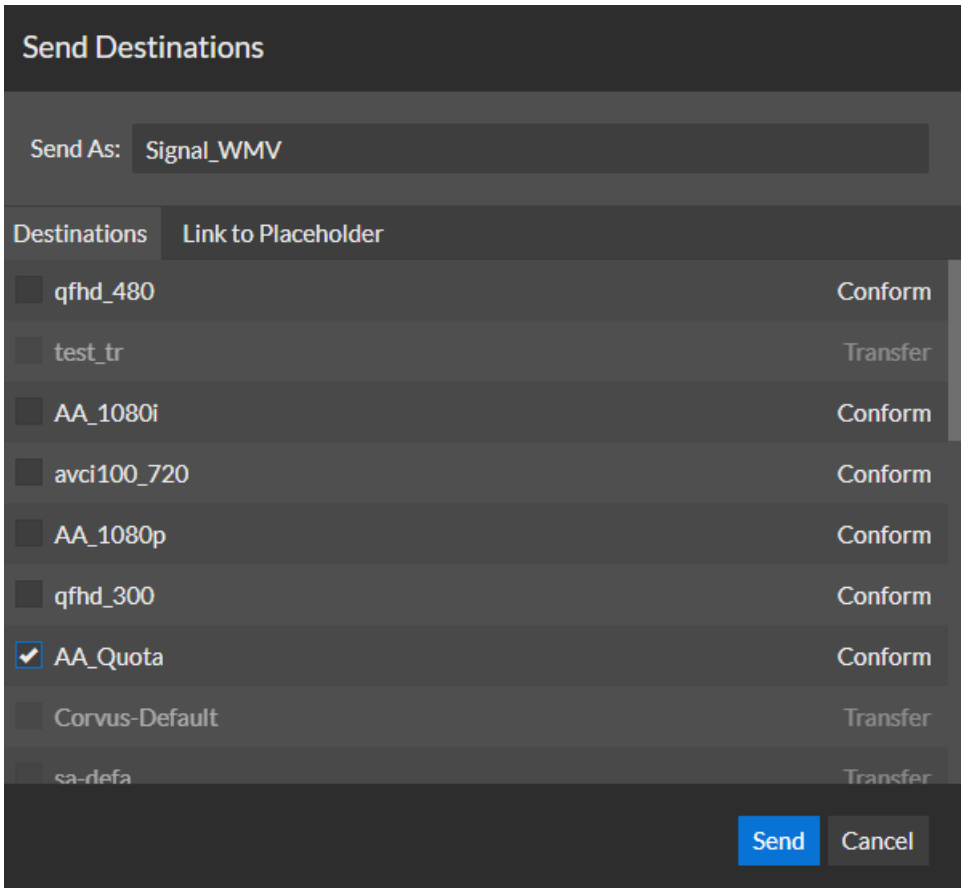
After the job is completed, you can see the rule name in the **Rules Applied** field on the Properties tab of the asset in Inspector.

Transferring assets using Send Destination

You can transfer assets to pre-configured destination locations using the Send Destination feature. The destination locations are configured in GV STRATUS Control Panel.

1. Right-click on the asset that you want to transfer and select **Transfer | Send**.

   The Send Destinations dialog box opens and displays the list of destinations.



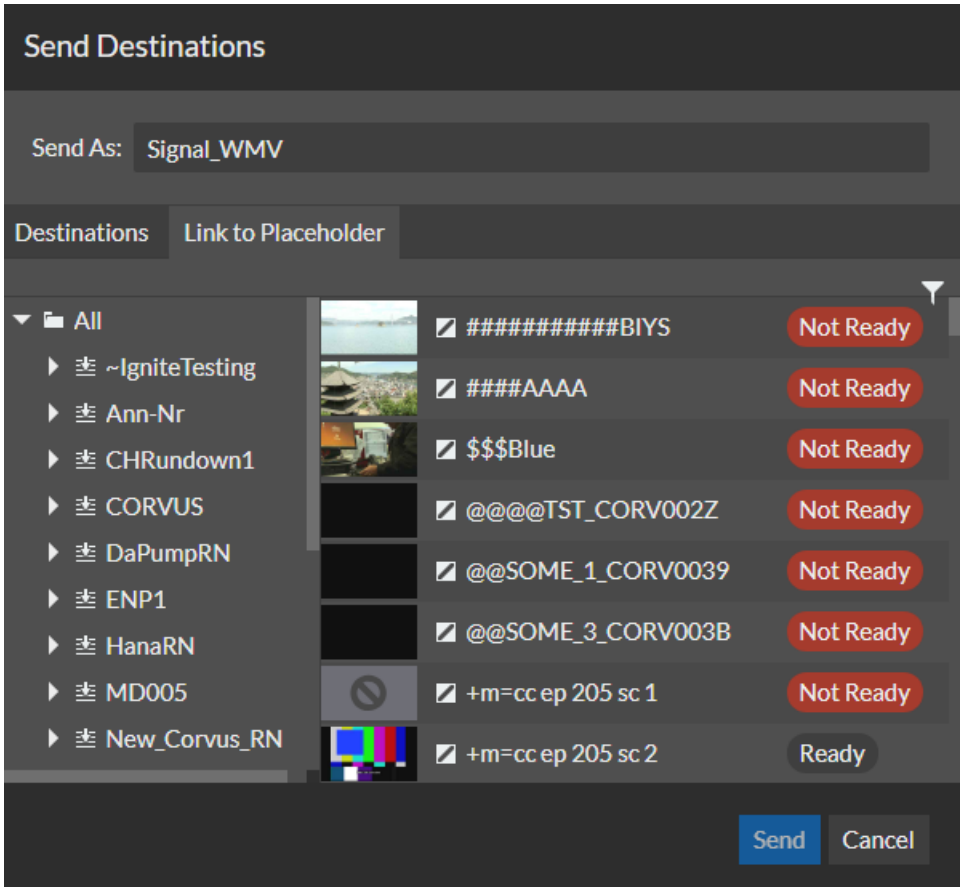
2. In the **Send As** text box, enter the asset name.
3. In the **Destination** tab, select one from the following:

   - Select one or more transfer destinations
   - Select one or more conform destinations

   You are not allowed to select both transfer and conform destinations at the same time.

   NOTE: If a local transfer destination is labeled as 'Remote Transfer', you need to re-save the send destination configuration on* GV STRATUS Control Panel *to get the correct label.

4. If configured for a Newsroom Computer System, you can also link the asset to a placeholder.
   a) On the **Link To Placeholder** tab, select a placeholder.

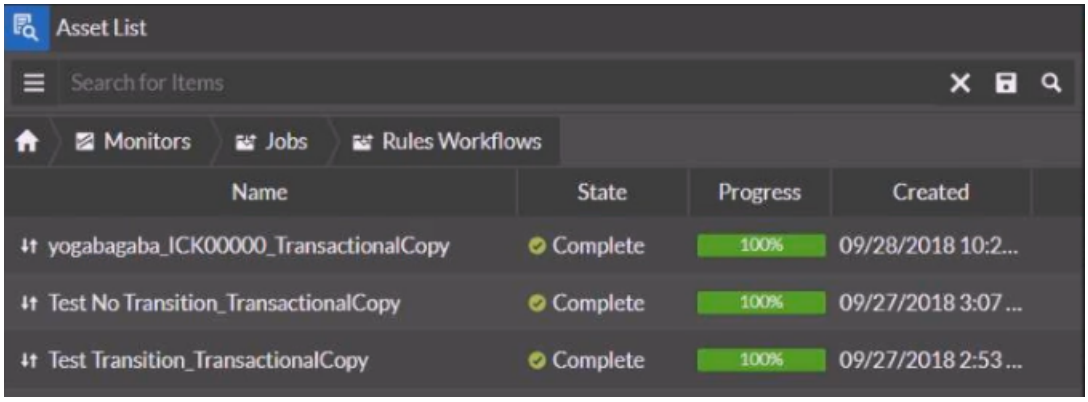


   If already linked to a placeholder, you can select a different placeholder.

5. Click **Send**.

To view the status of the transfer, open the Jobs Monitor.

The Rules Workflows job monitor provides the overall status of the send order.

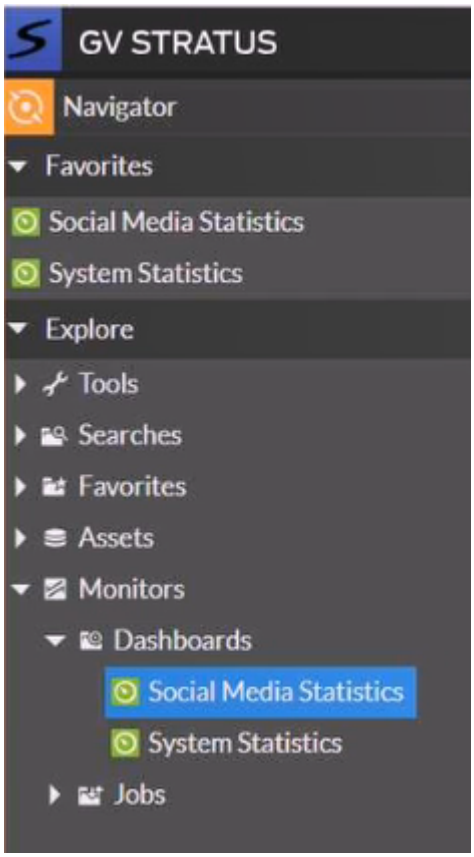


In case assets would exist at the destination with the same name, the rules workflow job handles that gracefully. In case one of the subsequent jobs would fail, the rules workflow job rolls back all other subsequent jobs in a transactional fashion.

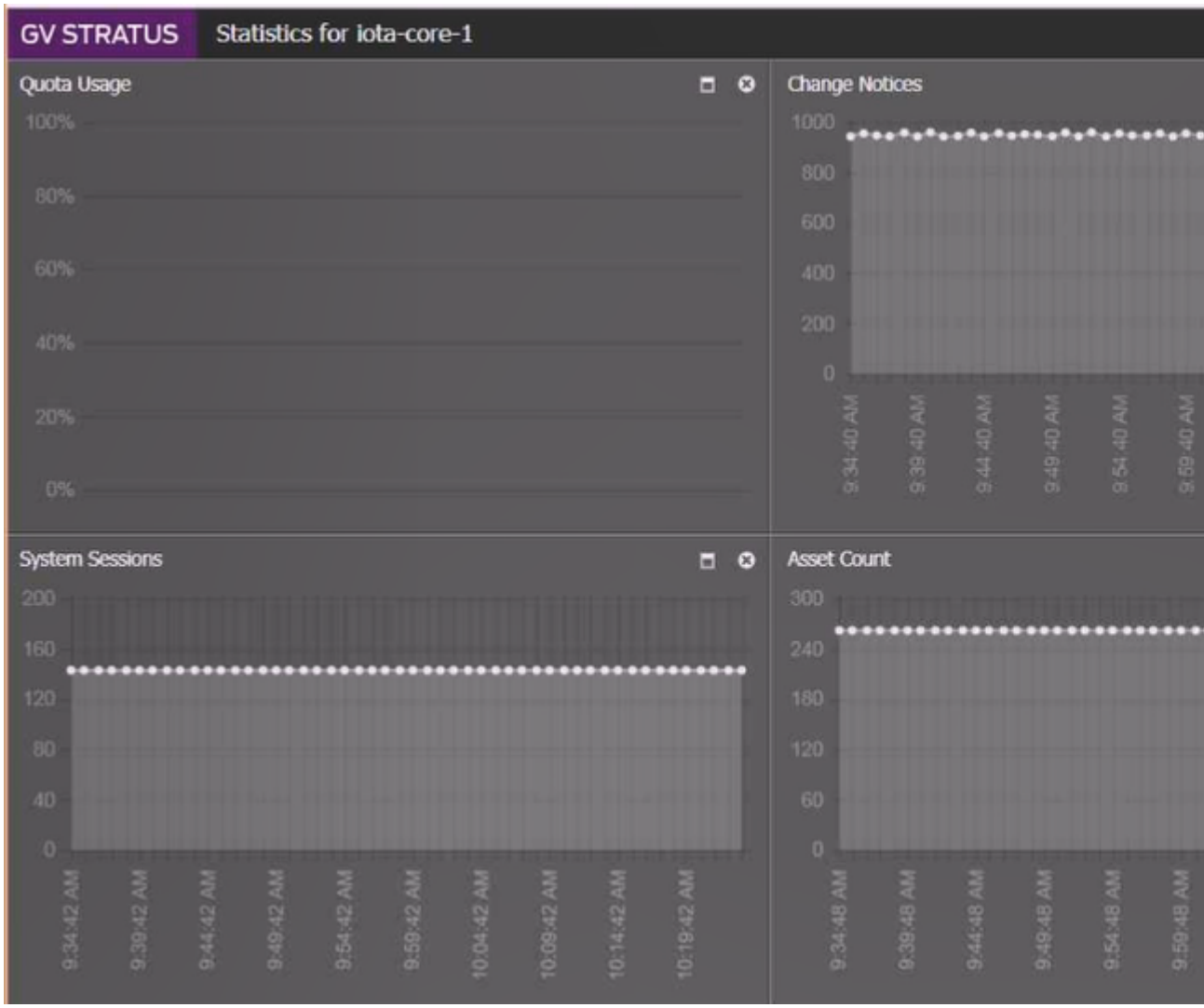
The Dashboards

The Dashboard monitor allows you to view statistical information of the GV STRATUS system and activities via social media.

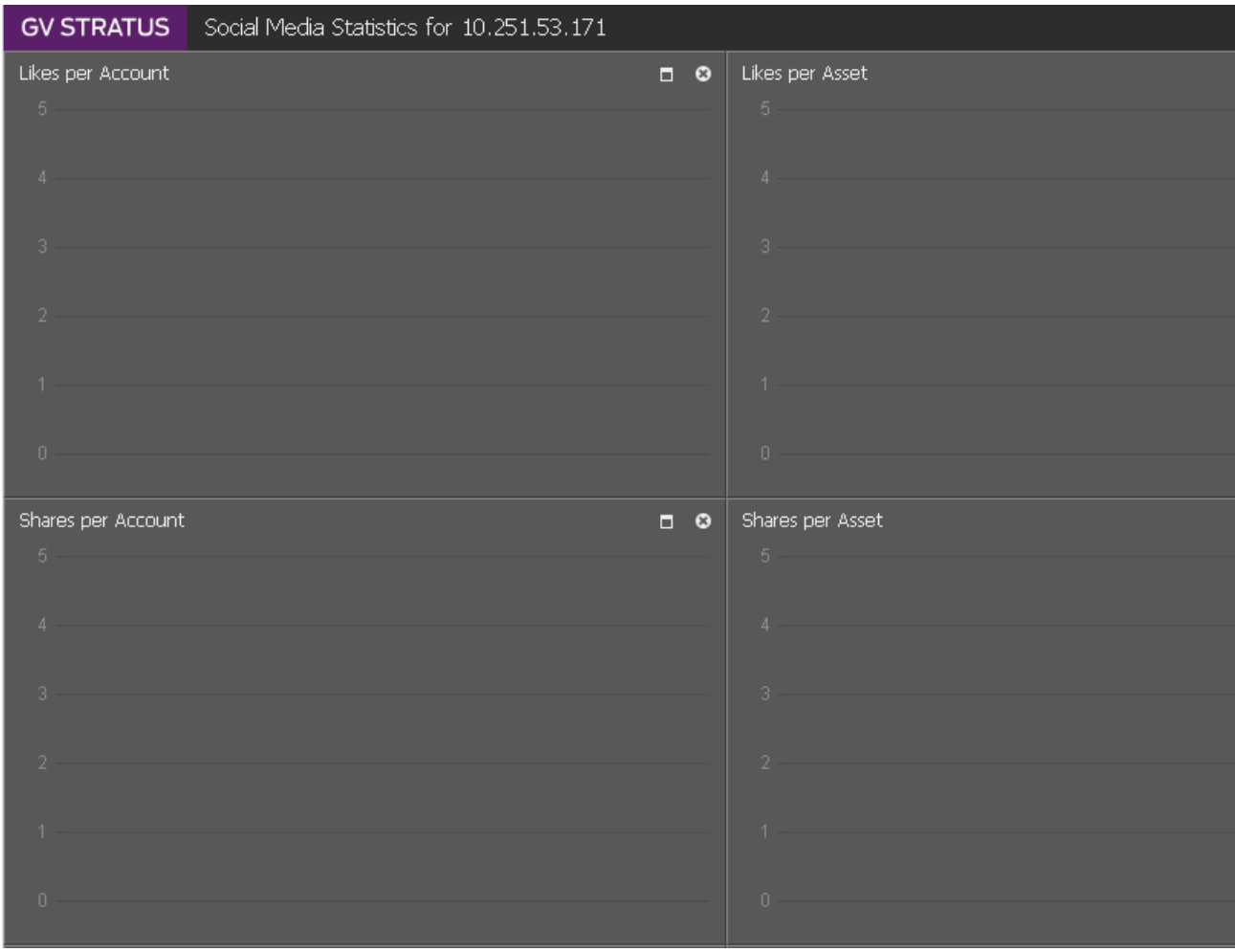
You can access and launch Dashboards from the Monitors node in the GV STRATUS Web Client. You can also drag and drop any Dashboard panel into the **Favorites** section in the Navigator to easily access your Dashboard status. If you are assigned with appropriate roles in the GV STRATUS Control Panel, these options are available via Dashboards under the Monitors node.



The System Statistics panel displays data in graphical form for change notices, asset count, user sessions, system sessions, quota usage, and top 5 of assets per bin in the GV STRATUS system. In order for the Statistics panel to display via the Dashboard, the **GV STRATUS Web Apps** SiteConfig role must be installed on the GV STRATUS Core server. Users must also be assigned with the **Dashboard** and **Dashboard - Statistics** roles in GV STRATUS Control Panel to view the dashboard. When you double-click on **System Statistics** under the Dashboards node, those statistics are launched as a new tab in the GV STRATUS Web Client.



The Social Media Statistics dashboard displays data in graphical form for statistical information of all Social Media platforms. You must be assigned with the **Dashboard** and **Dashboard - Social Media** roles in order to view the tab. Once an asset is published via the configured social media account, GV STRATUS system gathers statistical data such as (View-, Like- and Share-) counts from the social media platform and displays them via the dashboard.



If a webpage is configured in GV STRATUS Control Panel for display in the Dashboard tool, you can select the webpage under Dashboard options and view the display on a separate tab.

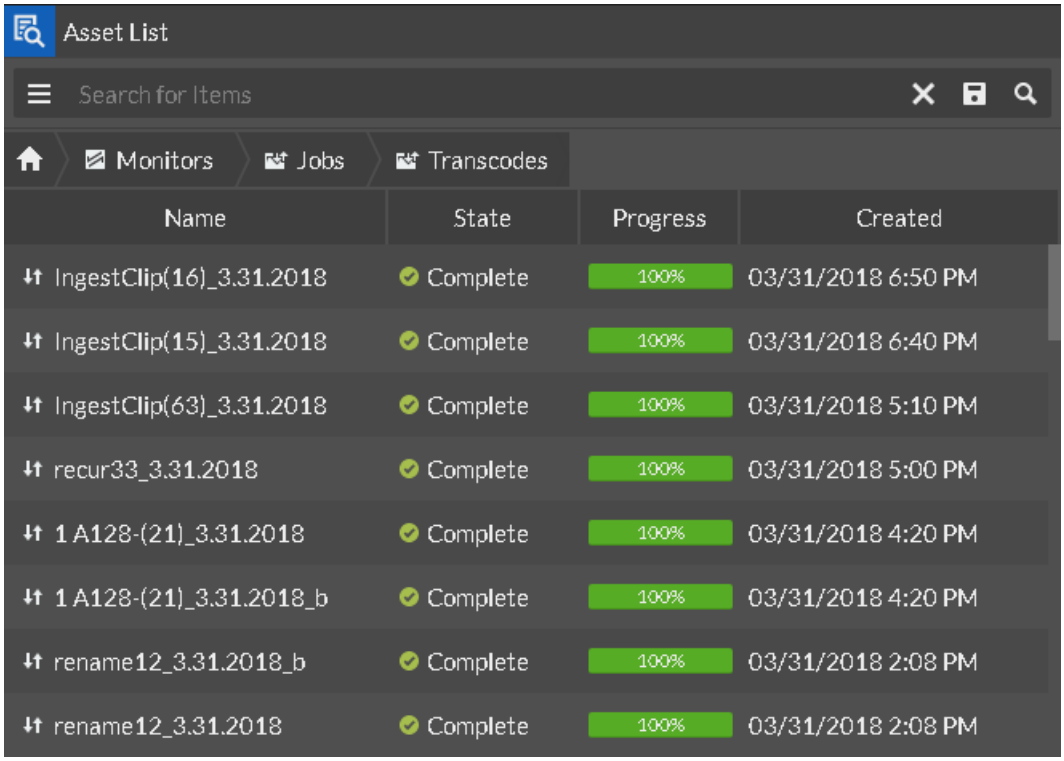
Monitoring imports, exports, or transfers

You can monitor the status of archive, transfer, conform, and transcode jobs in the Jobs Monitor.

1. To monitor GV STRATUS system jobs triggered by you and by others, in the Navigator panel, do the following according to the types of jobs you are monitoring:

   - Click one of the nodes under **Monitors | Jobs**.

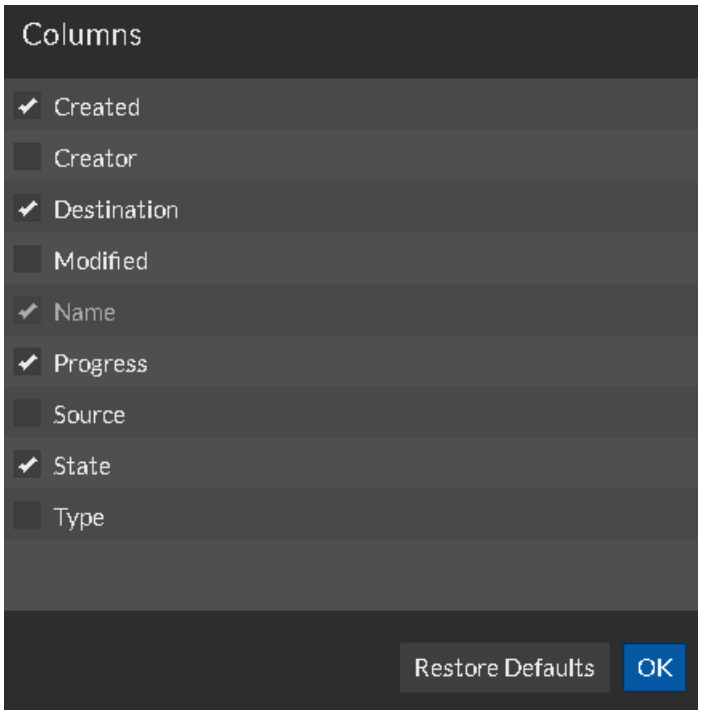
   The Jobs List displays GV STRATUS operations that can be monitored. Operations that are currently in progress or have failed are also displayed.



While transferring, if the destination quota is reached, the transfer job will fail gracefully in the Jobs Monitor and the partial asset will be deleted from the destination.

The maximum number of jobs are limited to 2000 in the GV STRATUS 32-bit application, and 5000 in the 64-bit application.

2. Right-click and select **Columns** to display specific column on the Jobs Monitor.

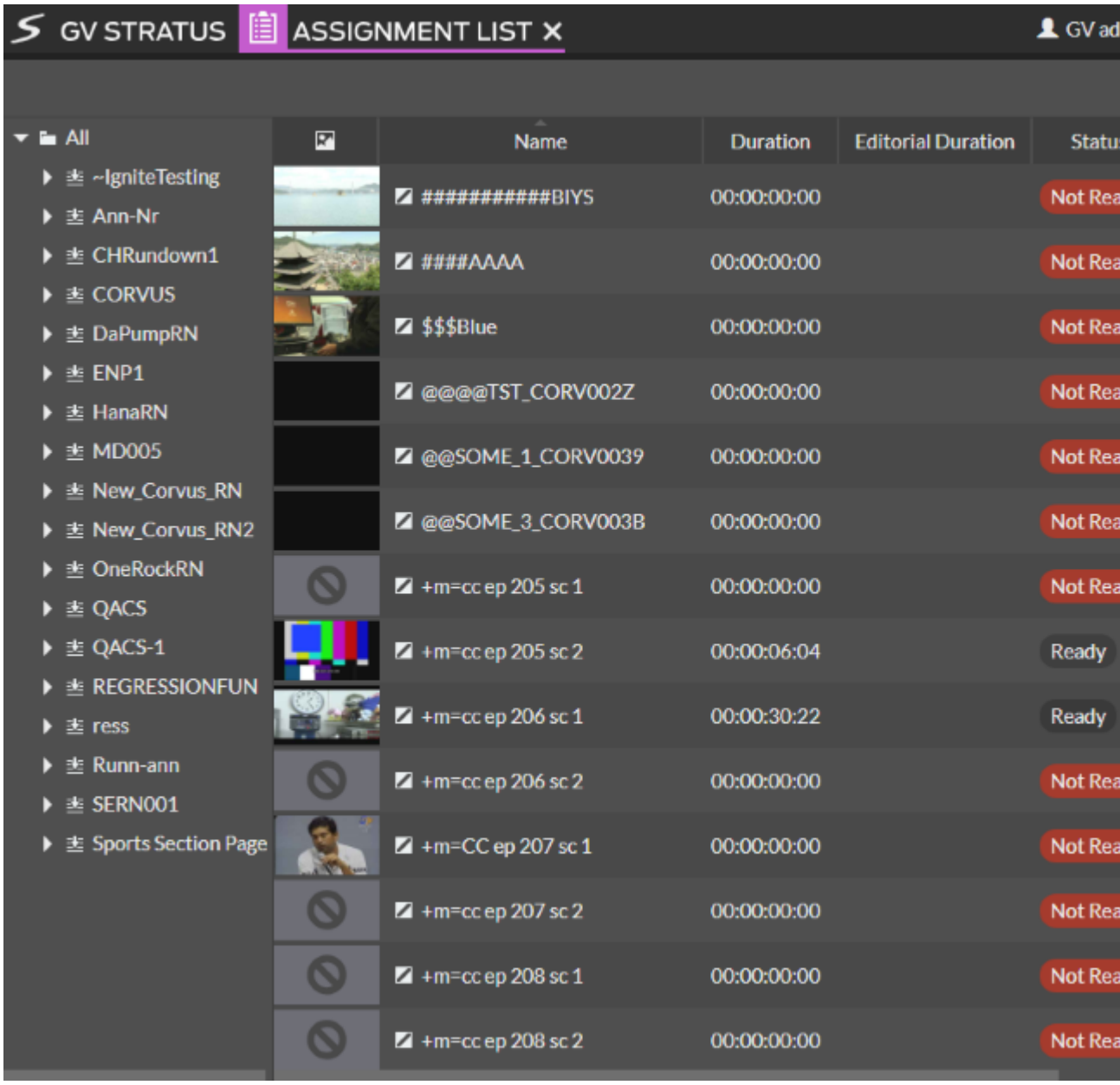


3. To stop the GV STRATUS system from running an upcoming job, right-click an upcoming job and select **Cancel**.
4. To remove a completed job from the list, right-click a completed job and select **Delete**.

The Assignment List

The Assignment List allows you to view incomplete and completed placeholders, and rundown stories on your Newsroom Computer System. You also need GV STRATUS Rundown components such as SDB Server and XMOS Server to run the Assignment List. The Assignment List appears in the GV STRATUS Web Client as a separate panel that can be accessed from the tool section of the Navigator.

You can only launch the tool if you have the Assignment List role.



The Assignment List panel features are as follows:

- Rundown view — Displays rundowns and stories for each rundown on the left panel. Rundowns display alphabetically in the panel, while stories appear in sequence as assigned in the Newsroom Computer System.
- Placeholder list — Displays incomplete and completed placeholders. When you select a rundown, all placeholders in that rundown appear in the placeholder list. When you select a story in the rundown, only placeholders in that story appear in the placeholder list in the same sequence as in the story. When you select **All**, all placeholders appear in the placeholder list.
- Missing clip indicator — Displays the number of missing clips that can help you determine the number of incomplete assignments.

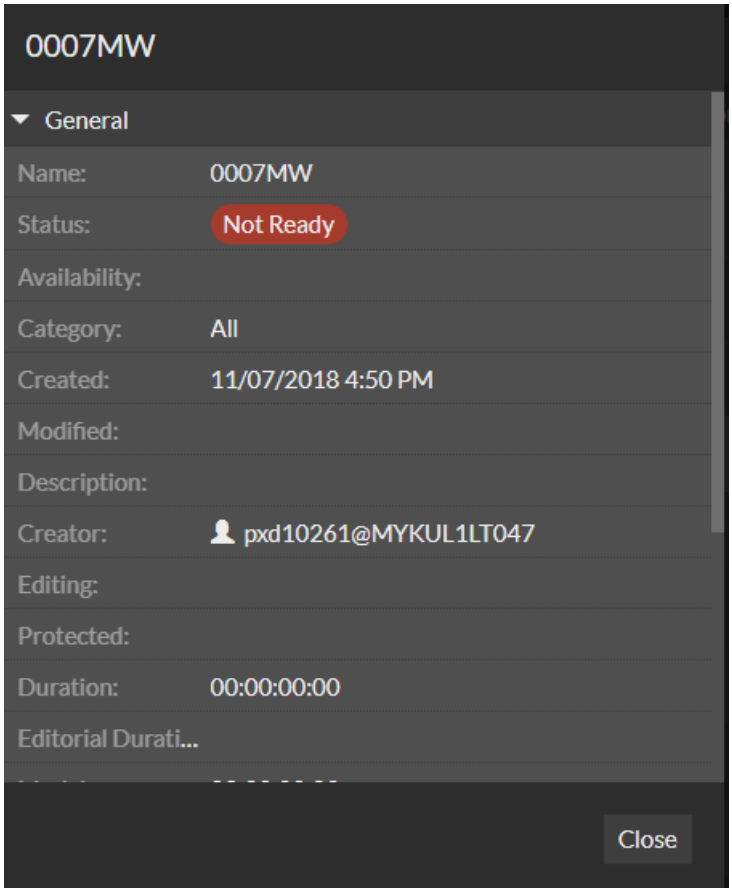
- Incomplete placeholder indicator — Displays blank thumbnails for incomplete placeholders. Completed placeholders are identified by the thumbnail display and **READY** status in the Status column.
- Status — Displays the status of placeholders. **Ready** status displays if the asset linked to the placeholder is already transferred to the Playout server.

Viewing placeholder properties

You can view the properties of a placeholder in the Assignment List or the Inspector panel.

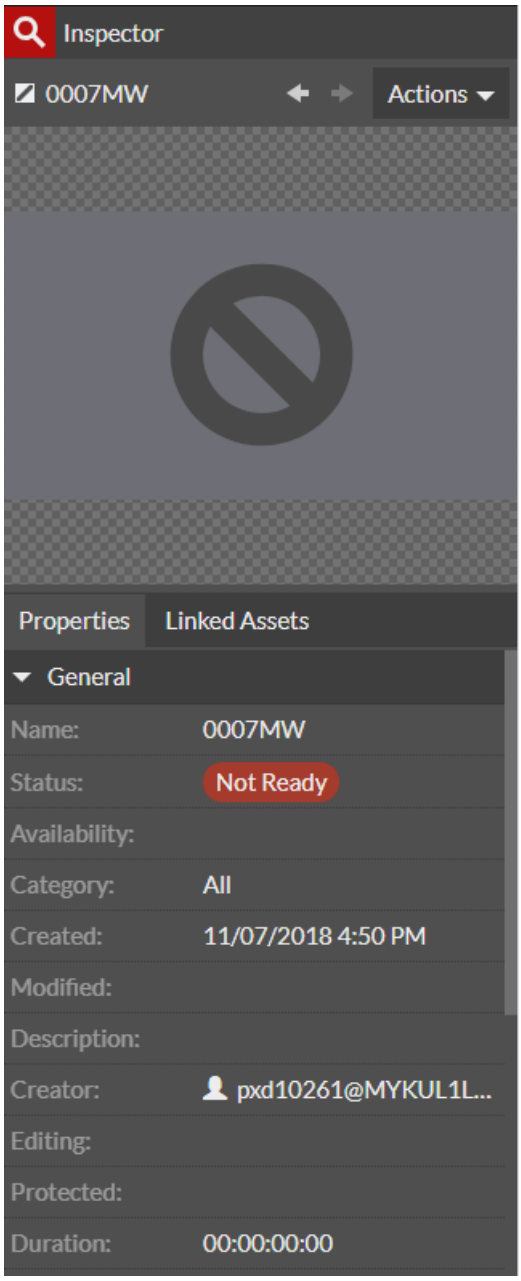
1. To view in the Assignment List, do one of the following:
   - Double-click on the placeholder.
   - Right-click on the placeholder and select **Open**.

   The placeholder properties dialog opens.



2. To view in the Inspector, do one of the following:
   - Right-click on the placeholder and select **Open With | Inspector**.
   - Drag the placeholder from the Assignment List into the Inspector.

   The placeholder properties display in the Inspector panel.



Checking missing clips

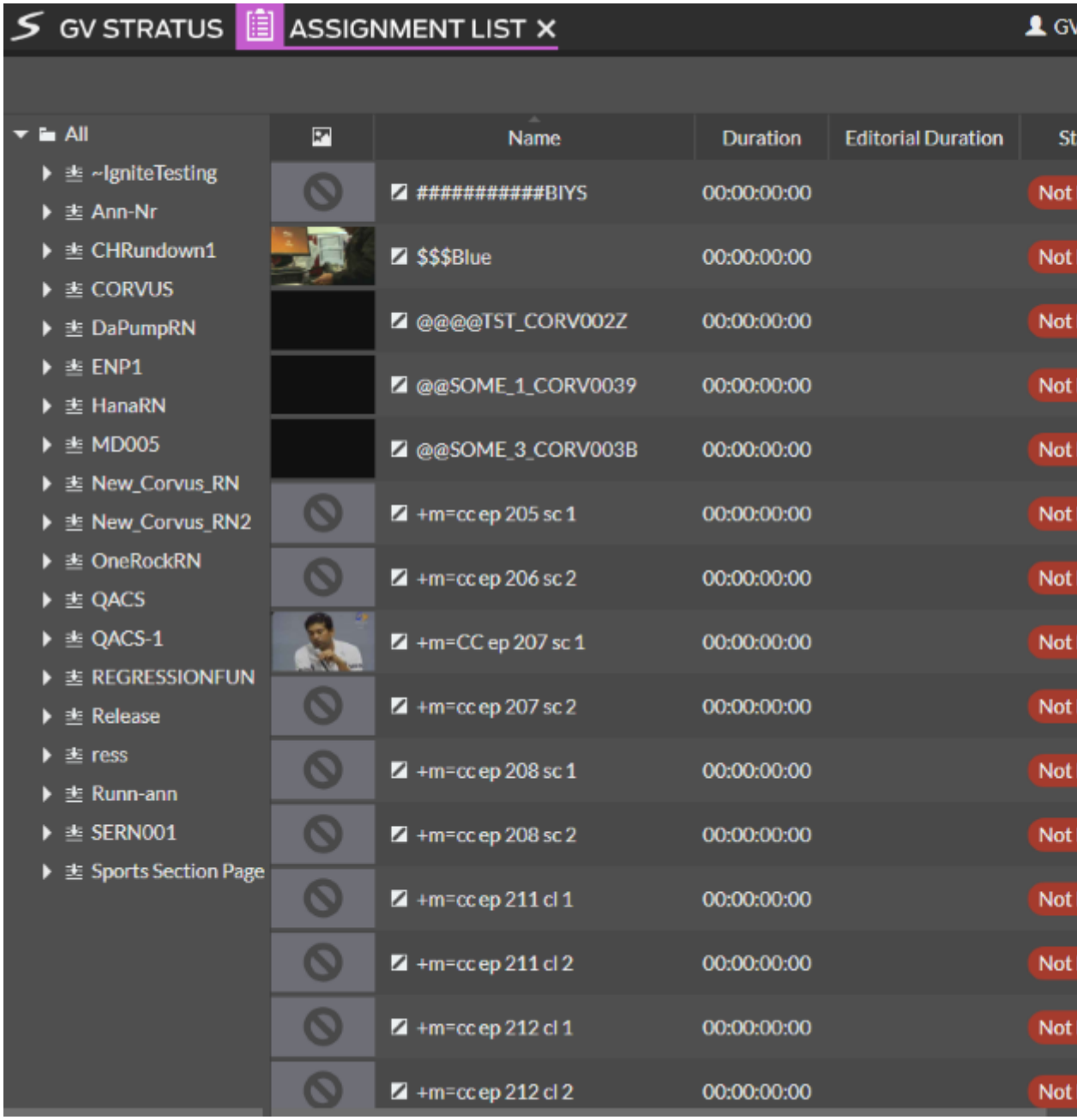
The Assignment List lets you see if placeholders are complete and ready for air.

You can see thumbnails for placeholders with linked clips, which can also be identified by **Ready** status in the Assignment List.

- To display placeholders with missing clips only, click the **Missing Placeholders Only** button.

  Only placeholders with missing clips and **Not Ready** status are displayed.

  The **Missing Placeholders Only** button displays in blue.

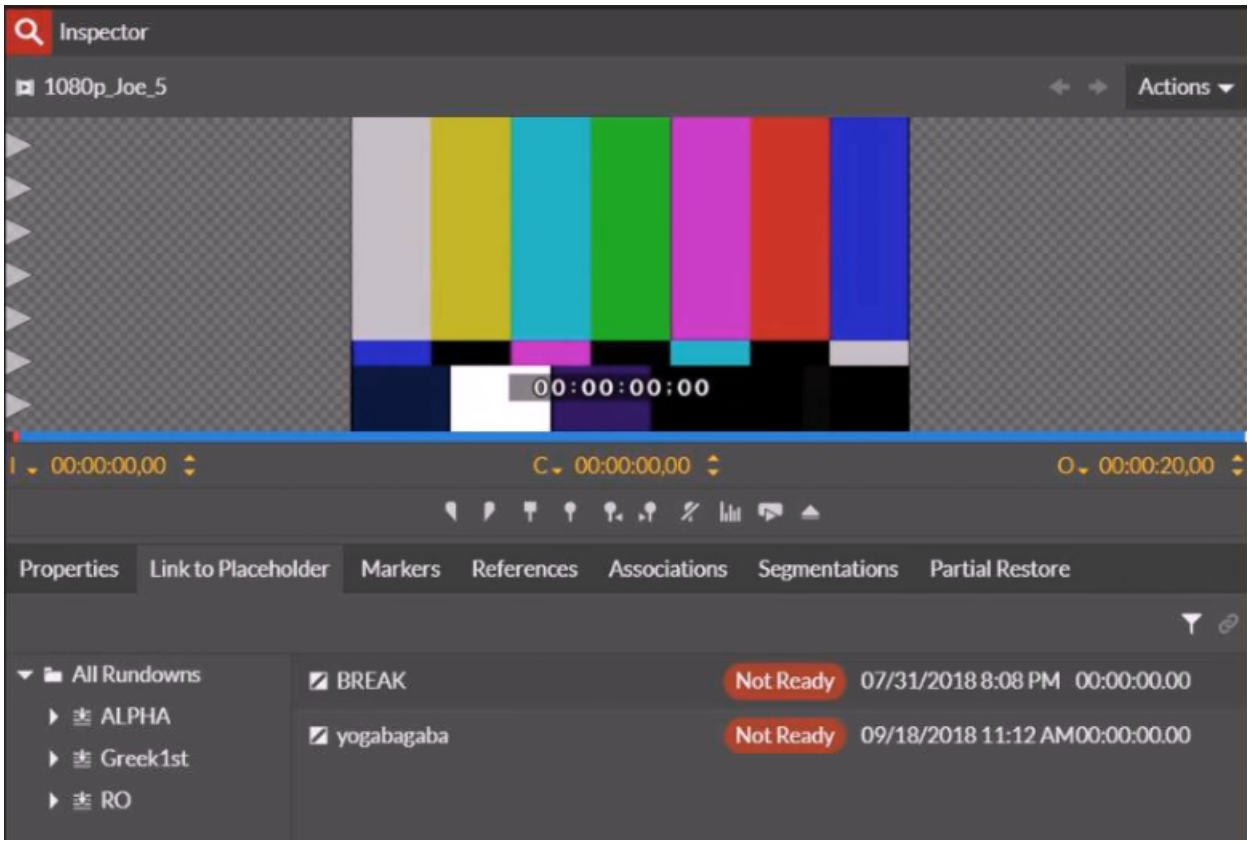


If you want to see the entire list of placeholders, click the **Missing Placeholders Only** button again.

Linking clip to a placeholder

1. Select and double-click a clip in the Asset List.

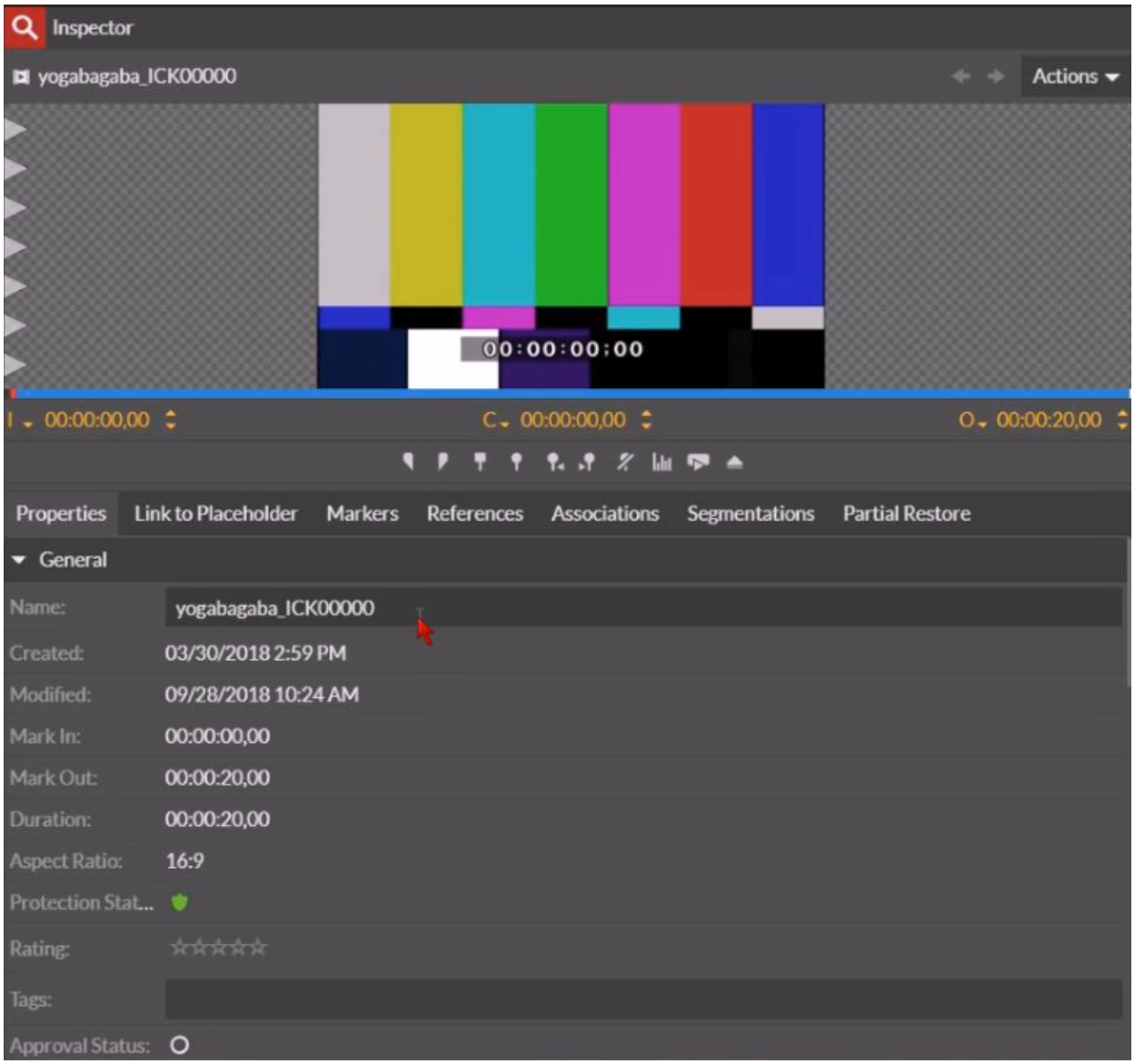
   The clip properties display in the Inspector.



2. In the **Link To Placeholder** tab, click the **Missing Placeholders Only** button to only display placeholders with missing clips.
3. Select a placeholder to link the clip to.

4. Click the **Link Selected Placeholder** button.

   The placeholder name and ID filled in to replace the previous name of the clip. The clip is now associated with the placeholder.



After the clip is transferred to the playout server, the placeholder status in the Assignment List changes to **READY** and the placeholder duration is updated.

The Segmentation tool

Prerequisite:

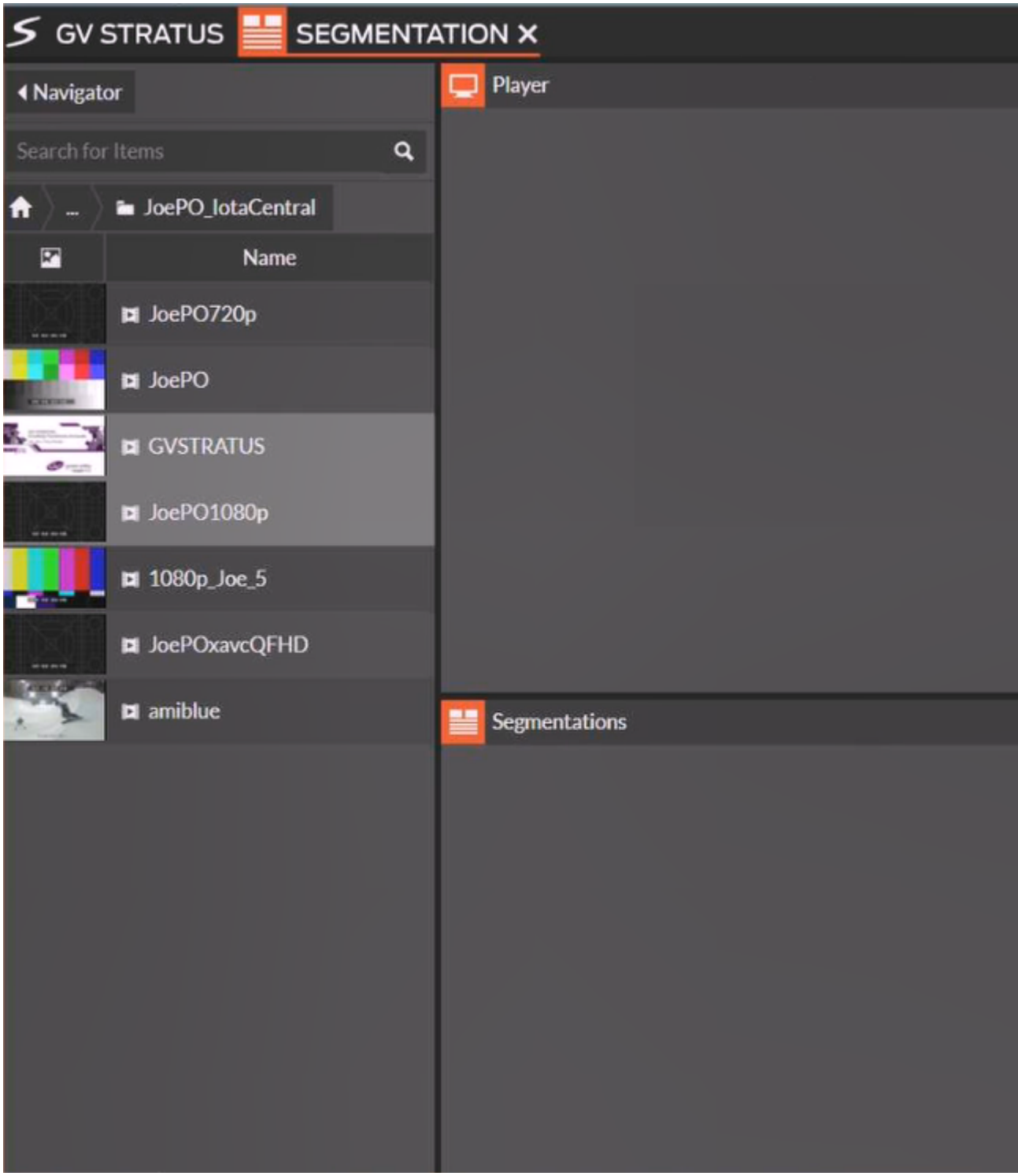
- This SiteConfig role must be assigned in the Express/Core server:
  - GV STRATUS Proxy Streaming Service

- This license must be installed in the Express/Core server via SabreTooth:
  - STRATUS-PROXYSTREAMING

The Segmentation tool allows you to assign an asset into multiple segments for insertion of commercials in between segments, or to create diverse segments of an asset for different broadcast times. You can easily create several Segmentation panels in the tool to create multiple types of segments to suit your broadcast schedule.

The Segmentation tool displays as a composite panel in the GV STRATUS Web Client application. It includes the Player, and Segmentation panel(s).

You can only create segments if you have the Segmentation role.



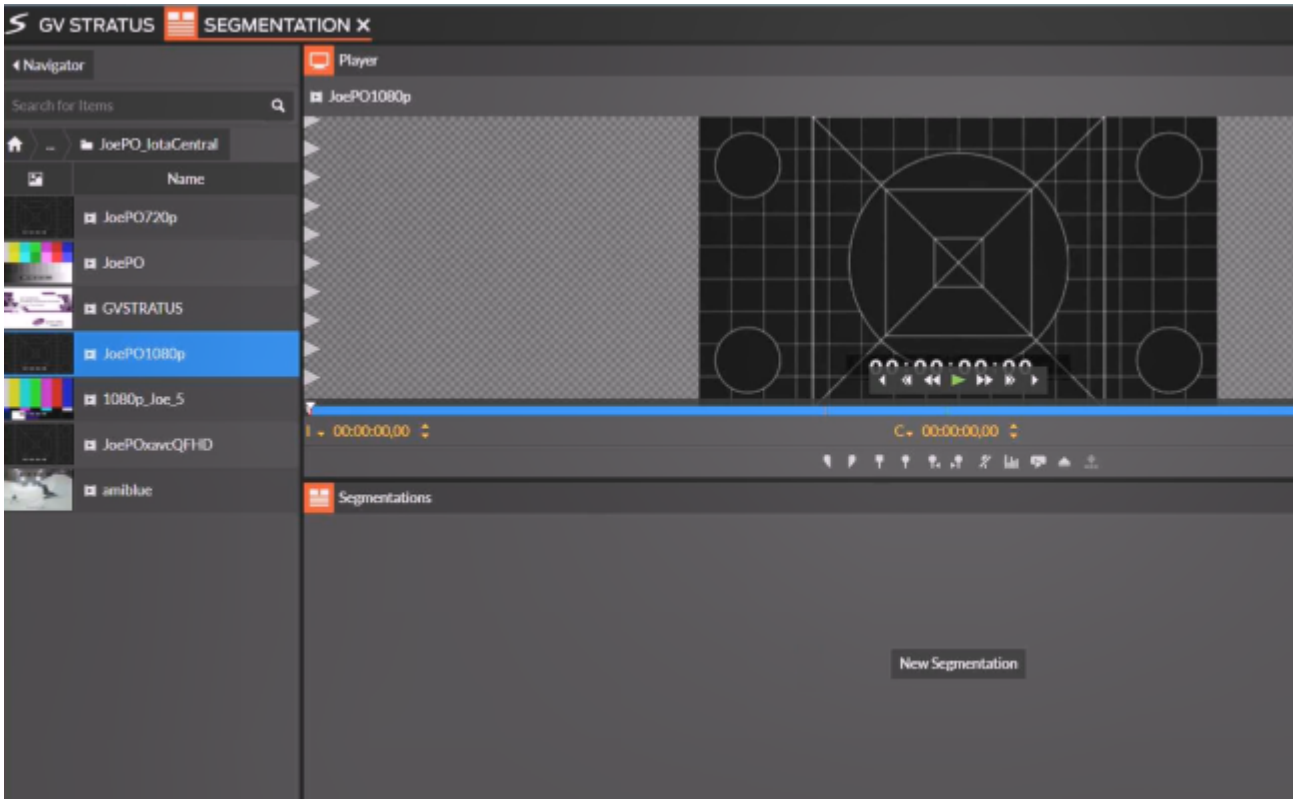
Segmentation tool features are as follows:

- Viewer — Loads assets to be previewed.
- Segmentation Panel — Displays the list of segments of the asset.

If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets, and metadata that do not have read permissions are not visible. Markers and segments permissions must be set to **Allow** in order to create, update, or delete markers and segments.

Adding a Segmentation panel

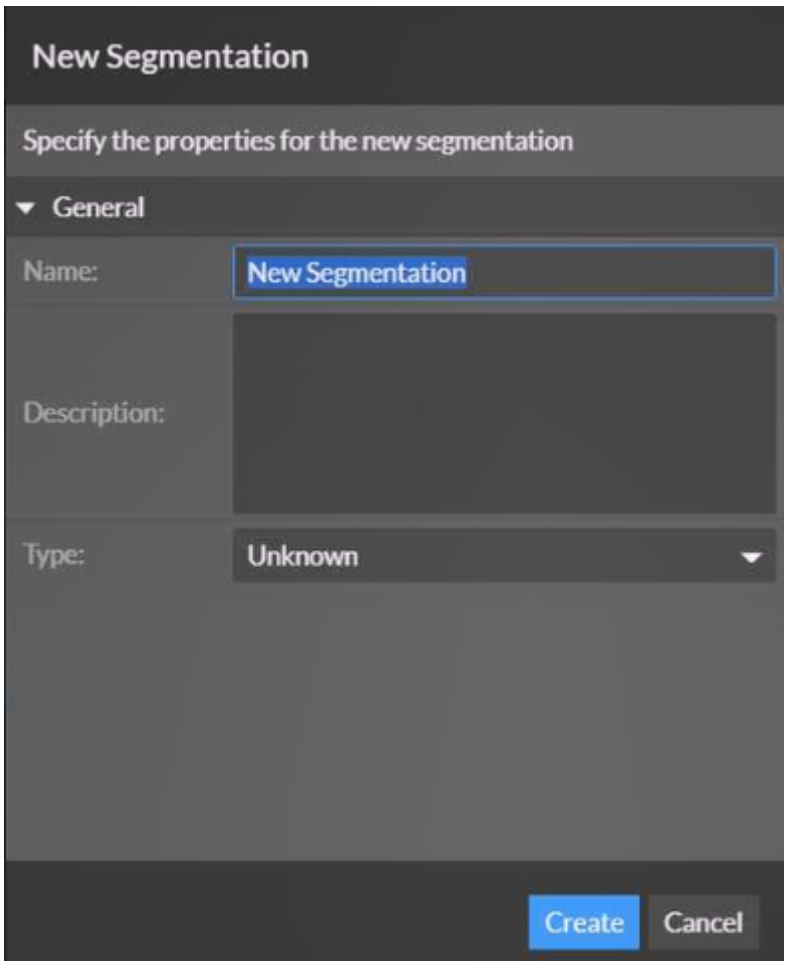
You can create and add segmentation panels to accommodate different kinds of asset segmentation in your operation.



1. Drag an asset into the Player.

2. Click the **New Segmentation** button.

   The New Segmentation dialog opens..

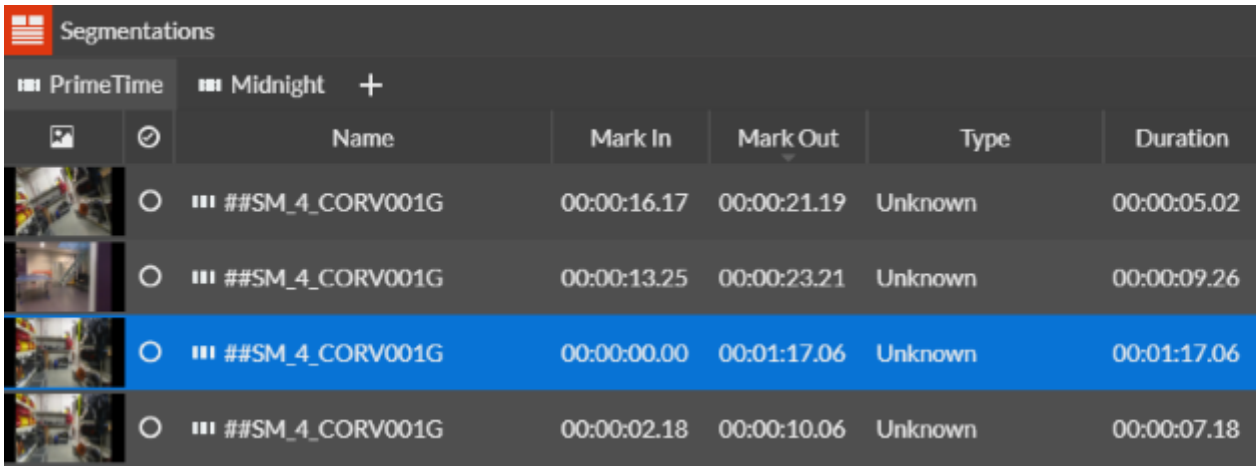


3. Enter the **Name** of the segmentation panel.
4. Enter the **Description** of the panel, if desired.
5. Select the **Type** of the segmentation panel from the drop-down list.
6. Click **Create** to save the segmentation panel.

   The new segmentation panel opens in the Segmentation Tool.

7. Click the + button to create more segmentation panels, if desired.

   You can create multiple Segmentation panels to assign different segments of an asset for different broadcast times.



Assigning segments to assets

- If GV STRATUS security is enforced, your credentials must give you full read and write permissions on bins, assets, and segments. You can only view segments with read permission, and modify segments with write permission.
- Create Segment and Update Segment permissions must be set to **Allow**, for you to create and update segments.

You can assign segments to an asset in the Segmentation panel. Segments are created in the Player panel by marking in and out specific part of the asset.

1. Drag the selected asset from Asset List into the Player.
2. Navigate to the starting point and click the **Mark In** button. (**I**)
3. Determine the end-point of your segment and click the **Mark Out** button. (**O**)
4. Click on the asset in the Player, then drag and drop the segment into the Segmentation panel.

   The segment adds into the Segmentation panel.

5. Repeat above steps to add more segments of the asset into the Segmentation panel.

   NOTE: Without Create Segment and Update Segment permissions, segments cannot be rearranged or dragged and dropped in the same Segmentation panel, or from one panel to another.

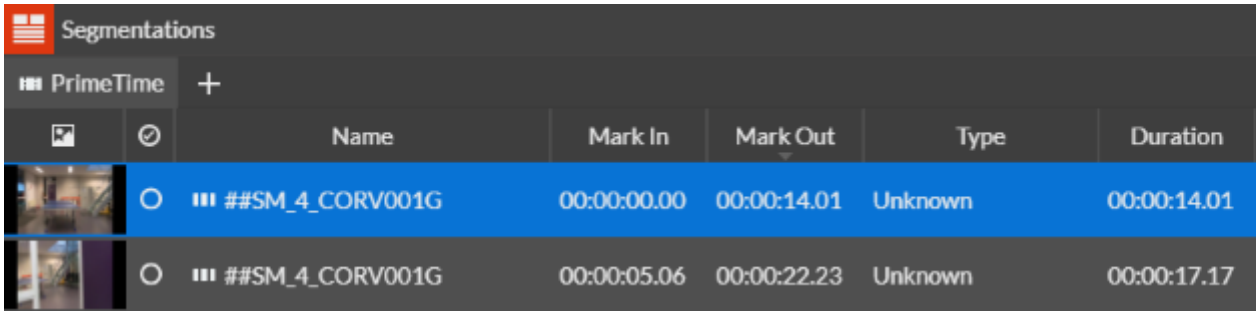
You can also create various segment lengths of an asset in multiple segmentation panels for different broadcast times. For example, a program that is scheduled for prime time has more commercial slots compared to the repeat of the same program at a later time. Therefore, several kinds of segments in multiple segmentation panels can be created for the same asset.

Protecting a segment

If it is not already displayed, display the Protection Status column.

1. In the Segmentation Panel, right-click and select **Columns | Protection Status**.

   The Protection Status column displays.



2. Select a segment to be protected and click the **Unprotected** button.

   The segment status toggled from unprotected to protected.

When it is protected, the Edit mode is not allowed and you can only be in the Preview mode.

Renaming a segment

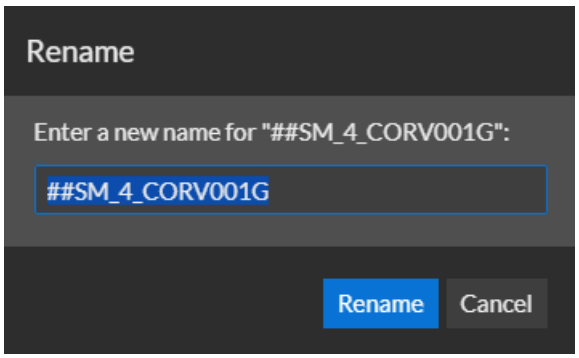
- Update Segment permission must be set to **Allow**, for you to rename segments.

You can rename segments to differentiate multiple segments of an asset.

1. Select a segment that you want to rename.

2. Right-click and select **Rename**. (**F2**)

   The **Rename** dialog opens.



3. Enter the new name for the segment.
4. Click **Rename**.
5. Repeat above steps to rename other segments.

   Segments are renamed on the segmentation panel.

Editing segments

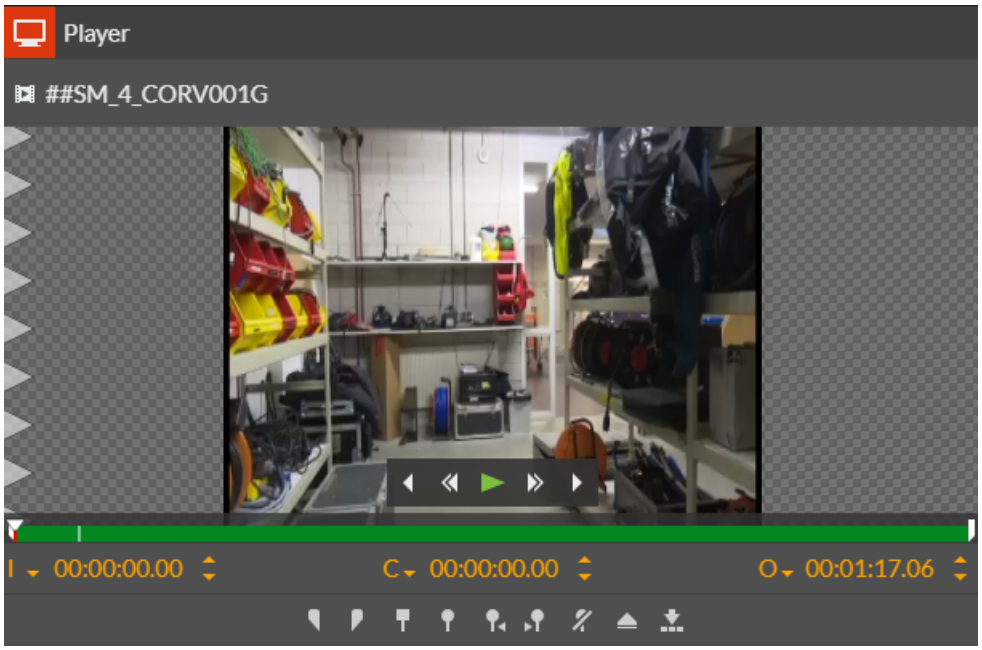
- If GV STRATUS security is enforced, your credentials must give you full read and write permissions on bins, assets, and segments. You can only view segments with read permission, and modify segments with write permission.

- Create Segment and Update Segment permissions must be set to **Allow**, for you to create and update segments.

When you edit a segment, you change the length of the viewable asset by changing the Mark In and Mark Out points of the segment.

1. Double-click a segment in the Segmentation panel.

   The segment displays in the Player. The scrub bar of the segment appears in green to indicate that the segment is editable and in the **Edit Mode**.



2. Navigate to the desired starting point using the scrub bar, and click the **Mark In** button. (**I**)
3. Navigate to the desired end-point using the scrub bar, and click the **Mark Out** button. (**O**)

   Your changes are saved to the segment.

4. Click anywhere on the Segmentation panel to exit the **Edit Mode**.

   The color of the Player scrub bar turns back to blue to indicate that the segment is no longer in the **Edit Mode**.

The Segmentation panel displays the new duration, mark in, and mark out points for the segment.

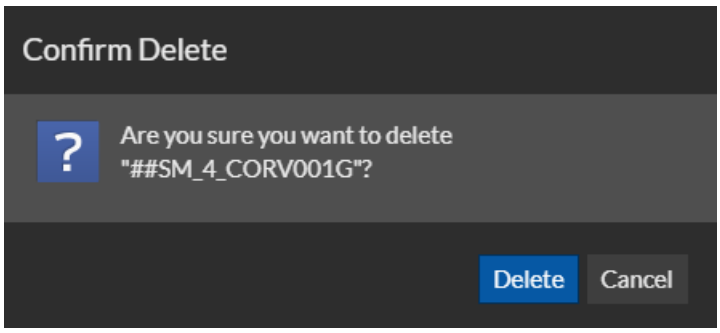
Deleting a segment

- Delete Segment permission must be set to **Allow**, for you to delete segments.

1. Select a segment that you want to delete.

2. Right-click and select **Delete**. (**Delete**)

   The Confirm Delete dialog opens.



3. Click **Delete**.

The selected segment is deleted from the segmentation panel.

The Simple Editor tool

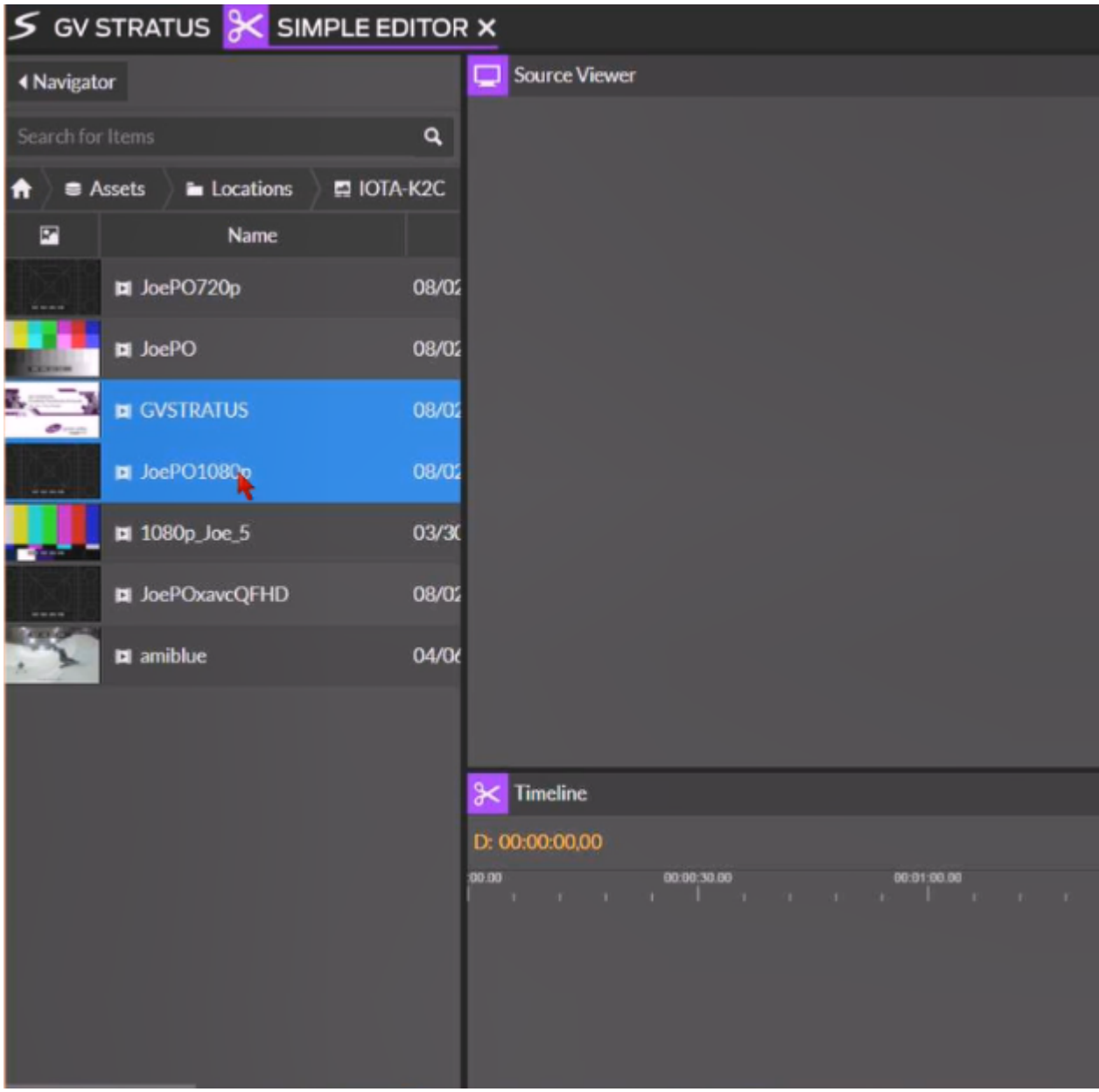
- The Proxy Streaming Server must be configured in order to use the Simple Editor tool in GV STRATUS Web Clients.
- This SiteConfig role must be assigned in the Express/Core server:
  - GV STRATUS Proxy Streaming Service

- This license must be installed in the Express/Core server via SabreTooth:
  - STRATUS-PROXYSTREAMING

  The Simple Editor tool allows you to create the STRATUS EDL (Edit Decision List) and access the editing workspace. Launch the Simple Editor tool by doing one of the following:

  - Right-click on an asset in the Asset List and select **Open With | Simple Editor**
  - In the Navigator panel, select **Tools | Simple Editor**

  The Simple Editor tool launches as a composite panel inclusive of Source Viewer, Sequence Viewer, and Timeline. The Navigator is available on the left for users to drag and drop assets into the tool.

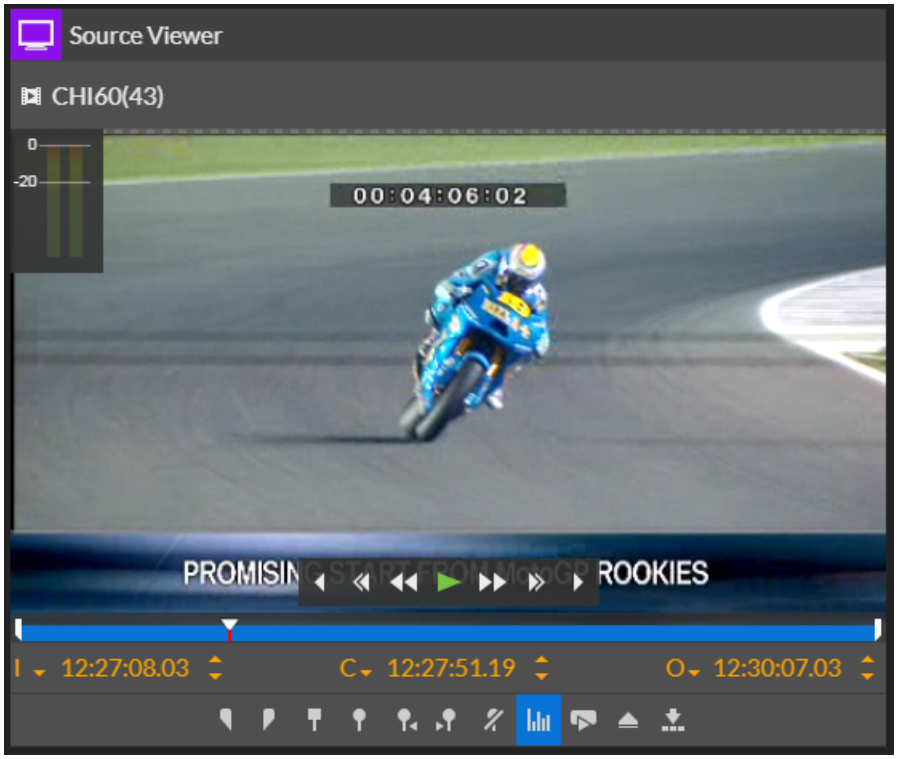


The Source Viewer

The Source Viewer appears in a composite panel when you launch the Simple Editor tool. The Source Viewer allows you to preview assets, both assets already recorded and assets currently being recorded.

To view asset in the Source Viewer, do one of the following:

- Drag the asset to the Simple Editor tab and drop it into the Source Viewer.
- Right-click an asset on the Asset List and select **Open With | Simple Editor**.

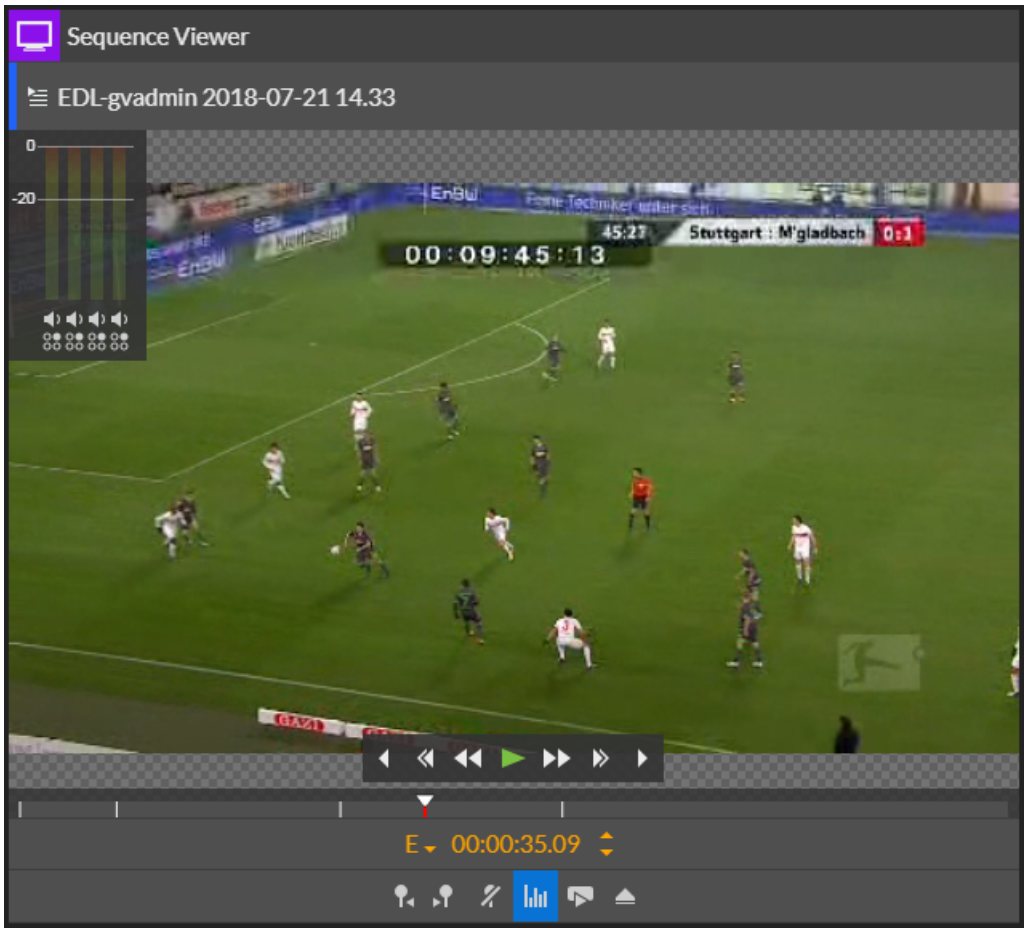


The Source Viewer includes the following components :

- Title bar — Displays the name of asset loaded in the Source Viewer.
- Overlay Transport Controls — Consists of transport controls to navigate through the asset. Visible when you hover the mouse pointer over the viewer.
- Clip Viewer — Displays the asset.
- Audio Overlay — Displays audio settings embedded within the asset. Audio Overlay display can be toggled from the button on Viewer Controls.
- Scrub Bar — Scrubs through the asset.
- Viewer Controls — Allows you to mark in/out the asset, insert markers and keywords, go to previous/next event, toggle hide events, toggle the display of the audio overlay, toggle loop play, add asset into the Timeline, and eject the asset.
- Timecode Controls — Allows you to select the mark in/out and other timecode types to display. Also lets you navigate through the clip to a specific timecode.

The Sequence Viewer

The Sequence Viewer allows you to play assets (also called events) that have been assembled into a STRATUS EDL in the Simple Editor. The Sequence Viewer appears in the application as a panel in the Simple Editor tool.



The Sequence Viewer includes the following components:

- Title bar — Displays the name of the EDL.
- Viewer — Displays the event currently playing in the EDL.
- Overlay Transport controls — Navigates through the EDL. Visible when you hover the mouse pointer over the viewer.
- Audio Overlay — Displays audio settings embedded within each event in the EDL. Audio Overlay display can be toggled from the button on Viewer Controls.
- Scrub bar — Lets you scrub through the EDL.
- Viewer Controls — Allows you to go to previous/next event, toggle hide events, toggle the display of the audio overlay, toggle loop play, and eject the EDL.
- Timecode Controls — Allows you to navigate through the EDL to a specific timecode. Also lets you select the mark in/out and other timecode types to be displayed.

The Sequence Viewer in the Simple Editor can only load EDLs. You can navigate through the EDL by using the transport controls. Each event in the EDL is indicated by a symbol on the scrub bar.

Viewer buttons

These transport control buttons on the Source Viewer and Sequence Viewer let you move through the viewed asset:

-1 Frame: Goes back one frame.

-10 Frames: Goes back ten frames.

Rewind: Rewinds the current asset. First press, rewinds -8x speed. Second press, increases to -16x speed.

Play: Plays the clip. Toggles with the Pause button.

Fast Forward: Fast Forwards the current asset. First press, fast forwards to 8x speed. Second press, increases to 16x speed.

+10 Frames: Goes forward ten frames.

+1 Frame: Goes forward one frame.

These buttons and controls located below the viewer let you perform various functions:

Mark In: Sets the Mark In point.

Mark Out: Sets the Mark Out point.

Create Keyword: Logs an item from mark in to mark out.

Create Marker: Logs an item for the current position.

 Go to Previous Event: Goes to previous event.

Go to Next Event: Goes to next event.

Toggle Hide Events: Hides marker and keyword indicators on the scrub bar.

Toggle Show Audio Meters: Toggles the display of audio overlay on the Source Viewer.

Toggle Loop Play: Loops the playback of current asset between mark in to mark out.

Eject: Ejects the current asset.

Add to Timeline: Adds the asset into the Timeline.

Timecode: Displays timecode and allows you navigate to a specific timecode. Also lets you select the timecode type for display.

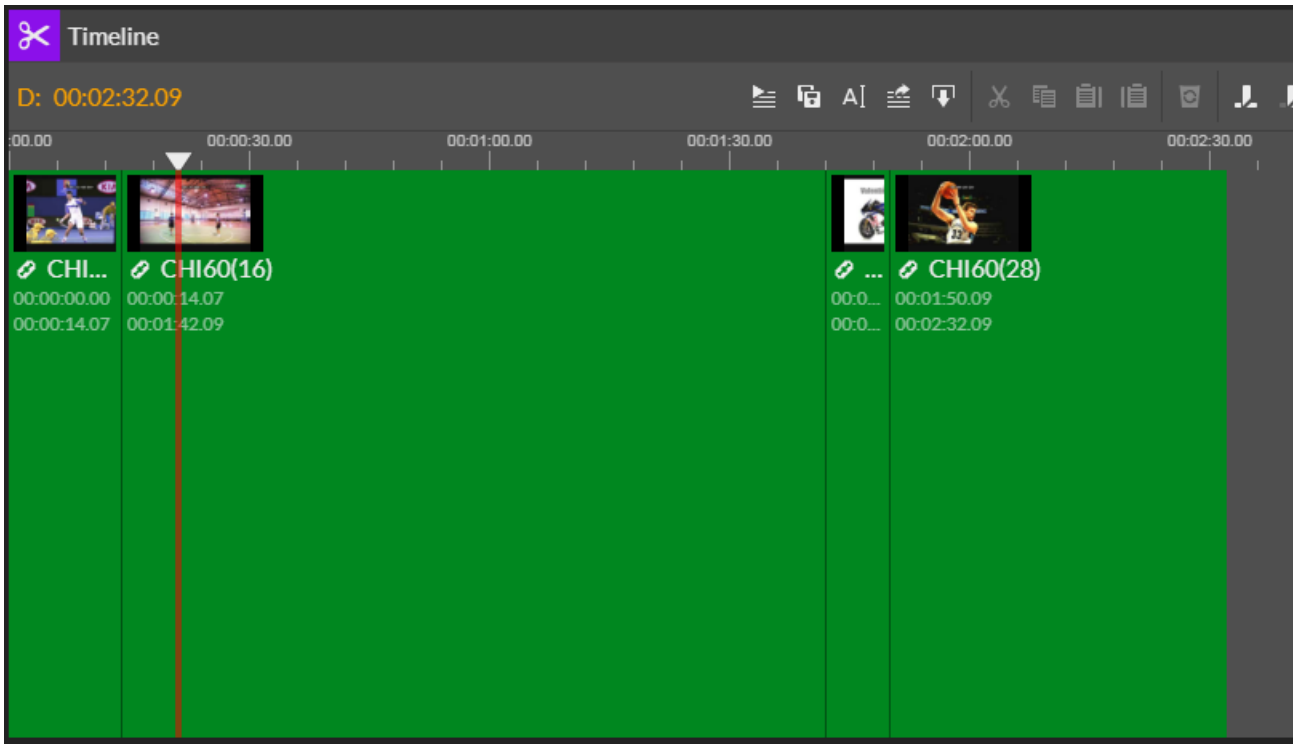
These control buttons on the audio overlay let you control the audio of the viewed asset:

Mute: Silences the selected audio channel.

Solo: Isolates the selected audio channel.

The Timeline

The Timeline panel in the Simple Editor tool allows you to assemble and edit reference to sequences known as the STRATUS EDL (Edit Decision List). You can drag assets into the panel to create or add to an EDL. On the Timeline, those EDL assets are called events.



The toolbar in the panel consists of buttons to edits the series of events in the EDL.

Once you have assembled the EDL, you can preview it in the Sequence Viewer. On the Timeline panel, the progress bar indicates the current play location when that event is being played in the Sequence Viewer. The Timeline panel supports the insertion of clips, sub-clips, and EDLs only.

Timeline buttons

These buttons and controls located on the Timeline let you perform various functions:

Create EDL: Create an EDL in the Timeline.

Save As: Save the EDL in the Timeline.

Rename EDL: Rename the EDL in the Timeline.

Conform EDL: Conform and Send the EDL in the Timeline to a configured GV STRATUS location.

Export to FCP XML: Generate the EDL in FCP XML format.

Cut: Cut an event from the EDL in the Timeline.

Copy: Copy an event from the EDL in the Timeline.

Paste Top: Paste a copied event before the currently selected event in the EDL.

Paste Tail: Paste a copied event after the currently selected event in the EDL.

Delete: Delete an event from the EDL in the Timeline.

Split: Splits the item at the current position.

Trim Top: Trims the start of the event at the current position.

Trim Tail: Trims the end of the event at the current position.

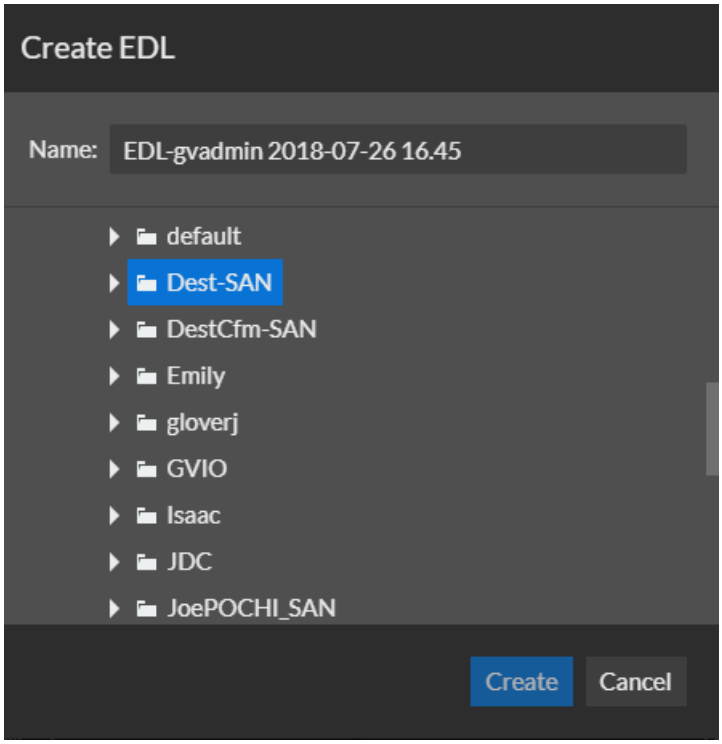
Zoom In: Zooms in the view of the Timeline. The slider also can be used to zoom in the Timeline.

Zoom Out: Zooms out the view of the Timeline. The slider also can be used to zoom out the Timeline.

Creating an EDL

1. Open the Simple Editor tool and click the **Create EDL** button on the Timeline toolbar.

   The Create EDL dialog box opens.



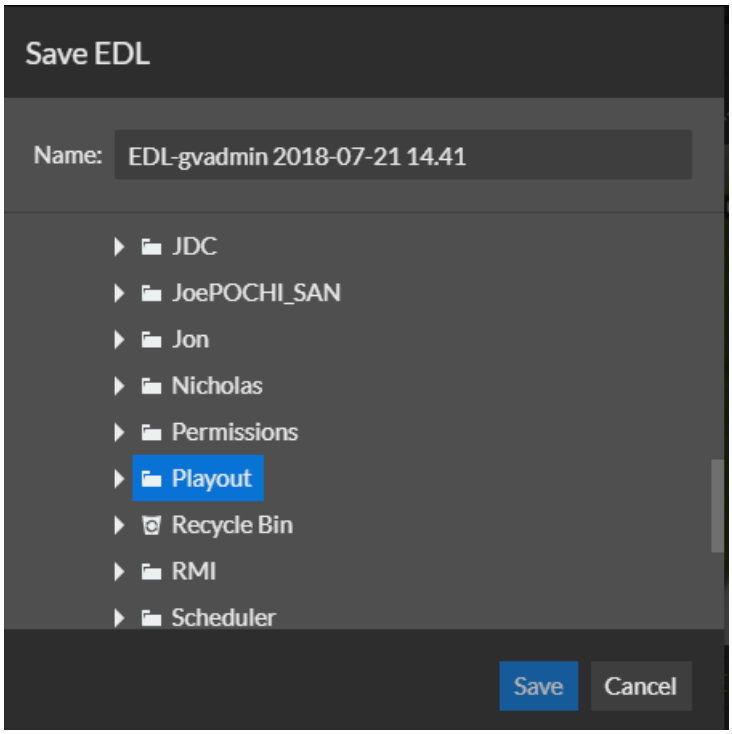
2. Enter the name of your EDL, select a K2 bin to save the EDL into, and click **Create**.
3. Select an asset in the Asset List, drag it to the Simple Editor tab, and drop it into the Source Viewer panel.

   The asset loads in the Source Viewer and the asset name displays in the title bar.

4. Choose one of the following actions:
   - To preview the asset, click the **Play** button or use the appropriate transport controls.
   - To create a mark-in point, click the the **Mark In** button.
   - To create a mark-out point, click the **Mark Out** button.
5. Drag the asset into the Timeline panel.

   The asset is now in the Timeline of the Simple Editor and referred to as an *event*.
6. Repeat above steps to add additional events.
7. In the Timeline panel, use the toolbar buttons to modify events.
8. To save as a different EDL, click the **Save As** button.

   The Save EDL dialog box opens.



9. Enter the name of the EDL, select the K2 bin to save the list of events into, and click **Save**.

To preview the EDL, use the transport controls in the Sequence Viewer.

You can also drag an asset or multiple assets into the Simple Editor without first creating a new EDL, then those assets load into the Timeline panel. By default, your EDL will be automatically saved in the Lost and Found bin.

Editing an event

1. Double-click an event on the Timeline.

   The event opens in the Source Viewer.
2. To edit, mark in and mark out the event.

The event duration automatically updates in the Timeline.

There is no Undo feature for these operations.

Rearranging or deleting events

Select the event in the panel and choose one of the following actions:

- To move the selected event, drag the event to a new location in the Timeline.
- To copy the selected event, click the **Copy** button.
- To cut the selected event, click the **Cut** button.
- To paste before the selected event, click the **Paste Top** button.
- To paste after the selected event, click the **Paste Tail** button.
- To delete the selected event, click the **Delete** button.

There is no Undo feature for these operations.

Splitting an event

1. Navigate to the desired location in the event on the Timeline.
2. Select the **Split** button.

The event is divided into two events with identical names.

There is no Undo feature for these operations.

Playing an EDL

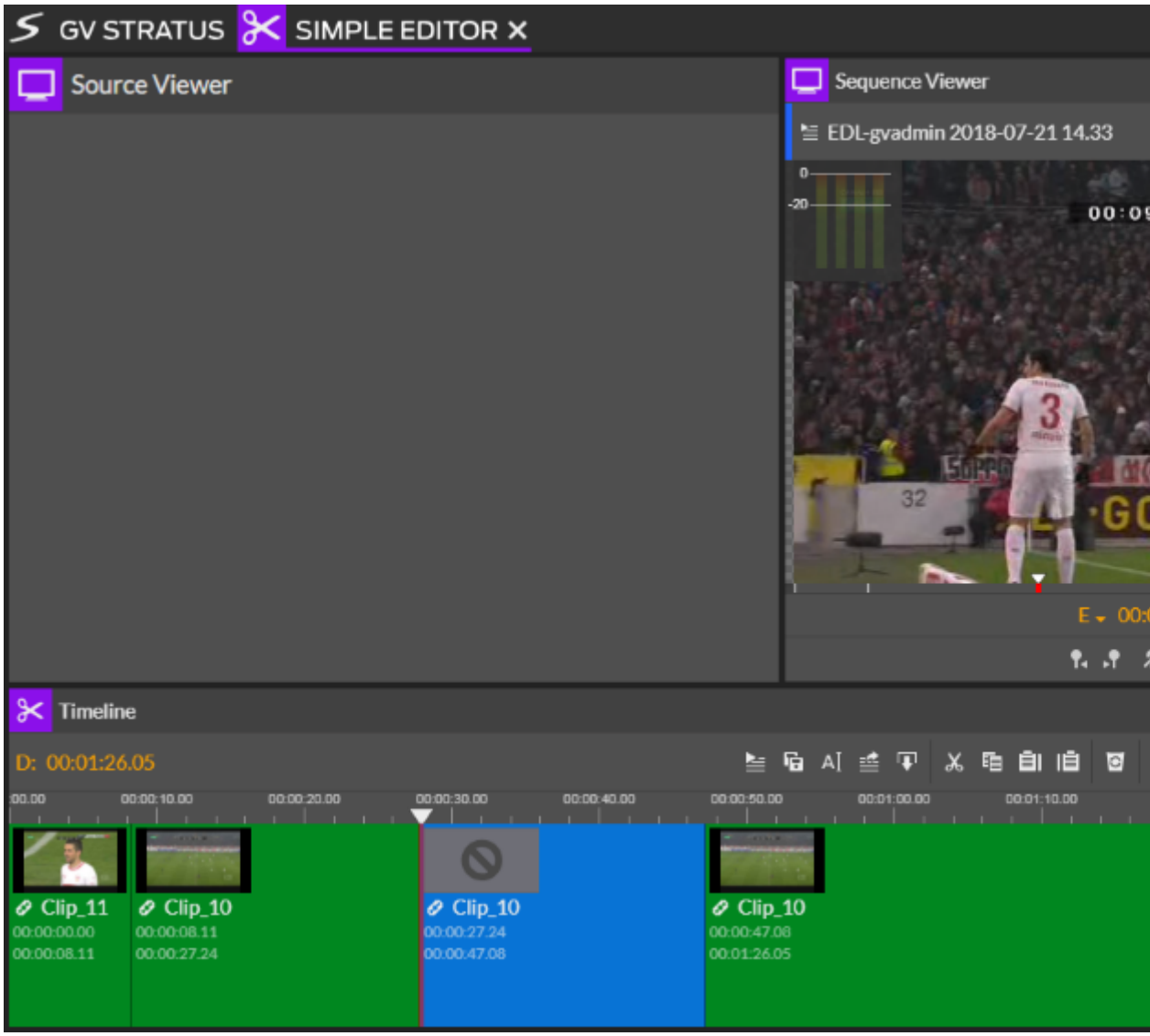
1. Right-click on an EDL in the Asset List and select **Open With | Simple Editor**.

   The EDL loads into the Sequence Viewer and the Timeline.

2. In the Sequence Viewer, use the transport controls to navigate through the EDL. Each event is indicated by a symbol in the scrub bar.

3. Click the **Play** button in the Sequence Viewer to play the EDL.

   As the event plays in the Sequence Viewer, the event's progress indicator in the Timeline displays the current location.



GV STRATUS Rundown Operation

Introducing GV STRATUS Rundown

About GV STRATUS Rundown

GV STRATUS Rundown is a playback control system that controls media servers for live playback. It includes tools to integrate the program production workflow between a media server, editing application, GV STRATUS media workflow application framework, and optionally a newsroom computer system.

GV STRATUS Rundown is compatible with these systems:

Media Server	K2 Media Server and Media Client
	K2 Summit 3G Production Client
	GV I/O Live Ingest and Playback Server
Editing Application	Apple Final Cut Pro
	Adobe® Premiere® Pro CC
	Avid Media Composer
	EDIUS Workgroup and EDIUS XS
	Storyboard Editor tool in GV STRATUS
Media Workflow Application Framework	GV STRATUS Media Workflow Application Framework
Newsroom Computer System	Associated Press Electronic News Production System (ENPS)
	Avid Technology iNEWS
	Octopus Newsroom
	Annova OpenMedia
	Evoxe NIS5
	Netia Media
	Ross Inception

By using GV STRATUS Rundown with a media server for server playout in live programs you can effectively replace four to six tape machines, depending on your media server. GV STRATUS Rundown displays each channel simultaneously and you can control playout with a keyboard and mouse, or with GPI buttons.

GV STRATUS Rundown consists of five software components:

- GV STRATUS Rundown application
- Assignment List Plug-in
- Assignment List Manager

- SDB Server
- XMOS Server

Terms You Should Know

To use GV STRATUS Rundown effectively and efficiently, you should become familiar with terms that are frequently used.

Term	Definition
Clip	A piece of media you can edit, containing video, audio, or both. Once a sequence is sent from EDIUS XS or GV STRATUS client to a media server it becomes a clip again. All clips and subclips merge into one clip.
Logical Asset	Combination of the GV STRATUS database information, metadata, physical assets or assets on the server, and proxy assets.
Metadata	Data about data; it can include keywords, timecode information, and other terms that help you find a particular asset.
Physical Asset	The raw program material, such as video or audio.
Placeholder	An item (in the GV STRATUS Rundown Assignment List Manager or the GV STRATUS Assignment List) reserved for a clip that doesn't yet exist or is not complete. Clips are linked to a placeholder in NCS rundowns or via GV STRATUS ActiveX Plug-in.
Proxy	A low-resolution clip that represents high-resolution material.
Script	The textual information for a news story in the newsroom computer system (NCS) rundown. Scripts can also reference electronic media, such as clips from a media server.
Sequence	Edited media, consisting of pointers to different clips and subclips edited using the EDIUS XS or GV STRATUS application.
Story	The story — a collection of clips, sequences, and scripts — is the complete news segment that plays to air.

Overview of GV STRATUS Rundown

GV STRATUS Rundown is a playout control system that links a nonlinear editing system with an electronic news production system, media workflow application framework, and a media server for a complete digital solution.

Playback operators use the main GV STRATUS Rundown application to create new playlists, and to control playlists before and during broadcasts. GV STRATUS Rundown application consists of several components such as Clip Browser, Playlist Overview, Rundown List, Channel windows and Playlist to coordinate playback.

With the integration of GV STRATUS Media Workflow Application Framework in GV STRATUS Rundown, playback operators can search, add, and edit metadata of assets created for broadcasts. The GV STRATUS ActiveX Plugin also allows playback operators to preview assets via the Source Viewer or the Inspector without taking up a channel on the playout server. In order to use GV STRATUS within GV STRATUS Rundown, the STRATUS-ELITE license is needed on the GV STRATUS Core Services server.

If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets, and metadata that do not have read permissions are not visible. Markers and segments permissions must be set to **Allow** in order to create, update, or delete markers and segments.

Using GV STRATUS Rundown

GV STRATUS Rundown includes tools to integrate the program production workflow between a media server, an editing application, a newsroom computer system, and the GV STRATUS ActiveX Plug-in.

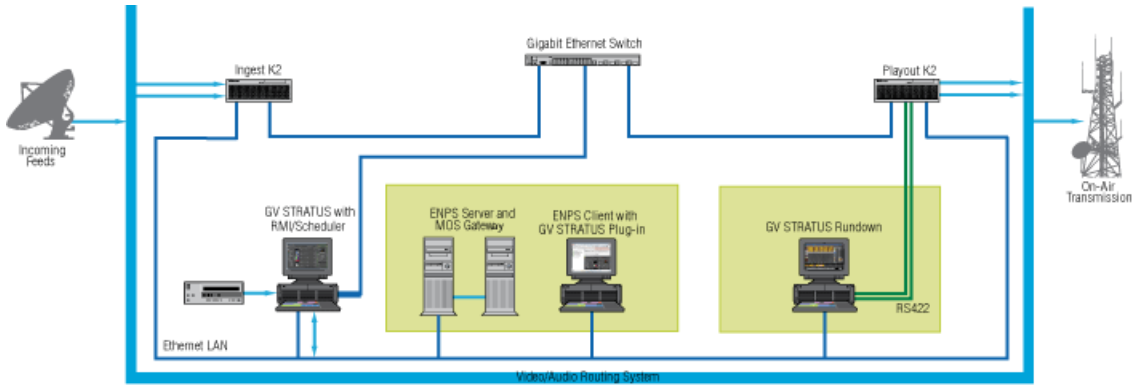
With GV STRATUS Rundown, you can control live playback for your broadcast. You can use GV STRATUS Rundown in two ways:

- Create playlists by linking to a newsroom computer system (NCS)
- Create playlists manually in GV STRATUS Rundown

Linking to a Newsroom Computer System (NCS)

The most efficient way to use GV STRATUS Rundown is with a MOS-compatible newsroom computer system.

The producer uses the newsroom computer system to create rundowns for news shows, and links clips to rundown scripts. After the clips are complete, control room personnel use GV STRATUS Rundown to play out the clips to air.



A typical newsroom workflow using a newsroom computer system (NCS) is:

1. The news producer creates a rundown using NCS.
2. The news producer uses the Assignment List in GV STRATUS ActiveX Plug-in to:
   - Create placeholders for scripts that require clips
   - Assign placeholders to editors
   - Link placeholders to scripts in the rundown
3. The news producer assigns playback channels within the NCS rundown.
4. The news editor creates sequences for assignments.
5. The news editor uses the GV STRATUS Rundown Assignment List Manager to:
   - Receive assignments from the producer
   - Create additional clip placeholders
   - Reassign placeholders to other editors
6. Control room personnel use the main GV STRATUS Rundown application to:
   - Open the producer's rundown playlist
   - Assign clips to specific channels for playback
   - Rearrange, insert, or delete clips prior to broadcast if necessary
   - Play back clips during the news broadcast

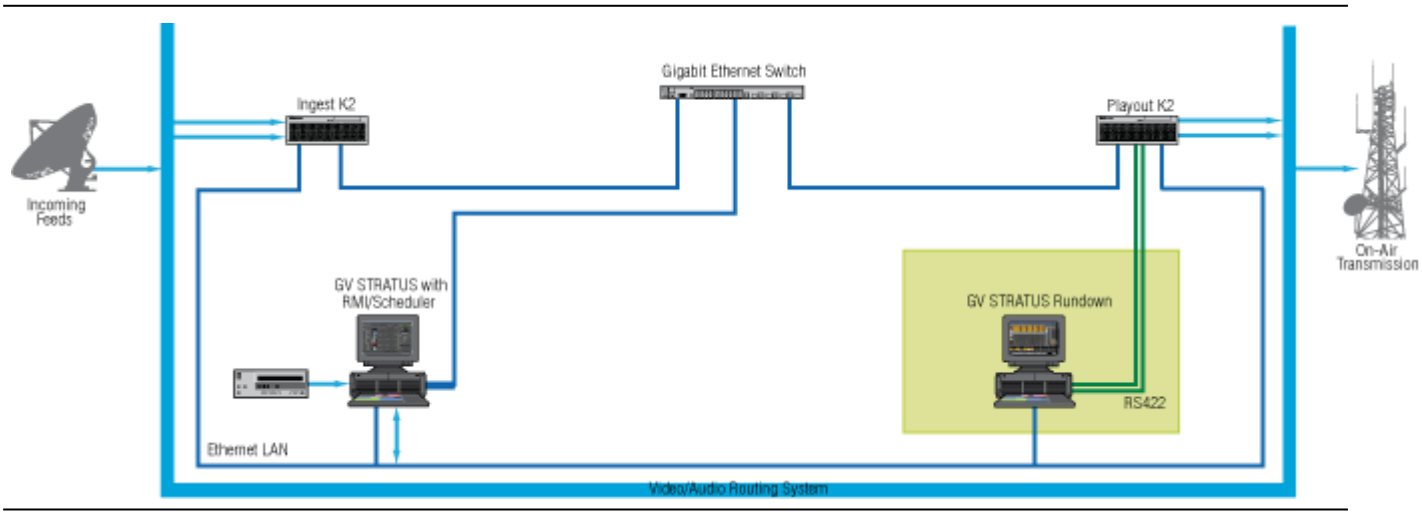
Related Topics

Using GV STRATUS Rundown on page 1496

Creating playlists manually

When a MOS-compatible NCS is not available, you can manually create rundowns and playlists.

After creating playlists and using placeholders to link to clips, you can cue and play the clips for broadcast.



A typical newsroom workflow using GV STRATUS Rundown to create playlists is:

1. The news producer creates a rundown.
2. The news editor creates sequences for assignments using Storyboard Editor tool in GV STRATUS.
3. The news producer uses the GV STRATUS Rundown Assignment List Manager to:
   - Create placeholders for clips
   - Assign placeholders to editors
4. The news editor uses the GV STRATUS Rundown Assignment List Manager to:
   - Create placeholders for clips
   - Reassign placeholders to other editors
5. Control room personnel use the main GV STRATUS Rundown application to:
   - Create a new playlist and rundown using the scripts from the producer and the clip database
   - Assign clips to specific channels for playback
   - Rearrange, insert, or delete clips prior to broadcast if necessary
   - Play back clips during the news broadcast

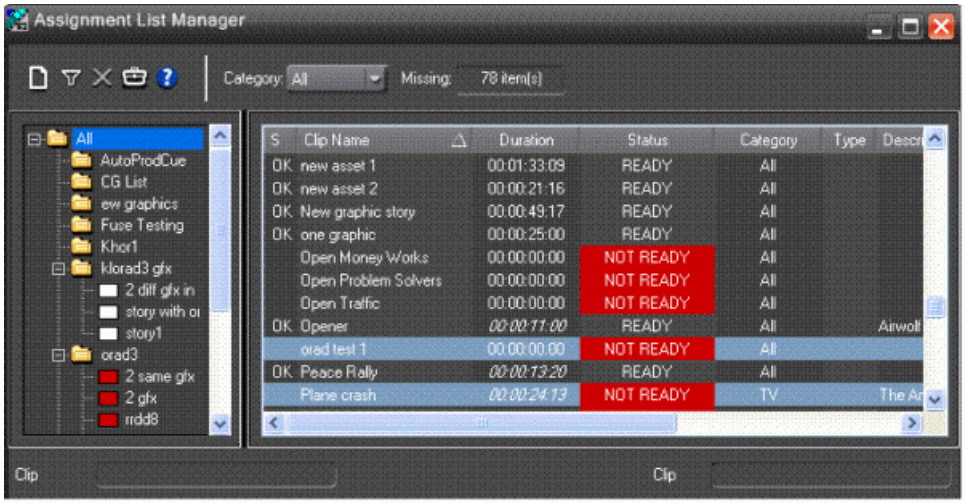
Related Topics

Using GV STRATUS Rundown on page 1496

Overview of the Assignment List Manager

Producers (or other station personnel) use the standalone Assignment List Manager to determine how many clips are missing for a given news show. Editors use the embedded Assignment List Manager to receive assignments from the producer. Both forms of the Assignment List Manager are used to create additional placeholders for clips and to reassign placeholders to other categories.

The standalone Assignment List Manager runs on any computer on the network—an icon in the task bar flashes red when items in the selected category or rundown are missing.

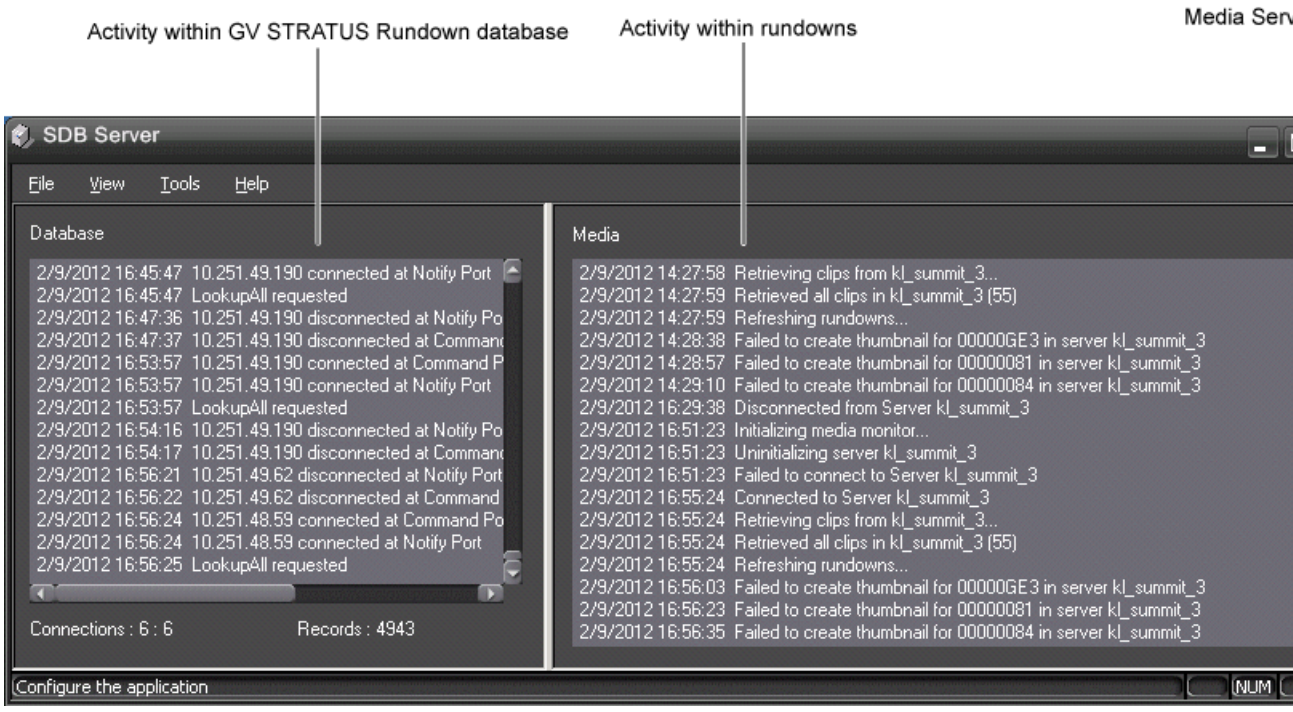


Overview of the Simple Database (SDB) Server

The SDB Server runs in the background to keep clip status current.

When the status of a clip changes, the SDB Server updates available status and clip duration in the database, which in turn updates the GV STRATUS Rundown application. When a clip is associated with a placeholder, the SDB Server updates the number of missing items in the Assignment List Manager, Assignment List Plug-in, and Assignment List tool in the GV STRATUS application.

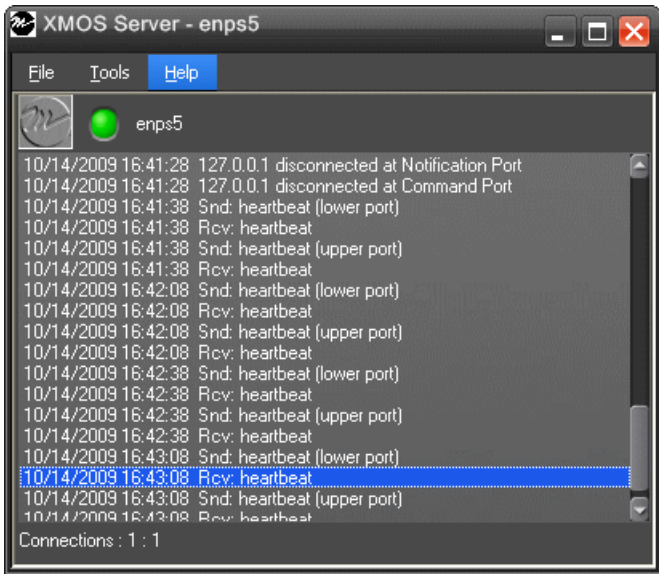
The SDB Server runs on the same computer as the XMOS Server, and optionally on a second system as a hot standby backup database.



Overview of the XMOS Server

The XMOS Server displays the communication between the Newsroom Computer System and GV STRATUS Rundown.

It runs on the same computer as the primary SDB Server.



Installing GV STRATUS Rundown hardware

Hardware installation checklist

Use items in this checklist as appropriate for the optional equipment you are installing for your GV STRATUS Rundown.

	Task	Comment
☐	Connect GPI inputs and outputs depending on your device type	GPI inputs and outputs can be connected through PCI board or ethernet
☐	Connect the RDU 1510 Under Monitor Display	
☐	Install X-keys Jog/Shuttle Controller	
☐	Next: Network setup and installation checklist	

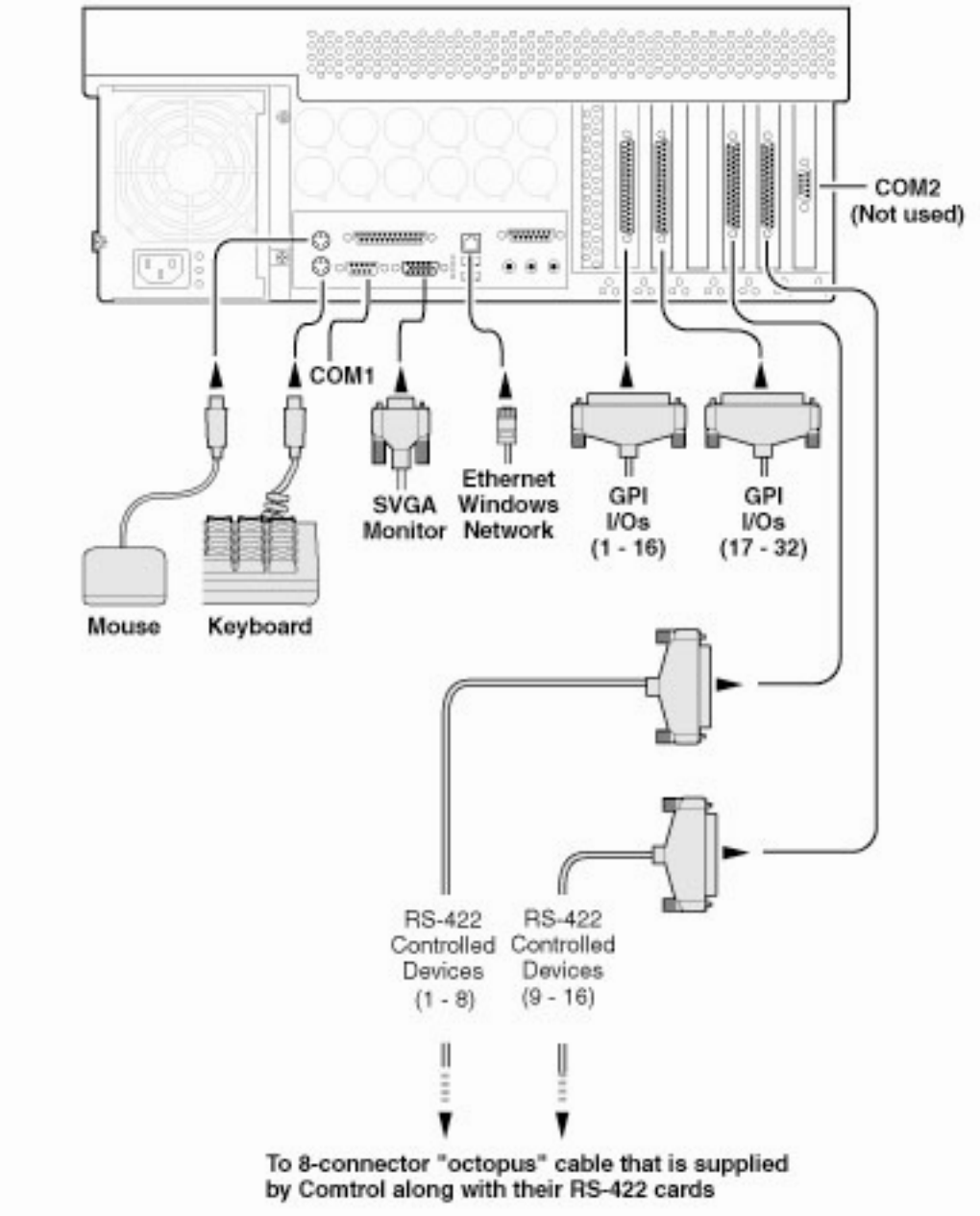
Installing GV STRATUS Rundown Hardware

The GV STRATUS Rundown system which runs on a standard PC, offers coordinated news playback from the K2 Media Server, K2 Summit Production Client and the GV I/O Live Ingest and Playback Server. The GV STRATUS Rundown Server can be supplied with all the necessary hardware and software installed. Other GV STRATUS Rundown components can be installed on any PC which meets the system requirement.

Cabling the GV STRATUS Rundown computer

GV STRATUS Rundown is typically installed on a computer with RS-422 boards and GPI boards. Proper cabling is needed for flawless use of the application.

The following illustration provides an example of a typical computer. Your particular computer might be different.



Connect the GPI inputs and outputs using the separate cables and connection blocks as instructed in the Sealevel manuals included with your system.

Related Topics

Installing GV STRATUS Rundown Hardware on page 1501

Connecting the RDU 1510 Under Monitor Display

A Remote Display Unit (RDU) can be controlled via GV STRATUS Rundown.

Use a cable that has a DB9 serial connector on one end and an RJ11 connection on the other. The DB9 end connects to the COM1 serial port on the back of the GV STRATUS Rundown, and the RJ11 end connects to the port labeled "Control" on the back of the RDU-1510. This is an RS-422/RS-232 serial communication port.

The RJ11 connector's pinout is described in the table below. Pin 1 is at the bottom of the connector. GV STRATUS Rundown can be connected to either pins 3 and 4 for RS-422 or pin 4 for RS-232. When using RS-232, pin 3 must be connected to ground. The remote display unit does not transmit data to this serial port connector.

Pin	Function
1	No connection
2	Ground
3	RS-422 non-inverted data or grounded for RS-232
4	RS-422 inverted data or RS-232 data
5	No connection
6	No connection

Related Topics

Installing GV STRATUS Rundown Hardware on page 1501

Installing the Sealevel SeaI/O-410E GPIO Controller

GV STRATUS Rundown has been qualified to work via ethernet connection with the following device:

- Sealevel SeaI/O-410E GPIO Controller

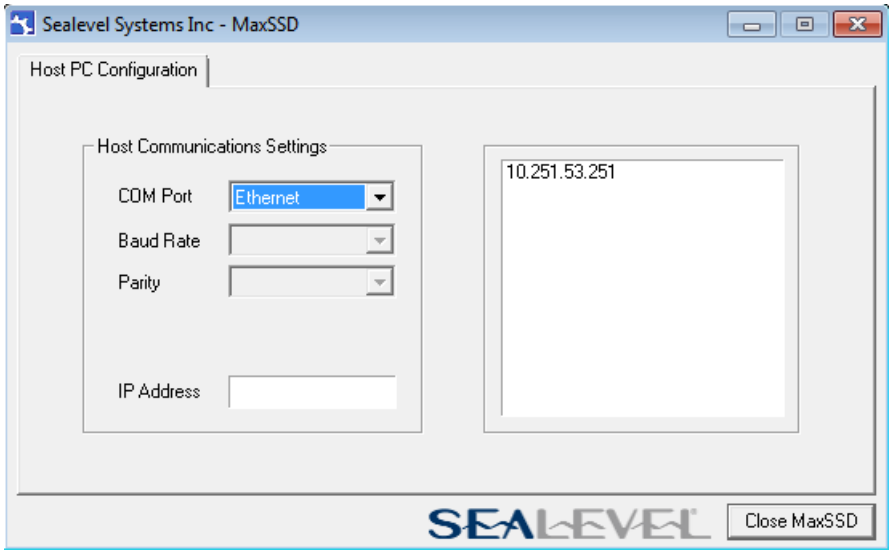
1. Download and install the Sealevel GPIO SeaI/O-410E device software from the *Sealevel download page*.

   The Software Installation window appears and the driver software installs automatically.

2. Go to **Start | Programs | Sealevel Systems - SeaMAX** and launch the **MaxSSD** application.

3. Click the COM Port drop-down list and select **Ethernet**.

   The configured IP address of the device appears on the right of the Host PC Configuration tab.

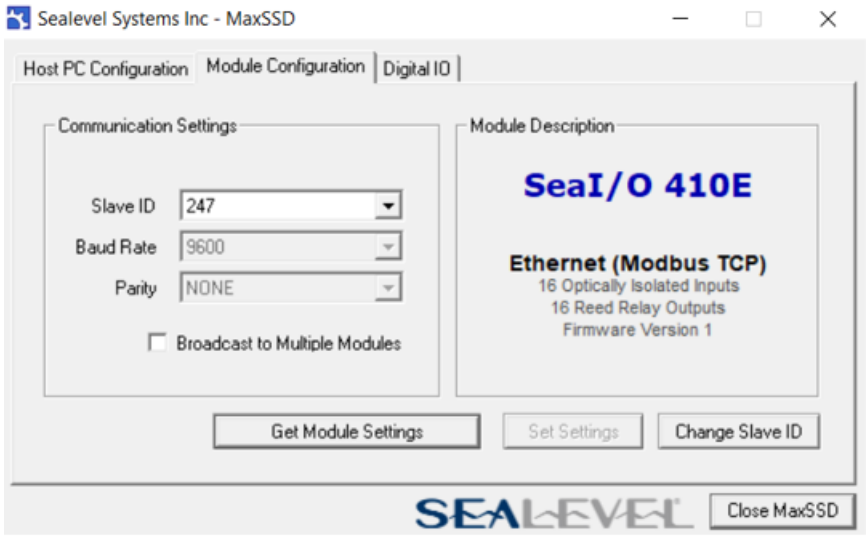


4. Select the IP address.

   The selected IP address automatically populates after a connection verification process.

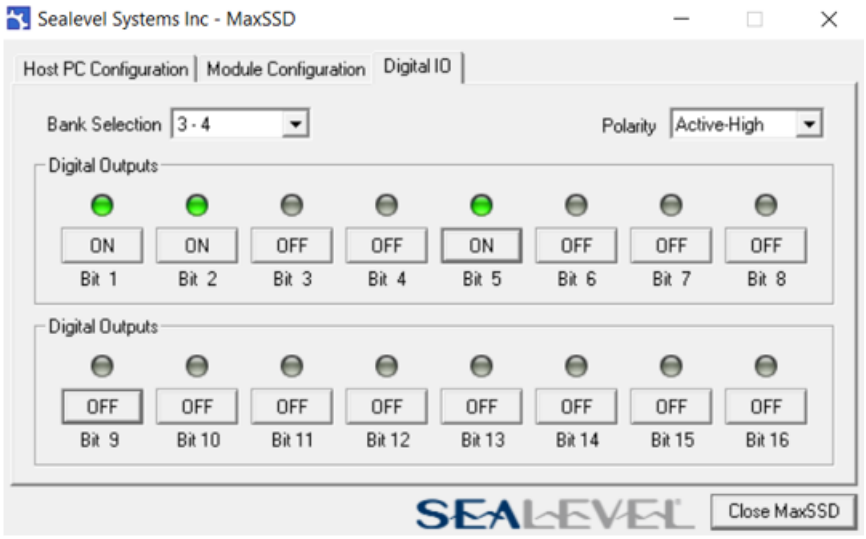
   The Module Configuration tab appears.

5. Go to the **Module Configuration** tab and select the configured Slave ID of the device.



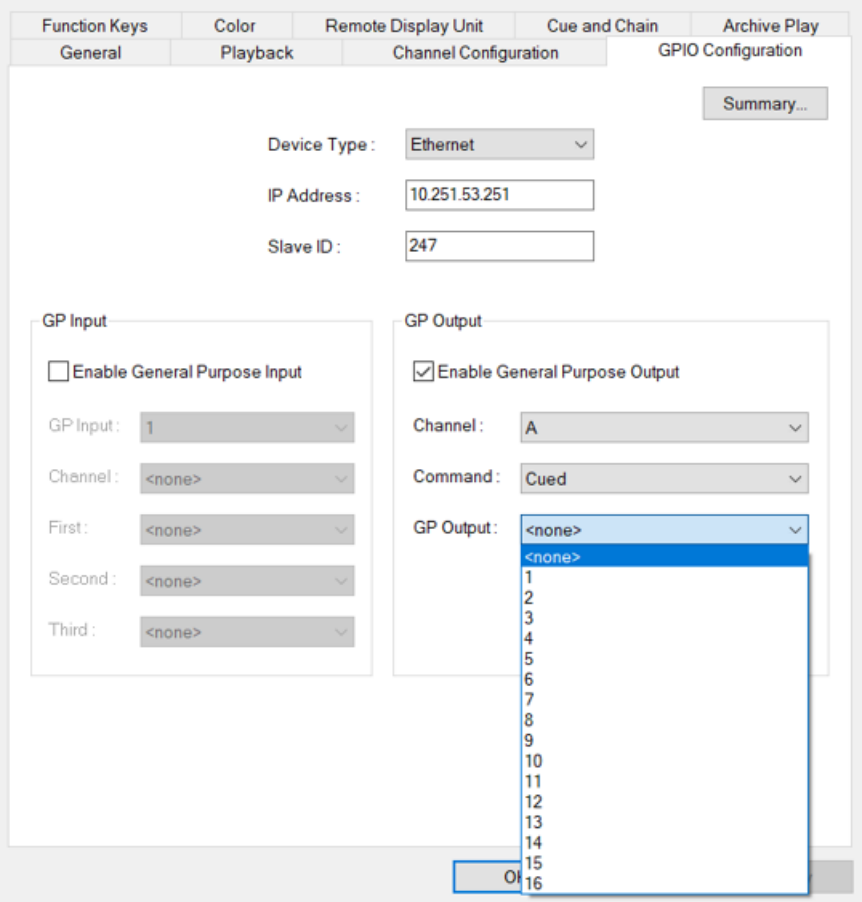
6. Click on the **Get Module Settings** button to get the device settings.

7. Go to the **Digital IO** tab and set the Bank Selection setting to **3-4** from the drop-down list.



8. Under Digital Outputs setting, set **Bit 1, Bit 2, and Bit 5** to **ON**.
9. Click the **Close MaxSSD** button to close the application.
10. Relaunch the GV STRATUS Rundown application.
11. Go to **Tools | Options** and select the **GPIO Configuration** tab.

12. Select **Ethernet** for the Device Type, set the IP Address, Slave ID, and select the **Enable General Purpose Output** check-box.



Now you can configure the GP Output and use the Sealevel SeaI/O-410E GPIO device to control the playout channel.

Related Topics

Installing GV STRATUS Rundown Hardware on page 1501

Installing the X-keys Jog/Shuttle Controller

Once you have installed GV STRATUS Rundown, you can connect and install the optional X-keys Jog/Shuttle controller.

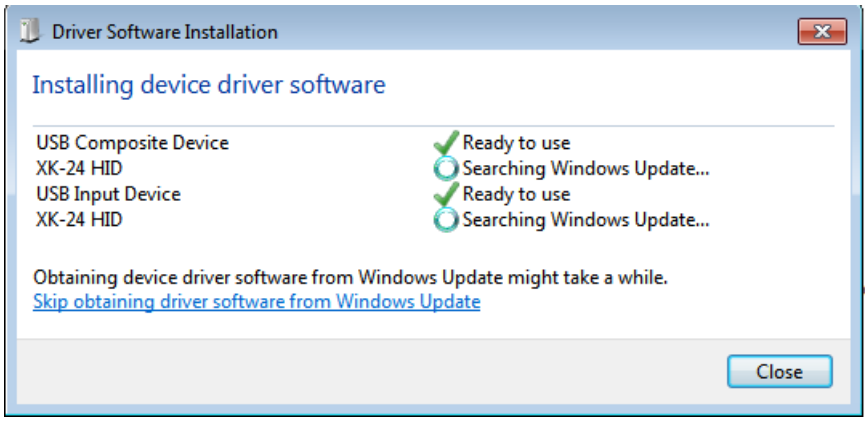
GV STRATUS Rundown has been qualified to work with these X-keys Jog/Shuttle controllers:

- XK-24-USB Keypad Controller

- XK-68-Jog/Shuttle USB Controller

1. Plug in the X-keys Controller to the USB port on GV STRATUS Rundown machine.

   The **Driver Software Installation** window appears and the driver software installs automatically.



2. Wait for all status to change to **Ready to use** and green check marks appear for all items, then click **Close**.
3. Start GV STRATUS Rundown.
4. In the GV STRATUS Rundown Tools menu, select **Options**.
5. Select the **Function Keys** tab.
6. Verify the "Enable X-keys" box is checked and click **Configure**.

Now you can configure and use the X-keys Jog/Shuttle controller.

You can customize the X-keys to suit your needs.

Related Topics

Installing GV STRATUS Rundown Hardware on page 1501
Configuring the X-Keys Controller on page 1518

Configuring GV STRATUS Rundown

Configuring GV STRATUS Rundown

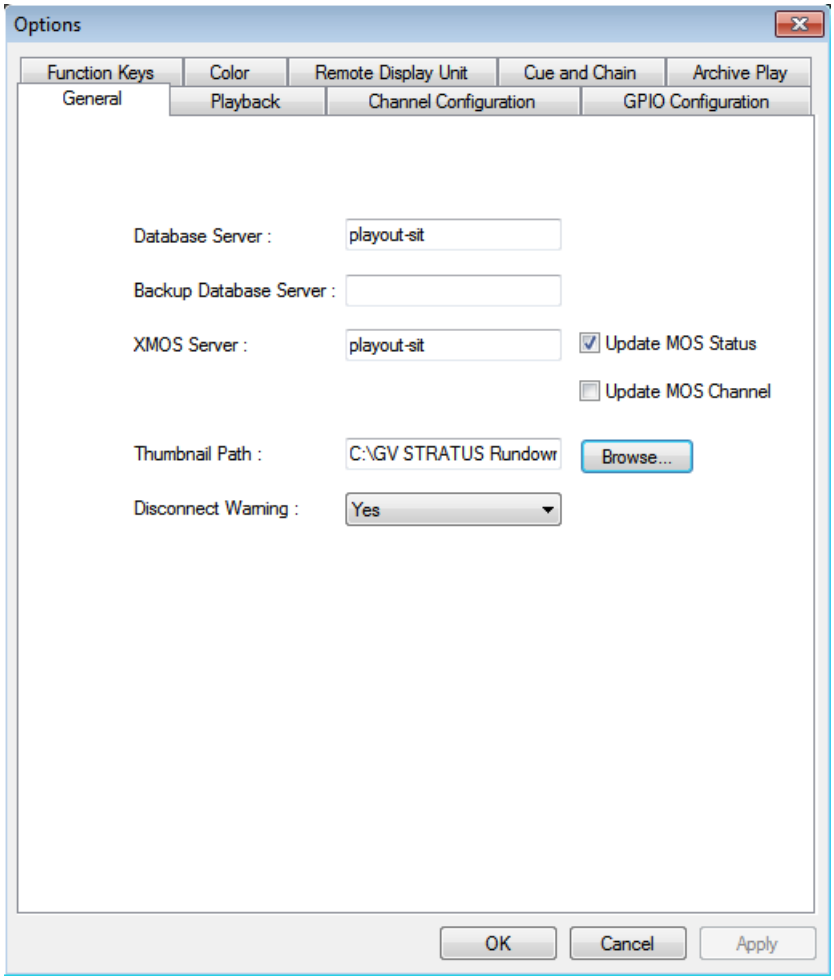
GV STRATUS Rundown has many options that let you define how your system is set up.

If your system is already pre-configured at the factory, you might want to adjust some options based on how you use GV STRATUS Rundown.

Configuring the GV STRATUS Rundown application

Each setting of the GV STRATUS Rundown application is discussed in case you need to reconfigure your system.

1. Choose **Tools | Options**.



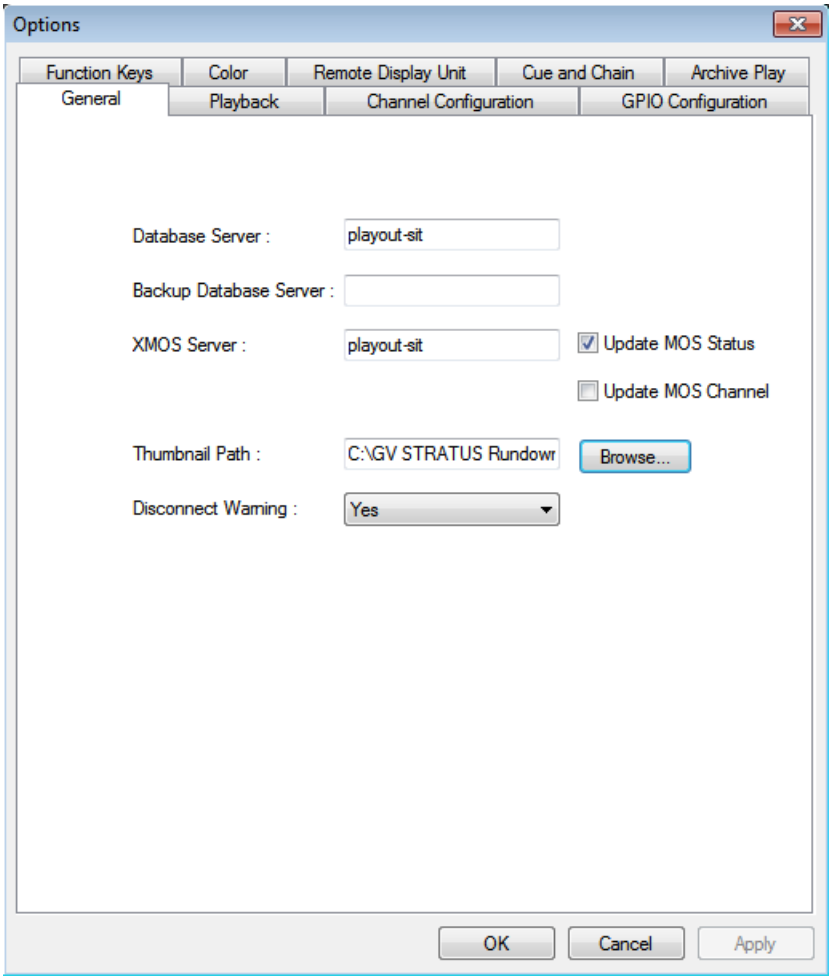
The Options window appears.

2. Go through each tab in the Options window and configure GV STRATUS Rundown using the description for each tab.
3. Click **Apply** to apply your settings to each tab.
4. Click **OK** when you are done setting options.

Related Topics

Configuring GV STRATUS Rundown on page 1507

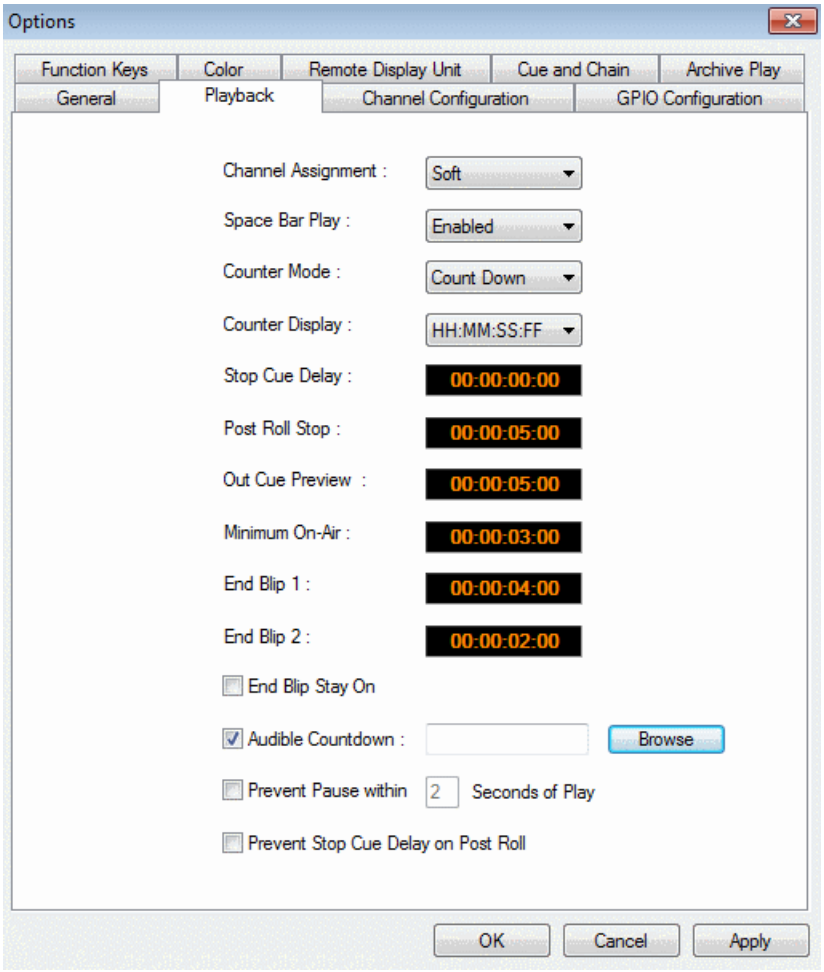
Setting General options



Setting	Options	Description
Database Server		Enter the name of the computer hosting the primary SDB Server.
Backup Database Server		Enter the name of the computer hosting the hot-standby SDB Server.
XMOS Server		Enter the name of the computer hosting the XMOS Server.
Update MOS Status		By default, the Update MOS Status checkbox is selected. If you have two or more GV STRATUS Rundown systems running, deselect the box on the **Tools I Options** of the backup system. This is to avoid MOS status conflicts when the same rundown is loaded by more than one GV STRATUS Rundown system.
Update MOS Channel		When the checkbox is selected, it enables channel assignments in GV STRATUS Rundown to be updated to the Newsroom Computer System.

Setting	Options	Description
Thumbnail Path		Enter the full path to the shared thumbnail directory on the computer where thumbnails are stored, in the format `\\server\foldername`; e.g., if you have a shared folder named “thumbnails” on your playout system named “Playout1”, the path would be `\\Playout1\thumbnails`. This path needs to match the path set in GV STRATUS Control Panel — Applications | Rundown | SDB | SDB Thumbnail Path.
Disconnect Warning	Yes; No	Select **Yes** to be alerted before GV STRATUS Rundown disconnects synchronization with the Newsroom Computer System.

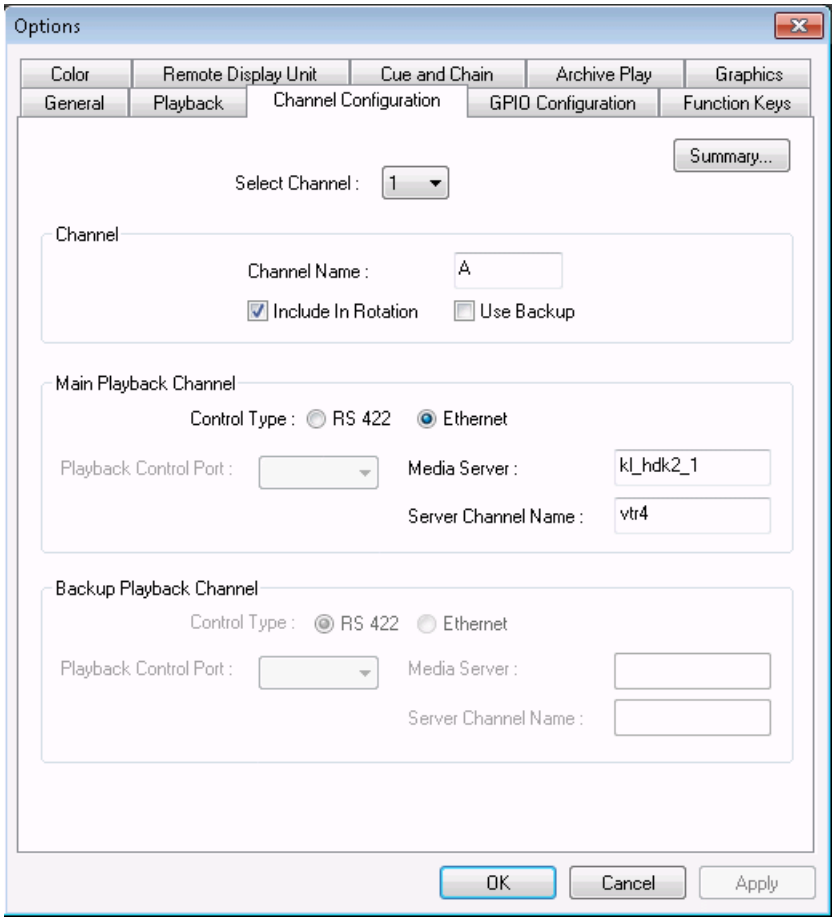
Setting Playback options



Setting	Option	Description
Channel Assignment	Soft	When a rundown is loaded, GV STRATUS Rundown does not assign channels to stories; clips will be cued to the first available channel.
	Hard	When a rundown is loaded, GV STRATUS Rundown assigns channels to all stories without a current channel assignment and maintains that assignment regardless of the available channels.
Space Bar Play	Enabled	Enables or disables use of the space bar to play the next cued clip.
	Disabled	
Counter Mode	Count Down	Sets the clip duration counter to count time down from the clip duration to zero, or from zero up to the clip duration.
	Count Up	
Counter Display	HH:MM:SS:FF	Determines how the counter is displayed.
	MM:SS	
Stop Cue Delay		Determines the amount of time to freeze a clip on its last frame before cueing the next clip on that channel.
Post Roll Stop		When a channel is playing and Play Next is pressed, determines the amount of time that the clip continues to post roll before cueing the next clip to that channel.
Out Cue Preview		Previews the last few seconds of the clip and immediately recues. (The number of seconds that previews is determined by your studio's needs.)
Minimum On-Air		Determines the minimum time that the On-Air GPI trigger must be on before releasing it will send the clip into post-roll and cue the next clip.
End Blip 1 and 2		Determines the amount of time prior to the end of a clip to display an audio/visual warning.
End Blip Stay On		Determines whether the End Blip visual signal remains on once triggered, or just flashes momentarily.
Audible Countdown		Sets an audible countdown before the start of a playback. Only .wav files are supported for the audible countdown setting.
Prevent Pause within X Seconds of Play		Determines whether stop commands (through GPI input or mouse click) can occur within a determined period of time after the playing of a clip begins.

Setting	Option	Description
Prevent Stop Cue Delay on Post Roll		Determines whether there should be a Stop Cue Delay duration when a clip goes into post roll mode by a play next command or tally off-air.

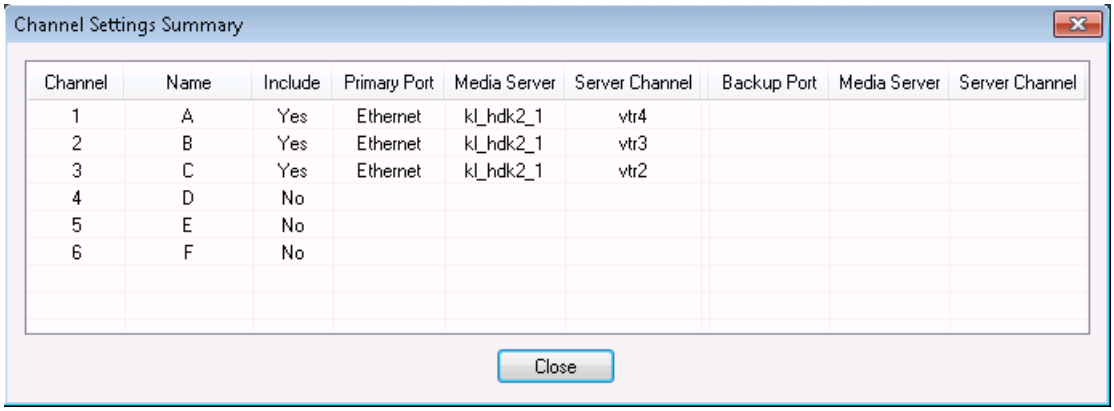
Setting channel configuration



Setting		Options	Description
Select Channel		1-6	Select the channel to configure.
Channel	Channel Name		Enter a name for the channel.
	Include in Rotation	On; Off	Check Include in Rotation to include this channel when automatically assigning channels.
	Use Backup	On; Off	Check Use Backup if you are using a second media server for mirrored playback.

Setting		Options	Description
Main Playback Channel/Backup Playback Channel	Control Type	RS 422; Ethernet	Select the type of channel connection.
	Playback Control Port		Select the primary port for this channel.
	Media Server		Enter the name of the K2 Media Client, K2 Summit Production Client or M-Series.
	Server Channel Name		Enter the name of the channel you are using for this playback channel. Use the naming convention VTR1, VTR2, etc., for the channel name.

- Click the Summary... button to view the complete list of channel information after the configuration.



This symbol indicates that a GV STRATUS Rundown channel is no longer connected to its corresponding channel on the media server. Check the following possible problems; as you cannot remotely control the media server while this symbol is present:

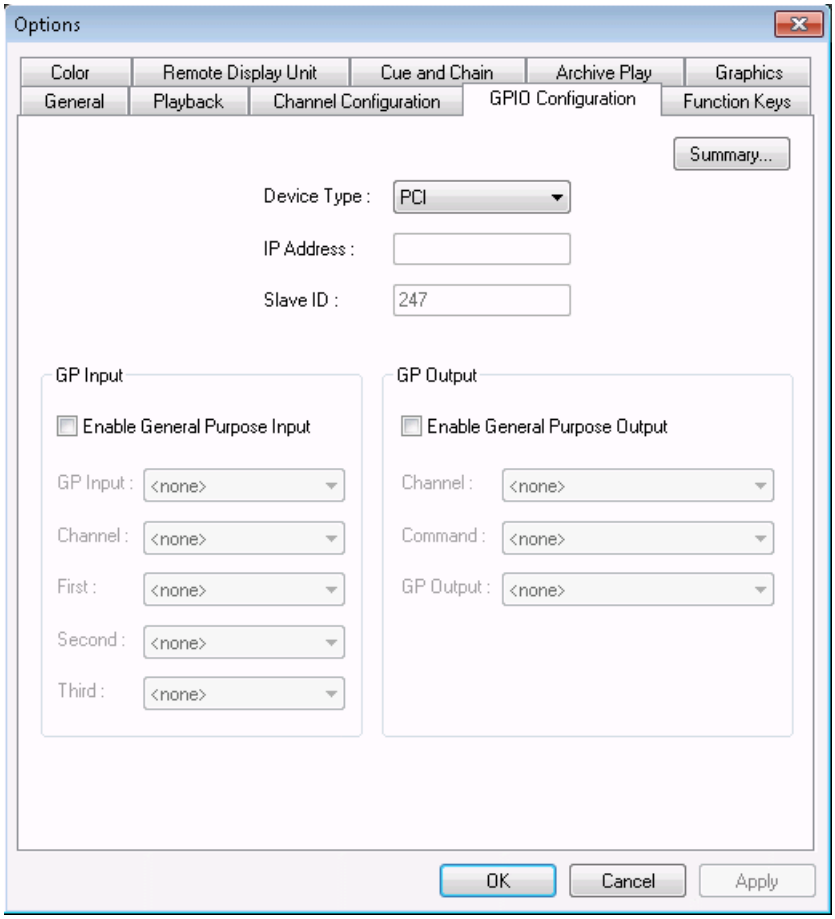
- Playout channels on the media server are not set to use the remote AMP protocol.
- If you are using RS-422, there is no physical serial/network cable connection between GV STRATUS Rundown and the media server used for playout.
- If you are using Ethernet channel connections, the entries for media server or Server Channel Name are not set correctly in the GV STRATUS Rundown Channel Configuration.
- COM ports are set incorrectly in the GV STRATUS Rundown Channel Configuration.

Related Topics

About Playout channels on page 1568

Configuring General Purpose Input and Output

General Purpose Input Output (GPIO) configuration allows you to connect a switcher or other control device to the GV STRATUS Rundown system and use it to control the GV STRATUS Rundown software.



GV STRATUS Rundown supports both PCI and ethernet based GPIO depending on your choice of GPIO device. You can select either PCI or Ethernet from the Device Type drop-down list.

For ethernet based GPIO connection, you then need to enter the IP address and slave ID of your GPIO device.

- Check the Enable General Purpose Input box to start configuring your GP Input.

  To assign the function of a GP input, select the GP Input number, the channel it affects, and the function you want the GPI to perform.

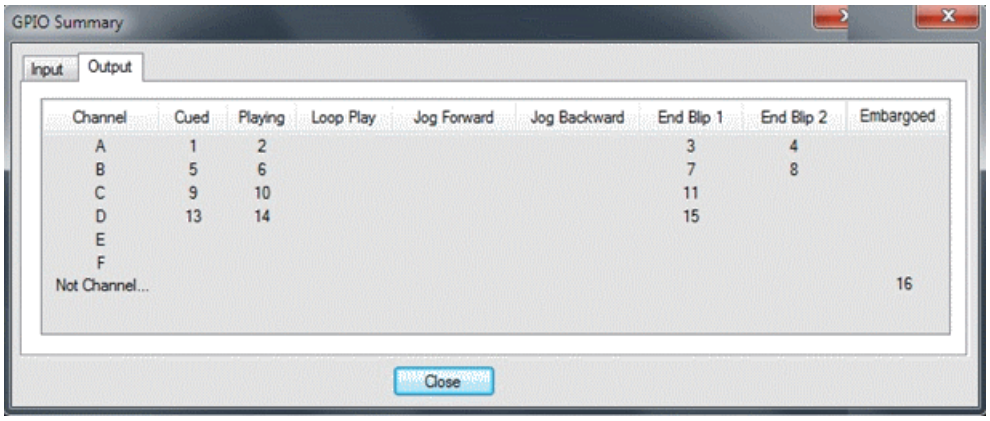
Setting	Options	Description
Enable GP Input	On (checked); Off (unchecked)	Check Enable General Purpose Input to control the GV STRATUS Rundown software via GP input.
GP Input	1 through 16 or 32	Select the GP input you are configuring.
Channel	<none>; Channel A - F; Not Channel Specific	Select the channel that this GP Input trigger will affect.
GP Input Function for Channel A-F labels: First; Second; Third	Select a function for each GP Input. Each input usually has only one function, though it can perform up to three functions.	
	<none>	The GP Input has no assigned function.
	Play/Stop	Plays or stops the current clip.
	Play	Plays the current clip.
	Stop	Stops playing the current clip.
	Recue	Recues the current clip.
	Cue Previous	Cues the previous clip in the playlist.
	Cue Next	Cues the next clip in the playlist.
	On-Air	Only used with the First GP Input function. Sends the specified channel an On-Air signal. When GV STRATUS Rundown detects a signal, the channel window becomes red to indicate the channel is playing to air. When the On-Air GP Input trigger is held longer than the Minimum On-Air duration specified under Options and then released, the channel goes into post-roll and then cues the next clip.
GP Input Function for Not Channel Specific:	<none>	The GP Input has no assigned function.
	Cue All	Cues a clip into each available channel, starting with the selected clip.
	Play Next	Plays the next clip in the playlist.
	Stop All	Stops all playing channels in the playlist.
	Cursor Up	Selects the previous item in the playlist.
	Cursor Down	Selects the next item in the playlist.

- Check the Enable General Purpose Output box to start configuring your GP Output.

  To assign the function of a GP output, select the channel it affects, the command in GV STRATUS Rundown that triggers GP output and the GP output number.

Setting	Options	Description
Enable GP Output	On (checked); Off (unchecked)	Check Enable General Purpose Output to allow GV STRATUS Rundown to trigger GP outputs.
Channel	<none>; Channel A - F; Not Channel Specific	Select the channel that will trigger the General Purpose output. If you select the **Not Channel Specific** option, the only available option in the **Command** dropdown is **Embargoed**.
Command	Cued	The output is set when the channel is cued; reset when the channel is playing or if the clip is ejected.
	Playing	The output is set when the channel is playing; reset when the channel is stopped or the clip is ejected.
	Loop Play	The output is set when the channel is in loop play mode; reset if not in loop play mode.
	Jog Forward	The output is set when the Jog Forward or Jog Backward buttons are pressed; reset when the Play, Stop, or Eject buttons are pressed, or when the channel is re-cued.
	Jog Backward	
	End Blip 1 (Hold till End of Clip)	The output is set when the playing channel reaches End Blip 1; reset when the channel is stopped or the clip is ejected.
	End Blip 2 (Hold till End of Clip)	The output is set when the playing channel reaches End Blip 2; reset when the channel is stopped or the clip is ejected.
	Embargoed	The output is set when the clip is played; reset when the clip is stopped or if the clip is ejected. ***NOTE: This option is only available when the Channel is set to "Not Channel Specific".***
GP Output	<none>; 1-16 or 1-32 (depending on your configuration)	Select the GP output you want to activate. ***NOTE: If you selected Ethernet GPIO device type but the GP Output list shows <none>, you must install the driver of Sealevel GPIO SeaI/O-410E ethernet device.***

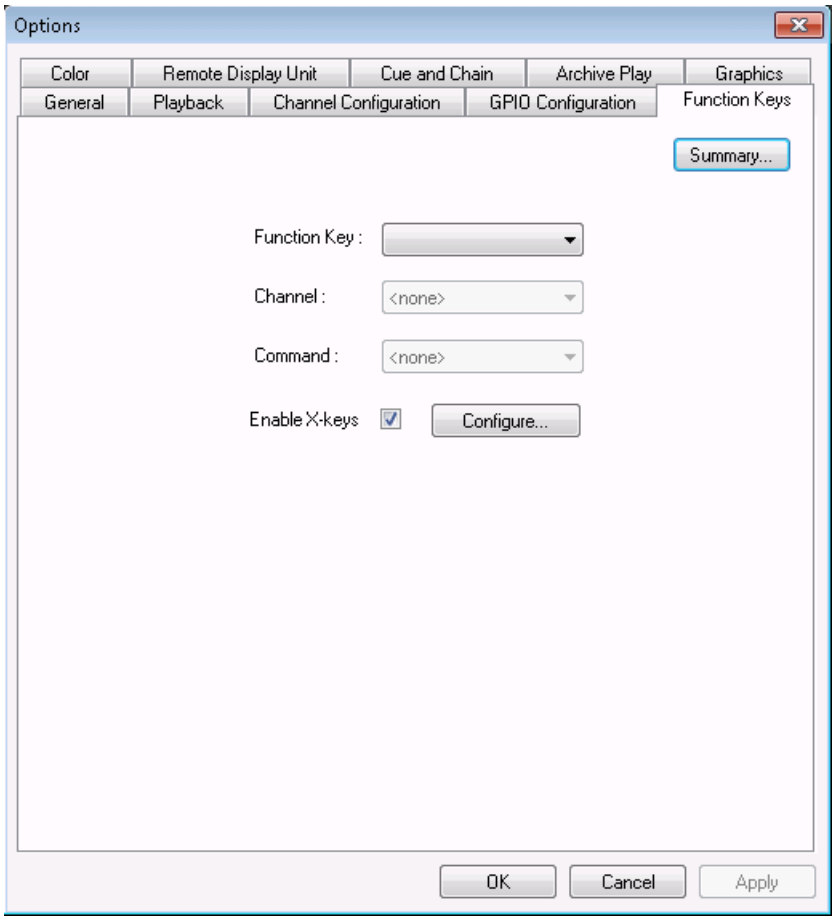
After configuring your GP inputs and outputs, you can see the overview of your current GPIO setting by clicking the Summary... button.



Related Topics

Installing the Sealevel SeaI/O-410E GPIO Controller on page 1503

Defining Function Keys



The computer function keys (F1 - F12) provide shortcuts to some GV STRATUS Rundown commands, and are pre-configured by default to control the following functions for channels 1

through 3. You can click the Summary... button to view the summary of those pre-configured function key assignments.

GV STRATUS Rundown function	Function Key		
	Channel 1	Channel 2	Channel 3
Play/Stop Cued Clip	F1	F5	F9
Recue Current Clip	F2	F6	F10
Cue Previous Clip	F3	F7	F11
Cue Next Clip	F4	F8	F12

To reassign a function; select the Function Key number, the channel it affects, and the command you want the function key to perform.

Setting	Option	Description
Function Key	F1 through F12	Select the function key you want to set.
Channel	<none>	Select the channel on which the function key will operate.
	Channel 1-6	
Command	<none>	Select the command the function key will perform on the specified channel.
	Play/Stop	
	Recue	
	Cue Previous	
	Cue Next	
	Enable X-keys	On (checked)
Off (unchecked)		Select the Enable X-keys check box to allow GV STRATUS Rundown to use an X-keys Jog/Shuttle controller. Click Configure to define the function of each X-key.

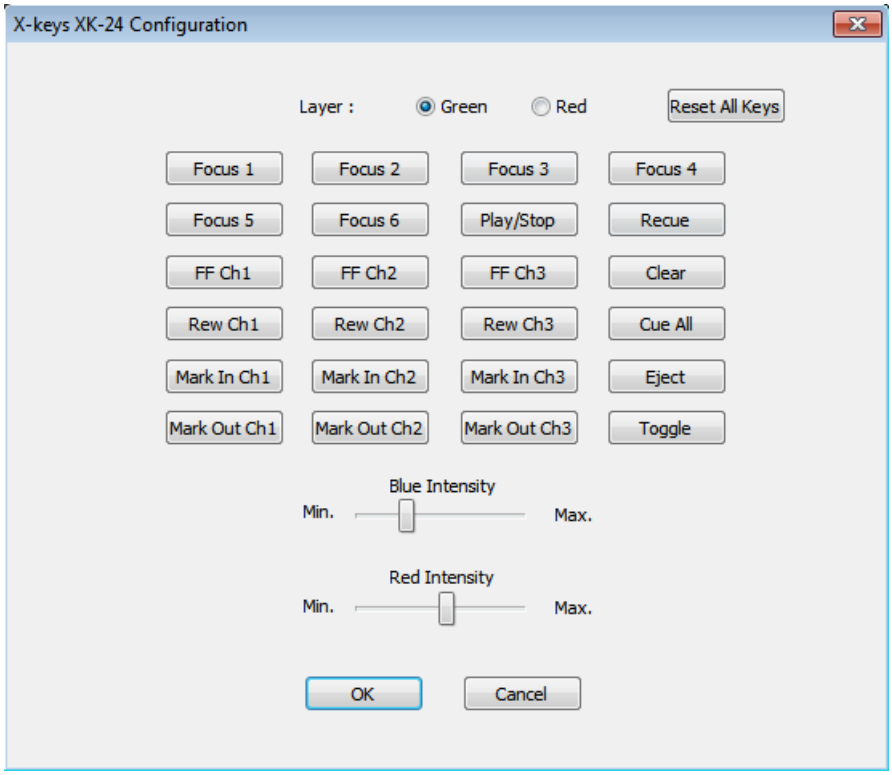
Configuring the X-Keys Controller

Optionally, GV STRATUS Rundown can be used with the X-keys Jog/Shuttle controller.

You can change current commands or add new commands to the X-keys in the GV STRATUS Rundown configuration settings.

1. Check **Enable X-keys** on the Function Keys tab and click **Configure**.

   The X-keys Configuration dialog appears.



2. Click on the key that you want to configure or modify.

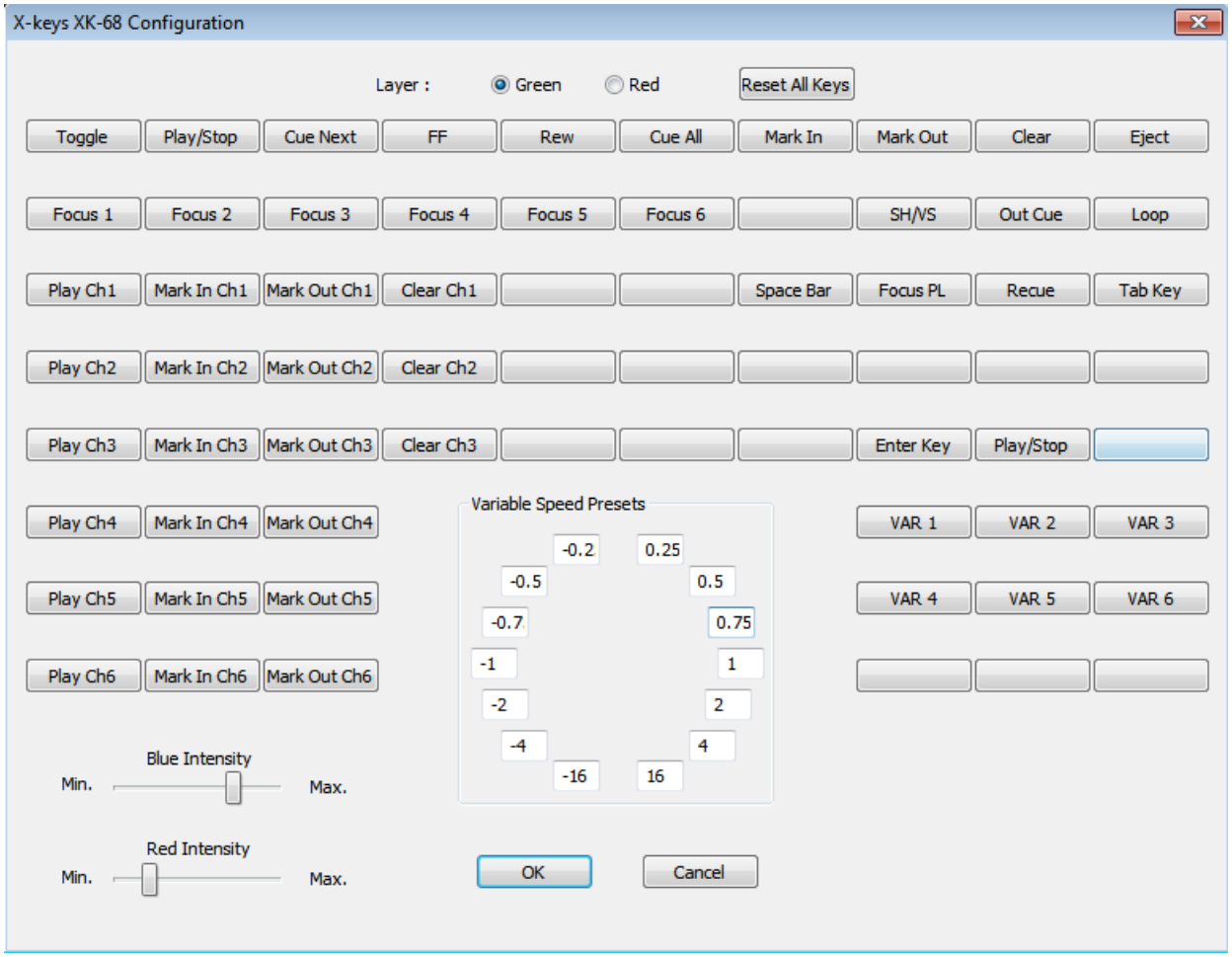
   A drop-down list displays the available commands.

3. Select a command to apply to this key.
4. Repeat steps 2 and 3 to configure additional keys.
5. To configure the back light intensity of the X-keys controller, drag the pointer on the **Blue Intensity** and **Red Intensity** scrub bars towards the minimum or maximum value.

   The back light of the X-keys controller illuminates according to selected intensity on those scrub bars. To differentiate between the Green and Red layer, you can set a different back light color to each layer.

6. Once you have finished the configuration, click **OK**.

   In addition to keys, some controllers include the jog/shuttle knob. The jog control, the center disk of the knob, allows you to make precise frame by frame selections for editing that can be configured in the **Variable Speed Presets** section in the configuration dialog.



   The outer rim can be used in Shuttle or Varispeed mode. The SH/VS key toggles between the two modes.

   Shuttle and Varispeed modes both allow you to play clips at various preset fast forward, rewind, and slow-motion speeds. In Shuttle mode, when you release the knob the clip stops. In Varispeed mode, when you release the knob the clip keeps playing until you press the Stop key.

Related Topics

Installing the X-keys Jog/Shuttle Controller on page 1506

Using the X-keys Jog/Shuttle Controller

The X-keys controller allows you to simplify your workflow. For example, you can use the default layout to easily navigate between different channels or between the Playlist and Clip Browser windows.

Any commands you send using the X-keys controller apply to the currently active channel or window, which is considered to have **focus**. When a channel has focus, you can perform tasks such as navigating through a clip or trimming a clip. When a window has focus, you can scroll through the clips or the playlist. Always bear in mind that you need to give focus to a channel or window before you can apply the X-keys controller commands to it.

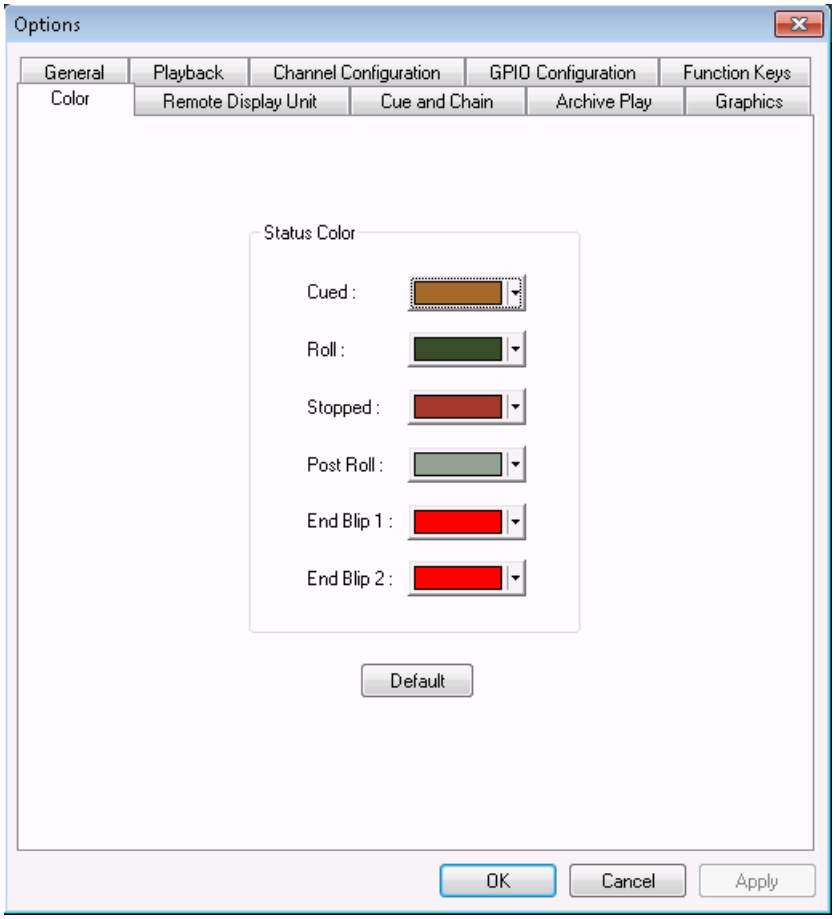
The following table describes the pre-configured keys on the X-keys Jog/Shuttle controller.

Setting	Description
Enable X-keys	Enables or disables the X-keys Jog/Shuttle controller.
Layer	Indicates whether you are configuring the Red or Green layer.
Reset All Keys	Resets all the keys on the particular layer that you are configuring. Reset All Keys does not affect keys that shift between the layers, i.e. the Toggle, Red, and Green keys.
Toggle	While you are using the X-keys controller, Toggle switches between the Red and Green layers.
Focus PL	Gives focus to the main GV STRATUS Rundown Playlist window, that is, makes the Playlist window active. X-keys commands such as scrolling will apply to the window that has focus.
Focus CB	Gives focus to the Clip Browser window, if open. X-keys commands such as scrolling will apply to the window that has focus.
Scr Up , Scr Down	When the focus is on the Clip Browser window, you can press the Scroll Up or the Scroll Down button to select a clip in the Clip Browser. When the focus is on the main Playlist window, you can press the Scroll Up or the Scroll Down button to select a clip in the Rundown.
Focus 1-6	Gives focus to the specified channel. X-keys commands such as those related to playing, shuttling, or trimming a clip in a channel will apply to the channel that currently has focus.
Focus Next	Gives focus to the next channel. All X-keys commands will apply to the channel that currently has focus.
10 Back	Jogs the clip backward 10 frames.
10 Fwd	Jogs the clip forward 10 frames.
1 Back	Jogs the clip backward 1 frame.
1 Fwd	Jogs the clip forward 1 frame.
Rew	When the focus is on a channel, you can press the Rew button to rewind the clip in that channel.
FF	When the focus is on a channel, you can press the FF button to fast forward through the clip in that channel.
Tab Key	In message dialog boxes, functions in the same manner as the Tab key on a computer keyboard.
Enter Key	In message dialog boxes, functions in the same manner as the Enter key on the computer keyboard.
SH/VS	Toggles between Shuttle and Varispeed modes.

Setting	Description
Mark In	Marks a new In point for a clip. After trimming, the clip must be recued to apply the new Mark In.
Mark Out	Marks a new Out point for a clip. After trimming, the clip must be recued to apply the new Mark Out.
Clear	Clears the trim marks of a clip.
Out Cue	When a channel has focus, you can use the Out Cue key to activate Out Cue Preview for that channel. This allows you to preview the end of a clip by playing the last few seconds, followed by a recue to the beginning. The duration of the preview can be configured by going to the Tools menu and selecting Options, then changing the Out Cue Preview field on the Playback tab.
VAR -1; VAR 1; VAR -3; VAR 3; VAR -5; VAR 5; VAR -7; VAR 7	These seven speeds correspond to whatever values are typed into the fields in the Variable Speed Presets section of the X-keys Configuration dialog box. When you press a VAR key, the clip plays at the preset speed for that key until you press the Stop key. You can move the wheel to the left to access the negative (backward) speeds, move the wheel to the right to access the positive (forward) speeds.
Recue	Recues the clip.
Play/Stop	Plays or stops the clip.
Variable speed presets	Preset speeds that you can access by using the shuttle/varispeed wheel of the controller or by using the VAR keys. You can modify these to your own settings.

Defining status colors

GV STRATUS Rundown uses color to show clip status.



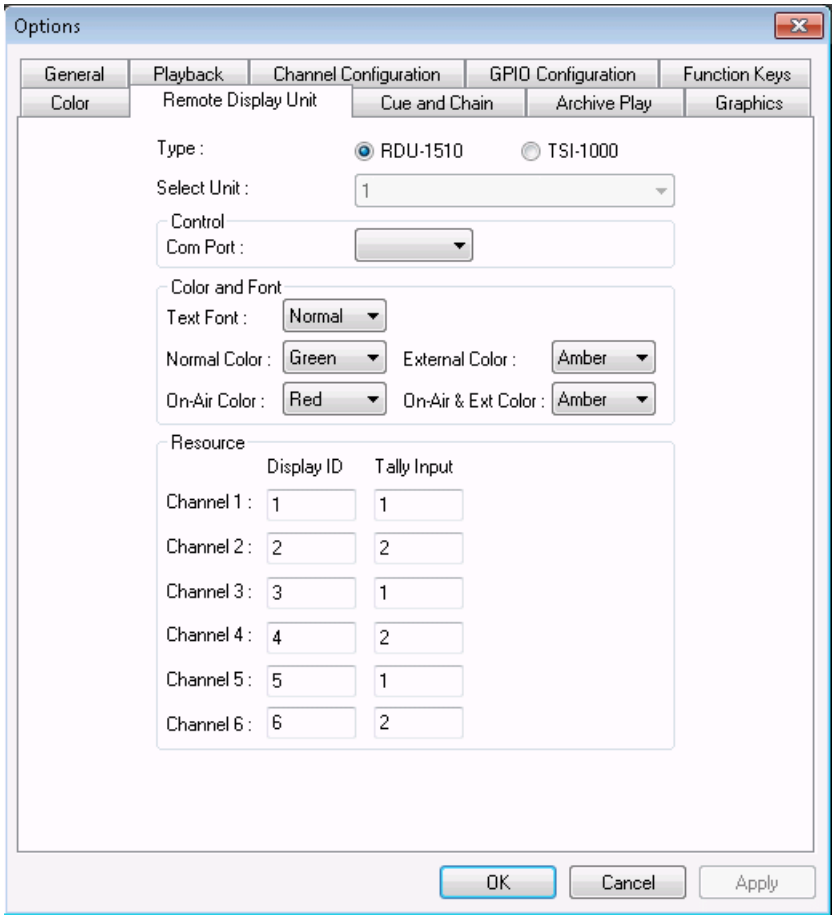
To change a color, open the drop-down menu for the color you want to change and select a new color.

Setting	Status Description
Cued	The color to indicate that a clip is cued.
Roll	The color to indicate that a clip is playing.
Stopped	The color to indicate that a clip is stopped during play.
Post Roll	The color to indicate that a clip is in post roll.
End Blip 1	The color to indicate the first audio/visual warning.
End Blip 2	The color to indicate the second audio/visual warning.
Default	Resets those colors to the default system colors.

Configuring the Remote Display Unit (RDU)

A Remote Display Unit (RDU) lets you see the clips playing on each channel and the status of each clip.

The RDU usually resides in the control room so that operators can monitor playback status during a broadcast. There are two different RDUs you can use with GV STRATUS Rundown: RDU 1510 or TSI 1000.

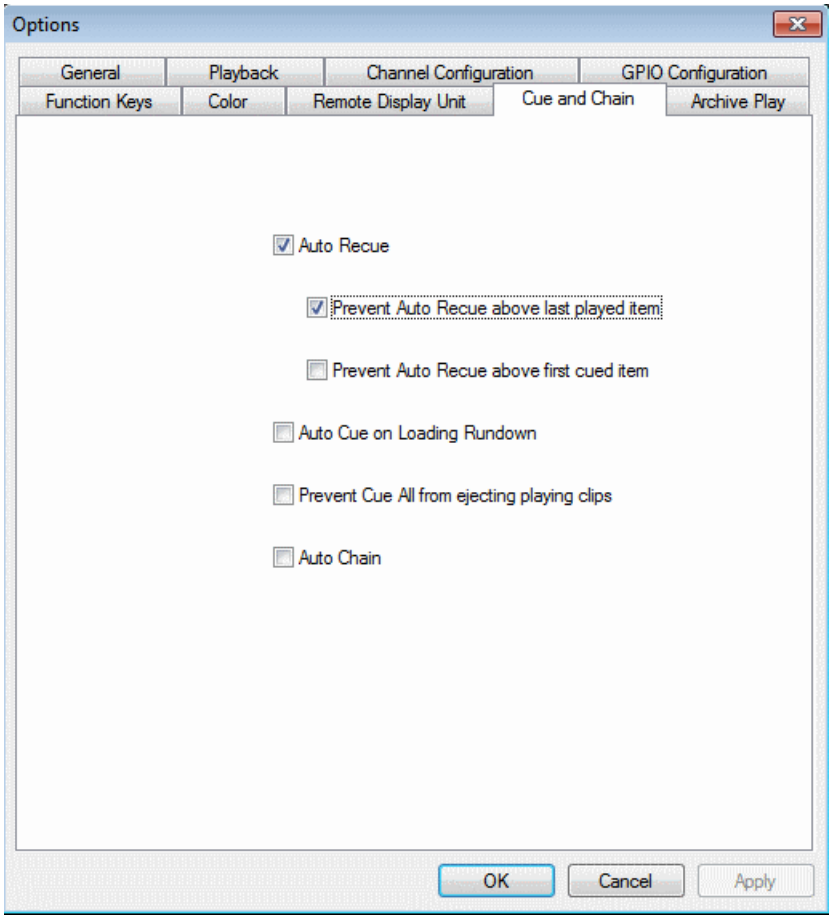


Setting		Options	Description
Type of Display Unit		RDU-1510; TSI-1000	Select your type of Remote Display Unit.
Select Unit		1; 2; 3	For the TSI, select the unit that you want to use. You can connect the GV STRATUS Rundown system to up to three TSI Remote Display Units. The default values of these units are 1,2, and 3. You can configure these to more appropriate names for your needs.
Control	Com Port; Machine Name		For the RDU 1510, select the Com Port on the GV STRATUS Rundown that the RDU is connected to (usually COM1). For the TSI 1000, enter the IP address or the host name of the TSI 1000 machine.
Color and Font	Text Font	Normal; Spaced; Thin; Small	Select the text format to display on the RDU.

Setting		Options	Description
	Normal Color	Red; Green; Amber	Select the color to display on the RDU during normal operation.
	On-Air Color	Red; Green; Amber	Select the color to display on the RDU to indicate a GPI On-Air trigger.
	External Color	Red; Green; Amber	Select the color to display on an external tally device to indicate an input trigger.
	On-Air and External Color	Red; Green; Amber	Select the color to display on the RDU to indicate that both the GPI On-Air and Tally Input are triggered.
Resource	Display ID (1-6) / Resource ID		Enter the Display ID number for each channel on the RDU. The Display ID determines the position of the clip information on the RDU.
	Tally Input (1-2) / Input ID		The Tally Input determines the state of the channel, and the color display associated with the current channel state on the RDU. Typically, these settings should be left at their default values. For more information about tally states, please see the user manual for your RDU.
	Display Size		Check the Size checkbox to display the clip name with the full number of characters allowed. If Full is checked, 19 characters can be displayed. If Full is not checked, 13 characters can be displayed. (TSI-1000 only)

Setting		Options	Description
	Duration		Check the Duration box to display the minute and seconds. (TSI-1000 only)

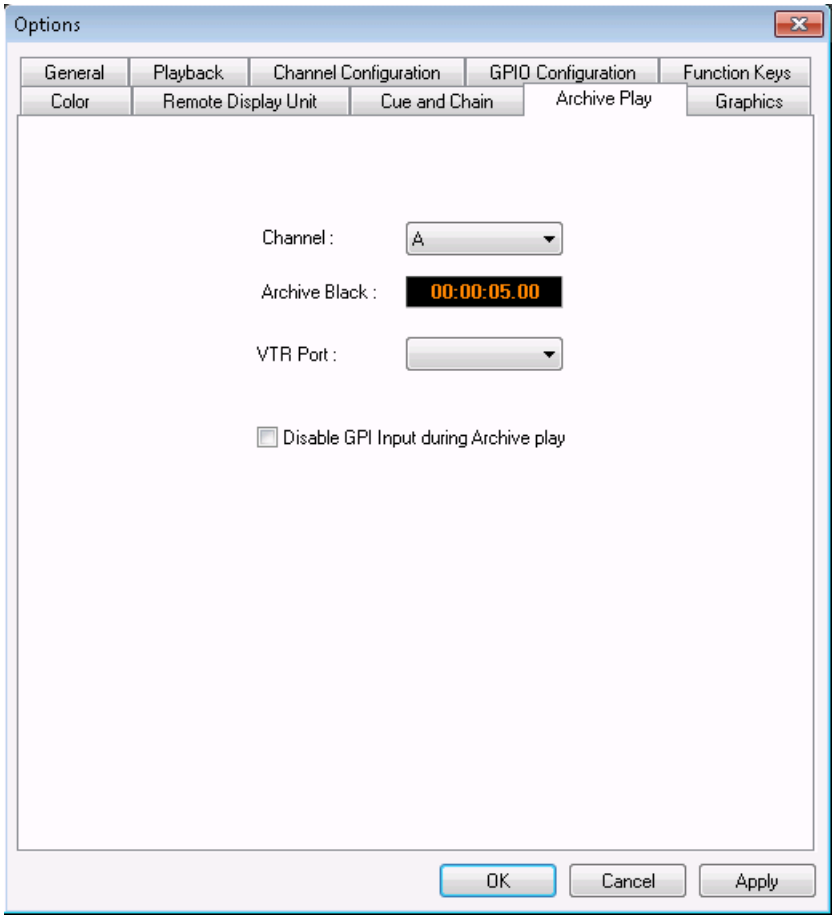
Setting Cue and Chain options



Setting	Description
Auto Recue	Check **Auto Recue** to automatically recue clips in the playlist when a clip is moved to a new position within the GV STRATUS Rundown playlist or the NCS rundown, or when the status of clips changed to Ready. ***NOTE: Only one Prevent Auto Recue option can be selected at a time after selecting the Auto Recue check box.***
Prevent Auto Recue above last played item	Check **Prevent Auto Recue above last played item** to avoid automatic recue of clips above the last played item in the playlist. However, clips above the last played item can still be cued manually by the operator.

Setting	Description
Prevent Auto Recue above first cued item	Check **Prevent Auto Recue above first cued item** to avoid automatic recue of clips above the first cued clip in the playlist. However, clips above the first cued item can still be cued manually by the operator.
Auto Cue on Loading Rundown	Check **Auto Cue on Loading Rundown** to automatically cue clips into all available channels when you open a rundown.
Prevent Cue All from ejecting playing clips	Check **Prevent Cue All from ejecting playing clips** to prevent a playing clip from being ejected when the Cue All command is issued.
Auto Chain	Check **Auto Chain** to have GV STRATUS Rundown automatically chain two or more consecutive clips in a playlist that are assigned to the same channel.

Configuring Archive Play



Setting	Options	Description
Channel	Channel A-F	Select the channel to use for Archive Play. When in Archive Play mode, clips can be cued only to this channel.
Archive Black		Specify the Archive Black duration. Archive Black is the black video that separates each archived clip from the next. The default time is 5 seconds. If it does not already exist on your media server, you must record a black clip and place it in the default media bin. The clip should be about 10 seconds long and must be named “BLACK”.
VTR Port		Select the COM port you are using to connect the VTR.
Disable GPI Input during Archive Play	On (checked); Off (unchecked)	Determines whether to disable GPI Input while archiving clips.

Configuring the Simple Database (SDB) Server

When using a Hot Standby SDB Server, you should be logged in as Administrator while making any changes to the Options settings.

NOTE: If you want to configure the GV STRATUS application with* GV STRATUS Rundown, *refer to related topics about Rundown configuration settings in the this Topic Library in order to configure the SDB Server.

The SDB Server provides you with status on all GV STRATUS Rundown playlists associated with NCS rundowns and media servers.

1. Double-click **SDB Server** button

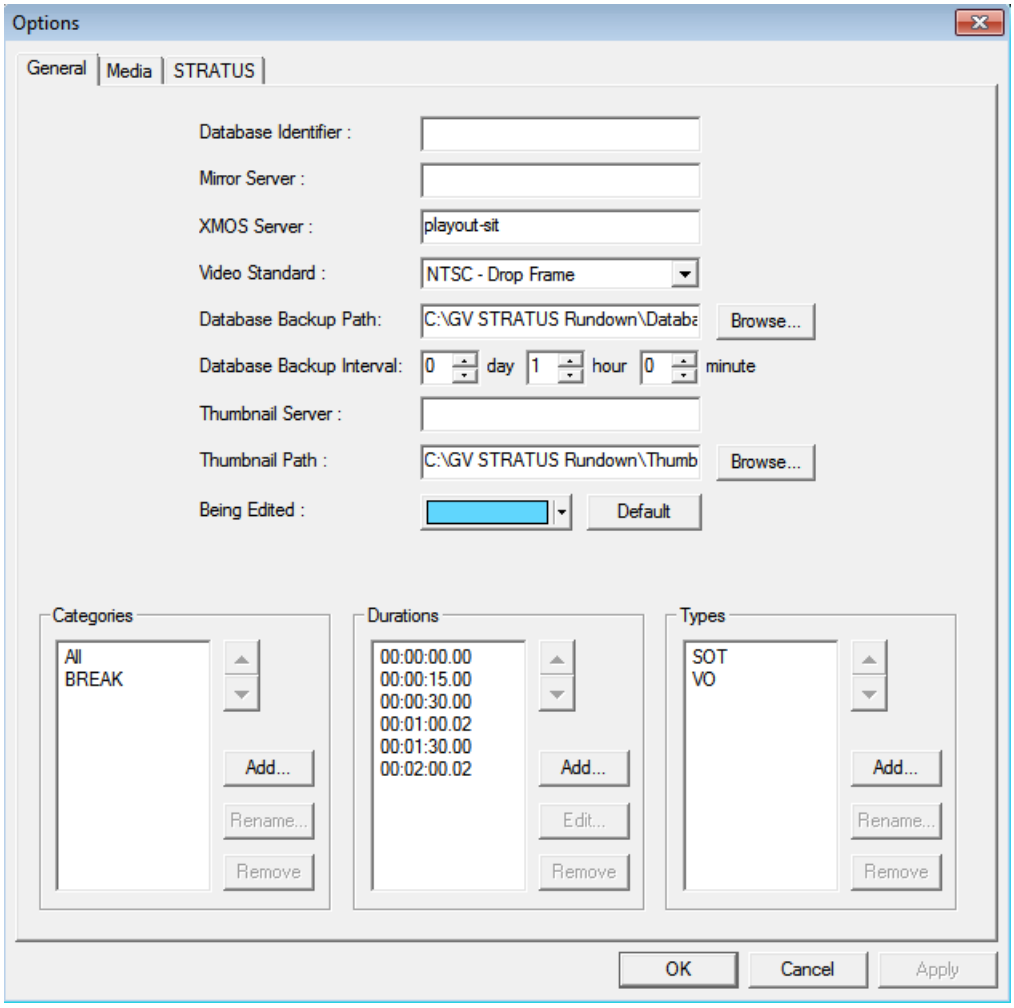
on the desktop; or click the **Start** menu and choose **Programs | Grass Valley | GV STRATUS Rundown | SDB Server**.
2. Choose **Tools | Options**.

   The Options window appears.
3. Go through each tab on the Options window and configure SDB Server using descriptions in the following sections.
4. Click **OK**.

Related Topics

Configuring GV STRATUS Rundown on page 1507

Setting General Options of SDB Server



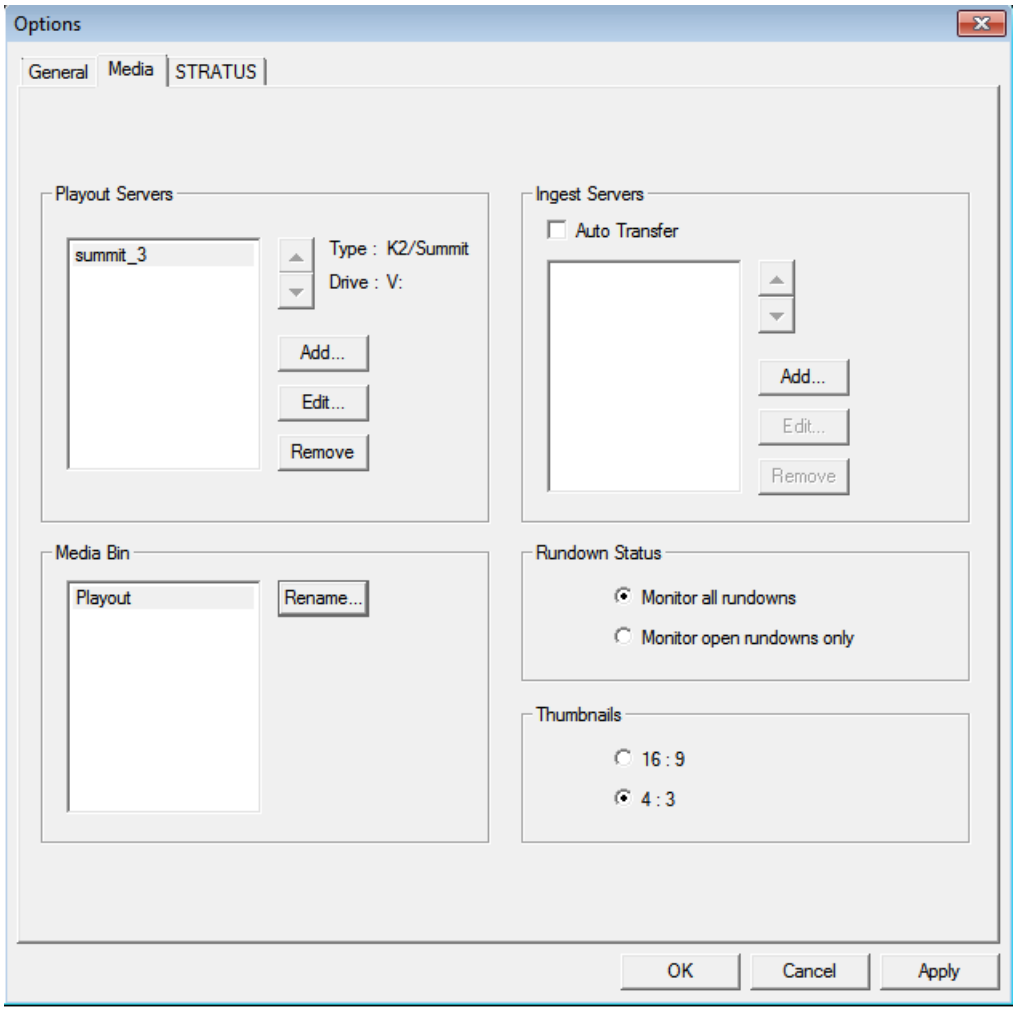
Setting	Description
Database Identifier	Enter an ID for the database, up to 4 characters, such as your station call letters. All clip IDs will begin with this identifier. This is an optional field.
Mirror Server	Enter the name of the computer hosting the backup database server. For the primary SDB Server, this is the system hosting the hot standby database server; for the hot standby database server, this is the system hosting the primary SDB Server.
XMOS Server	Enter the name of the computer hosting the XMOS Server.
Video Standard	Select your newsroom video standard: PAL, NTSC - Drop Frame, or NTSC - Non-drop Frame.
Database Backup Path	Enter the path for the database backups.
Database Backup Interval	Enter how often you want the database to back up automatically.

Setting	Description
Thumbnail Server	Specifies the name of the computer running the Thumbnail Server application (if used).
Thumbnail Path	Sets the path where the thumbnails will be stored.
Being Edited	Select the color that displays in the Assignment List to alert editors that a sequence is being edited.
Categories	Lets you define categories for sorting and assigning placeholders. To add a category, click Add, enter the name of the category, and click OK. Categories appear in these locations: Assignment List Manager; GV STRATUS Rundown Clip Browser, and Assignment List in the GV STRATUS ActiveX Plug-in.
Durations	Lets you set default estimated durations for new placeholders. To add a duration, click Add, enter the duration in the format hours:minutes:seconds:frames, and click OK.

Setting	Description
Types	Lets you define story types for placeholders. Two story types, SOT (Story on Tape) and VO (Voice Over) are default types. To add a story type, click Add, enter the type, and click OK.

Setting Media options of SDB Server

A K2 system that is a playout server must have a Grass Valley Media Server MDI configured in GV STRATUS Control Panel. Refer to related topics in this Topic Library.



Setting	Options	Description
Playout Servers		Defines playout media servers, as configured in Grass Valley Media Server MDI settings. Click Add, enter the Name and Drive where the media is stored on the playout server, and click OK. If you are using mirrored playback, add both servers here.

Setting	Options	Description
Ingest Servers		Use the Auto Transfer feature to automatically transfer media from a source (ingest) server to a destination (playout) server. The Auto Transfer takes place only when media that is sent to or recorded on the ingest server is associated with a Playout placeholder that is part of a MOS-Active rundown. To add an ingest server, check Auto Transfer, click Add, enter the name, and click OK. To change the ingest server to a different server, select the server and click Rename. A media server can only be either a source or destination server for Auto Transfer, so the same media server should never be added to both the Playout and Ingest sections. If you are not using Auto Transfer, leave this section blank.
Media Bin		GV STRATUS Rundown creates a default Media Bin where playout media is sent; also used for monitoring ready status and clip duration.
Rundown Status	Monitor all rundowns	Select Monitor all rundowns to update statuses for stories in all active rundowns in your newsroom computer system, regardless of whether they are currently open in GV STRATUS Rundown; this is the default.
	Monitor open rundowns only	Select Monitor open rundowns only to update statuses for only the rundowns that are open in GV STRATUS Rundown; when set, only updates the status column in your newsroom computer system for open rundowns.
Thumbnails	16:9; 4:3	Select the video aspect ratio for thumbnails displayed in GV STRATUS Rundown components.

Related Topics

Grass Valley Media Server MDI standalone settings on page 304
Grass Valley Media Server MDI SAN settings on page 306
Media settings on page 393
Rundown Add/Modify Server settings on page 394

Setting up STRATUS Database Server in SDB Server

To connect to the host of STRATUS Database Server:

1. Click on the **STRATUS** tab.

2. Enter the following system information:

Setting	Description
STRATUS Database Server	Enter the name of the computer hosting the STRATUS Database Server.

3. Click **Apply** and **OK**.

After this setting is configured, STRATUS database can be accessed via the STRATUS ActiveX Plug-in within GV STRATUS Rundown, and proxy paths of assets are available to the newsroom computer system.

NOTE: If the STRATUS Database Server setting is changed in the STRATUS Control Panel application, you also need to launch and save the Rundown settings in the STRATUS Control Panel to update the configuration. Then, SDB Server needs to be restarted to get the new setting of the STRATUS Database Server.

Reinitializing media monitor of SDB Server

To refresh rundowns, reinitialize media server connections and update database records, you can select the option to Reinitialize Media Monitor.

This is an option for you to manually execute the refresh function, even though SDB Server would be automatically updated each time there is a new change to your rundown.

To reinitialize media monitor:

1. Click **SDB Server** on the taskbar of your desktop to display the window.
2. Select **Tools | Reinitialize Media Monitor or press F5 for the shortcut button.**

Repopulating rundown items from SDB Server

The option to repopulate rundown items is useful if you were to accidentally delete placeholders in an active rundown. You can repopulate those placeholders by selecting this option within SDB Server.

However, this option only repopulate empty placeholders and you still need to associate clips to those placeholders before the rundown is ready for playback.

In the case of a complete loss or corruption of the SDB database, repopulate could be used to rebuild the database by importing placeholders from all MOS active rundowns.

To repopulate rundown items:

1. Click **SDB Server** on the taskbar of your desktop to display the window.
2. Select **Tools | Repopulate Rundown Items.**

   You could see the change from "Unknown Placeholder" to the previous name of the placeholder in the rundown list.
3. Launch the GV STRATUS ActiveX plug-in to associate assets to the repopulated placeholders.

Restoring backup database of SDB Server

You also have the option to restore your backup database in case the current database is corrupted or your system crashed.

For extra precaution, it is also advisable to have a backup database server on another machine on your network.

To restore the backup database:

1. Click **SDB Server** on the taskbar of your desktop to display the window.
2. Select **Tools | Restore Backup Database.**

Creating a Thumbnail folder

Regardless of which media server you're using, you need to create a directory in which to store video thumbnails.

To create the Thumbnail folder:

1. Navigate to **C:\GV STRATUS Rundown**.
2. Create a folder and name it **Thumbnails**.
3. Right-click on the folder, select **Sharing**, and click **Share this folder**.
4. Click **OK**.

Configuring the XMOS Server

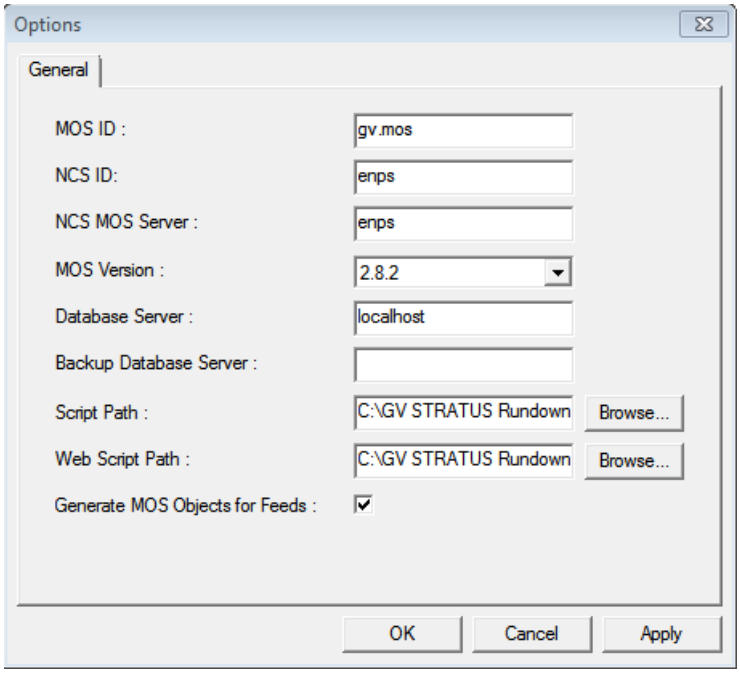
The XMOS Server provides communication between the Newsroom Computer System and GV STRATUS Rundown.

NOTE: If you want to configure the GV STRATUS application with* GV STRATUS Rundown, *refer to related topics about Rundown configuration settings in the this Topic Library in order to configure the XMOS Server.

To configure the XMOS Server:

1. From the **Start** menu, choose **Programs | Grass Valley | GV STRATUS Rundown | XMOS Server**.

2. Choose **Tools | Options**.



The Options window appears.

3. Enter the following system information:

Setting	Description
MOS ID	Enter your MOS ID: • For ENPS, see **ENPS | System Maintenance | MOS Configuration** in the ID column. • For iNEWS, this value matches the <mos> value within the configuration file on the iNEWS MOS Gateway at `C:/Program Files/Avid/MOS Gateway/mosconfig.xml`. • For Octopus, see **Admin | MOS | Devices**. • For OpenMedia, see **OMIS | OMIS Plugin Types | MOS Device**.
NCS ID	Enter the name of the server hosting your newsroom computer system: • For ENPS, the name of the ENPS Server. If you have an ENPS Buddy server, you need to enter both the main and buddy server names in both the NCS ID and NCS MOS Server fields, in the format "MAIN,BUDDY". • For iNEWS, the name of the iNEWS Server. • For Octopus, see **Admin | MOS | Devices**. • For OpenMedia, see **OMIS | OMIS Service Instances | OMIS MOS Gateway | Properties**.
NCS MOS Server	Enter the name of the server hosting the NCS MOS Server component: • For ENPS, the same value you entered for the NCS ID. • For iNEWS, the name of the iNEWS MOS Gateway machine. • For Octopus, the name of the Octopus Server machine. • For OpenMedia, the name of the MOS Device.
MOS Version	The version number of MOS you are using. Refer to compatible versions in this Topic Library. If your version is unknown, leave the setting at the default value.
Database Server	Enter the name of the server hosting the GV STRATUS Rundown database (primary SDB server).
Backup Database Server	Enter the name of the server hosting the backup GV STRATUS Rundown database (hot standby SDB server).If you are not using a hot standby SDB server, leave this field blank.
Script Path	Enter the full path (or browse) to the directory where scripts are stored.
Web Script Path	Enter the full path (or browse) to the directory where web scripts are stored. Users are able to view scripts created through NCS from a standard web browser such as Internet Explorer and Firefox.
Generate MOS Objects for Feeds	Check the box to enable an enhanced MOS workflow which requires MOS Objects generated for feeds. As assets are embedded with MOS Object IDs in ENPS, they can be searched throughout ENPS and inserted below the black line of the script.

4. Click **OK**.

Related Topics

Configuring GV STRATUS Rundown on page 1507

Refreshing rundowns in XMOS Server

To reflect new changes on your rundown, you can select the option to refresh rundowns within XMOS Server.

This is an option for users to manually execute the refresh function, even though XMOS Server would be automatically updated each time there is a new change to your rundown.

To refresh rundowns:

1. Double-click **XMOS Server** on the desktop or click the **Start** menu and choose **Programs | Grass Valley | GV STRATUS Rundown | XMOS Server**.
2. Click **Tools | Refresh Rundowns.**

Configuring the standalone Assignment List Manager

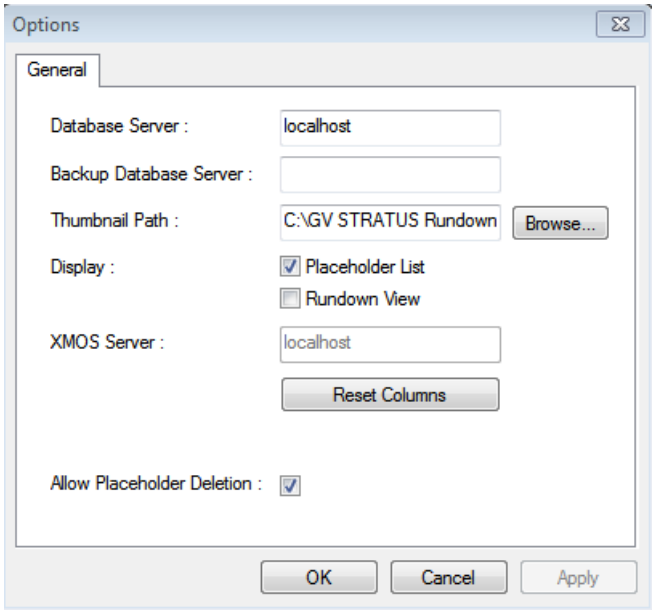
The Assignment List Manager lets producers create placeholders for clips, assign or reassign placeholders to editors, and monitor clip status.

To configure the Assignment List Manager:

1. Click the **Start** menu and select **Programs | Grass Valley | GV STRATUS Rundown | Assignment List Manager**.

   The Assignment List Manager appears.

2. Click **Options** button .



The Options window appears.

3. Enter the following system information:

Setting	Options	Description
Database Server		Enter the name of the server where the GV STRATUS Rundown database resides (primary SDB server).
Backup Database Server		Enter the name of the server for the backup GV STRATUS Rundown database (hot standby SDB server).
Thumbnail Path		Enter the full path to the shared thumbnail directory on the computer where thumbnails are stored, in the format \\server\foldername; e.g., if you have a shared folder named “thumbnails” on your playout system named “Playout1”, the path would be \\Playout1\thumbnails.
Display	Placeholder List; Rundown View	Select Placeholder List to display placeholders in the Assignment List Manager or select Rundown View to display the list of rundowns. Both can also be selected to display placeholders and rundowns in the Assignment List Manager.
XMOS Server		Enter the name of the computer hosting the XMOS Server.
Reset Columns		Click the button to reset columns to their original placement if they have been rearranged.
Allow Placeholder Deletion		Check the box to allow placeholders to be deleted within the Assignment List Manager.

4. Click **OK**.

Related Topics

Configuring GV STRATUS Rundown on page 1507

Setting up your NCS for GV STRATUS Rundown

Setting Up Your NCS for GV STRATUS Rundown

With GV STRATUS Rundown, you can use your Newsroom Computer System (NCS) to create rundowns and link clips to rundown scripts via Assignment List in the STRATUS ActiveX Plug-in. The MOS-compatible NCS needs to be configured for use with GV STRATUS Rundown.

- ENPS
- iNEWS
- Octopus
- OpenMedia
- NIS5

- Netia
- Inception

To integrate Netia and Inception into the GV STRATUS system, contact Grass Valley Service.

Setting up ENPS for GV STRATUS Rundown

To set up ENPS for use with GV STRATUS Rundown, you need to modify your ENPS configuration.

1. On the ENPS server, find the *enps.ini* file and add the following to the **[ENPS]** section:
   ```
   QTMediaExtensions=.mov,.mp4
   ```
2. On an ENPS client, log on as the administrator and start up ENPS.
3. From the ENPS folder, select **System Maintenance | Groups | New** and create a new group with these parameters:

ID	KXYZGVG
Description	GV Clips
Server	Select the name of your ENPS server from the drop-down list

4. Click **Save** and close ENPS on the workstation.
5. Close the News Object Manager and it should restart automatically. After the NOM has started, restart the ENPS client.

6. From the ENPS folder, select **System Maintenance | MOS Configuration | New** and create a new MOS entry with these parameters:

ID	The MOS ID; this value is case sensitive and must match the MOS ID configured in the XMOS Server Options. The recommended format is <family>.<machine>.<location>.<enterprise>.mos. Standard practice is to use station call letters for location and station group abbreviation for enterprise.
Description	GV STRATUS - for operation with GV STRATUS. GV Assignment List - for GV STRATUS Rundown operation only.
IP	The IP address or host name of the machine hosting the SDB Server and the XMOS Server.
ActiveX	GV.STRATUS.1 - for operation with GV STRATUS. GVG.XMOSCtrl.1 - for GV STRATUS Rundown operation only.
Default Settings	Leave blank. These settings are configured during installation.
Program	The group ID you configured in step 3.
MOS Version	2.6 or 2.8.2
Local DragDrop	Off
Auto Create	On
Story Send	On

7. From the ENPS folder, select **System Maintenance | Global Configuration Options**, add a new property named `AddMOSObjDuration` and set its value to **1**.

   NOTE: `AddMOSObjDuration` is the optional setting that allows the duration of clips to be automatically included in the rundown timing. If you prefer to manually enter the duration of your story and clips, do not activate this setting.

8. Add **mp4** to the `MOSBrowseMediaExtensions` property, as can be seen below:

```
MOSBrowseMediaExtensions=bmp,jpg,jpeg,mp4,3gp,wmv,wav,sdp,ts
```

9. Restart the ENPS client application.

Related Topics

Setting Up Your NCS for GV STRATUS Rundown on page 1538

Sending scripts with ENPS

The ENPS MOS Story Send feature allows Aurora Edit systems to view scripts.

1. For an existing rundown or template in ENPS, go to Properties.
2. Temporarily toggle the **MOS Control Active** field to **OFF**.
3. Click in the **MOS Story Send** field and turn on the checkbox for the MOS ID used for GV STRATUS Rundown.

4. Toggle the MOS Control Active to ON to make the rundown available to GV STRATUS Rundown.
5. Configure the XMOS Server to write scripts.

Aurora Edit systems will then be able to use the "Link to Story" and "Story View" features.

Setting ENPS MOS ready to air

If you want producers to have the ability to indicate to the GV STRATUS Rundown operation when a rundown is ready, use the ENPS MOS Ready to Air feature.

To set the feature:

- Set the ENPS rundown property “Ready to air” to ON.

A corresponding READY flag is set to ON in the GV STRATUS Rundown rundown window Status column.

Setting up iNEWS for GV STRATUS Rundown

To set up iNEWS for use with GV STRATUS Rundown, you need to add a new MOS device to the iNEWS configuration file:

1. On the MOS gateway machine, open the file C:\Program Files\Avid\MOSGateway\mosconfig.xml.
2. Modify the following lines of the file, adding values for your location:

Value	Description
ncs id	Your Newsroom Computer System name; this value is case sensitive and must match the NCS ID configuration in the XMOS Server options.
host	The hostname of the iNEWS server.
mos	Your MOS ID; this value is case sensitive and must match the MOS ID configuration in the XMOS Server options.
amcp	The tag displayed in iNEWS scripts for placeholders embedded in scripts. This value should match the device name that appears in the iNEWS SYSTEM.MAP file.
network	The hostname of the machine running the XMOS Server.

NOTE: With iNEWS, <handlesRoItemLevelCommands> default setting could cause stories to drop to the bottom of the playlist when they are newly inserted, or when their channel assignment is changed. Therefore, <handlesRoItemLevelCommands> value should be set to NO in the mosconfig.xml file.

Related Topics

Setting Up Your NCS for GV STRATUS Rundown on page 1538

Configuring status translations for iNEWS

To ensure correct status reporting between GV STRATUS Rundown and iNEWS server, you need to edit the status translation table in the iNEWS configuration file.

- The status translation table within the mosconfig.xml file should appear as below:

```
<statusTranslations>
   <statusUnavailable>NOT READY</statusUnavailable>
   <statusCueing>CUEING</statusCueing>
   <statusAvailable>READY</statusAvailable>
   <statusCued>STAND BY</statusCued>
   <statusPlaying>PLAY</statusPlaying>
   <statusPaused>STOPPED</statusPaused>
   <statusStopped>END</statusStopped>
   <statusUnknown>DISCONNECTED</statusUnknown>
</statusTranslations>
```

- On the iNEWS server, your MCS dictionary (located at /site/dict/mcs) would typically contain these lines:

```
A_EVERR                    /5ERROR
A_CAFRZ                    /END
A_CATREL                   /2STANDBY
A_CATHRD                   /THREAD
A_CACUING                  /2CUEING
A_CACUED                   /2CUED
A_CANOTAPE                 /4NOT READY
A_CABIN                    /READY
A_CAPLAY                   /3PLAY
A_CAPAUSE                  /3STOPPED
A_CAREW                    /REWIND
A_CAEJECT                  /EJECT
A_CAINCMPLT                /TRANSFER
```

NOTE: Since the statuses that appear in this dictionary can be customized, the values shown in the right column of your MCS dictionary may vary slightly from the ones shown here.

To ensure correct configuration with iNEWS, a sample of the mosconfig.xml file is provided in the appendix section.

Setting up Octopus for GV STRATUS Rundown

In order to use Octopus with GV STRATUS Rundown, you need to configure it first.

To configure Octopus for GV STRATUS Rundown, you need to create an ActiveX device, and modify the MOS Devices configuration.

Related Topics

Setting Up Your NCS for GV STRATUS Rundown on page 1538

Configuring the MOS Device for Octopus

You need to configure the MOS Device before using Octopus with GV STRATUS.

1. Launch the Octopus client, and click the **Devices** button.

   The **Devices** page opens.

2. Click the **New** button on the toolbar.

   The **Device** window opens.

3. Configure the Basic tab as follows:

mosID	These values must match those set for the XMOS Server.
ncsID	
Version	This value must match with the version set for the XMOS Server.
Disabled	Unchecked
Media host	Name or IP address of machine hosting the SDB Server.
Media port	SDB Server port (normally won't change from default setting)
Rundown host	Name or IP address of machine hosting the XMOS Server.
Rundown port	XMOS Server port (normally won't change from default setting)

4. Configure the Stories tab as follows:

Option	Setting
Send empty stories	✓
Send production requirements	✓
Send story custom fields	✓
Use standard ed times	✓

5. Configure the Rundowns tab as follows:

Refresh method	roReplace
Send roMetadataReplace	✓
Send broadcast channel name in roChannel	✓
roSlug pattern	%TYPE% %START%

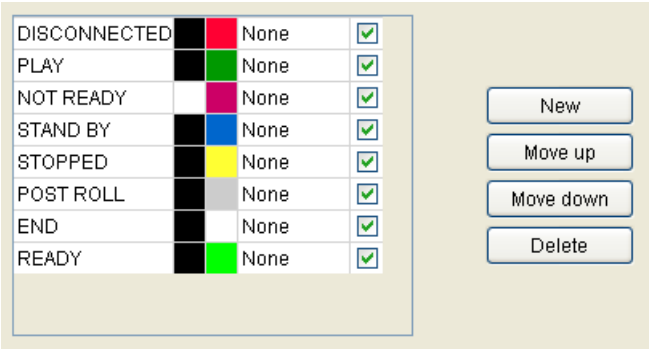
6. Configure the Prompting tab as follows:

Send story text	✓
Keep sending roStoryReplace or roElementAction	✓

7. Configure the Status tab as follows:

Accepts on-air status	✓
Accept status for slugs in not-ready rundowns	✓

a) Create these status categories (these are the suggested names and order):



8. Configure the MOS Objects tab as follows:

Update private objects	✓
Translate redirected IDs	✓
Supports mosListAll	✓
Display name instead of jobID	✓

9. Configure the Placeholders tab as follows:

Allow MOS object creation	✓
Default MOS object creation device	✓
Allow automatic MOS object creation	✓
Use the <mosObjCreate> message	✓
Default duration of created MOS objects	00:00:00:00
Naming pattern of created MOS objects	%NAME

10. On the Other tab, configure as follows:

Send and receive times in UTC	✓

11. Click **OK**.

Creating an ActiveX Device for Octopus

You need to create an ActiveX device before using Octopus with GV STRATUS.

1. Launch the Octopus client, and click the **Devices** button.

   The **Devices** page opens.
2. Highlight the MOS ID for GV STRATUS.
3. Click the **Edit** button on the toolbar.

   The **Device** window opens.
4. Select the **Plugins** tab, and click **Add**.

   The **Plugin** window opens.
5. Configure the device as follows:

Option	Setting
Short Name	User preference (e.g., GV Plug-in)
Long Name	User preference (e.g., GV STRATUS Plug-in)
Size	800 width x 600 height
Type	Player (ActiveX)
Version	1.0 ENPS
Platform	ActiveX
Placement	Modeless
Implementation	GV.STRATUS.1

6. Click **OK** twice.

Using NCS Rundowns and GV STRATUS Rundown

Using NCS rundowns and GV STRATUS Rundown

Producers can use GV STRATUS Rundown with a MOS-compatible newsroom computer system (NCS) to create rundowns, create placeholders for editor assignments, link clips to the rundown and frame-accurately triggered to play-to-air.

Producers can also use the NCS to assign clips to specific playback channels, eliminating the need for a playback operator to assign channels for the rundown.

In sites without an NCS, an editor can follow the producer's script and create placeholders using another component of GV STRATUS Rundown, such as the Assignment List Manager, and have a playback operator manually create playlists.

Using the Assignment List in GV STRATUS ActiveX Plug-in

The Assignment List in GV STRATUS ActiveX Plug-in integrates with your NCS and allows you to create placeholders for clips, assign those placeholders to newsroom editors, and link the resulting clips back to your NCS rundown.

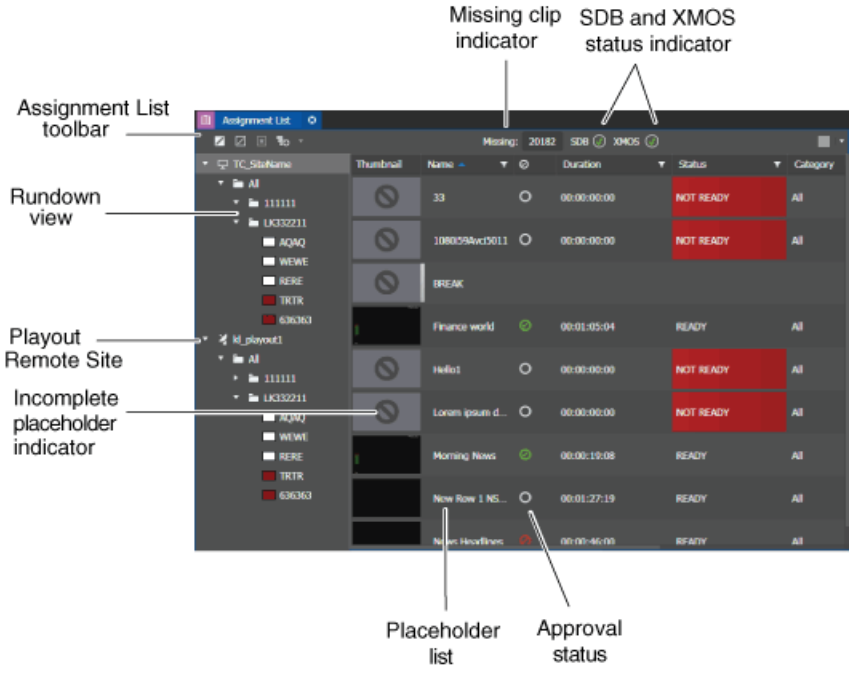
As you use your NCS to create rundowns for news programs and add scripts for each story, you can check the Assignment List in the GV STRATUS ActiveX Plug-in to ensure that the related news clip is ready for your story.

With the integration, you can also add general metadata, keywords and custom metadata on a placeholder. Once the metadata is added, it will be searchable and editable throughout all GV STRATUS clients.

If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, and metadata. In order to link to a placeholder, you must be assigned with write permission for the **Name** property in Metadata section of GV STRATUS Control Panel.

The Assignment List tool

The Assignment List tool allows you to create placeholders for clips, assign those placeholders to newsroom editors, add new sequence, and link the resulting clips to rundown stories on your Newsroom Computer System. You also need GV STRATUS Rundown components such as SDB Server and XMOS Server to run the Assignment List tool. With the proper license and assigned role, Assignment List appears in the GV STRATUS application as a panel that can be accessed from the Window menu, the tool section of the Navigator panel, and the **Link to Placeholder** tab in the Inspector panel.



The Assignment List panel features are as follows:

- Toolbar — Displays buttons to add placeholders, show placeholders with missing clips, delete placeholders, and add new sequence to placeholders.
- Missing clip indicator — Displays the number of missing clips that can help you determine the number of incomplete assignments.
- Incomplete placeholder indicator — Displays blank thumbnails for incomplete placeholders. Completed placeholders are identified by the thumbnail display and **READY** status in the Status column.
- Placeholder list — Displays incomplete and completed placeholders. When you select a rundown, all placeholders in that rundown appear in the placeholder list. When you select a story in the rundown, only placeholders in that story appear in the placeholder list in the same sequence as in the story.
- Approval status — Displays the approval status of placeholders. You can only set the approval status on linked placeholders with **Ready** status in the Inspector panel.
- Playout Remote Site — Displays placeholders in the remote site. The Playout remote site must be configured in the GV STRATUS Control Panel before it can be accessed via the Assignment List.
- Rundown view — Displays rundowns and stories for each rundown. Rundowns display alphabetically in the panel, while stories appear in sequence as assigned in the Newsroom Computer System.
- SDB status indicator — Displays the connection status between Assignment List and Simple Database (SDB) Server. The SDB Server updates clip status, clip duration, and amount of missing clips for the Assignment List tool.
  - — Connected
  - — Disconnected
- XMOS status indicator — Displays the status of XMOS Server. The XMOS Server provides the communication between the Newsroom Computer System and the Assignment List tool.
  - — Connected
  - — XMOS Server is disconnected with the GV STRATUS application
  - — XMOS Server is disconnected with the Newsroom Computer System

With the Assignment List tool, you can create placeholders, monitor rundown or clip status, and view or change placeholder properties.

Standard Asset List features such as filter list, sort list, asset tooltip, and customization of **View Mode** are available in the Assignment List tool.

If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets, and metadata that do not have read permissions are not visible.

Assignment List buttons

These buttons located on the Assignment List panel let you perform various functions.

New Placeholder: Adds a new placeholder in the Assignment List tool.

Missing Placeholders Only: Shows placeholders with missing clips only in the Assignment List tool.

Delete: Deletes the selected item or items. Disabled if delete rights denied in GV STRATUS Control Panel and/or turned off in User Preferences.

New Sequence: Creates a new sequence.

New Project in EDIUS: Creates a new project in the EDIUS XS application.

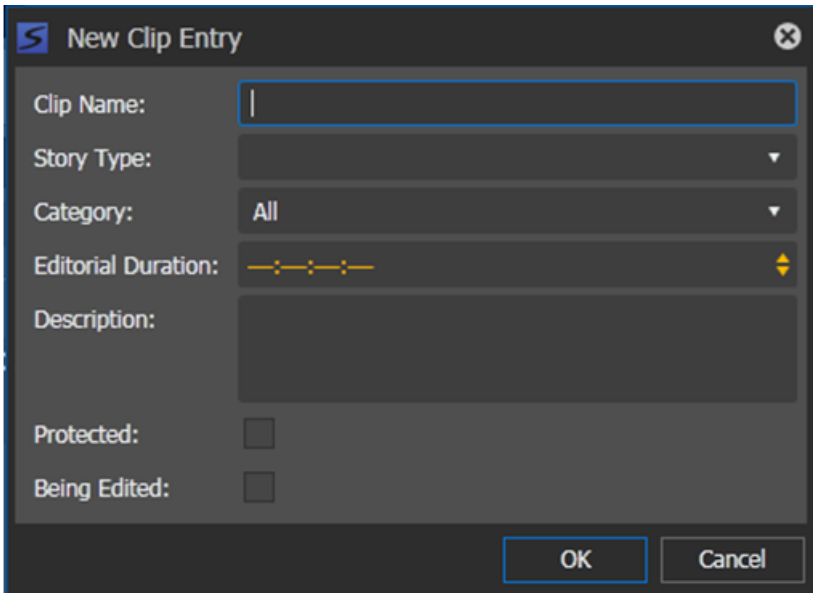
Missing : 86 **Missing Clip indicator**: Shows the number of placeholders with missing clips in the Assignment List tool.

Adding placeholders

Placeholders are essentially assignments for editors, who can then create clips for the story, and send them to a K2 Summit/SAN system for playback. You need to create a placeholder for each clip that you link to a rundown.

NOTE: Grass Valley recommends no more than 2,000 placeholders in the system for optimal performance.

1. In the Assignment List tool, click the **New Placeholder** button.



The New Clip Entry dialog box opens.

2. Enter the clip name.

   The name identifies the placeholder in the Assignment List (which can also be seen in the Newsroom Computer System).

3. You can also provide additional information about the placeholder:

   - **Story Type** — Select a Story Type from the drop-down menu. Available story types are **SOT** (Sound On Tape) or **VO** (Voice Over). You can also leave this field blank.
   - **Category** — Select a category from the drop-down menu. The category determines how stories are grouped and sorted.
   - **Editorial Duration** — Enter a duration for the placeholder. The Editorial Duration is an optional value you can set for an estimated on-air duration of the clip that can be changed to a more precise value later.

     NOTE: Editorial Duration has the priority over clip duration. Once an Editorial Duration is set; it will not be adjusted to clip duration, even after clip is associated with the placeholder. The editor needs to set the final Editorial Duration before the clip is sent for playback.
   - **Description** — Enter a description for the placeholder. The description helps editors to identify the clip that they need.
   - **Protected** — Check this box to prevent the clip from being deleted by other users.
   - **Being Edited** — Check this box to indicate when the sequence for a placeholder is currently being edited.

4. Click **OK**.

The new placeholder appears on the Assignment List tool.

NOTE: The Clip ID and Date are set automatically when you create a new placeholder.

Related Topics

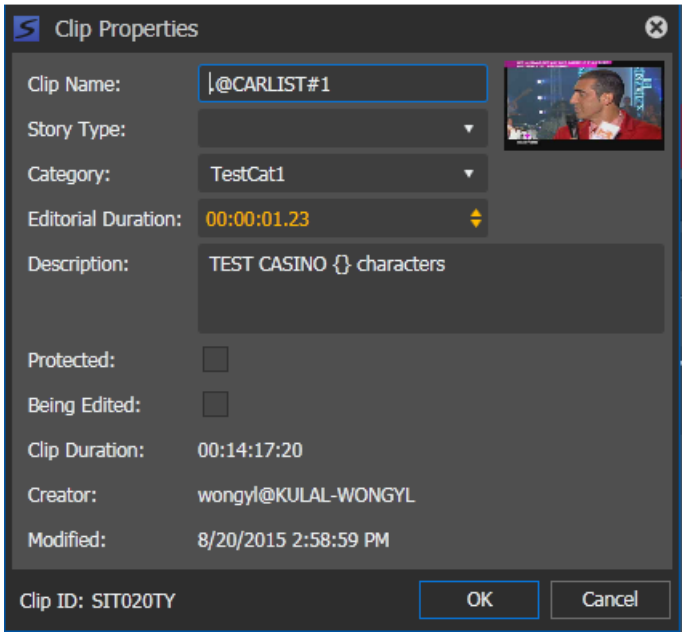
Limitations for creating and naming assets and bins on page 1428

Modifying a placeholder

If you need to, you can change or modify properties of a placeholder.

1. Right-click on the placeholder that you want to modify and select **Edit Properties**.

   The Clip Properties dialog box opens.



2. Modify any properties in the dialog box.

   NOTE: Properties that cannot be modified are creator, modified date and clip ID.

3. Click **OK**.

   The placeholder properties are modified on the Assignment List tool.

Related Topics

Limitations for creating and naming assets and bins on page 1428

Deleting a placeholder

If desired, you can delete placeholders, associated assets, and essences from the Assignment List tool.

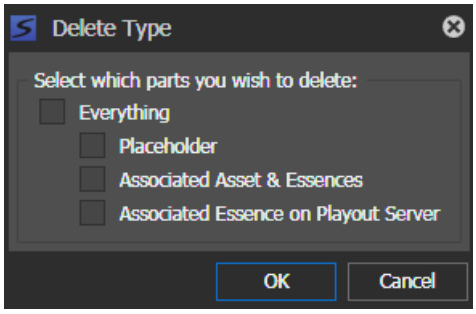
1. Do one of the following to delete a placeholder:

   - Select the placeholder that you want to delete and click the **Delete** button.
   - Right-click on the placeholder and select **Delete Placeholder**.

2. Select your options as follows:

   - Everything — Select this to delete the entire asset including placeholder, associated asset and essences, and associated essence on the managed Playout Server.
   - Placeholder — Select this to only delete the placeholder on the GV STRATUS application.
   - Associated Asset & Essences — Select this to only delete the associated asset and essences on your K2 Summit/SAN system.
   - Associated Essence on Playout Server — Select this to only delete the associated essence on the managed Playout Server if you already sent it out for playback.

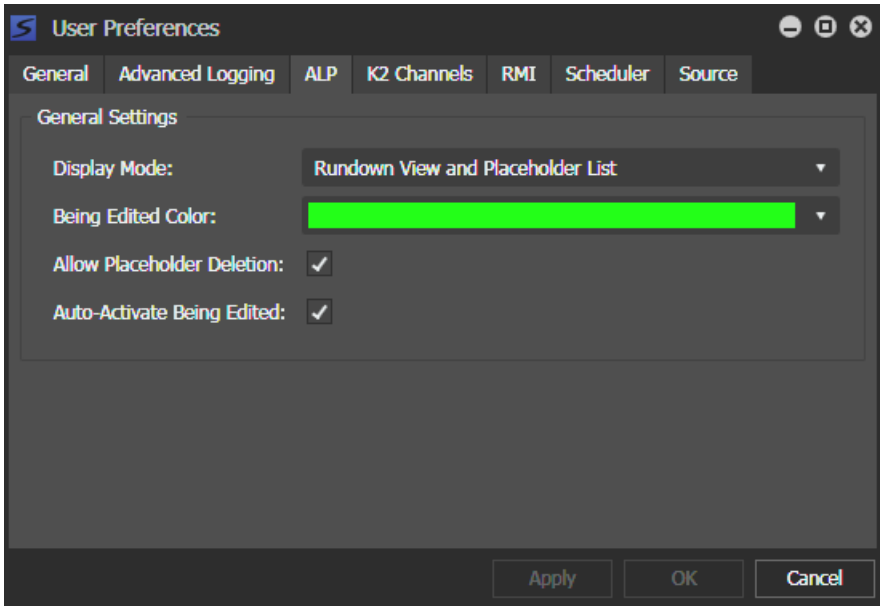
     NOTE: Deletion of essence on an unmanaged playout server is not supported. However, you can still delete via the Aurora Playout Housekeeper application or delete directly on the unmanaged playout server.



3. Click **OK**.

If the **Delete** button is not selectable or **Delete Placeholder** is grayed out in the context menu, you need to check ALP settings in the User Preferences menu.

Select **Edit | User Preferences | ALP** and check the **Allow Placeholder Deletion** box.



Related Topics

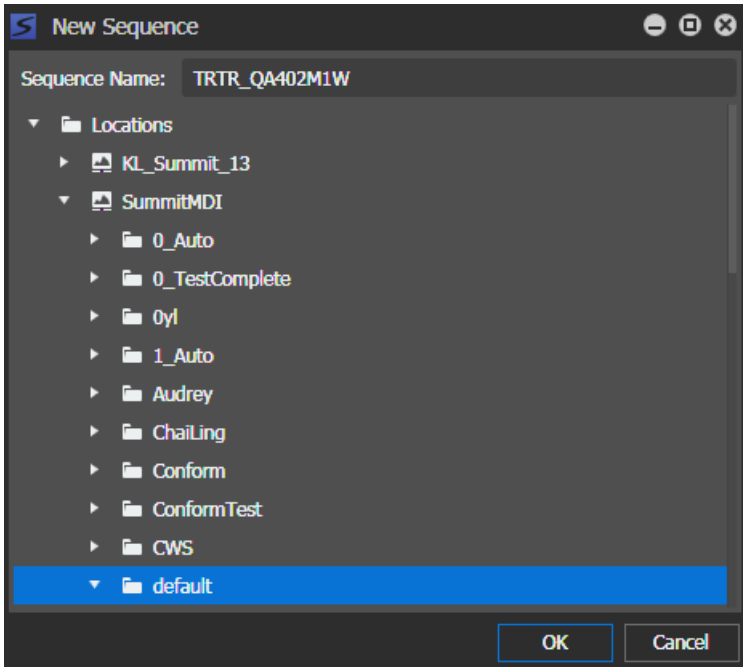
Deleting assets on page 985

Adding a new sequence

You can add a new sequence to a placeholder in the Assignment List tool.

1. Select a placeholder that you want to add a new sequence into.
2. Click the **New Sequence** button.

   The New Sequence dialog opens.



   The sequence name is automatically populated with the placeholder name and ID. You can still change the sequence name if you want to.

3. Select a location for the sequence and click **OK**.

   The Storyboard Editor tool launches automatically if it is not already opened. The sequence name can be viewed in the Sequence Viewer and Storyboard panels.

4. Add events as necessary to the sequence.

If configured in ALP user preferences settings, the placeholder row color changes to the being edited color in the Assignment List.

Checking missing clips

The Assignment List lets you see if clips are complete and ready for air.

You can only see thumbnails for placeholders with completed clips, which can also be identified by **Ready** status in the Assignment List. The thumbnail column is blank for placeholders with missing clips.

- To display placeholders with missing clips only, click the **Missing Placeholders Only** button.

  You can also see the number of placeholders with missing clips from the indicator on the toolbar.

If you want to see the entire list of placeholders, click again the **Missing Placeholders Only** button.

Viewing and modifying metadata of linked placeholders

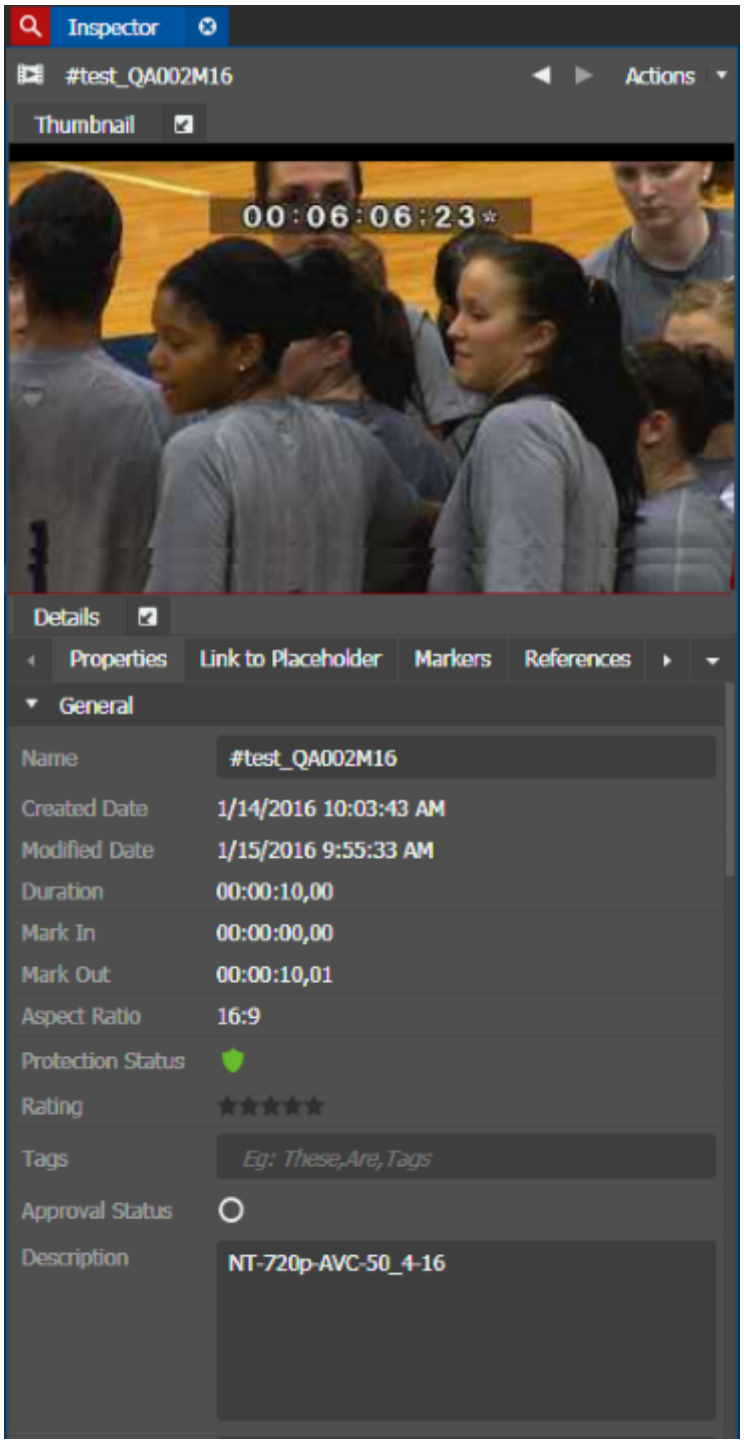
You can view and modify metadata of placeholders with **Ready** status. When you modify the metadata, you are actually modifying the metadata of the asset that is already associated with the placeholder.

The inserted metadata can then be used as the search criteria to easily search assets in the Asset List panel.

1. To view or modify the metadata, do one of the following below:

   - Drag and drop the placeholder into the Inspector panel.
   - Double-click the placeholder.

   The metadata loads into the Inspector panel.



2. On the **Properties** tab, you can view or modify metadata of placeholders.

   You can also add and customize metadata fields in the Metadata settings within the GV STRATUS Control Panel application.

3. To lock the status, click the **Unprotected** button.

   The asset is now locked. To unlock, click the **Protected** button.

4. To add a star rating, click the star or stars next to Rating.
   When you add a star, it retains the color fill even when the mouse is no longer hovering over it.

5. Click the **None** icon to change the approval status.

   The approval status changes to **Approved**.

   You can click the icon to toggle the approval status of the linked placeholder. The selected approval status displays on the Assignment List.

   None: Identifies the approval status of the clip as none.

   Approved: Identifies the approval status of the clip as approved.

   Rejected: Identifies the approval status of the clip as rejected.

6. Set the **MetadataExpireDate** and **Source ID**, if needed.
7. To view lists of related assets and relationships, see other tabs of the Inspector panel.

Related Topics

Viewing relationships on page 1020
Verifying proxy association on page 1021

Editing and GV STRATUS Rundown

Editing and GV STRATUS Rundown

Editing and GV STRATUS Rundown

News editors use the Assignment List Manager component of GV STRATUS Rundown to receive assignments from the producer and return completed assignments. The Assignment List tool in GV STRATUS application can also be used by news editors, producers, and journalists in the newsroom.

Editors create clips and sequences in the editing application and send them to a media server. A playlist is received from the NCS or a playback operator uses the clips in GV STRATUS Rundown to create a playlist, and then controls the playback of clips to air.

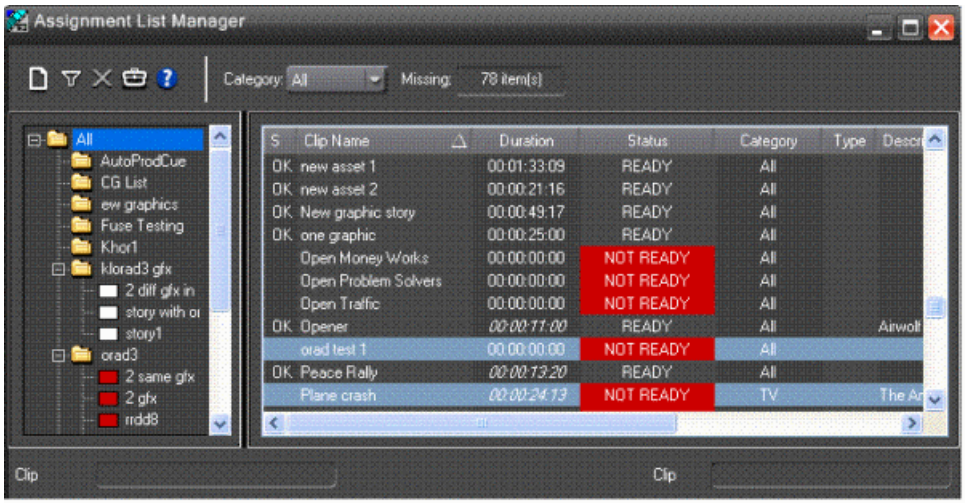
With GV STRATUS within the GV STRATUS Rundown, you can explore assets using the Navigator and Asset List panel. To quickly edit assets, you can also launch the Storyboard workspace which includes the Source Viewer, the Sequence Viewer and the Storyboard Editor. To use the GV STRATUS application within GV STRATUS Rundown, the STRATUS-ELITE license must be installed on the GV STRATUS Core Services server. For more information regarding licensing, refer to the GV STRATUS Rundown *Release Notes*.

Using the Assignment List Manager

The Assignment List Manager is for editors to receive assignments from the producer, to create additional placeholders for clips, and to reassign placeholders to other editors.

The standalone Assignment List Manager runs on any computer in the network.

- In the standalone Assignment List Manager, maximize the window:



The list of assignments shows each clip/placeholder and its properties:

Column	Description
S	The clip status: displays OK if a clip has been completed, sent to the media server, and is ready for playback. Status is blank if a clip is incomplete and not ready for playback.
Clip Name	The name of the clip/placeholder.
Duration	The duration of the clip when the placeholder was created. This estimated value will be changed later when media is associated with the placeholder. A duration displayed in italics in the Assignment List indicates that the Editorial Duration property has been set to be different than the actual duration of the clip.
Status	MOS status: matches the NCS status. Includes READY/NOT READY, PLAYED, etc.
Category	The category assigned to the clip; you can assign categories based on the editor to receive the assignment, for instance.
Type	The type of story or sequence an editor needs to create: Voice Over (VO), Sound on Tape (SOT), or other types set in SDB Server Options.
Description	Brief description of the clip an editor needs to create.
Clip ID	The clip ID, which is automatically defined when the placeholder is created.
Date	The date the placeholder was created.

Column	Description
P (Protected)	Protected status; displays P if the clip is protected, which prevents it from being erased or deleted from the database. Column is blank if the clip is unprotected.

Related Topics

Editing and GV STRATUS Rundown

Receiving Editing Assignments

Assignments automatically appear in your GV STRATUS Assignment List when they are sent from the producer or assigned from another editor.

Producers create those assignments as clip placeholders for use in an upcoming news broadcast. You can edit clips in EDIUS XS or Storyboard Editor, and link them to the placeholders in the Assignment List.

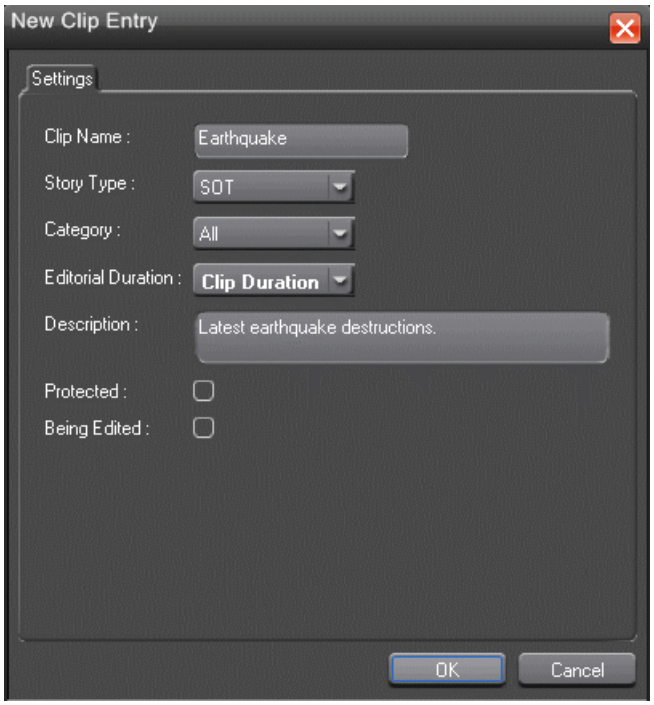
Additional features of Assignment List Manager

In addition to creating clips for assigned placeholders and sending them to the server for playback, there are other features of the Assignment List Manager that you can use.

Creating placeholders in Assignment List Manager

In addition to the assignments you receive from your producer, you can create additional placeholders for clips you want to include in a broadcast.

1. Click the **New Clip** button.



   The New Clip Entry window appears.

2. Enter a clip name.

   The placeholder name identifies the placeholder in your Assignment List Manager, the Assignment List Plug-in on the ENPS system, and the GV STRATUS Rundown playlist.

3. Optionally, enter additional information about the placeholder:

   - **Story Type**— If desired, specify whether this is a SOT (story on tape), VO (voice over), etc.
   - **Description** — Enter a description for the placeholder to help identify the clip you need to create.
   - **Category** — Select a category from the drop-down menu. The category determines who receives the placeholder as an assignment. Selecting **ALL** makes the placeholder accessible to all editors who select **ALL** in their Assignment List Manager.
   - **Editorial Duration** — If desired, enter an estimated duration for the story or select one from the drop-down list. The editor can also enter an editorial duration that is less than the clip length, which is sent back to the NCS for show timing.

     NOTE: Editorial Duration has the priority over media duration. Once an Editorial Duration is set; it will not be adjusted to clip duration, even after media is associated with the placeholder. The editor needs to set the final Editorial Duration before the clip is sent for playback.

   - **Protected** — Check this box to prevent the clip from being deleted from the database.
   - **Being Edited** — Check this box to show that the clip for a placeholder is being edited. This field allows editors to easily see that a clip is already being worked on in another edit room.

     NOTE: This field allows users to easily determine that a clip is already being worked on. When checked, these areas designate that the clip is Being Edited: the clip in the* GV STRATUS Rundown *playlist and in the Assignment List Manager changes color, and the text for the clip in the standalone Assignment List Manager changes color.

4. Click **OK**.

The Clip ID and Date are automatically set when you create the placeholder.

Related Topics

Additional features of Assignment List Manager on page 1558

Deleting placeholders in Assignment List Manager

If you need to, you can delete placeholders from the Assignment List Manager.

However, deleting items using the Assignment List Manager only deletes the placeholder, not the corresponding media. For this reason, you should only delete empty placeholders from the Assignment List Manager and use GV STRATUS ActiveX plug-in to delete clips.

- Select the placeholder that you want to delete and click the **Delete** button.

  The placeholder is deleted from the Assignment List Manager.

Related Topics

Additional features of Assignment List Manager on page 1558

Changing clip category in Assignment List Manager

If you need to, you can change a clip or placeholder category in the Assignment List Manager.

1. In the Clips window, double-click on the placeholder you want to assign.
2. Select a new editor, workstation name, or other category from the **Category** list.

3. Click **OK**.

The placeholder appears on the edit workstation when that particular category is selected.

Related Topics

Additional features of Assignment List Manager on page 1558

Viewing by category in the Assignment List Manager

In the Assignment List Manager, you can choose to view assignments within a selected category or all of the assignments in the list.

- Select a category from the **Category** drop-down list.

The list displays only the placeholders and clips in that category.

Select **All** to view all assignment placeholders again.

Related Topics

Additional features of Assignment List Manager on page 1558

Identifying missing clips

In the Assignment List Manager, you can filter the list of clips to show only missing clips.

- Click the **Missing Clips Only** button.
  Only placeholders with missing clips will be shown on the Assignment List Manager.

Click the button again to show the entire clip list.

NOTE: If you are using the Rundown View, you can further filter the list by selecting only the rundown you want to view.

Related Topics

Additional features of Assignment List Manager on page 1558

Using the GV STRATUS application in GV STRATUS Rundown

You can launch GV STRATUS in an ActiveX window within the GV STRATUS Rundown application. This allows you to use all GV STRATUS application tools and GV STRATUS Rundown to consolidate your entire operation including playback into one workspace.

With GV STRATUS within the GV STRATUS Rundown application, you can easily drag clips from Asset List into GV STRATUS Rundown's playlist. In addition, the Assignment List lets you create a placeholder for a clip and link it into the accompanying story in the NCS rundown. You can also assign channels for clips via the NCS for playout. For more information regarding GV STRATUS tools, refer to the *GV STRATUS Topic Library*.

Related Topics

Editing and GV STRATUS Rundown

Overview of GV STRATUS Rundown on page 1495

Logging on to the GV STRATUS application

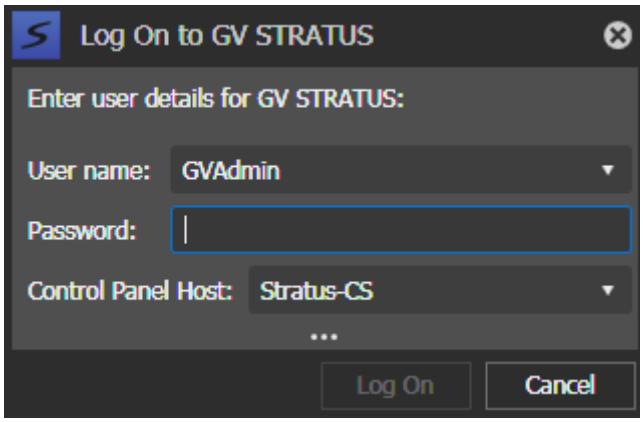
When you log on to the GV STRATUS system, the GV STRATUS application assigns GV STRATUS licenses and roles based on your user account credentials, as set by the system administrator in the GV STRATUS Control Panel application. If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins and assets that are part of your workflow. If GV STRATUS metadata access control is enforced, your credentials must give you adequate permissions

on metadata fields that are part of your workflow. Your credentials must also give you access to all your K2 systems.

1. From the Windows desktop, do the following:

   - Click **Start | All Programs | Grass Valley | GV STRATUS Rundown**

   A **GV STRATUS** Log On dialog box opens.



2. Enter your user name.

   If you use domain credentials, enter in format `<domain>\<username>`. For example, if your domain is "gv" and your username is "GVuser", enter `gv\GVuser`.

   If you have successfully logged on before, select your user name from the drop-down list.

3. Enter your password.
4. Verify that the application is correctly referencing the Control Panel Services Host as follows:
   a) If not already showing, click the **Options** button ... to show settings.
   b) Verify or enter the hostname (do not enter the IP address) of the GV STRATUS server with the SiteConfig role of GV STRATUS Control Panel Service. This is the Control Panel Services Host. In most systems this is the main GV STRATUS Core server.

      If you have successfully logged on before, your hostname is automatically populated. You can select a hostname from the drop-down list if you have previously logged on to multiple hosts in your operation.

5. Click **Log On**.

The GV STRATUS Rundown application opens.

To launch the GV STRATUS Plug-in within GV STRATUS Rundown, click **View** and select **GV STRATUS**.

GV STRATUS features are enabled according to the roles associated with your log on credentials.

When you log on to the application, the settings you make on one PC are available on other PCs when using the same user credentials, including the following:

- Settings from the User Preferences dialog box
- Workspaces
- Channel Panel configurations and Salvos
- Searches

Inserting placeholders from GV STRATUS

You can create placeholders in the GV STRATUS ActiveX plugin and insert them automatically into the playlist or any channels of GV STRATUS Rundown.

1. Select a placeholder from the Assignment List panel in the GV STRATUS ActiveX workspace.
2. Drag and drop the placeholder into GV STRATUS Rundown's playlist or channel.

   The placeholder appears in the playlist or channel.

Inserting clips from GV STRATUS

You can insert clips from the GV STRATUS ActiveX plugin into an out of rotation channel of GV STRATUS Rundown.

1. Select a clip from any bin in the Asset List panel of the GV STRATUS ActiveX workspace.
2. Drag and drop the clip into an out of rotation channel of GV STRATUS Rundown.

   The clip appears in the out of rotation channel.

3. Click **Play** to play the clip.

   You can also use other controls to manage the clip playback on the channel.

Linking clips automatically from GV STRATUS

- If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins, assets, and metadata.
- In order to link to a placeholder, you must be assigned with the **Rename Asset Rights** role and write permission for the **Name** property in Metadata section of GV STRATUS Control Panel.

You can automatically create placeholders and link them when you drag and drop assets into the playlist.

1. Create a new playlist in the GV STRATUS Rundown application.
2. Select a clip from the Asset List in the GV STRATUS ActiveX Plug-in.
3. Drag and drop the clip into GV STRATUS Rundown's playlist.

   The clip is linked to a placeholder that is automatically generated in the Assignment List of GV STRATUS ActiveX Plug-in.

4. Click **Save** to save the playlist.

Playing clips to air

Playing Clips to Air

Playback operators use the GV STRATUS Rundown application to control the playback of news clips to air.

Using a playlist linked to an NCS rundown or the local GV STRATUS Rundown playlist, playback operators cue and play clips as required during a broadcast.

The Clip Browser, Rundowns, and Playlist Overview are all dockable; you can rearrange windows or close windows you aren't using (such as unused channels). The channel windows are not dockable, but each can be opened or closed.

To restore a window you have closed, choose the name of the window from the View menu. To restore all windows to their default locations, choose **Tools | Reset Windows**.

With the integration of GV STRATUS ActiveX Plugin, you can preview a clip prior to air using the Source Viewer and view metadata properties that had been created for the clip.

About GV STRATUS Rundown Toolbar

The GV STRATUS Rundown Toolbar lets you access common features.

Icon	Function	Other Ways to Access...
	Creates a blank playlist.	File | New Playlist or Ctrl + N
	Opens a saved local (.pls) playlist.	File | Open Playlist orCtrl + O

Icon	Function	Other Ways to Access...
	Saves the current playlist as a local (.pls) playlist.	File | Save Playlist orCtrl + S
	Cuts selected clips from the playlist to the clipboard.	Edit | Cut or Ctrl + X
	Copies selected clips from the playlist to the clipboard.	Edit | Copy or Ctrl + C
	Pastes clips from the clipboard into the playlist.	Edit | Paste or Ctrl + V
	Opens the Clip Browser, so you can add clips to the playlist.	Ctrl + I
	Cues all channels specified in the automatic channel assignment starting with the currently selected story.	
	Plays the next clip in the playlist.	Spacebar (if enabled) and external GPI
	Stops playing all clips.	
	Puts the GV STRATUS Rundown application into Archive Play mode, which lets you archive stories to tape.	
	Re-syncs the GV STRATUS Rundown playlist with the NCS when sync has been broken with the NCS rundown, such as by reordering stories.	

About the Playlist

The playlist lists each clip and its properties.

You can rearrange the order of the columns in the playlist by dragging the title of the column to a new location. To restore all columns to their default position, choose **Tools | Reset Playlist Columns**.

You can also resize the columns by dragging to expand or shrink the column name.

Column	Description
Thumb	Displays a video thumbnail of the clip, if available. To change the thumbnail size, click the Thumb column heading or select View | (Small) or (Large) Thumbnail.A red border appears around a blank thumbnail if the clip is not ready for playback.
Clip Name	Displays the name of the clip. A scissors icon appears next to a clip that has been trimmed.
Duration	Displays the full duration of the media, not the editorial duration.
Hit Time	Counts up the relative time that the clip plays from when the Reset button was pressed, which is usually when a show starts.

Column	Description
Status	Displays the available channels and the status of the clip: [Not Ready] — The clip is not ready to play. [Ready] — The clip is ready to play. [Blank] — Clip has not yet been cued. [Cued] — The clip is cued to a specific channel and is ready to play. [Roll] — The clip is playing to air. [Stopped] — The clip has been manually stopped during play. [Played] — The clip has finished playing.
Channel	Displays the channel in which a clip is currently cued or playing.
Assign	Displays the channel assigned through the NCS or GV STRATUS Rundown. Allows you to assign a clip to a channel, overriding automatic channel assignment.
Page	Corresponds to the page of the NCS rundown. This column is blank if you are not using ENPS or Octopus with GV STRATUS Rundown or if the producer did not select Freeze Page Numbers for the rundown properties in ENPS.
Story Slug	Displays the name of the story from the NCS rundown.
ID	Displays the clip ID, which is automatically set when you create the placeholder.
Description	Displays any descriptive text entered in placeholder properties.

Understanding Playlist colors

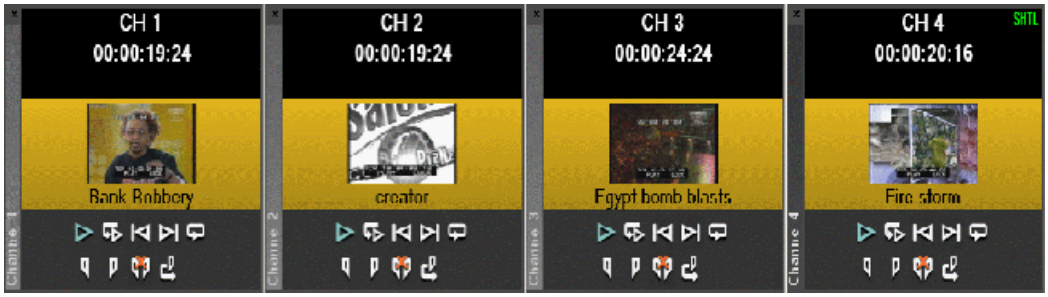
Each playlist entry appears in a color that identifies its status in GV STRATUS Rundown:

Row Background Color	Description
Yellow	The clip is cued for playback.
Green	The clip is playing.
Orange	The clip is stopped during play.
Gray	The clip is in post roll.

1. Select **Tools | Options**.
2. Click on the **Color** tab.
3. Click the row color box that you want to change and select a new color.

About Playout channels

The channel area displays all channels available on your system.



You can perform the following functions for each channel.

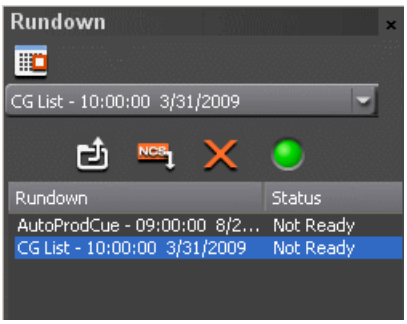
Icon	Function
	Plays the current clip in the channel. If a clip is playing, clicking this button pauses the clip; click it again to resume playback.
	Recues the current clip.
	Cues the previous clip in the channel.
	Cues the next available clip.
	Loops playback for the current clip.
	Sets a Mark In point to begin trimming the clip. A Scissors icon appears next to the clip name in the playlist to indicate a trimmed clip.
	Sets a Mark Out point to end trimming the clip.
	Clears both the Mark In and Mark Out points from the clip.

Icon	Function
	Previews the last few seconds of the clip and immediately recues. (The number of seconds that previews is set under Options and determined by your studio's needs.)

This symbol indicates that a GV STRATUS Rundown channel is no longer connected to its corresponding channel on the media server.

About Rundowns

The rundown area displays the open rundowns and their status, a list of available rundowns, server status, and control buttons.



You can open up to five rundowns at once; all open rundowns merge into a composite playlist, allowing seamless control of back-to-back rundowns.

Clicking **Date** toggles a calendar which lets you filter the display of rundowns to a specific date.

Selecting a rundown from the rundowns list selects all clips in that rundown in the playlist area.

Icon	Function
	Opens the selected rundown and creates a playlist.
	Appends the selected rundown to the end of the current playlist.
	Removes the selected rundown from the playlist.

Icon	Function
	Indicates the connection status between GV STRATUS Rundown and the XMOS Server; green indicates a successful connection.

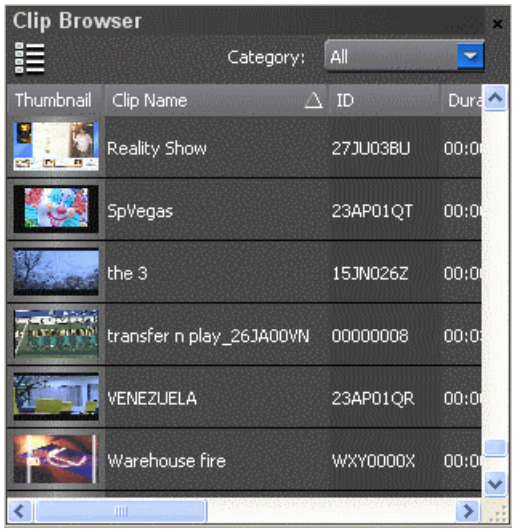
The status displays READY when the “MOS Ready to Air” property is enabled for a rundown through ENPS or Octopus. The Status column is not used with iNEWS; the column can be resized off of the screen if desired.

About the Clip Browser

Clip Browser displays thumbnails and information of clips and placeholders from GV STRATUS Rundown database, allowing you to easily add them to your playlist.

If the Clip Browser window is not open, click **Clip Browser button** from the toolbar.

The Clip Browser opens, displaying clips and placeholders from GV STRATUS Rundown database. Dragging a clip from the Clip Browser window and dropping it on the Playlist window appends the clip to the playlist.



You can add clips that are ready or empty placeholders to which media will be sent later.

To filter display items on the Clip Browser window, you can select a specific category from the category dropdown list. Select All to view all clips and placeholders again.

To toggle the thumbnail size on Clip Browser window, you can click on the Toggle Thumbnail View button .

The Clip Browser also consists of clip and placeholder information as described below:

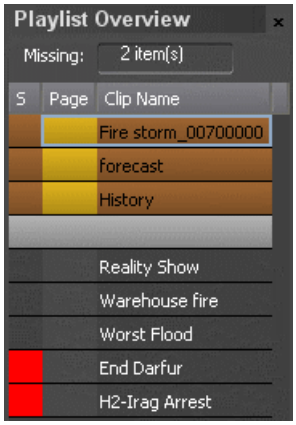
Column	Description
Thumbnail	Displays a video thumbnail of the clip, if available. A red border appears around a blank thumbnail if the clip is not ready for playback.To change the thumbnail size, click the Toggle Thumbnail View button.
Clip Name	Displays the name of the clip.
ID	Displays the clip ID, which is automatically set when you create the placeholder.
Duration	Displays the full duration of the media, not the editorial duration.
In Use	Displays a check sign if the clip is appended manually to the playlist.
Category	Displays the category assigned to the placeholder.
Type	Displays the story type of placeholder that had been created: Sound on Tape (SOT), Voice Over (VO), or other types set in in the SDB Server options.
Date	Displays the date the placeholder was created.
Description	Displays any descriptive text entered in placeholder properties.

You have several ways to search for clips and placeholders in Clip Browser. The most common way is to scroll down through the window to find the placeholder that you need. You can also get to a specific placeholder by entering the first few characters of the placeholder name.

- Click on one of the placeholders in the Clip Browser window and scroll down to search for other placeholders.
- Use the up and down arrow keys on your keyboard to navigate through the list.
- To search for a specific placeholder, type the first character and the active bar will automatically go to a placeholder that starts with that character. If you type a second character within 1 second of the first character, the active bar will go to a placeholder that starts with those 2 characters. If you enter the same character repeatedly, the active bar will navigate through all placeholders that start with that character.

About the Playlist overview

The playlist overview displays a subset of the playlist columns, allowing you to scroll to other parts of the playlist without disrupting the view in the main playlist window.



The Playlist Overview window shows clip's status, page and clip name.

Column	Description
Status	Displays the status color of the clip: Black — The clip has not yet been cued. Yellow (Cued) — Clip is cued to a specific channel and is ready to play. Green (Roll) — The clip is playing to air. Gray (Played) — The clip has finished playing. Orange (Stopped) — The clip has been manually stopped during play. Red Square — Clip not ready for playback.
Page	Corresponds to the page of the ENPS or Octopus rundown. This column is blank if you are not using ENPS or Octopus with GV STRATUS Rundown or if your Producer didn't choose the **Freeze Page Numbers** option in ENPS.
Clip Name	Displays the clip name.

Creating a Playlist

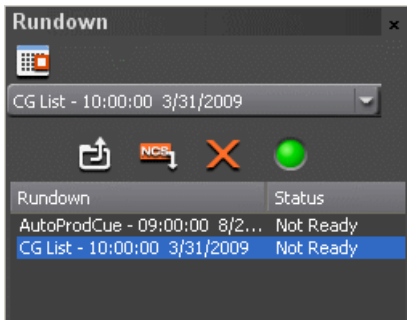
You need to create a playlist before you can play clips to air.

- By opening a rundown that you created in a newsroom computer system
- By manually creating a playlist in GV STRATUS Rundown

Opening an NCS Rundown

If you use a newsroom computer system such as ENPS, iNEWS, Octopus, OpenMedia, or NIS5 to create news rundowns, you can open those rundowns in GV STRATUS Rundown.

- Select a rundown from the drop-down list and click the **Open Rundown** button.



The rundown opens in the GV STRATUS Rundown application, displays all clips in the rundown, and cues clips to channels if **Auto Cue on Loading Rundown** is enabled. The playlist displays a headframe for each clip; while a red border and blank thumbnail appear for clips that are not yet ready for playback.

Appending rundowns to a playlist

With GV STRATUS Rundown and your NCS, you can add rundowns to create a playlist that includes all of the clips and other information from each of the rundowns. Appended rundowns are added to the end of the current playlist.

1. Select the rundown from the drop-down list.
2. Click the **Append Rundown button** .

The rundown is added to the end of the current Playlist, displays in the Playlist Overview, and the rundown name is added to the Rundown list.

NOTE: You can open up to five rundowns in the playlist at a time.

Removing rundowns from a Playlist

If you don't need a certain rundown anymore, you can remove the rundown from the playlist.

1. Select the rundown to remove from the rundown list window.
2. Click the **Close Rundown button** .

The rundown is removed from the playlist.

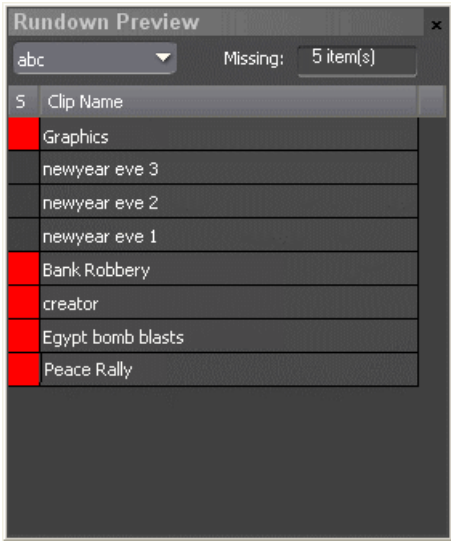
Previewing other rundowns

If you need to look at another rundown, you can open it without disrupting the current GV STRATUS Rundown playlist.

1. Select **View | Rundown Preview** or press **Ctrl + R** on the keyboard.
   The Rundown Preview window appears.
2. Select a rundown from the Rundown drop-down list.

   The Rundown Preview window displays all placeholders and completed clips for the rundown.

   A red square in the status column indicates that the clip is not complete. You can also see at a glance how many clips are missing.



3. Select other rundowns from the drop-down list if you wish to preview other rundowns.
4. Click the **X** icon on top right of the window if you want to close the Rundown Preview window.

Creating a new playlist manually

Another way to create a playlist is manually using GV STRATUS Rundown.

1. Click the **New Playlist** button in the main toolbar.
   An empty playlist appears.

2. If the Clip Browser isn't open, click the **Clip Browser** button .

   The Clip Browser opens, displaying all available clips and placeholders from the GV STRATUS Rundown database.

3. Drag a clip into the Playlist window or the Playlist Overview window.

   The clip appears in the main playlist window.

4. Continue adding clips to the playlist as necessary.

   Dragging a clip from the Clip Browser window and dropping it onto the horizontal scroll bar at the bottom of the Playlist window appends the clip to the end of the playlist.

You can add clips that are ready or empty placeholders to which media will be sent later.

Saving local playlists

You can save a playlist if you need to re-use it in a later broadcast.

For example, you could create a playlist for a 6 PM broadcast and then modify it for the 10 PM broadcast.

1. When you are done adding clips, click the **Save** button on the main toolbar.
2. Select a location for the playlist and enter a file name.
3. Click **Save**.

The playlist is saved with a .pls extension.

To save a playlist with a different name, select **File | Save As**, enter a new filename, and click **Save**.

You can also save an NCS rundown as a local playlist. This creates a "snapshot" of the current state of the rundown. If the rundown is then changed on the NCS and you need to revert to the previous version, you can open the local .pls version.

Opening saved Playlists

You can open a saved playlist and re-use it if needed.

1. Click the **Open Playlist button** on the main toolbar.
2. Select a playlist and click **Open**.

The playlist opens and displays the list of clips it contains.

You can modify, review, or play the playlist to air.

Appending a Playlist

If you want to add another local playlist, you can append one to the current playlist in GV STRATUS Rundown.

1. Select **Append Playlist** from the File menu.

   The Open window appears.

2. Select the playlist you want to append by browsing to a .pls file, and click **Open**.

The playlist appends to the end of the open playlist in GV STRATUS Rundown.

Exporting a Playlist

You can also export a playlist, open it in a text editor or spreadsheet program, and then print it.

1. Select **Export Playlist** from the File menu.
   The Save As window appears.
2. Enter a name for the playlist and click **Export**.

The playlist is saved as a .TXT file.

You can import the .TXT file into a spreadsheet program that supports comma delimited format and it sorts the playlist data into columns.

Chaining Clips in a Playlist

Sometimes you may want to group two or more clips together so the clips play back-to-back as one continuous clip. This grouping is called chaining, and provides the advantage of playing clips in succession without having to cue and play each one individually.

You can also chain clips through your NCS through the Auto-Chain feature by setting up your system so that any two or more consecutive clips assigned to the same channel will chain automatically.

1. Select the clips you want to chain by clicking on one clip and holding down the Shift key while selecting the other clip(s).
2. Right-click on one of the selected clips and select **Chain Clips**.

The clips are now chained together, indicated by a blue rectangle around the clips.

Cueing Clips

Once you have a playlist, you can cue the clips to the appropriate channels and play them to air.

The playlist automatically cues the first clip if the Auto Cue on Loading Rundown option is on, and cues subsequent clips when prior clips have played. If a clip isn't ready for playback, the clip is skipped and the next available clip cues. You can also cue clips manually.

- Select the clip that you want to cue and click the **Cue All** button on the toolbar.
  All channels are cued as specified in the automatic channel assignment, starting with the selected clip.
- Manually cue a clip by dragging it to the target channel.

- In the channel window, click one of the following buttons:
  - **Recue Current Clip** — Resets the current clip in the channel back to the beginning; the clip is ready to play.
  - **Cue Previous Clip** — Cues the previous clip assigned to the particular channel; if no channel assignment is specified, GV STRATUS Rundown cues the first previously available clip.
  - **Cue Next Clip** — Cues the next clip assigned to the particular channel; if no channel assignment is specified, GV STRATUS Rundown cues the next available clip.
  - **Turn Loop Playback On/Off** — When on, continuously loops the currently playing clip. To turn loop playback off, click this button again.
  - **Set Mark In** — Marks the starting point of the trimming of the clip.
  - **Set Mark Out** — Marks the ending point of the trimming of the clip.
  - **Clear Marks** — Clears all the trim marks on the clip.
  - **Out Cue Preview** — Automatically plays the last few seconds of the clip and immediately recues. (The number of seconds that is previewed is determined by your studio's needs).

Using the Jog feature

If you need to change the start position of a cued clip, you can jog to the desired frame.

- Use the left and right arrow keys to step through 1 frame at a time.
- Use Ctrl + the arrow keys to step through 10 frames at a time.
- Use Shift + the arrow keys to step through 1 second at a time.

  If desired, you may display trim controls by selecting **View | Channel Edit Controls** and setting a new starting point with the Mark In button.

When you play the clip, the clip starts at the new position.

NOTE: The X-keys jog/shuttle controller can be used as an alternative to jogging via the keyboard and also allows shuttling of the clip.

Playing clips

During a news broadcast, you play clips either according to the script or when the director signals you. If not already cued, cue the clip to the desired channel. To cue a clip, drag and drop it into a channel window.

- Click the **Play** button in the channel window.

The Play button is a toggle and changes to **Stop** when clicked; to stop a clip during play, click the **Stop** icon to pause it. Click **Play** to resume playing the clip.

You can also play the next clip in the playlist by clicking the **Play Next** button on the GV STRATUS Rundown toolbar.

For ease of operation, you can control clips in the playlist using GPI inputs, X-keys and keyboard function keys.

Archiving Clips

The Archive Play feature allows you to automatically play all clips in a playlist on a selected channel and record the output of that channel on a VTR.

To configure Archive Play, you must select the archive channel from the Archive Play configuration tab. You can also change the Archive Black duration on that tab; GV STRATUS Rundown rolls five seconds of black between each archived clip by default. You need to create a black clip if you don't have one.

1. Click the **Archive Play** button to enable Archive Play.

   A message indicating successful connection to the VTR appears.

2. Cue a clip to the archive channel.

   Select the first clip and click the **Cue All** button on the toolbar.

   NOTE: If you are archiving clips to a VTR, the first clip cued is the BLACK file.

3. Click the **Play** button in the channel window.

   GV STRATUS Rundown starts the VTR deck recording and a message indicating play has started appears.

After all clips have played, the VTR deck stops recording and Archive Play mode automatically turns off.

You can use the Run Time counter to determine if you have enough room on the VTR tape to record all of the clips in a rundown for archiving.

In Archive Play mode, Run Time displays as current hit time/total run time, including black clip duration. You can also clear the Run Time counter by clicking the **Reset Counter** button.

GV STRATUS Rundown logs "as run" data in a comma-delimited log file (C:\GV STRATUS Rundown\Log\ArchivePlay.log). Each line includes the Date, Time (start time to the nearest second), VTR Tape Time Code, Rundown Name, Clip Name, Clip ID, and Duration. You can use log data to determine where a specific story starts.

Each time you enable Archive Play, you can choose whether to clear the existing log file or append the new data.

Recording a black clip for Archive Play

To archive clips, you need to create a file called "**BLACK**" that contains black video.

NOTE: The file BLACK needs to be in the bin used for playout of clips (normally V:/default bin) in order to work properly.

- Using media server:
  a) Pull the input source (make sure you don't have a video feed on this source).
  b) Create a new clip and name it **BLACK**.
  c) Record for approximately 10 seconds.
  d) Eject **BLACK** from the record channel.

Customizing playlist for broadcast

In addition to cueing and playing clips, there are many other features of GV STRATUS Rundown that let you customize a playlist for your broadcast.

Rearranging the Playlist layout

You can change the order of the displayed playlist columns by dragging a column heading to the left or right.

The Thumb column is always the first column in the playlist; you can't move it or move another column in front of it.

- Select **Tools | Reset Playlist Columns**.

Viewing clip properties

You can view the properties of a clip in the playlist at any time.

The clip properties window displays the clip story type, category, and editorial duration, which are not shown in the playlist.

1. Double-click the clip in the Playlist Window.

   The Clip Properties window appears.

2. Click **OK** to close the window.

Assigning clips to channels

If you don't specify a specific channel for a clip, the system automatically assigns it to the next available channel. Channels can be set to be in rotation when you configure your Playout channels.

- Right-click on a clip in the playlist and select **Assign to "X".**

  New channel assignment appears on the Assign column.

> For instance, you may have a small clip that you want to play in between two longer clips to create a smooth transition. So, you can assign the small clip to a specific channel.
>
> ***NOTE: If you are using an NCS, you should assign channels through the NCS instead of using this method.***

You can remove the clip assignment by right-click on the clip and select **Unassign Clip**.

All clips that are unassigned to specific channels will be cued to any channels in rotation, while a clip that is assigned to a specific channel will only be cued to that channel regardless of the current rotation status.

Rearranging clips in a Playlist

You can rearrange clips in the playlist of GV STRATUS Rundown.

However, doing so breaks the link between GV STRATUS Rundown and the NCS rundown. Therefore, you won't see any subsequent changes made to the NCS rundown. For this reason, you should reorder the rundown through the NCS when possible.

If you created a playlist manually, you can rearrange clips as necessary.

To rearrange clips, you can use one of the following methods:

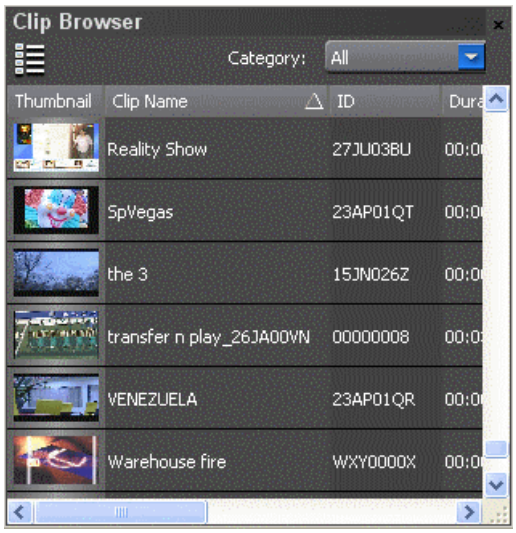
- Using the toolbar icons or keyboard shortcuts, you can cut (**Ctrl + X**), copy (**Ctrl + C**), and paste (**Ctrl + V**) clips in any order in the playlist.
- You can also just drag clips to another position in the playlist.

Adding new clips to a playlist

Occasionally, you may need to add a news clip directly to the playlist if you aren't able to add it to the NCS rundown first.

However, doing so breaks the link between GV STRATUS Rundown and the NCS rundown, and the Sync button on the toolbar flashes to indicate that the playlist is not synced anymore. In that case, you won't see any subsequent changes made to the NCS rundown.

1. If the Clip Browser isn't open, click the **Clip Browser button** .



   The Clip Browser appears, displaying all available clips.

2. Drag a clip into the Playlist window. To append the clip to the bottom of the playlist, drag the clip onto the scroll bar at the bottom of the playlist window.

   The clip appears in the Playlist window and the Playlist Overview window.

3. Continue adding clips to the playlist as necessary.

To re-link the GV STRATUS Rundown playlist with the NCS rundown, click the flashing Sync rundown icon on the GV STRATUS Rundown toolbar. You will be prompted to save changes as a local playlist before re-syncing.

Using the context-sensitive playlist menu

Several GV STRATUS Rundown features are available by right-clicking in the Playlist window.

Menu Item	Description
Assign to channel_name	Assigns the selected clip to channel_name for playback. Choose **Tools | Options | Channel Configuration** to change channel names; you may configure up to six channels.
Unassign Clip(s)	Removes the channel assignment from the selected clip(s).
Mark Played	Marks the currently selected clip(s) as played.
Unmark Played	Removes the played status from the currently selected clips.
Unmark All Played	Removes the played status from all clips marked played.

Menu Item	Description
Chain Clips	Chains two or more selected clips together for continuous playback.
Unchain Clips	Unchains the selected clips.
View Asset	Displays the low-resolution proxy of the selected clip.
View Properties	Displays the properties of a selected clip.

GV STRATUS Rundown Appendix

Sample of MOS Gateway configuration file

NOTE: Due to the book's margin requirements, some wrapping of the text may occur in the following sample file that should not appear in the actual file.

For use with GV STRATUS Rundown, the iNEWS mosconfig.xml file should be configured as follows:

```
<?xml version="1.0" encoding="UTF-16" standalone="no"?>

<!-- This file contains configuration settings for the iNEWS MOS Gateway.
 xmlns="http://www.
inewsroom.com/mosgateway"-->

<!-- It is in an XML-based format, with the root element being
mosGatewayConfiguration. -->

<mosGatewayConfiguration
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespace
SchemaLocation="mosconfig.xsd">

<!-- The logging element specifies the directory in which to put log files,
 -->

<!-- the maximum number of log files to create, and how big each one can
 grow. -->

<logging>
    <directory>C:\Program Files\Avid\MOSGateway\Logs</directory>
    <maxFileCount>1</maxFileCount>
    <maxFileBytes>10000000</maxFileBytes>
   <!-- YES/NO Also sends all logging to OutputDebugString so any Windows
 debugger will see it. -->
    <winDebugTrace>NO</winDebugTrace>
    <!-- on/off Sends all incoming socket traffic to seperate log files.
 -->
    <socket>off</socket>
</logging>

<!-- -->

<!-- The tcpPorts element specifies the TCP ports on which the MOS Gateway
 listens for -->
```

```
<!-- MOS connections. Every MOS that connects to the MOS Gateway must use
 the same ports. -->

<tcpPorts>
    <out_upper>10541</out_upper>
    <out_lower>10540</out_lower>
    <in_upper>10541</in_upper>
    <in_lower>10540</in_lower>
</tcpPorts>

<!-- -->

<!-- Newsroom system info -->

<ncs>
    <!-- -->
    <!-- The ncsID used for replication-->
    <ncsID>WXYZ</ncsID>
    <!-- -->
    <!-- NCS's Host Name -->
    <!-- Make sure this is resolvable -->
    <host>WXYZ</host>
    <!-- -->
    <!-- Allow or Disallow Replication -->
    <!-- YES/NO -->
    <!-- default is YES -->
    <AllowReplication>NO</AllowReplication>
    <!-- -->
    <!-- This is the NCS username that the replication service logs into
 the ncs with. -->
    <!-- default is mosrep -->
    <ReplicationUsername>mosrep</ReplicationUsername>
    <!-- -->
    <!-- This is the password the ReplicationUsername uses to log into
the ncs. -->
    <!-- default is mosrep -->
    <ReplicationPassword>mosrep</ReplicationPassword>
    <!-- -->
    <!-- Allow or Disallow mosItemReplace -->
    <!-- YES/NO -->
    <!-- default is YES -->
    <AllowMosItemReplace>YES</AllowMosItemReplace>
</ncs>

<!-- -->
<!-- The listDevices element contains device-specific configurations. It
 contains -->
<!-- one or more mosDevice elements. The mosDevice element contains
configuration -->
<!-- settings that are specific to a particular MOS. -->

  <listDevices>

     <mosDevice>
        <!-- The names element contains the mapping of the MOS's mosID
value to -->
       <!-- an NRCS device name, as well as the network name of the MOS.
 -->
            <names>
                <mos>GVMOS</mos>
```

```
                <amcp>playout</amcp>
                <network>sdbserver1</network>
            </names>

            <roChannels>
                <roChannel>
                    <iNewsChannel>A</iNewsChannel>
                    <MosDevChannel>A</MosDevChannel>
                </roChannel>

                <roChannel>
                    <iNewsChannel>B</iNewsChannel>
                    <MosDevChannel>B</MosDevChannel>
                </roChannel>

                <roChannel>
                    <iNewsChannel>C</iNewsChannel>
                    <MosDevChannel>C</MosDevChannel>
                </roChannel>

                <roChannel>
                    <iNewsChannel>D</iNewsChannel>
                    <MosDevChannel>D</MosDevChannel>
                </roChannel>

                <roChannel>
                    <iNewsChannel>E</iNewsChannel>
                    <MosDevChannel>E</MosDevChannel>
                </roChannel>
            </roChannels>

            <handlesRoStorySend>YES</handlesRoStorySend>

            <!-- -->
            <!-- The handlesEmptyStories element specifies whether this
device accepts -->
            <!-- a roStoryInsert message that contains no item. -->

            <handlesEmptyStories>NO</handlesEmptyStories>

            <!-- -->
           <!-- The handlesRoStoryMoveMultiple element specifies whether
 this device supports -->
            <!-- the roStoryMoveMultiple message. The router defaults to
 YES. -->
            <!-- Valid settings are YES or NO -->

            <handlesRoStoryMoveMultiple>NO</handlesRoStoryMoveMultiple>


            <!-- -->
           <!-- The handlesRoItemLevelCommands element specifies whether
 this device supports -->
           <!-- roItemInsert, roItemDelete and roItemReplace. The router
 defaults to YES. -->
            <!-- Valid settings are YES or NO -->

            <handlesRoItemLevelCommands>NO</handlesRoItemLevelCommands>

            <!-- -->
```

```
            <!-- the sendRoCreateOnStartLoad element specifies whether
the rundown is created -->
            <!-- by sending a blank roCreate command to the MOS device
then add each story -->
            <!-- separately (YES) or whether one large roCreate message
will be sent with the -->
            <!-- entire rundown (NO). The default is YES. -->

            <sendRoCreateOnStartLoad>NO</sendRoCreateOnStartLoad>

            <!-- -->
           <!-- The statusTranslations element defines the status strings
 that correspond -->
            <!-- to the various NRCS status codes. This allows the MOS
Gateway to translate -->
          <!-- the roItemStatus messages received from a MOS into status
 codes that NRCS -->
            <!-- can recognize and display. -->

            <statusTranslations>
                <statusUnavailable>NOT READY</statusUnavailable>
                <statusCueing>CUEING</statusCueing>
                <statusAvailable>READY</statusAvailable>
                <statusCued>STAND BY</statusCued>
                <statusPlaying>PLAY</statusPlaying>
                <statusPaused>STOPPED</statusPaused>
                <statusStopped>END</statusStopped>
            </statusTranslations>

            <mosObjReplication>
                <trigger>manual</trigger>
                <replicationTime>12:31:15 PM</replicationTime>
                <clearQueue>false</clearQueue>
                <path>clips.gvg</path>
            </mosObjReplication>

        </mosDevice>

    </listDevices>

</mosGatewayConfiguration>
```

GV STRATUS VTR Ingest Operation

Configuring GV STRATUS VTR Ingest

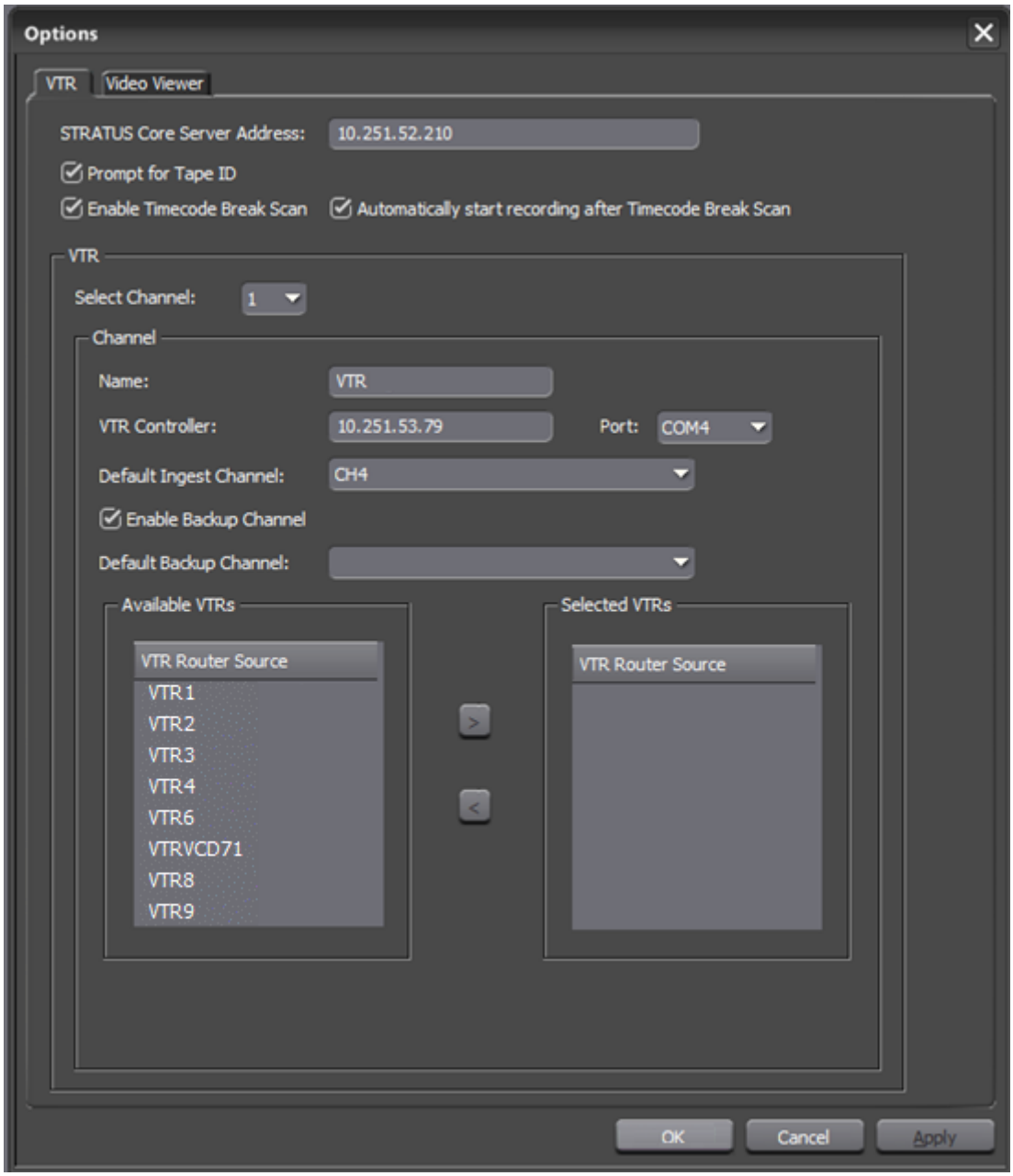
Configuring GV STRATUS VTR Ingest application

You need to configure the GV STRATUS VTR Ingest application before using it.

- STRATUS-VTR-ING license must be installed on the GV STRATUS Core server.

Make sure you have already configured the GV STRATUS VTR Controller application before completing this section. The VTR information in these two applications needs to match.

1. In the GV STRATUS VTR Ingest application, select **Tools | Options**.



2. In the VTR tab, enter the IP address or the host name of the GV STRATUS Core Server in the **Stratus Core Server Address** field.
3. Select the **Prompt for Tape ID** box.

   This feature allows you to customize the identification of your tape. If you don't enter a tape ID, GV STRATUS VTR Ingest prompts you to enter the ID before you ingest the first clip.
4. Select **Enable the Timecode Break Scan** to allow you to scan and capture media from a tape according to timecode breaks.
5. If needed, you can select the option to automatically start recording after the Timecode Break Scan.

6. Select a channel from the drop-down list and enter the name of the channel.
7. Enter the IP address or name of the computer where GV STRATUS VTR Controller is installed. (If GV STRATUS VTR Controller is installed on the same machine, enter **localhost**.)
8. Select the COM Port from the drop-down list.
9. If you want to record to two different locations through GV STRATUS VTR Ingest, you can check the Enable Backup Channel box and select a channel from the Default Backup Channel drop-down list.

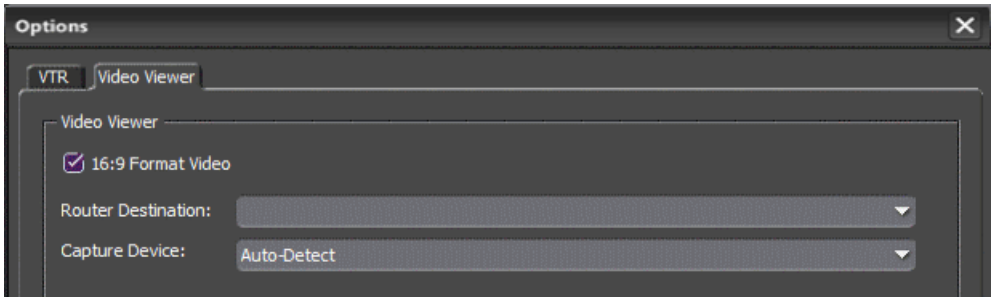
   NOTE: Once the option to enable backup channel is selected, a Backup channel drop-down list appears within GV STRATUS VTR Ingest channel windows. You can easily select other backup channels from the drop-down list if needed.

10. From the list of available VTRs, select the VTR router source.

    Once selected, the router source is displayed in the Selected VTR box.
11. To make the changes but keep the Options dialog box open, click **Apply**.
12. Proceed to configure video viewer in the Video Viewer tab.

    If you have the optional Hauppage WinTVGo video capture card or Blackmagic Design DeckLink video capture card installed in your GV STRATUS VTR Ingest machine, you will need to define the destination of the router connected (via digital to analog converters, if needed) to your video capture card.
13. In the Video Viewer tab, check the 16:9 format video if desired.

    The GV STRATUS VTR Ingest client displays video in the Video Viewer according to the primary format set in GV STRATUS Control Panel **Format** settings.
14. Select the router destination from the drop-down list. If no router has been configured, this field will be grayed out.



15. For the Capture Device drop-down list, select **No Capture Device** if you want to view the asset via a separate video monitor.
16. If you have installed a video capture card, select the device in the capture device drop-down list.
17. Click **OK** after you are done with the configuration.

The GV STRATUS VTR Ingest application is now ready for use.

Using GV STRATUS VTR Ingest

GV STRATUS VTR Ingest allows you to record footage from VTRs or feeds from a router directly to a media server in your newsroom.

With GV STRATUS VTR Ingest, you can select clips from multiple VTR tapes, create a batch (also known as a segment) list, and record it to the server. You can also export the segment list as an EDL and import it into an editing application.

With GV STRATUS integration, you can add and edit the description of a tape or clips in a batch list. The description that had been keyed-in will be searchable within the GV STRATUS application.

If GV STRATUS security is enforced, your credentials must give you adequate permissions. If permission is restricted, buttons, list items, and other controls can be disabled or hidden. Bins, assets, and metadata that do not have read permissions are not visible. Markers and segments permissions must be set to **Allow** in order to create, update, or delete markers and segments.

If GV STRATUS metadata access control is enforced, your credentials must give you adequate permissions. You can only view metadata with read permissions, and modify metadata with write permissions. If read or write permissions are denied, your metadata fields will be disabled.

Opening the GV STRATUS VTR Ingest application

- STRATUS-VTR-ING license must be installed on the GV STRATUS Core server.

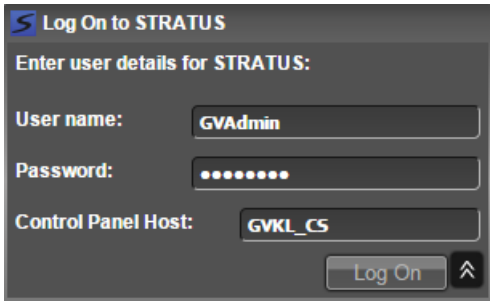
To authenticate with GV STRATUS security, you must log on to the GV STRATUS system when opening the GV STRATUS VTR Ingest application.

When you log on to the GV STRATUS system, the GV STRATUS application assigns GV STRATUS licenses and roles based on your user account credentials, as set by the system administrator in the GV STRATUS Control Panel application. If GV STRATUS security is enforced, your credentials must give you adequate permissions on bins and assets that are part of your workflow. If GV STRATUS metadata access control is enforced, your credentials must give you adequate permissions on metadata fields that are part of your workflow. Your credentials must also give you access to all your K2 systems.

1. From the Windows desktop, do the following:

   - Click **Start | All Programs | Grass Valley | GV STRATUS VTR Ingest**

   A **GV STRATUS** Log On dialog box opens.



2. Enter your user name.

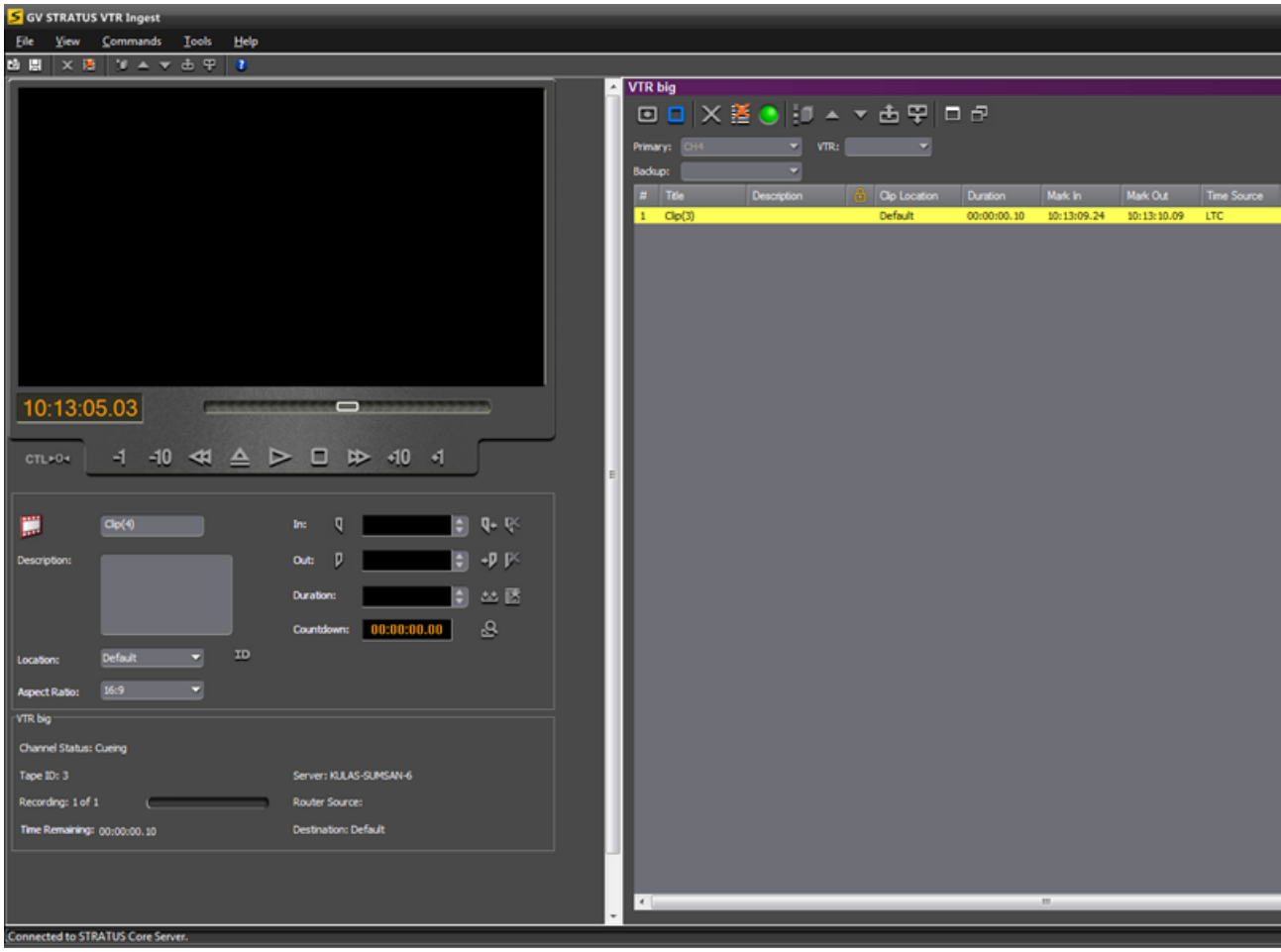
   If you use domain credentials, enter in format `<domain>\<username>`. For example, if your domain is "gv" and your username is "GVuser", enter `gv\GVuser`.

3. Enter your password.
4. Verify or enter the name of the Control Panel Host for the GV STRATUS Control Panel Service. In most systems, this is the main GV STRATUS Core server.
5. Click **Log On**.

The GV STRATUS VTR Ingest application opens.

Overview of the GV STRATUS VTR Ingest window

The GV STRATUS VTR Ingest window consists of one to eight channel windows, a viewing window, and a dynamic clip record area.



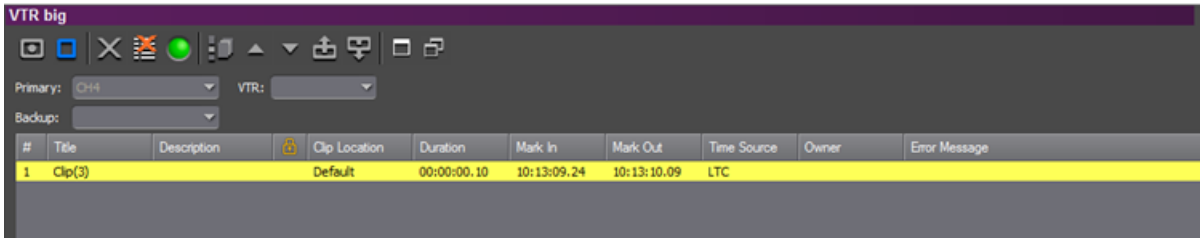
Overview of clip record area

The clip record area of GV STRATUS VTR Ingest window consists of a viewing window, VTR control buttons, clip details and recording status.

Users can also use buttons within the clip record area to add clips to a segment list, record handles, clear the tape ID, scan and ingest tapes with broken timecodes, add metadata to the clips and scan tapes to ingest segments.

Overview of channel window

The channel window on the GV STRATUS VTR Ingest user interface consists of channel lists, VTR source list, segment list buttons and list of clips to be ingested.



The Toolbar lets you perform common functions for recording clips.

Icon	Function
	Displays channel status—A green icon indicates status is OK; a red icon indicates a problem. Click on this icon to see status for the VTR.
	Deletes the selected clip(s).
	Clears the segment (batch) capture list.
	Organize the segment (batch) capture list firstly by tape IDs, and then by mark in points.
	Move up the selected clip in the capture list.
	Move down the selected clip in the capture list.
	Move segments within the same tape up in the capture list.
	Move segments within the same tape down in the capture list.
	Maximize display of the channel window.
	Restore the previous display of channel window.

Each channel window lists clips that need to ingested on that particular channel and details of each clip can be seen easily as they are arranged in columns.

Column	Description
Title	The name of the clip. The number of characters in a clip name is allowed to exceed 32 characters. For more info, refer to *Asset and bin name limitations* on page 1428.
Description	The content description of the clip.
Clip Location	The name of the folder where the clip resides in the media server.
	GV STRATUS Security: Indicates the asset or bin has restricted access.
Duration	The duration of the clip.
Mark In	The mark points for the clip.
Mark Out	
Time Source	Control track (CTLTRACK), LTC, or VITC. Note: if using CTL, clip will not be frame accurate, instead it will be +/- 10 frames.
Owner	The name of the person who marked the clip
Error Message	Any error messages describing why the clip was not recorded to the server.
Use Handles	Indicate whether handles have been added to the clip.
Tape ID	The identification of the particular tape

Recording with GV STRATUS VTR Ingest

You can use GV STRATUS VTR Ingest to create a segment (batch) list of clips from videotape recordings, which you then record to your media server.

1. Decide if you want to add handles to your clips.
2. Create a segment list or import an EDL.

   NOTE: The number of characters in a clip name is allowed to exceed 32 characters. For more info, refer to Asset and bin name limitations on page 1428.

3. Record the segment list to your media server.

Adding Handles

If you add handles to your clips, you will have additional frames to choose from when trimming your clips. Grass Valley recommends handles to be used.

- Click the **Record Handle** button .

  Handles will automatically be added to your clip.

You can set the duration of the handles in the **VTR Ingest** section of the **Ingest Settings** tab under the Applications in the GV STRATUS Control Panel application.

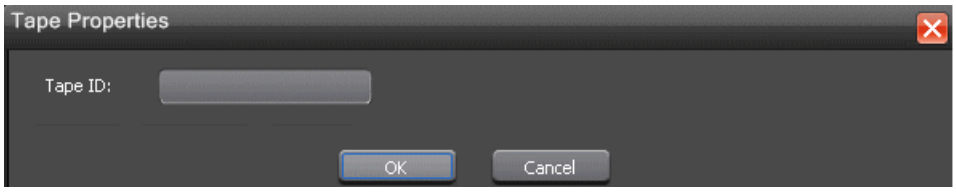
Creating a segment list

You can create a segment (or batch) list using GV STRATUS VTR Ingest.

You must have the **Write** permission for **Name** and **Asset Type** fields for VTR Ingest in the GV STRATUS Control Panel to be able to ingest the segments.

1. Insert a tape into the VTR.
2. Click the **Tape ID** button .

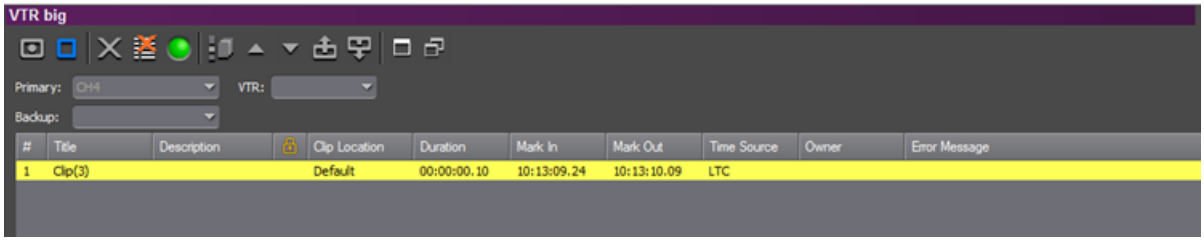
   If you don't enter a Tape ID and you already checked the **Prompt for Tape ID** box within GV STRATUS VTR Ingest configuration, GV STRATUS VTR Ingest prompts you before you add the first clip. The Tape Properties dialog box displays on the screen.



3. Enter the Tape ID.
4. Play through the videotape to get the footage you need.
5. Select a different record location for the clip, if you want to.
6. Mark an In and Out point for a clip.

7. Click **Add Segment to List** button or press **C** on your keyboard.

   The clip is added to the list on the Channel Window.



8. Repeat steps 5-8 for additional clips.
9. To use additional tapes, insert a new tape into the VTR and repeat the steps above.

When you eject a tape, GV STRATUS VTR Ingest clears the tape ID field. You can add the new videotape name anytime after you insert a new tape. If you haven't entered a new Tape ID before you add the first clip from that tape to the segment (batch) list, GV STRATUS VTR Ingest prompts you to add one.

Deleting the Segment List

You can delete a clip or the entire segment list.

Button	Function	Other Ways to Access
	Deletes the selected clip.	Right-click in segment list and select Delete.
	Clears the segment list.	Right-click in segment list and select Clear All.

Controlling the VTR with GV STRATUS VTR Ingest

To get the footage you need to create clips, you need to play through the videotape in the VTR. GV STRATUS VTR Ingest provides transport control buttons like those on a tape deck.

Button	Function
	Jogs one frame back.
	Jogs 10 frames back.
	Jogs one frame forward.
	Jogs 10 frames forward.
	Ejects the tape.
	Rewinds the tape.
	Plays the tape.
	Fast forwards the tape.

Button	Function
	Stops the tape.

Marking In and Out Points

Mark points are used to determine the length of a clip.

1. Find the spot on the videotape where you want your clip to begin.
2. Mark an In Point using any of the following methods:
   - Press **I** on your keyboard.
   - Click the **Mark In** button on the GV STRATUS VTR Ingest window.
   - Type the timecode in the In field.
   - Create a Mark In on the VTR.
3. Play through the tape until you reach the point where you want the clip to end.
4. Mark an Out Point using any of these methods:
   - Press **O** on your keyboard.
   - Click the **Mark Out** button on the GV STRATUS VTR Ingest window.
   - Use the up or down arrows to find the correct timecode.
   - Type the ending timecode in the Out field.
   - Create a Mark Out on the VTR.

Ingesting clips to the media server

After you've created a segment (batch) list, you can ingest and record those clips to your media server.

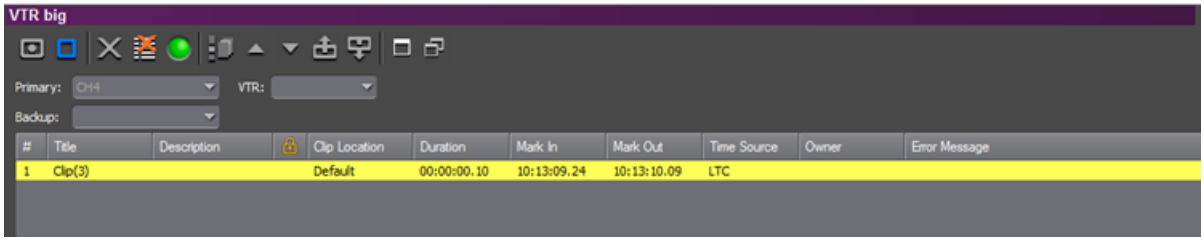
If you want to reserve a channel to record a clip using GV STRATUS VTR Ingest, you can configure this in the channel setup within Ingest setting in the GV STRATUS Control Panel.

If you are recording to SD channels of K2 version 3.2 or higher, you can also set the clip aspect ratio in the clip record area of GV STRATUS VTR Ingest. The option to switch aspect ratio is set in the GV STRATUS Control Panel | **Applications** | **Ingest** and it depends on the user administration setup of your ingest operation.

1. Make sure the Channel Window is selected.
2. Click the **Record** button .

   While the clip is recording, the record button flashes to indicate an active record.

   GV STRATUS VTR Ingest records clips from the VTR tape to the server for later use in a news story.



   The clip status in the GV STRATUS VTR Ingest window changes from Ready -> Cueing -> Recording -> Done. If the clip didn't record for some reason, status shows as Failed.

   NOTE: The video display supports both HD and SD assets and you can configure this in the GV STRATUS Control Panel | Format | View Format.

Scanning tape with broken timecodes

Regardless of which timecode mode is used with your VTR; you can scan tapes with broken timecodes and capture clips according to timecode breaks. A batch list will automatically be created and saved as the .vlg EDL type.

To enable the feature, you need to select the **Enable Timecode Break Scan** checkbox in the VTR tab within Tools | Options of GV STRATUS VTR Ingest. Once selected, the following button appears on the clip record interface of GV STRATUS VTR Ingest.

Button	Function
	Find and ingest segments in tape according to timecode breaks.

1. Insert a tape into the VTR and click the **Timecode Break Scan** button .
2. You can choose to scan for timecode changes from the beginning of the tape or you can choose to start the scan from the current position of the tape. GV STRATUS VTR Ingest will rewind the tape if you choose to scan from the beginning.

3. GV STRATUS VTR Ingest will insert mark in and mark out points around timecode changes, and the clip is then automatically added to the segment list.
4. When all clips have been logged, GV STRATUS VTR Ingest will then ingest all clips in the batch list at the end of the operation.

   NOTE: You can also choose not to ingest segments automatically by deselecting the Automatically start recording after Timecode Break Scan checkbox within Tools | Options of GV STRATUS VTR Ingest.

Do not save the EDL in .ale or .edl format, as the internal "control track" to properly locate broken timecodes could be lost and may result in standard VTR confusion when dealing with timecode direction. Save the EDL as .vlg type only.

Importing an EDL

You can also import an Edit Decision List (EDL) to use as your segment (batch) list. Supported EDL formats are .ale, .edl, .vlg, and .xml. Clip names in the imported file cannot be longer than 32 characters.

1. Choose **File | Import EDL**.
2. In the Open window, navigate to the correct folder, select the EDL to import, and click **Open**.

   NOTE: If your* GV STRATUS *metadata access control is restricted, some fields will be disabled when you import the EDL.

3. Enter the Tape ID and select where to record the clips and click **OK**.

   The EDL appears in the segment (batch) list for the selected channel and is ready to record:

4. Click Record to record your clips to the media server.

   If you have a clip that failed to record for some reason, you can change its status back to Ready by highlighting the clip, right-clicking and selecting **Mark Ready**.

Importing an EDL will clear any existing segments in a VTR's segment list.

Exporting an EDL

Instead of recording your clips to a media server, you can export them as an EDL file, which can be used by other programs. By default, EDLs are saved in a .vlg format.

1. Highlight the file or group of files you want to export.
2. Choose **File | Export EDL**.
3. Navigate to the folder where you want to export the EDL.
4. Enter a name for the file and click **Save**.

The EDLs can also be opened using an editing application's batch (segment) capture feature.

Software licenses

cmemdc

License

You may freely use or modify this code provided this Copyright is included in all derived versions. See below.

CMemDC - memory DC

/Author: Keith Rule

Email: keithr@europa.com

Copyright 1996-2002, Keith Rule

You may freely use or modify this code provided this Copyright is included in all derived versions.

History

10/3/97 Fixed scrolling bug. Added print support. - KR

11/3/99 Fixed most common complaint. Added background color fill. - KR

11/3/99 Added support for mapping modes other than MM_TEXT as suggested by Lee Sang Hun. - KR

02/11/02 Added support for CScrollView as supplied by Gary Kirkham. - KR

This class implements a memory Device Context which allows flicker free drawing.

cping

License

Copyright

- You are allowed to include the source code in any product (commercial, shareware, freeware or otherwise) when your product is released in binary form.
- You are allowed to modify the source code in any way you want except you cannot modify the copyright details at the top of each module.
- If you want to distribute source code with your application, then you are only allowed to distribute versions released by the author. This is to maintain a single distribution point for the source code.

CSizingToolBar

License

CSizingControlBar Version 2.43

Created: Jan 24, 1998 Last Modified: August 03, 2000

See the official site at www.datamekanix.com for documentation and the latest news.

Copyright (C) 1998-2000 by Cristi Posea. All rights reserved.

This code is free for personal and commercial use, providing this notice remains intact in the source files and all eventual changes are clearly marked with comments.

You must obtain the author's consent before you can include this code in a software library.

No warrantee of any kind, express or implied, is included with this software; use at your own risk, responsibility for damages (if any) to anyone resulting from the use of this software rests entirely with the user.

Send bug reports, bug fixes, enhancements, requests, flames, etc. to cristi@datamekanix.com or post them at the message board at the site.

The sources and a short version of the docs are also available at www.codeproject.com . Look for a "Docking Windows" section and check the version to be sure you get the latest one ;)

Hint: These classes are intended to be used as base classes. Do not simply add your code to these file - instead create a new class derived from one of CSizingControlBarXX classes and put there what you need. See CMyBar classes in the demo projects for examples.

Modify this file only to fix bugs, and don't forget to send me a copy.

Acknowledgements:

- Thanks to Harlan R. Seymour for his continuous support during development of this code.
- Thanks to Dundas Software for the opportunity to test this code on real-life applications.
- Some ideas for the gripper came from the CToolBarEx flat toolbar by Joerg Koenig. Thanks, Joerg!
- Thanks to Robert Wolpow for the code on which CDockContext based dialgonal resizing is based.
- Thanks to the following people for various bug fixes and/or enhancements: Chris Maunder, Jakawan Ratiwanich, Udo Schaefer, Anatoly Ivasyuk, Peter Hauptmann.
- And, of course, many thanks to all of you who used this code, for the invaluable feedback I received.

MIT

License

Copyright (c)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY

CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

mozilla

License

Mozilla Public License 1.1 (MPL 1.1)

1. **Definitions.**

1.0.1. "Commercial Use" means distribution or otherwise making the Covered Code available to a third party.

1.1. "Contributor" means each entity that creates or contributes to the creation of Modifications.

1.2. "Contributor Version" means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. "Covered Code" means the Original Code or Modifications or the combination of the Original Code and Modifications, in each case including portions thereof.

1.4. "Electronic Distribution Mechanism" means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. "Executable" means Covered Code in any form other than Source Code.

1.6. "Initial Developer" means the individual or entity identified as the Initial Developer in the Source Code notice required by **Exhibit A**.

1.7. "Larger Work" means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1.8. "License" means this document.

1.8.1. "Licensable" means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. "Modifications" means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

A. Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.

B. Any new file that contains any part of the Original Code or previous Modifications.

1.10. "Original Code" means Source Code of computer software code which is described in the Source Code notice required by **Exhibit A** as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.10.1. "Patent Claims" means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. "Source Code" means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. "You" (or "Your") means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. **Source Code License.**

2.1. The Initial Developer Grant. The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:

(a) under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and

(b) under Patents Claims infringed by the making, using or selling of Original Code, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Code (or portions thereof).

(c) the licenses granted in this Section 2.1(a) and (b) are effective on the date Initial Developer first distributes Original Code under the terms of this License.

(d) Notwithstanding Section 2.1(b) above, no patent license is granted: 1) for code that You delete from the Original Code; 2) separate from the Original Code; or 3) for infringements caused by: i) the modification of the Original Code or ii) the combination of the Original Code with other software or devices.

2.2. Contributor Grant. Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license

(a) under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and

(b) under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: 1) Modifications made by that Contributor (or portions thereof); and 2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

(c) the licenses granted in Sections 2.2(a) and 2.2(b) are effective on the date Contributor first makes Commercial Use of the Covered Code.

(d) Notwithstanding Section 2.2(b) above, no patent license is granted: 1) for any code that Contributor has deleted from the Contributor Version; 2) separate from the Contributor Version; 3) for infringements caused by: i) third party modifications of Contributor Version or ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or 4) under Patent Claims infringed by Covered Code in the absence of Modifications made by that Contributor.

3. **Distribution Obligations.**

3.1. Application of License.

The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section **2.2**. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section **6.1**, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section **3.5**.

3.2. Availability of Source Code.

Any Modification which You create or to which You contribute must be made available in Source Code form under the terms of this License either on the same media as an Executable version or via an accepted Electronic Distribution Mechanism to anyone to whom you made an Executable version available; and if made available via Electronic Distribution Mechanism, must remain available for at least twelve (12) months after the date it initially became available, or at least six (6) months after a subsequent version of that particular Modification has been made available to such recipients. You are responsible for ensuring that the Source Code version remains available even if the Electronic Distribution Mechanism is maintained by a third party.

3.3. Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters

(a) Third Party Claims .

If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs .

If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the LEGAL file.

(c) Representations.

Contributor represents that, except as disclosed pursuant to Section 3.4(a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

3.5. Required Notices.

You must duplicate the notice in **Exhibit A** in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in **Exhibit A**. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients

of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear than any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.6. Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Section **3.1-3.5** have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under the terms of this License, including a description of how and where You have fulfilled the obligations of Section **3.2**. The notice must be conspicuously included in any notice in an Executable version, related documentation or collateral in which You describe recipients' rights relating to the Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

3.7. Larger Works.

You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

4. **Inability to Comply Due to Statute or Regulation.**

   If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the LEGAL file described in Section **3.4** and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. **Application of this License.**

   This License applies to code to which the Initial Developer has attached the notice in **Exhibit A** and to related Covered Code.

6. **Versions of the License.**

   6.1. New Versions.

   Netscape Communications Corporation ("Netscape") may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

   6.2. Effect of New Versions.

   Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License published by Netscape. No one other than Netscape has the right to modify the terms applicable to Covered Code created under this License.

   6.3. Derivative Works.

   If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrases "Mozilla", "MOZILLAPL", "MOZPL", "Netscape", "MPL", "NPL" or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the Mozilla Public License and Netscape Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in **Exhibit A** shall not of themselves be deemed to be modifications of this License.)

7. **DISCLAIMER OF WARRANTY.**

   COVERED CODE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED CODE IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGING. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE COVERED CODE IS WITH YOU. SHOULD ANY COVERED CODE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER OR ANY OTHER CONTRIBUTOR) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED CODE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

8. **TERMINATION.**

8.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2. If You initiate litigation by asserting a patent infringement claim (excluding declatory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You file such action is referred to as "Participant") alleging that:

(a) such Participant's Contributor Version directly or indirectly infringes any patent, then any and all rights granted by such Participant to You under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively, unless if within 60 days after receipt of notice You either: (i) agree in writing to pay Participant a mutually agreeable reasonable royalty for Your past and future use of Modifications made by such Participant, or (ii) withdraw Your litigation claim with respect to the Contributor Version against such Participant. If within 60 days of notice, a reasonable royalty and payment arrangement are not mutually agreed upon in writing by the parties or the litigation claim is not withdrawn, the rights granted by Participant to You under Sections 2.1 and/or 2.2 automatically terminate at the expiration of the 60 day notice period specified above.

(b) any software, hardware, or device, other than such Participant's Contributor Version, directly or indirectly infringes any patent, then any rights granted to You by such Participant under Sections 2.1(b) and 2.2(b) are revoked effective as of the date You first made, used, sold, distributed, or had made, Modifications made by that Participant.

8.3. If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken into account in determining the amount or value of any payment or license.

8.4. In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

9. **LIMITATION OF LIABILITY.**

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED CODE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

10. **U.S. GOVERNMENT END USERS.**

    The Covered Code is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Code with only those rights set forth herein.

11. **MISCELLANEOUS.**

    This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by California law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. With respect to disputes in which at least one party is a citizen of, or an entity chartered or registered to do business in the United States of America, any litigation relating to this License shall be subject to the jurisdiction of the Federal Courts of the Northern District of California, with venue lying in Santa Clara County, California, with the losing party responsible for costs, including without limitation, court costs and reasonable attorneys' fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License.

12. **RESPONSIBILITY FOR CLAIMS.**

    As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

13. **MULTIPLE-LICENSED CODE.**

    Initial Developer may designate portions of the Covered Code as Multiple-Licensed. Multiple-Licensed means that the Initial Developer permits you to utilize portions of the Covered Code under Your choice of the NPL or the alternative licenses, if any, specified by the Initial Developer in the file described in Exhibit A.

EXHIBIT A -Mozilla Public License.

``The contents of this file are subject to the Mozilla Public License Version 1.1 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.mozilla.org/MPL/

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specificlanguage governing rights and limitations under the License.

The Original Code is _____.

The Initial Developer of the Original Code is _____. Portions created by _____ are Copyright (C) _____ _____. All Rights Reserved.

Contributor(s): _____.

Alternatively, the contents of this file may be used under the terms of the _____ license (the [___] License), in which case the provisions of [_____] License are applicable instead of those above. If you wish to allow use of your version of this file only under the terms of the [____] License and not to allow others to use your version of this file under the MPL, indicate your decision by deleting

the provisions above and replace them with the notice and other provisions required by the [___] License. If you do not delete the provisions above, a recipient may use your version of this file under either the MPL or the [___] License."

[NOTE: The text of this Exhibit A may differ slightly from the text of the notices in the Source Code files of the Original Code. You should use the text of this Exhibit A rather than the text found in the Original Code Source Code for Your Modifications.]

resizeable lib

License

This file is part of ResizableLib

http://sourceforge.net/projects/resizablelib

/Copyright (C) 2000-2004 by Paolo Messina

/http://www.geocities.com/ppescher - mailto:ppescher@hotmail.com

The contents of this file are subject to the Artistic License (the "License").

You may not use this file except in compliance with the License.

You may obtain a copy of the License at:

http://www.opensource.org/licenses/artistic-license.html

If you find this code useful, credits would be nice!

The Artistic License

Preamble

The intent of this document is to state the conditions under which a Package may be copied, such that the Copyright Holder maintains some semblance of artistic control over the development of the package, while giving the users of the package the right to use and distribute the Package in a more-or-less customary fashion, plus the right to make reasonable modifications.

Definitions:

- "Package" refers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification.
- "Standard Version" refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder.
- "Copyright Holder" is whoever is named in the copyright or copyrights for the package.
- "You" is you, if you're thinking about copying or distributing this Package.
- "Reasonable copying fee" is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.)
- "Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

1. You may make and give away verbatim copies of the source form of the Standard Version of this Package without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers.
2. You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.
3. You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when you changed that file, and provided that you do at least ONE of the following:

   a) place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as ftp.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.

   b) use the modified Package only within your corporation or organization.

   c) rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide a separate manual page for each non-standard executable that clearly documents how it differs from the Standard Version.

   d) make other distribution arrangements with the Copyright Holder.

4. You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:

   a) distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.

   b) accompany the distribution with the machine-readable source of the Package with your modifications.

   c) accompany any non-standard executables with their corresponding Standard Version executables, giving the non-standard executables non-standard names, and clearly documenting the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version.

   d) make other distribution arrangements with the Copyright Holder.

5. You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. You may not charge a fee for this Package itself. However, you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided that you do not advertise this Package as a product of your own.
6. The scripts and library files supplied as input to or produced as output from the programs of this Package do not automatically fall under the copyright of this Package, but belong to whomever generated them, and may be sold commercially, and may be aggregated with this Package.
7. C or perl subroutines supplied by you and linked into this Package shall not be considered part of this Package.
8. The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission.
9. THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The End

GV STRATUS VTR Controller Operation

Installing GV STRATUS VTR Controller Hardware

Installing RS-422 card for GV STRATUS VTR Controller

To connect a VTR to a GV STRATUS VTR Controller PC, you need to install a PCI 422 SMPTE 8 Port RoHS RS-422 card.

1. If you are connecting one or more VTRs to GV STRATUS VTR Controller, install the RS-422 card in your computer, making sure the dip switches are set to the down position as shown, and install the card's driver.

NOTE: If only one VTR is to be connected to a GV STRATUS VTR Controller PC, you can use an alternative connection method with an RS-422 to RS-232 cable connected to the onboard COM1 port.

2. Connect the VTR(s) to the GV STRATUS VTR Controller machine via RS-422 cable.
3. If you are using LTC for timecode, connect a timecode cable from the timecode source (VTR) to the media server.

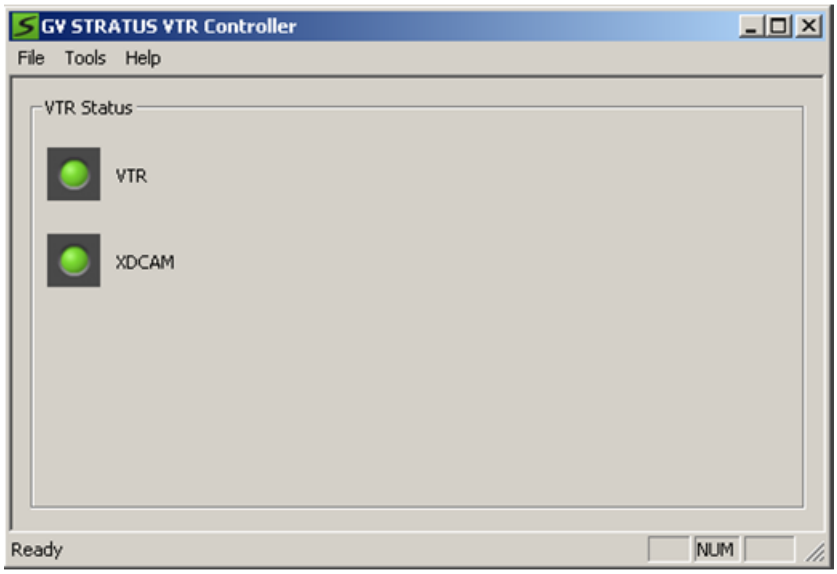
Configuring GV STRATUS VTR Controller

Configuring GV STRATUS VTR Controller Application

In order to establish a connection between GV STRATUS VTR Ingest and a VTR, you need to configure the GV STRATUS VTR Controller application.

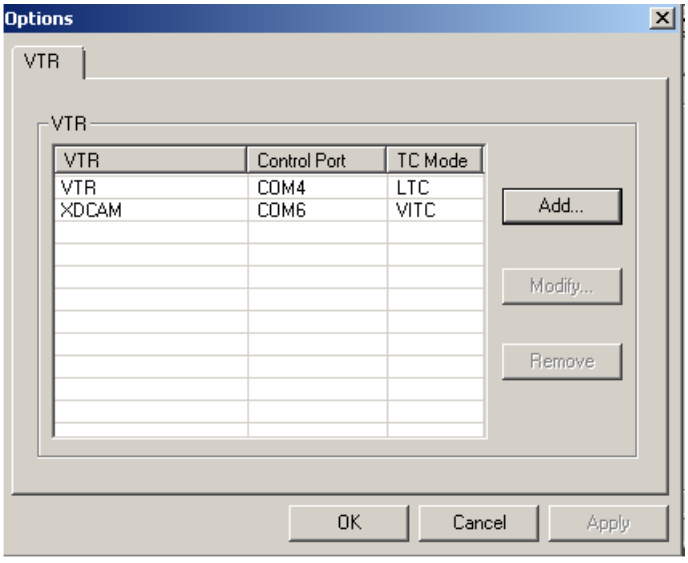
GV STRATUS VTR Controller can be installed on the same machine as the GV STRATUS VTR Ingest application, but this is not required.

1. From the Windows Start menu, select **Programs | Grass Valley | GV STRATUS VTR Controller**.



The GV STRATUS VTR Controller application opens.

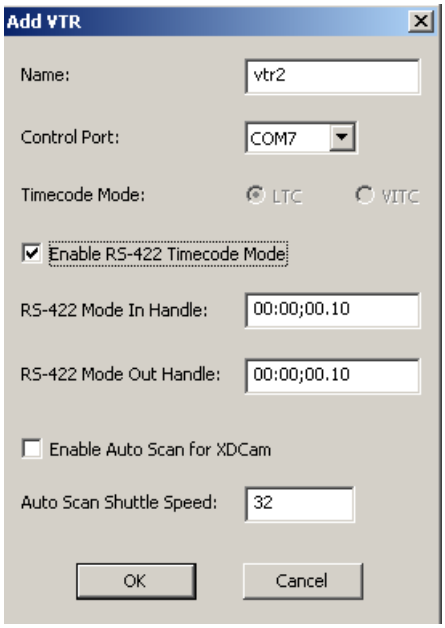
2. Select **Tools | Options**.



The GV STRATUS VTR Controller Options dialog box displays.

3. Click the **Add** button.

   The Add VTR dialog box displays.



4. Enter the VTR name.
5. Select the control port and timecode mode.

   NOTE: The RS-422 timecode is not supported in this release.

6. If you are using an XDCAM VTR, you can select the checkbox to enable auto scan for the XDCAM VTR.

   The XDCAM VTR does not adhere to typical RS-422 shuttle commands. By enabling the auto scan feature for XDCAM VTR, previous and next commands will be used instead of the usual shuttle forward and back.

7. You can also change the shuttle speed for the auto scan feature.

   The default is set to 32, but you can change to any value depending on the type of VTR that you use. When XDCAM mode is selected, the field to set the shuttle speed of auto scan will be disabled.

8. Click **OK** to add the VTR.

   After you have successfully added the VTR, you should see it displayed in the VTR Status window with a green indicator next to its name.

Once you have added VTRs, you can modify or delete them. However, if you only have one VTR displayed in the status window, you cannot delete it and have an empty status window.

Troubleshooting GV STRATUS VTR Controller configuration

If you see a red indicator next to the VTR's name, try restarting GV STRATUS VTR Controller.

If the VTR status still displays a red indicator, verify the following:

- Check your GV STRATUS VTR Ingest configuration and make sure the VTR information matches the information you entered when configuring GV STRATUS VTR Controller.
- The correct COM port has been specified for the VTR.
- The COM port is not being used by another application controlling the VTR.
- The VTR is turned on.
- The hardware has been correctly installed.
- The IP address or computer name where GV STRATUS VTR Controller is installed matches the address or name in the GV STRATUS VTR Ingest application.

Using GV STRATUS VTR Controller

Using GV STRATUS VTR Controller

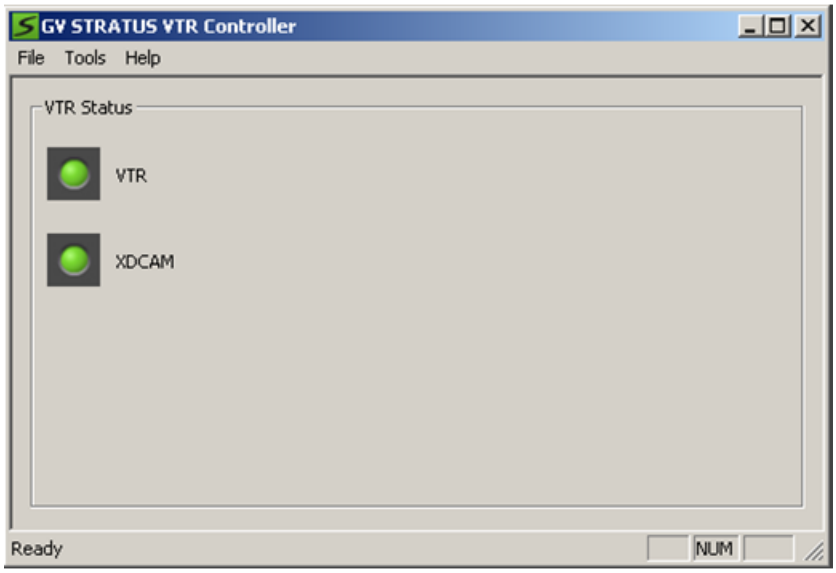
GV STRATUS VTR Controller allows you to control up to eight VTRs for GV STRATUS VTR Ingest application. Furthermore, GV STRATUS VTR Controller allows you to add, modify, or edit VTRs and configure them to work with other Ingest applications.

You can have GV STRATUS VTR Controller and GV STRATUS VTR Ingest on the same machine or on two machines connected via Ethernet. If you modify a VTR in GV STRATUS VTR Controller, verify the change doesn't conflict with the VTR settings in the GV STRATUS VTR Ingest application.

Overview of the GV STRATUS VTR Controller Window

The GV STRATUS VTR Controller window shows the status of one to eight VTRs.

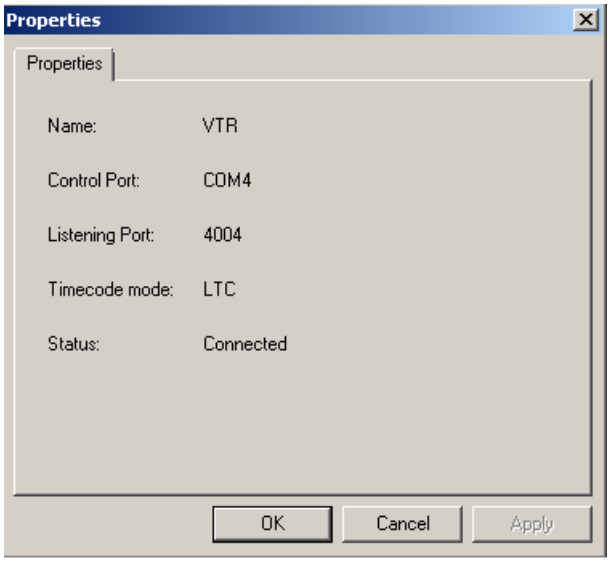
The status of each VTR is indicated by the colors: a green indicator shows that the VTR is connected, while a red indicator shows that the VTR is not connected. The status bar at the bottom of the window shows the status of the GV STRATUS VTR Controller application.



Viewing VTR Properties

Properties of each VTR can be viewed via the GV STRATUS VTR Controller user interface.

- Click on the red or green icon next to the VTR.



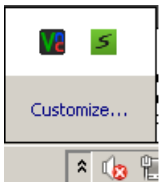
The Properties window displays.

Accessing GV STRATUS VTR Controller

There are two ways to launch the GV STRATUS VTR Controller application.

- Click on the GV STRATUS VTR Controller shortcut icon on the desktop.
- From the Start button follow this path: **Start | Program | Grass Valley | GV STRATUS VTR Controller**

When GV STRATUS VTR Controller is first started, it automatically minimizes to an icon in the right-hand corner of the Windows taskbar.



Double-click on the GV STRATUS VTR Controller icon to bring up the main GV STRATUS VTR Controller window.

NOTE: If you click the X in the upper-right corner of the GV STRATUS VTR Controller window or select File | Exit, the application does not exit. Instead, it is minimized, and the GV STRATUS VTR Controller icon appears in the Windows taskbar. You can exit the GV STRATUS VTR Controller application by right click on the icon and select Exit.

Software licenses

Software Licenses

cping

License

Copyright

- You are allowed to include the source code in any product (commercial, shareware, freeware or otherwise) when your product is released in binary form.
- You are allowed to modify the source code in any way you want except you cannot modify the copyright details at the top of each module.
- If you want to distribute source code with your application, then you are only allowed to distribute versions released by the author. This is to maintain a single distribution point for the source code.

CSizingToolBar

License

CSizingControlBar Version 2.43

Created: Jan 24, 1998 Last Modified: August 03, 2000

See the official site at www.datamekanix.com for documentation and the latest news.

Copyright (C) 1998-2000 by Cristi Posea. All rights reserved.

This code is free for personal and commercial use, providing this notice remains intact in the source files and all eventual changes are clearly marked with comments.

You must obtain the author's consent before you can include this code in a software library.

No warrantee of any kind, express or implied, is included with this software; use at your own risk, responsibility for damages (if any) to anyone resulting from the use of this software rests entirely with the user.

Send bug reports, bug fixes, enhancements, requests, flames, etc. to cristi@datamekanix.com or post them at the message board at the site.

The sources and a short version of the docs are also available at www.codeproject.com . Look for a "Docking Windows" section and check the version to be sure you get the latest one ;)

Hint: These classes are intended to be used as base classes. Do not simply add your code to these file - instead create a new class derived from one of CSizingControlBarXX classes and put there what you need. See CMyBar classes in the demo projects for examples.

Modify this file only to fix bugs, and don't forget to send me a copy.

Acknowledgements:

- Thanks to Harlan R. Seymour for his continuous support during development of this code.
- Thanks to Dundas Software for the opportunity to test this code on real-life applications.
- Some ideas for the gripper came from the CToolBarEx flat toolbar by Joerg Koenig. Thanks, Joerg!
- Thanks to Robert Wolpow for the code on which CDockContext based dialgonal resizing is based.
- Thanks to the following people for various bug fixes and/or enhancements: Chris Maunder, Jakawan Ratiwanich, Udo Schaefer, Anatoly Ivasyuk, Peter Hauptmann.
- And, of course, many thanks to all of you who used this code, for the invaluable feedback I received.

CTextProgressCtrl

License

Written by Chris Maunder (chrismaunder@codeguru.com)

Copyright 1998.

Modified : 26/05/98 Jeremy Davis, jmd@jvf.co.uk

Added colour routines

TextProgressCtrl is a drop-in replacement for the standard CProgressCtrl that displays text in a progress control.

This code may be used in compiled form in any way you desire. This file may be redistributed by any means PROVIDING it is not sold for profit without the authors written consent, and providing that this notice and the authors name is included. If the source code in this file is used in any commercial application then an email to the me would be nice.

This file is provided "as is" with no expressed or implied warranty. The author accepts no liability if it causes any damage to your computer, causes your pet cat to fall ill, increases baldness or makes you car start emitting strange noises when you start it up.

Expect bugs.

Please use and enjoy. Please let me know of any bugs/mods/improvements that you have found/implemented and I will fix/incorporate them into this file.

Chris Maunder is the original author.

MIT

License

Copyright (c)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

mozilla

License

Mozilla Public License 1.1 (MPL 1.1)

1. **Definitions.**

1.0.1. "Commercial Use" means distribution or otherwise making the Covered Code available to a third party.

1.1. "Contributor" means each entity that creates or contributes to the creation of Modifications.

1.2. "Contributor Version" means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. "Covered Code" means the Original Code or Modifications or the combination of the Original Code and Modifications, in each case including portions thereof.

1.4. "Electronic Distribution Mechanism" means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. "Executable" means Covered Code in any form other than Source Code.

1.6. "Initial Developer" means the individual or entity identified as the Initial Developer in the Source Code notice required by **Exhibit A**.

1.7. "Larger Work" means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1.8. "License" means this document.

1.8.1. "Licensable" means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. "Modifications" means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

A. Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.

B. Any new file that contains any part of the Original Code or previous Modifications.

1.10. "Original Code" means Source Code of computer software code which is described in the Source Code notice required by **Exhibit A** as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.10.1. "Patent Claims" means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. "Source Code" means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. "You" (or "Your") means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. **Source Code License.**

2.1. The Initial Developer Grant. The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:

(a) under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and

(b) under Patents Claims infringed by the making, using or selling of Original Code, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Code (or portions thereof).

(c) the licenses granted in this Section 2.1(a) and (b) are effective on the date Initial Developer first distributes Original Code under the terms of this License.

(d) Notwithstanding Section 2.1(b) above, no patent license is granted: 1) for code that You delete from the Original Code; 2) separate from the Original Code; or 3) for infringements caused by: i) the modification of the Original Code or ii) the combination of the Original Code with other software or devices.

2.2. Contributor Grant. Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license

(a) under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and

(b) under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: 1) Modifications made by that Contributor (or portions thereof); and 2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

(c) the licenses granted in Sections 2.2(a) and 2.2(b) are effective on the date Contributor first makes Commercial Use of the Covered Code.

(d) Notwithstanding Section 2.2(b) above, no patent license is granted: 1) for any code that Contributor has deleted from the Contributor Version; 2) separate from the Contributor Version; 3) for infringements caused by: i) third party modifications of Contributor Version or ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or 4) under Patent Claims infringed by Covered Code in the absence of Modifications made by that Contributor.

3. **Distribution Obligations.**

3.1. Application of License.

The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section **2.2**. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section **6.1**, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section **3.5**.

3.2. Availability of Source Code.

Any Modification which You create or to which You contribute must be made available in Source Code form under the terms of this License either on the same media as an Executable version or via an accepted Electronic Distribution Mechanism to anyone to whom you made an Executable version available; and if made available via Electronic Distribution Mechanism, must remain available for at least twelve (12) months after the date it initially became available, or at least six (6) months after a subsequent version of that particular Modification has been made available to such recipients. You are responsible for ensuring that the Source Code version remains available even if the Electronic Distribution Mechanism is maintained by a third party.

3.3. Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters

(a) Third Party Claims .

If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs .

If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the LEGAL file.

(c) Representations.

Contributor represents that, except as disclosed pursuant to Section 3.4(a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

3.5. Required Notices.

You must duplicate the notice in **Exhibit A** in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in **Exhibit A**. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients

of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear than any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.6. Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Section **3.1-3.5** have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under the terms of this License, including a description of how and where You have fulfilled the obligations of Section **3.2**. The notice must be conspicuously included in any notice in an Executable version, related documentation or collateral in which You describe recipients' rights relating to the Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

3.7. Larger Works.

You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

4. **Inability to Comply Due to Statute or Regulation.**

   If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the LEGAL file described in Section **3.4** and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. **Application of this License.**

   This License applies to code to which the Initial Developer has attached the notice in **Exhibit A** and to related Covered Code.

6. **Versions of the License.**

   6.1. New Versions.

   Netscape Communications Corporation ("Netscape") may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

   6.2. Effect of New Versions.

   Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License published by Netscape. No one other than Netscape has the right to modify the terms applicable to Covered Code created under this License.

   6.3. Derivative Works.

   If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrases "Mozilla", "MOZILLAPL", "MOZPL", "Netscape", "MPL", "NPL" or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the Mozilla Public License and Netscape Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in **Exhibit A** shall not of themselves be deemed to be modifications of this License.)

7. **DISCLAIMER OF WARRANTY.**

   COVERED CODE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED CODE IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGING. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE COVERED CODE IS WITH YOU. SHOULD ANY COVERED CODE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER OR ANY OTHER CONTRIBUTOR) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED CODE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

8. **TERMINATION.**

8.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2. If You initiate litigation by asserting a patent infringement claim (excluding declatory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You file such action is referred to as "Participant") alleging that:

(a) such Participant's Contributor Version directly or indirectly infringes any patent, then any and all rights granted by such Participant to You under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively, unless if within 60 days after receipt of notice You either: (i) agree in writing to pay Participant a mutually agreeable reasonable royalty for Your past and future use of Modifications made by such Participant, or (ii) withdraw Your litigation claim with respect to the Contributor Version against such Participant. If within 60 days of notice, a reasonable royalty and payment arrangement are not mutually agreed upon in writing by the parties or the litigation claim is not withdrawn, the rights granted by Participant to You under Sections 2.1 and/or 2.2 automatically terminate at the expiration of the 60 day notice period specified above.

(b) any software, hardware, or device, other than such Participant's Contributor Version, directly or indirectly infringes any patent, then any rights granted to You by such Participant under Sections 2.1(b) and 2.2(b) are revoked effective as of the date You first made, used, sold, distributed, or had made, Modifications made by that Participant.

8.3. If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken into account in determining the amount or value of any payment or license.

8.4. In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

9. **LIMITATION OF LIABILITY.**

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED CODE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

10. **U.S. GOVERNMENT END USERS.**

    The Covered Code is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Code with only those rights set forth herein.

11. **MISCELLANEOUS.**

    This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by California law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. With respect to disputes in which at least one party is a citizen of, or an entity chartered or registered to do business in the United States of America, any litigation relating to this License shall be subject to the jurisdiction of the Federal Courts of the Northern District of California, with venue lying in Santa Clara County, California, with the losing party responsible for costs, including without limitation, court costs and reasonable attorneys' fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License.

12. **RESPONSIBILITY FOR CLAIMS.**

    As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

13. **MULTIPLE-LICENSED CODE.**

    Initial Developer may designate portions of the Covered Code as Multiple-Licensed. Multiple-Licensed means that the Initial Developer permits you to utilize portions of the Covered Code under Your choice of the NPL or the alternative licenses, if any, specified by the Initial Developer in the file described in Exhibit A.

EXHIBIT A -Mozilla Public License.

``The contents of this file are subject to the Mozilla Public License Version 1.1 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.mozilla.org/MPL/

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specificlanguage governing rights and limitations under the License.

The Original Code is _____.

The Initial Developer of the Original Code is _____. Portions created by _____ are Copyright (C) _____ _____. All Rights Reserved.

Contributor(s): _____.

Alternatively, the contents of this file may be used under the terms of the _____ license (the [___] License), in which case the provisions of [_____] License are applicable instead of those above. If you wish to allow use of your version of this file only under the terms of the [____] License and not to allow others to use your version of this file under the MPL, indicate your decision by deleting

the provisions above and replace them with the notice and other provisions required by the [___] License. If you do not delete the provisions above, a recipient may use your version of this file under either the MPL or the [___] License."

[NOTE: The text of this Exhibit A may differ slightly from the text of the notices in the Source Code files of the Original Code. You should use the text of this Exhibit A rather than the text found in the Original Code Source Code for Your Modifications.]

Paintlib

License

If you redistribute paintlib, you should redistribute the whole library including documentation and copyright. If that is not possible, you must make it clear that you're distributing a changed version. In no event may any part of the library be distributed without this copyright notice.

Before the legalese starts, here's the translation to plain english:

1. Do whatever you want with paintlib. Just don't come running to me with a lawyer if something goes wrong.
2. If you redistribute paintlib, you should redistribute the whole library including documentation and copyright. If that is not possible, you must make it clear that you're distributing a changed version. In no event may any part of the library be distributed without this copyright notice.
3. If you use paintlib in your program, you must acknowledge this, preferably in the about box and the documentation.

The legalese itself is a derivative work. I modified the LIBPNG copyright notice. Thanks, guys :-).

The paintlib source code and all documentation are copyright (c) 1996-1999 Ulrich von Zadow.

The paintlib source code is supplied "AS IS". Ulrich von Zadow and other authors disclaim all warranties, expressed or implied, including, without limitation, the warranties of merchantability and of fitness for any purpose. The authors assume no liability for direct, indirect, incidental, special, exemplary, or consequential damages, which may result from the use of paintlib, even if advised of the possibility of such damage.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, without fee, subject to the following restrictions:

1. The origin of this source code must not be misrepresented.
2. Altered versions must be plainly marked as such and must not be misrepresented as being the original source.
3. This Copyright notice may not be removed or altered from any source or altered source distribution.
4. Executables containing paintlib or parts of it must state that the software "contains paintlib code. paintlib is copyright (c) 1996-1998 Ulrich von Zadow.". This notice must be displayed in at least one place where the copyright for the software itself is displayed. The documentation must also contain this notice.

Note that libpng, libtiff and the jpeg library have their own terms of use. You can find these in the documentation of the libraries.

resizeable lib

License

This file is part of ResizableLib

http://sourceforge.net/projects/resizablelib

/Copyright (C) 2000-2004 by Paolo Messina

/http://www.geocities.com/ppescher - mailto:ppescher@hotmail.com

The contents of this file are subject to the Artistic License (the "License").

You may not use this file except in compliance with the License.

You may obtain a copy of the License at:

http://www.opensource.org/licenses/artistic-license.html

If you find this code useful, credits would be nice!

The Artistic License

Preamble

The intent of this document is to state the conditions under which a Package may be copied, such that the Copyright Holder maintains some semblance of artistic control over the development of the package, while giving the users of the package the right to use and distribute the Package in a more-or-less customary fashion, plus the right to make reasonable modifications.

Definitions:

- "Package" refers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification.
- "Standard Version" refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder.
- "Copyright Holder" is whoever is named in the copyright or copyrights for the package.
- "You" is you, if you're thinking about copying or distributing this Package.
- "Reasonable copying fee" is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.)
- "Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

1. You may make and give away verbatim copies of the source form of the Standard Version of this Package without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers.
2. You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.

3. You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when you changed that file, and provided that you do at least ONE of the following:

    a) place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as ftp.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.

    b) use the modified Package only within your corporation or organization.

    c) rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide a separate manual page for each non-standard executable that clearly documents how it differs from the Standard Version.

    d) make other distribution arrangements with the Copyright Holder.

4. You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:

    a) distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.

    b) accompany the distribution with the machine-readable source of the Package with your modifications.

    c) accompany any non-standard executables with their corresponding Standard Version executables, giving the non-standard executables non-standard names, and clearly documenting the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version.

    d) make other distribution arrangements with the Copyright Holder.

5. You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. You may not charge a fee for this Package itself. However, you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided that you do not advertise this Package as a product of your own.
6. The scripts and library files supplied as input to or produced as output from the programs of this Package do not automatically fall under the copyright of this Package, but belong to whomever generated them, and may be sold commercially, and may be aggregated with this Package.
7. C or perl subroutines supplied by you and linked into this Package shall not be considered part of this Package.
8. The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission.
9. THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The End

tconvert

License

TCONVERT.H

SCA Software International S.A.

http://www.scasoftware.com

scaadmin@scasoftware.com

Copyright (c) 2000 SCA Software International S.A.

Date: 01.05.2000

Author: Zoran M.Todorovic

This software is provided "AS IS", without a warranty of any kind. You are free to use/modify this code but leave this header intact.

zlib

License

Zlib

zlib.h -- interface of the 'zlib' general purpose compression library version 1.2.2, October 3rd, 2004

Copyright (C) 1995-2004 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly Mark Adler

jloup@gzip.org madler@alumni.caltech.edu

The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files http://www.ietf.org/rfc/rfc1950.txt (zlib format), rfc1951.txt (deflate format) and rfc1952.txt (gzip format).

GV I/O Live Ingest and Playback

About the GV I/O Live Ingest and Playback Server

Introduction

The GV I/O Live Ingest and Playback Server provides the ability to build a non-K2 Summit based GV STRATUS solution on COTS (Commercial Off the Shelf) IT hardware and storage. GV STRATUS users can now purchase a commodity hardware solution and add the baseband HD-SDI support via an on-board video card. The GV I/O server may also be configured as a standalone device with local storage, or a shared storage client with Dell EMC Isilon network-attached storage system.

The GV I/O Live Ingest and Playback Server supports production requiring cost effective Ingest and Replay in a fast paced News or Sports workflow. In addition, it supports studio and web production, live audience studio shows, and any operation that requires multi-channel ingests and playbacks in the editing and production environment.

The GV I/O Live Ingest and Playback Server has up to four Recorder/Player channels that support SD, 720p, and 1080i video formats. As an alternative to K2 Summit systems, the GV I/O Live Ingest and Playback Server utilizes Dell PowerEdge R640 servers with an AJA® Corvid 88 card for SDI connections to support channel ingests and playback. The 1G/10G network adapters are provided for Control, and SMB, IP, or iSCSI connections. In addition, the Mellanox ConnectX®-4 25 GigE network adapter card is supported for IP ingests. The GV I/O Live Ingest and Playback Server also supports common SD and HD codecs without additional licenses.

Standard features

The GV I/O Live Ingest and Playback Server offers high performance, expansion options, and high reliability outlined in the summary below.

- The system comes ready to use with quick connections for the duplex LAN, USB, and monitor connections.
- The main enclosure is rack-mountable and the main components are easy to install.
- Includes a third-party SDI card (AJA CORVID 88) that supports up to 4 channels of Ingest and Playout.
- Supports a third party network adapter card (Mellanox ConnectX-4 25 GigE) for IP ingests.
- Support for common SD and HD codecs without additional licenses.
- ‘Store and Forward’ workflow ensures essence is cached locally and simultaneously sent to the system storage.
- High performance features include a powerful central processor and high speed Ethernet interface and disk access from SAS (Serial Attached SCSI) disk drives.
- Able to be configured as a standalone device with local storage, or a shared storage client with third party storage system.
- The following Dell EMC Isilon network-attached storage systems are qualified for use with the GV I/O Live Ingest and Playback Server: S210, X210, X410, H400, H500, and H600.

- As of GV STRATUS 6.8 release, the GV I/O does not support the following:
  - Multi-cam or ganging
  - Live-streaming
  - Renaming or transferring while recording
  - 1080p format

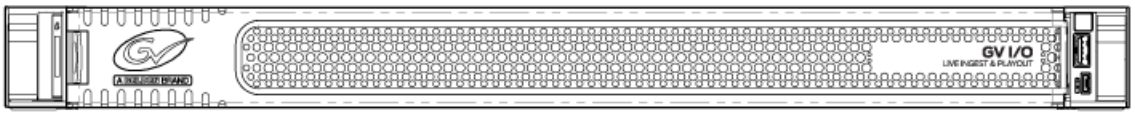
Product component summary

The main components of the GV I/O Live Ingest and Playback Server are the following:

- One RU rack-mountable chassis.
- Dual processors.
- Two hot-plug, redundant, and high-efficiency power supply units.
- Two RAID 1 Solid State Drives (240 GB drives, configured as **RAID 1** with **128k stripe** size)
- Five RAID 5 drives (1 TB drives, configured as **RAID 5** with **128k stripe** size) - For Standalone device only
- 1G/10G Ethernet LAN connectors.
- One monitor connector for connecting a display device.
- 3 USB ports for connecting devices.
- A third-party SDI card (AJA CORVID 88) for SDI connections.
- Or a third party network adapter card (Mellanox ConnectX-4 25 GigE) for IP ingest connections.

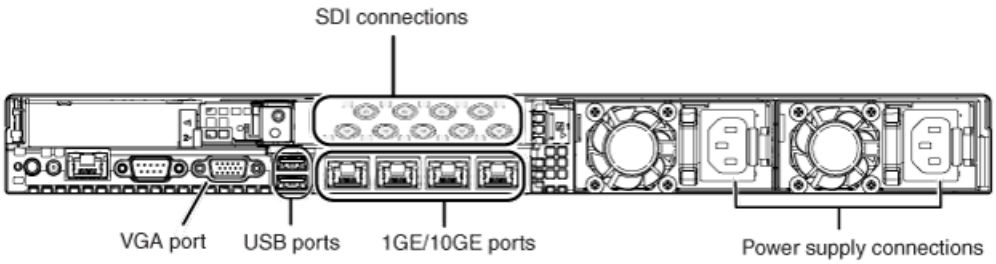
Front view

The front view of the GV I/O Live Ingest and Playback Server front bezel is shown below. The front bezel should be installed after rack mounting the server. It should remain installed during normal operation for proper cooling of the unit.



Rear view components

A rear view of the GV I/O Live Ingest and Playback Server is shown below.



The system backplane includes the AJA card for SDI connections, 1GE/10GE ports for Control, and SMB, IP, or iSCSI connections, USB ports for mouse and keyboard control, a VGA port to connect to a monitor, and two AC power supply units.

Cabling GV I/O Live Ingest and Playback Server

Rack mounting

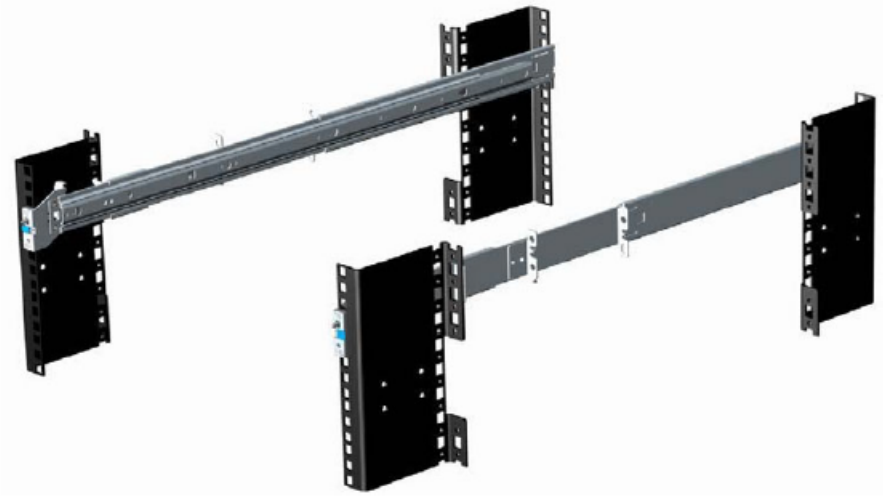
Rack-mount considerations

When planning the placement of equipment in your equipment rack, bear in mind the following:

- Ensure adequate air flow around the chassis to provide sufficient cooling. Operating ambient temperature will affect the amount of air circulation required to keep the system within its temperature limitations.
- Ensure that safety labels located on the top of the unit are visible after installation. This requires sufficient open space over the unit without cables or other devices impeding the view.
- If the system is installed with its ventilation intakes near another system's exhaust or in a closed or multi-unit rack assembly, the operating ambient temperature inside the chassis may be greater than the room's ambient temperature. Install the system in an environment compatible with this recommended maximum ambient temperature.
- Ensure that the power socket-outlet is installed near the equipment and is easily accessible.
- Ensure the rack is anchored to the floor so that it cannot tip over when the system is extended out of the rack.
- Be sure to mount the system in a way that ensures even weight distribution in the rack. Uneven mechanical loading can result in a hazardous condition. Secure all mounting bolts when installing the chassis to the rack.

Rack-mount device

Follow the instructions you received with the rack-mount hardware to install the system. One rack-unit spacing is recommended between components for ventilation.



Dell R640 Rack specifications

Use the following specifications to determine load, spacing, power, and other factors when planning system racks.

Table 19: Mechanical specifications

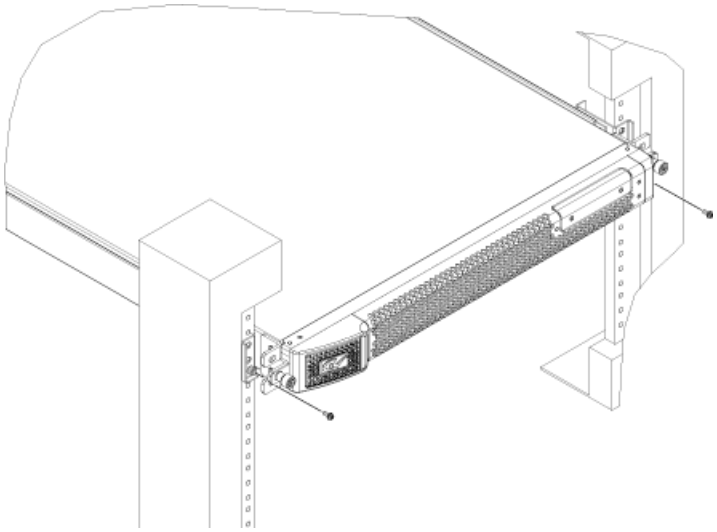
Characteristic	Specification
Cabinet Type	Rack-mount
Rack units	1
External Dimensions	482.0 (w) x 42.8 (h) x 683.05 (d) mm
Weight	Maximum 21.9 kg

Table 20: Power specifications

Specification	750W AC
Current consumption	10A-5A
Supply voltage	100-240VAC
Frequency	50/60Hz
Heat dissipation (BTU/hr max)	2891
Maximum inrush current	55A

Securing a server to a rack

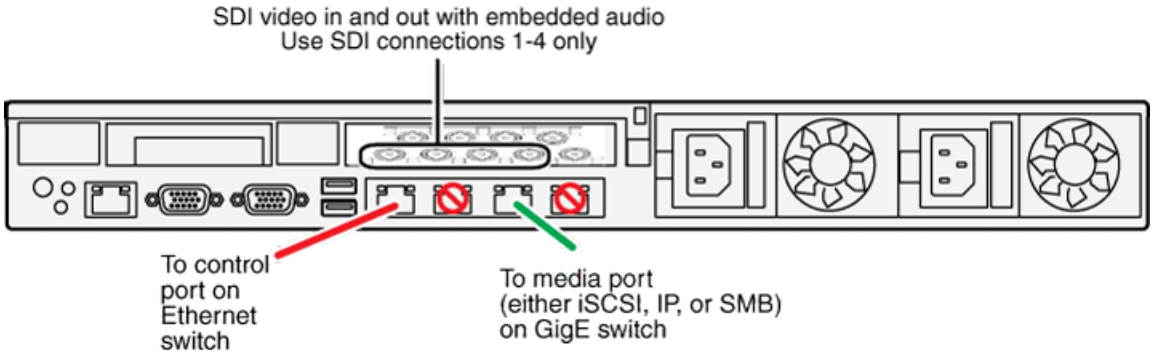
Follow the instructions provided in the shipping box to install the rack rails and position the server in the rack. For the Dell 1RU PowerEdge Server, follow the illustration below to secure the system to the rack.



Install a screw in the bottom hole of the bracket on each side. Do not attempt to install a screw in the top hole of the bracket.

Cabling GV I/O server: Dell R640

These cabling instructions apply to Dell R640 PowerEdge server, specified as follows:



The GV I/O server supports SDI, iSCSI, SMB, or IP media connection for ingests into the commodity storage based systems.

However, the GV I/O server supports SDI connection only for playout of simple clips, not including playlists. Each SDI channel (C1, C2, etc.) can be an input (recorder channel) or an output (player channel). Connect video/audio IN and OUT to each channel, as appropriate for your intended use.

Installing GV I/O Live Ingest and Playback Server

If you have received your GV I/O Live Ingest and Playback Server from the factory for use in a GV STRATUS Media Workflow system, it has been configured with all the necessary software and server functionality such as duplexed LANs and Rapid Disk Resync (RDR) has been performed at the factory. Refer to these topics for further installation instructions.

BIOS startup

Prerequisite:

- Verify that the AJA card is installed with the desired feeds attached
- The Control and iSCSI/IP/SMB network cables are connected to 1G and 10G ports respectively
- Verify that the nVidia card is installed

After the power-up of GV I/O Live Ingest and Playback Server, the VGA monitor displays BIOS information, with instructions on how to access settings.

1. Press the F2 key on the keyboard to enter System Setup pages.
2. On the System Setup screen, select **System BIOS**.
3. Configure settings as below:
    - **Boot Settings**: Boot Mode set to **BIOS** (not UEFI)
    - **System Profile**:
        - System Profile set to **Custom**
        - Energy Efficient Policy set to **Performance**
        - Disable the **C1E** option
    - **Processor Settings**: Enable the **Logical Processor** option

When BIOS settings have been completed, the Windows operating system begins to load.

Preparing for GV I/O installation

Before installing, do the following:

- Procure the software installation files for this release via the appropriate distribution method, such as download, network drive, or external drive.
- Image the GV I/O using the latest Dell image and its associated Acronis version.
- Allow the GV I/O Live Ingest and Playback Server to boot up for the first time, and name the server when prompted to after the first log in.
- Open Computer Management, Disk Management and do the following:
    - Split the C: and D: drive equally on the RAID 1 SSDs.
    - For Standalone client only - Create the V: Media drives on the four RAID 5 drives.
- Configure the Control network. Work with the IT personnel at the site to configure Domain, DNS, DHCP, or any other settings required by the site's LAN.
- Run the **WeightNetworkAdapters.ps1** file and enter the names of four adapters as follows:
    1. Control network
    2. FTP network, if applicable. (Enter **Unused 1** if the network adapter is not used)
    3. iSCSI A or Isilon network, if applicable. (Enter **Unused 2** if the network adapter is not used)
    4. iSCSI B network, if applicable. (Enter **Unused 3** if the network adapter is not used)
- Add the GV I/O Live Ingest and Playback Server to a domain, or update and use hosts files.
- Install the latest SiteConfig application.
- Install Discovery Agent 2.2.0.205 or higher, which includes the GV I/O Live Ingest and Playback Server.

- Install all Important Windows updates.

SiteConfig placeholder setup for GV I/O

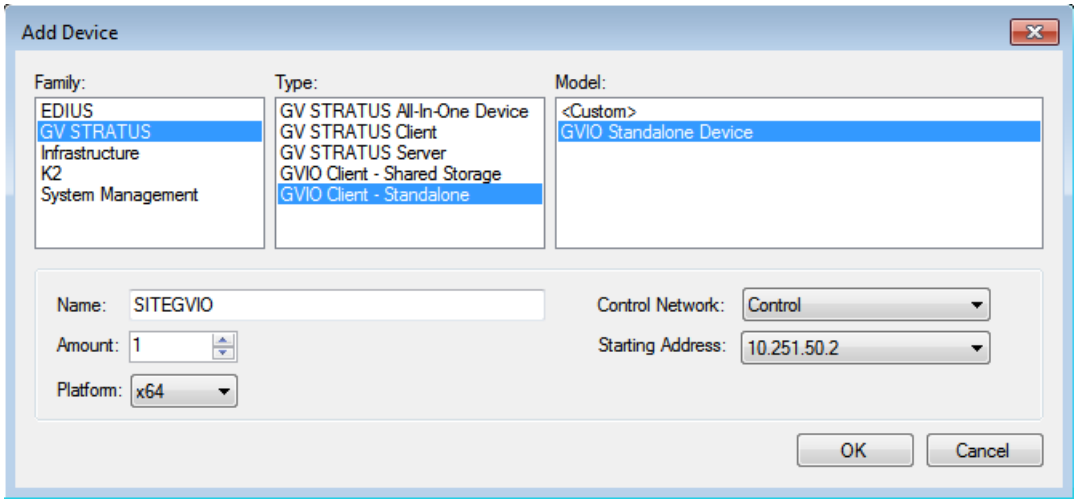
This process is required. You must add placeholder device for GV I/O Live Ingest and Playback Server to the SiteConfig system description.

Adding a GV I/O Client - Standalone to the system description

- The system description must contain a group.

1. In the **Network Configuration | Devices** tree view, right-click a group and select **Add Device**.

   The Add Device dialog box opens.



2. Configure settings for the device you are adding as follows:

   - Family – Select **GV STRATUS**.
   - Type – Select **GV I/O Client - Standalone**.
   - Model – Select **GV I/O Standalone Device**
   - Name – This is the device name, as displayed in the SiteConfig device tree view and device list view. This name can be different than the host name (network name). You can accept the default name or enter a name of your choice. Devices in the tree view are sorted alphabetically.
   - Amount – You can add multiple devices, as currently defined by your settings in the Add Device dialog box. An enumerator is added to the name to create a unique name for each device added.
   - Platform – Select **x86** for 32-bit operating system or **x64** for 64-bit operating system.
   - Control network – Select **Corporate LAN** or **Control**, as appropriate for the PC's network connection.
   - Starting Address – Select from the list of available addresses on the selected control network. If adding multiple devices, this is the starting address, with addresses assigned sequentially to each device added.

3. Click **OK** to save settings and close.
4. Repeat these steps for each of your devices.

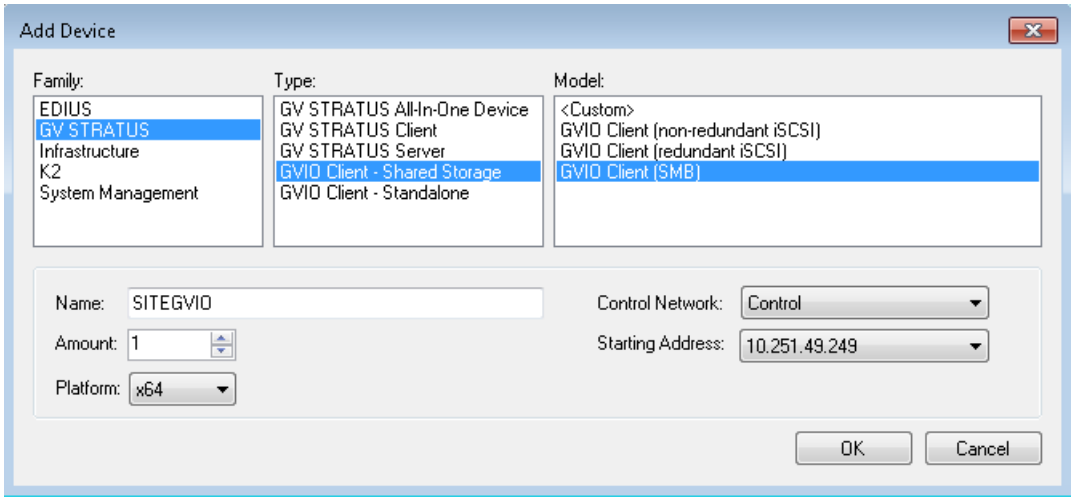
5. If the server is on the control network, verify that unmanaged control network interfaces are configured correctly and modify if necessary.

Adding a GV I/O Client - Shared Storage to the system description

- The system description must contain a group.

1. In the **Network Configuration | Devices** tree view, right-click a group and select **Add Device**.

   The Add Device dialog box opens.



2. Configure settings for the device you are adding as follows:

   - Family – Select **GV STRATUS**.
   - Type – Select **GV I/O Client - Shared Storage**.
   - Model – Select **GV I/O Client (SMB)**.
   - Name – This is the device name, as displayed in the SiteConfig device tree view and device list view. This name can be different than the host name (network name). You can accept the default name or enter a name of your choice. Devices in the tree view are sorted alphabetically.
   - Amount – You can add multiple devices, as currently defined by your settings in the Add Device dialog box. An enumerator is added to the name to create a unique name for each device added.
   - Platform – Select **x86** for 32-bit operating system or **x64** for 64-bit operating system.
   - Control network – Select **Corporate LAN** or **Control**, as appropriate for the PC's network connection.
   - Starting Address – Select from the list of available addresses on the selected control network. If adding multiple devices, this is the starting address, with addresses assigned sequentially to each device added.

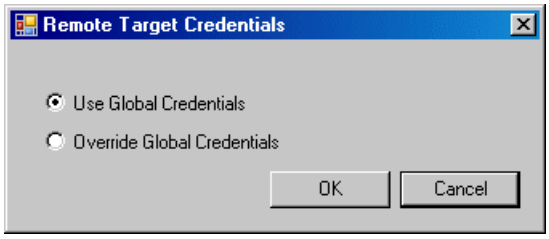
3. Click **OK** to save settings and close.
4. Repeat these steps for each of your devices.
5. If the server is on the control network, verify that unmanaged control network interfaces are configured correctly and modify if necessary.

Setting credentials for a specific device

For servers on the corporate LAN, override global credentials so that SiteConfig has access to the PC for software deployment.

1. In the tree view, right-click a device and select **Credentials**.

   The Remote Target Credentials dialog box opens.



2. Select **Override Global Credentials** and click **OK**.

   The Set Device Logon Credentials dialog box opens.

3. Enter the user name and password for the device and click **OK**. To test the credentials, right-click on the device and choose **Remote Desktop** to start a session to the device.

Adding GV I/O to the control network with SiteConfig

Before doing this task, make sure the GV I/O Live Ingest and Playback Server is added as a placeholder device to the SiteConfig system description.

The following steps are the standard tasks for adding a device to the control network using SiteConfig. Use these steps for the GV I/O Live Ingest and Playback Server you are adding.

1. Discover the device using SiteConfig device discovery.
2. Assign the discovered device to the placeholder device in the SiteConfig system description.
3. Modify the control network interface to ensure communication on the control network.
4. Modify the host name and/or device name as desired.
5. Ping the device to verify network communication.
6. Verify credentials to ensure SiteConfig can install software on the device.

Configuring deployment groups

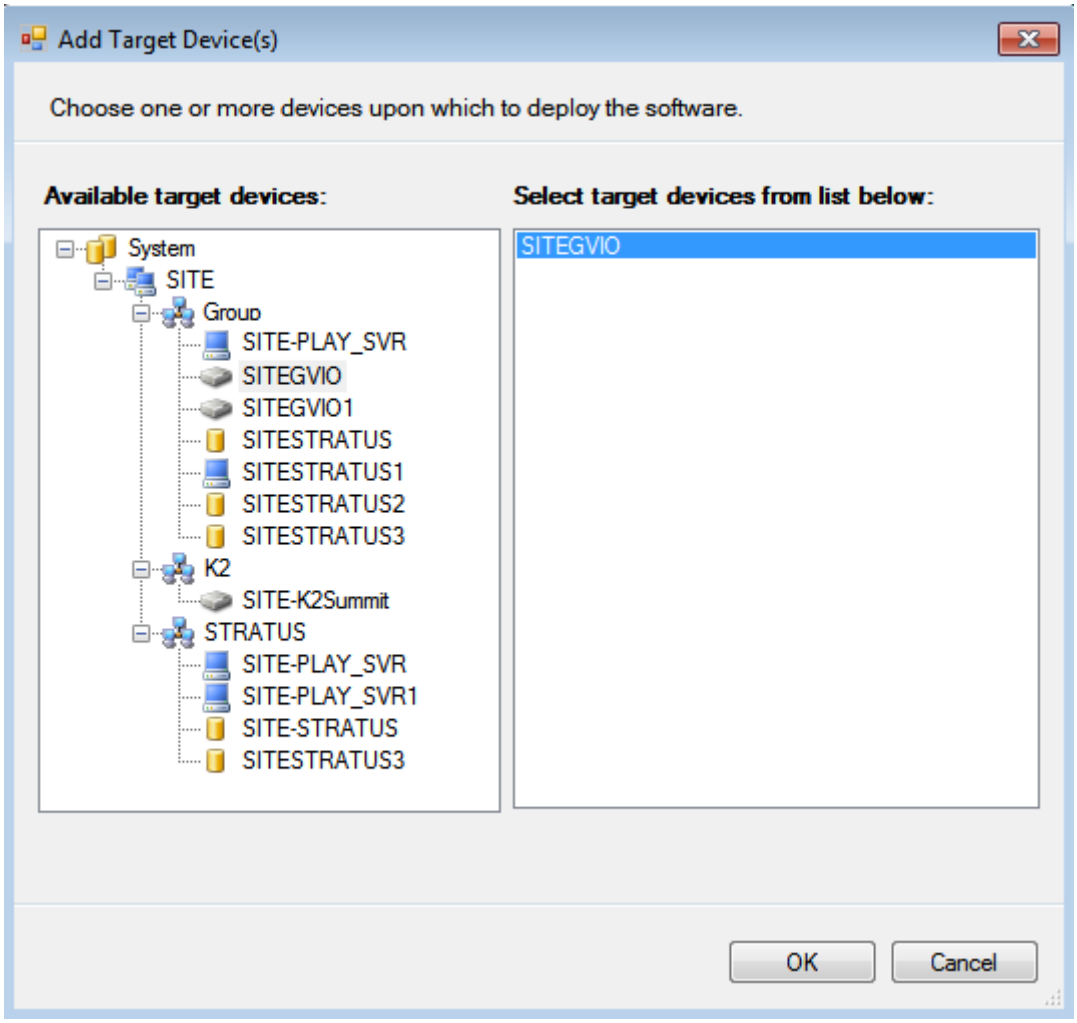
- The device must be assigned in the SiteConfig system description and network connectivity must be present.

1. In the **Software Deployment | Deployment Groups** tree view, right-click the top node and select **Add Deployment Group**.

   A deployment group appears in the tree view.

2. Right-click the deployment group, select **Rename**, and enter a name for the deployment group.

3. Right-click the deployment group and select **Add Target Device**.
   The Add Target Device(s) wizard opens.



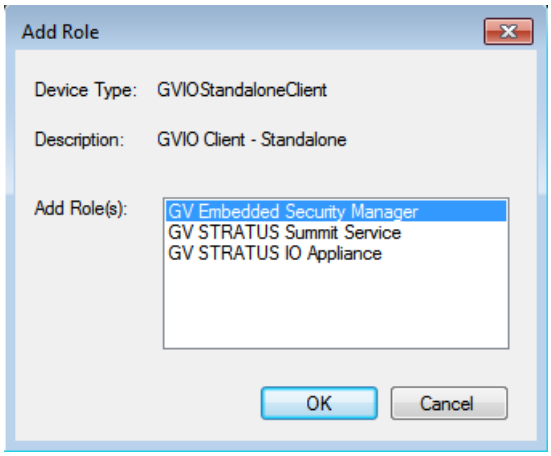
4. In the Available Target Devices tree view, select the node that displays the devices that you are combining as a deployment group.
5. In the right-hand pane, select the device that you are adding to the deployment group.
6. Click **OK**.

The devices appear in the Deployment Groups tree view under the deployment group. Before you perform a software deployment, you must check software on the devices that will be receiving new software.

Adding software roles to a GV I/O Client

1. In the **Software Deployment | Devices** tree view, right-click the device and select **Add Role**.

   The Add Role dialog box opens.



   The Add Role dialog box displays only those roles that SiteConfig allows for the selected device type.

2. Select the role or roles that you want to add to the device. Use Ctrl + Click or Shift + Click to add multiple roles.

   NOTE: If you added the correct GV I/O Client device (either for standalone or third party shared storage system), then the default roles are automatically added in SiteConfig.

   - GV I/O Live Ingest and Playback Server roles for standalone client from the following list:
     - GV STRATUS IO Appliance
     - GV Embedded Security Manager
     - GV STRATUS Summit Service
   - GV I/O Live Ingest and Playback Server roles for third party shared storage client with SMB connection from the following list:
     - GV STRATUS IO Appliance
     - GV Embedded Security Manager

3. Click **OK** to save settings and close.

   The new roles appear under the device in the tree view.

Installing software into a GV I/O Live Ingest and Playback Server

- The device on which you are installing software is in the SiteConfig system description and communicating on the control network.
- The device on which you are installing software has its credentials set in SiteConfig to allow access.

- The device to which you are deploying software must have their SiteConfig roles correctly configured.

1. On each GV I/O device, manually install the following:
   - **msxml.msi**
   - **Network_Driver_3PT51.exe**
   - **MLNX_WinOF2-1_80_51000_All_x64.exe**
   - **391.58-quadro-winserv-2016-64bit-international-whql.exe**
   - **GVEngineInstaller-x.x.x.xx_vcxxx.exe**
   - **MPIcore-x.xx.x.xxx** as follows:
     - Run the **setup64.exe**
     - On the GV I/O, go to *C | Program Files | Grass Valley | MPIO Core* and run **reg_mpicore.bat**
   - For SDI inputs, install AJA drivers below:
     - Run the **ntv2driver-xx.x.x.msi**
     - Run the **UpdateAjaFirmware.bat**
     - Power Cycle
   - For IP inputs, install the **VyDriver-x.x.x.xx.exe**
2. Launch the SiteConfig application.
3. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.
4. Click the **Add** button.
   The Add Package(s) dialog box opens.
5. Add the following cab files to the deployment group:
   - *GrassValley_GVIO_X.X.XX.XXXX.cab*
   - *GVEmbeddedSecurityManager_X.X.XX.XXXX.cab*
   - *DiscoveryAgent_X.X.XX.XXXX.cab*

   Refer to the compatibility table in release notes for specific version numbers.
6. If one or more EULAs are displayed, accept them to proceed. If you do not accept a EULA, the associated software is not assigned to the deployment group.
   SiteConfig adds the package to the deployment group.
7. Verify that deployment tasks are set to **Install** for the files listed above.
8. Run a **Check Software** on the GV I/O device.
9. Deploy software to the server.
10. Restart when prompted and log on to the GV I/O device.
11. Save SiteConfig to push the configuration to the core server.

The Grass Valley AppService console application will start automatically when a user logs on to the GV I/O device.

NOTE: Ensure the Grass Valley AppService stays running during normal operation of the GV I/O device.

Next, license the GV I/O Live Ingest and Playback Server.

About the Grass Valley AppService

To establish a connection between GV STRATUS software and the GV I/O Live Ingest and Playback Server, a user must log in to the GV I/O device and allow a console application named **Grass Valley AppService** to execute.

The **Grass Valley AppService** console application will start automatically when a user logs in to the GV I/O host. The user must stay logged in with the **Grass Valley AppService** running during normal operation of the GV I/O device.

NOTE: Only a single instance of Grass Valley AppService will execute on the host even if another user logs in to the same GV I/O host.

When using GV I/O Live Ingest and Playback Server with the Isilon shared storage, the user that executes the **Grass Valley AppService** console application must have read and write permissions to the UNC path configured for the GV I/O device to use in storing high resolution media files.

For proper operation of ingest and playout operation with Isilon shared storage, the UNC path used for media storage must be mapped to a V:\ drive on the GV I/O host.

Shutting down the Grass Valley AppService

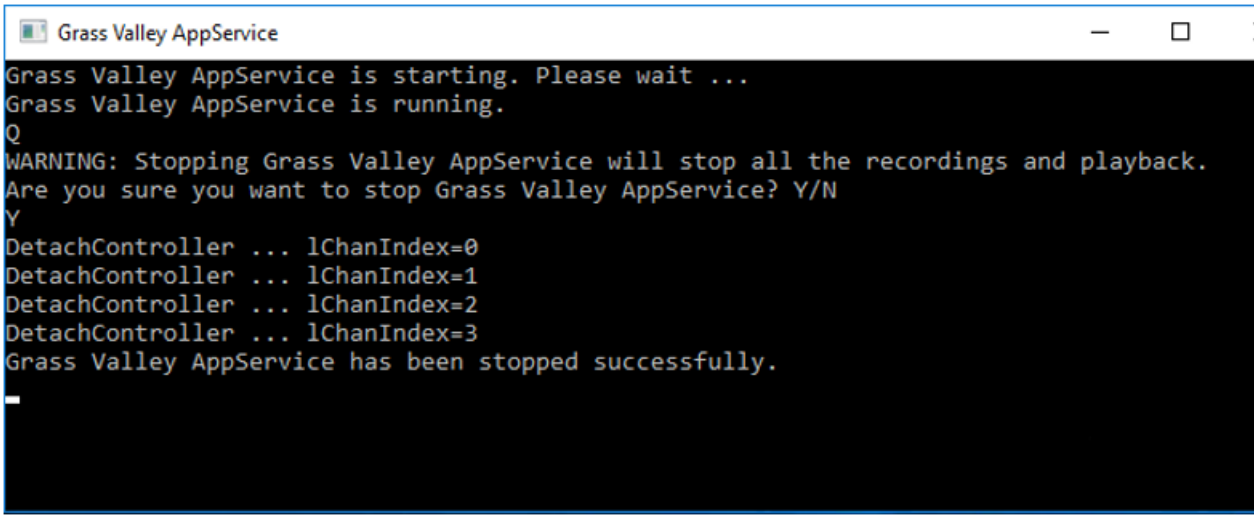
Prior to logging out of the GV I/O host, a user is recommended to shut down the Grass Valley AppService console application gracefully using the procedure below.

However, it is acceptable to reboot the GV I/O host without executing this shutdown process.

1. In the command line window for **Grass Valley AppService**, enter **Q** to start the shutdown process.

   A warning message appears to inform all recordings and playback will be stopped, and the user must confirm the decision to shutdown the **Grass Valley AppService**.

2. Enter **Y** to stop the **Grass Valley AppService**.



   A message appears to inform that the **Grass Valley AppService** has been stopped successfully.

3. Close the window.

4. Log out of the GV I/O host.

Licensing GV I/O Live Ingest and Playback server

Licenses are requested through email and managed through the SabreTooth License Manager, which is installed on the Grass Valley product with the Grass Valley software. The SabreTooth License Manager must be located on the Grass Valley product.

License information is stored in XML files that you can manage just like any other file on your system. Node-locked licenses are unique to the system for which they are requested and cannot be used on any other machine. You should back up the license text files to a separate drive or as part of a recovery image.

Licenses are based on your system's unique identifier, which is partially derived from your system's Media Access Control (MAC) address. If you change your system's MAC address by performing operations such as changing the System Processor card, you must obtain a new license based on the new MAC address.

SabreTooth GV I/O license process

The **GVIO-SVR-SW** license is required for each GV I/O Live Ingest and Playback Server device.

The **GVIO-SVR-ISCSI** license is required for GV I/O Live Ingest and Playback Server with iSCSI connection.

The **GVIO-SVR-SDI** license is required for GV I/O Live Ingest and Playback Server to record and playout via SDI channels. One license is required for each channel.

The **GVIO-SVR-IP** license is required for GV I/O Live Ingest and Playback Server to record via IP channels. One license is required for each channel.

The **GVIO-SVR-WEB** license is required for GV I/O Live Ingest and Playback Server to record via Web Stream channels. One license is required for each channel.

If you received your system pre-configured from Grass Valley, licenses are already installed, so you can skip these tasks. Otherwise, do the following:

1. Refer to the license sheet that you received with your GV STRATUS license. The license sheet has the Sales Order number that you need.
2. On the GV STRATUS server with role of Common Services, run the SabreTooth License Manager, generate a unique ID, and send the email to Grass Valley requesting your license or licenses.
3. When you receive your license file, use the SabreTooth License Manager and install it on the GV I/O Live Ingest and Playback Server.
4. Reboot the GV I/O Live Ingest and Playback Server device after installing the license.

Verifying the GV I/O configuration

- The required licenses have been added to the GV I/O Live Ingest and Playback Server.
- For the GV I/O client of Isilon shared storage system, the V: drive of the GV I/O had been mapped to the UNC path of the Isilon hi-res media storage.

- The GV I/O device had been set to Enabled mode.

Within the GV STRATUS system, do the following to verify the GV I/O Live Ingest and Playback Server is configured properly. Grass Valley recommends the GV STRATUS Control Panel is only configured on the Core server:

- For GV I/O Live Ingest and Playback Server with iSCSI connection, do the following:
  - Run the iSCSI Initiator on each GV I/O server before attempting to configure them in K2Config.
  - Add the GV I/O server(s) as **GV I/O Live Ingest & Playback** devices and configure them as you would a K2 Summit client.
  - Sync K2Config to the GV STRATUS Core server.
- In the GV STRATUS Control Panel application, do the following:
  - Verify that you can see the **STRATUS GV I/O Appliance** in the **Core | K2 Storage | K2 Standalone Storage** tab for the GV I/O standalone server.
  - Verify that you can see the **STRATUS GV I/O Client** in the **Core | K2 Storage | K2 SAN Storage** tab for the GV I/O client in Isilon network-attached storage system.
  - In **Core | Proxy Config | Proxy Settings** tab, re-select check-boxes, resave the proxy settings and verify in **Test Connections** tab that the **STRATUS GV I/O Client** Device Types are connected with the proxy server.
  - In **Core | MDI Configuration** settings, re-save all Grass Valley Media Server MDIs with GV I/O servers attached.
  - Reboot the GV STRATUS Core server and GV I/O servers for the changes to take effect.
  - Set the signal feed on the SDI input of the AJA card first when connecting a video feed to the GV I/O server, .
  - Then in **General | Format** tab, add formats according to signal formats already set to the AJA card, if they are not readily available.
  - In the **General | Channels | GV I/O** tab, verify that the GV I/O channels are displayed. The **Channel Format** should be set according to signal feeds configured to each channel. Change the **Channel Format** setting to match the format of signal feed already connected to the channel.
  - To add GV I/O channels to the Scheduler tool: In the **Applications | Ingest | Channel Setup** tab, add one or more **GV I/O Device** channels:
    - **Type of device**: Select either **SAN Client** or **Standalone Client**.
    - **SAN Name**: Choose a SAN with one or more GV I/O devices.
    - **Primary Device**: Select the desired GV I/O device in the drop-down list.
    - **Select Standalone**: Select the standalone GV I/O device in the drop-down list.
    - **Channel Type**: Select **Recorder**.
    - **Client Channel**: Select a channel from the drop-down list.
    - **Router Destination**: Select a router destination, if applicable.
    - **Timecode Format**: Select **Time of Day**.
- In the GV STRATUS application, do the following:
  - In the Scheduler tool, verify that GV I/O channels configured in Ingest settings of the GV STRATUS Control Panel are displayed and able to record.

- To add GV I/O channels to the Channel Panel: In the Navigator panel, expand the Tools node and select Channel Panels. Right-click on the desired Channel Panel and select **Open With | Inspector**.
  - Verify that all configured GV I/O Live Ingest and Playback Servers are displayed.
  - Add one or more channels from a GV I/O Live Ingest and Playback Server.
  - Verify that GV I/O channels have a **...** button and you can set the Timecode Source to **Time of Day** or a specific **Start Time** for each GV I/O channel.
  - Verify that you can record on those GV I/O channels.
- To add GV I/O servers to the GV STRATUS Rundown application: In the GV STRATUS Control Panel, go to **Applications | Rundown | Media** tab. Add one or more **GV I/O Device** as the Playout Server(s) and click **Save**.

  Then, launch the GV STRATUS Rundown application and go to **Tools | Options | Channel Configuration** tab to add GV I/O channels as playout channels.

  Verify that GV I/O channels configured in GV STRATUS Rundown are able to playback assets.

Setting backup and recovery of the GV I/O Live Ingest and Playback Server

About the recovery image process

An image of the GV I/O Live Ingest and Playback Server system drive is provided with the product package. You can restore the GV I/O Live Ingest and Playback Server from this image. This simplifies the process of rebuilding a system in a disaster recovery scenario.

When you receive your GV I/O Live Ingest and Playback Server new from the factory, you receive a system-specific image for that particular GV I/O Live Ingest and Playback Server. This factory image is stored on a bootable USB Recovery Flash Drive. Also on the Recovery Flash Drive is the Acronis True Image software necessary to create and restore an image.

After your GV I/O Live Ingest and Playback Server is installed, configured, and running in your system environment, you should create new recovery disk images for the machine to capture settings changed from default. These “first birthday” images are the baseline recovery image for the machine in its life in your facility. There is enough space on the Recovery Flash Drive to store the first birthday image along with the factory image.

You should likewise create new recovery disk images after completing any process that changes system software or data, such as a software upgrade. In this way you retain the ability to restore to a recent “last known good” state.

Creating a recovery disk image

Before creating a recovery image, determine the storage location for the image. Grass Valley recommends that you store the recovery image on the Recovery Flash Drive, and this task provides instructions for that location. If you use a different location, such as a network connected drive or another connected USB drive, alter the steps in this task as appropriate.

1. Make sure that media access is stopped and that the system on which you are working is not being used.

2. If you have not already done so, connect keyboard, monitor, and mouse.
3. Do the following:
   a) Insert the Recovery Flash Drive into the front USB port.
   b) Restart the machine, or power on if currently shut down.

      The machine boots from the Recovery Flash Drive, into a version of Windows stored on the drive.

      A MS-DOS command window opens.
   c) Press the **F11** key to enter Boot options.
   d) When prompted with a list of options, select the Acronis option and then press **Enter**.

   The Acronis program loads.
4. In the Acronis main window, click **Backup**.

   The Create Backup Wizard opens.
5. On the Welcome page, click **Next**.
6. On the Partitions Selection page, do the following:
   a) Select the **(C:)** and the **(D:)** partitions and then click **Next**.
7. On the Backup Archive Location page, do the following:
   a) In the tree view select the **Backup (E:)** partition and enter the name of the image file you are creating.

      Create the file name using the machine hostname and the date. Name the file with the .tib extension.

      For example, if the hostname is MySystem1, in the File name field you enter *E:\MySystem1_20180327.tib*.
   b) Click **Next**.
8. On the Select Backup Mode page, select **Create a new full backup archive** and then click **Next**.
9. On the Backup Options page, do not change any settings. Click **Next**.
10. On the Archive Comment page, if desired, enter image comments such as the date, time, and software versions contained in the image you are creating. Click **Next**.
11. On the "…ready to proceed…" page, do the following:
    a) Verify that you are creating images from the C: and D: partitions and writing to the E: partition, then click **Proceed**.
12. On the Operation Progress page, observe the progress report.
13. When a message appears indicating a successful backup, click **OK**.
14. Click **Operations | Exit** to exit the Acronis True Image program.

    The machine restarts automatically.
15. Remove the recovery media while the machine is shutting down.

Restoring from a system-specific recovery image

- Use Ctrl+R options during boot up to re-initialize the RAID1 and RAID5 virtual drives and wipe any previous configurations.

Use this task to restore using an image made from the particular GV I/O Live Ingest and Playback Server.

Before restoring from a recovery image, make sure that the GV I/O Live Ingest and Playback Server has access to the image from which you are restoring. This task provides instructions for accessing an image on the Recovery Flash Drive. If you access an image from a different location, such as a network connected drive or another connected USB drive, alter the steps in this task as appropriate.

1. Make sure that media access is stopped and that the system on which you are working is not being used.
2. Do the following:
   a) Insert the Recovery Flash Drive into the front USB port.
   b) Restart the machine, or power on if currently shut down.

      The machine boots from the Recovery Flash Drive, into a version of Windows stored on the drive.

      A MS-DOS command window opens.
   c) Press the **F11** key to enter Boot options.
   d) When prompted with a list of options, select the Acronis option and then press **Enter**.

   The Acronis program loads.
3. In the Acronis main window, click **Recovery**.

   The Restore Data Wizard opens.
4. On the Welcome page, click **Next**.
5. On the Backup Archive Selection page, in the tree view expand the node for **Removable Disk (E:)** and select the image file, then click **Next**.
6. On the Restoration Type Selection page, select **Restore disks or partitions** and then click **Next**.
7. On the Partition or Disk to Restore page, select **MBR and Track 0** and then click **Next**.
8. On the Disk Selection page, select **Disk 1** and then click **Next**.
9. On the Next Selection page, select **Yes, I want to restore another partition or hard disk drive** and then click **Next**.
10. On the Partition or Disk to Restore page, select **(C:)** and then click **Next**.
11. On the Restored Partitions Resizing page, select **Yes, I want to resize partitions** and then click **Next**.
12. On the Restored Location page, select **(C:)** and then click **Next**.
13. On the Restored Partition Type page, select **Active** and then click **Next**.
14. Do one of the following:
    - If the Restored Partition Size page does not appear. Skip ahead to the Next Selection page.
    - If the Restored Partition Size page appears. Continue with the next step.

15. On the Restored Partition Size page, do one of the following:
    - If **Free space after** reports 0 bytes, leave settings as they are. Click **Next**.
    - If **Free space after** does not report 0 bytes, increase **Partition size** until **Free space after** reports 0 bytes. Click **Next**.
16. On the Next Selection page, select **No, I do not** and then click **Next**.
17. On the Restoration Options page, do not make any selections. Click **Next**.
18. On the "…ready to proceed…" page, verify that you are restoring the correct image to the correct location. Click **Proceed**.
19. On the Operation Progress page, observe the progress report.
20. When a message appears indicating a successful recovery, click **OK**.
21. Click **Operations | Exit** to exit the Acronis True Image program.

    The machine restarts automatically.
22. Remove the recovery media while the machine is shutting down.
23. When prompted, enter the GV I/O Live Ingest and Playback Server machine name.

    Make sure the name is identical to the name it previously had.

    At first start up after reimage, the system is in Embedded Security Update mode by default.

Fault Tolerant Server

About the FT Server

Introduction

The FT server is a fault-tolerant server focusing on high reliability in terms of fault-tolerance, in addition to high performance, scalability, and general versatility. In the event of component failure on one CPU/IO module, its mirrored configuration on the other module will allow system control to be switched instantaneously to the other identical CPU/IO module to assure non-stop operation. This switching occurs seamlessly from the failed CPU/IO module to the other module, minimizing loss of data or application state. You can use the FT server series in a mission-critical system where high availability is required.

Grass Valley supplies FT servers at two performance levels. At each level, CPU, memory, and drives are configured to provide specified performance characteristics. Based on the performance required to support your small, medium, or large Grass Valley system, the appropriate FT server level is provided.

In addition, there is a Type I FT server and a Type II FT server. Each server type corresponds to a different generation of the base platform. Both the Type I FT server and the Type II FT server are provided at the two performance levels mentioned above.

Related Topics

Identifying the FT Server model on page 1708

Standard features

The FT server system has two CPU/IO modules with dual module redundancy, offering continuous operation in case of a failure. It offers high performance, expansion options, and high reliability outlined in the summary below.

- The system comes ready to use with quick connections for the duplex LAN, USB, and monitor connections.
- The main enclosure is rack-mountable and the main components are easy to install.
- The Fault Tolerant feature includes redundant hardware and software in one system with quick isolation of a failed module.
- The two CPU/IO modules and their hard disk drives come mirrored from the factory.
- High performance features include a powerful central processor and high speed Ethernet interface and disk access from SAS (Serial Attached SCSI) disk drives.
- High reliability is achieved by a memory monitoring feature, bus parity error detection, and error notification.
- Self diagnostics include a Power On Self-Test (POST) and a test and diagnostics utility.
- An off-line maintenance utility is also available.

To make the best use of these features, read this Instruction manual thoroughly to understand how to operate the FT server.

Product component summary

The main components of the FT server are the following:

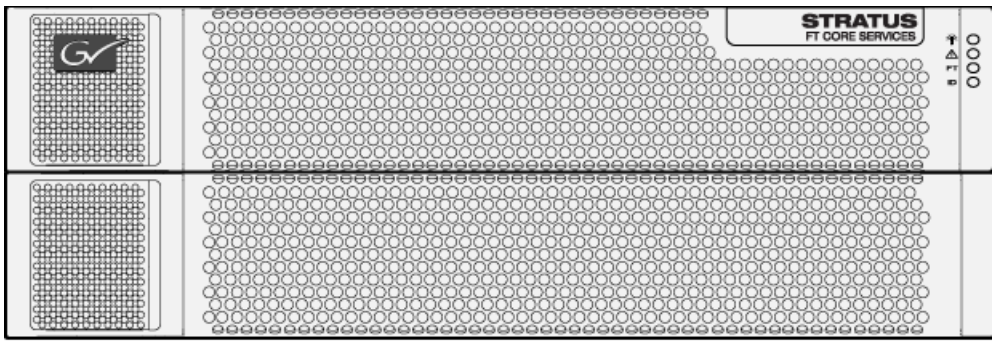
- One 4 RU high rack-mountable chassis.
- Two identical CPU/IO modules (module 0 and module 1).
- Two redundant power supplies, one in each CPU/IO module enclosure.
- Eight hard disk drive bays per CPU/IO module.
- One optical disk drive to read data from disks such as DVDs and CD-ROMs.

Main ports and connectors include:

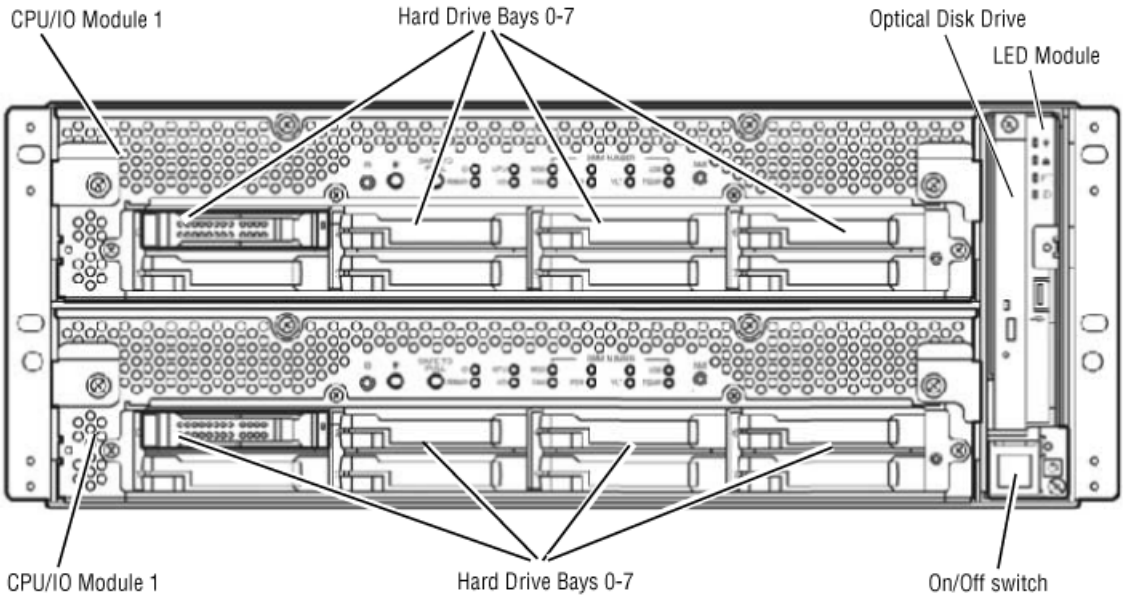
- 3 USB ports on the rear backplane for connecting devices supporting USB interface such as a mouse and keyboard.
- An Ethernet management port.
- Two Gbit Ethernet LAN connectors per CPU/IO module which are configured for teamed LAN control.
- Two COM ports for maintenance (for use with Customer Service only).
- One monitor connector for connecting a display device.

Front view

The front view of the FT server front bezel is shown below. The front bezel comes packaged separately and should be installed after rack mounting the FT server. It should remain installed during normal operation for proper cooling of the unit.



A fully loaded system is shown below with the front bezel removed. Front LED indicator states on the front bezel and on each CPU/IO module and other components visible when the bezel is removed are described in detail in the Monitoring section of this manual.

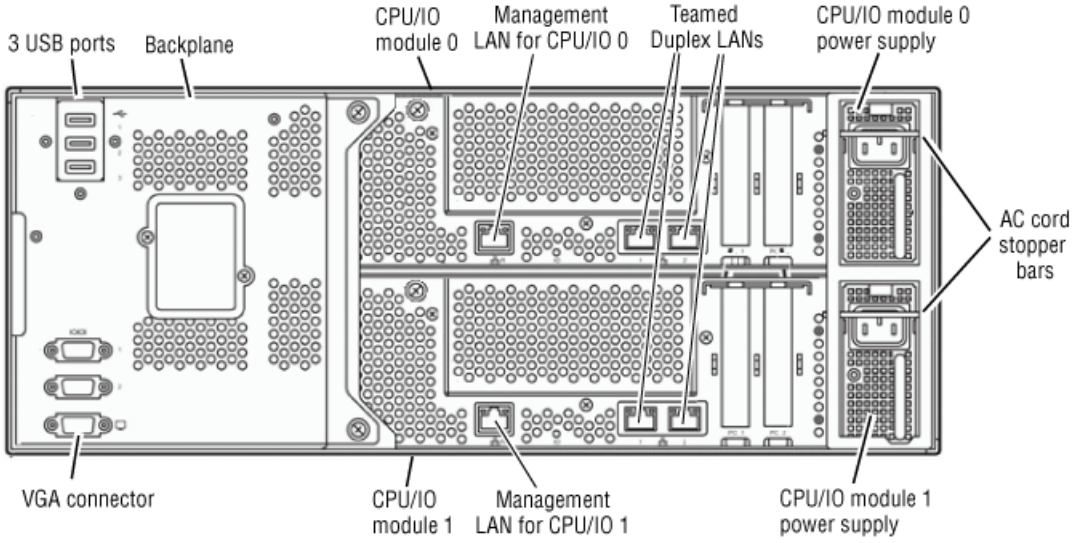


Related Topics

Front status LEDs (bezel removed) on page 1700

Rear view components

A rear view of the main components of the FT server is shown below.



The system backplane connects to the left rear of both CPU/IO modules. It provides USB connectors for mouse and keyboard control and serial connectors for maintenance when working with Customer Service and a VGA connector for connecting to a monitor.

The CPU/IO modules each have a separate removable power supply. When an AC cord in installed in the receptacles for each power supply, the AC cord stopper bars will be pushed up. In this position, the CPU/IO modules cannot be removed until the AC cords are removed (no power to CPU/IO modules).

Each CPU/IO module has a Maintenance LAN connector and dual LAN connectors for communication. Three USB ports are available on the system backplane for mouse and keyboard connection. All system cabling is described later in this manual.

Related Topics

Cable connections on page 1666

FT Server Installation Information

Installation overview

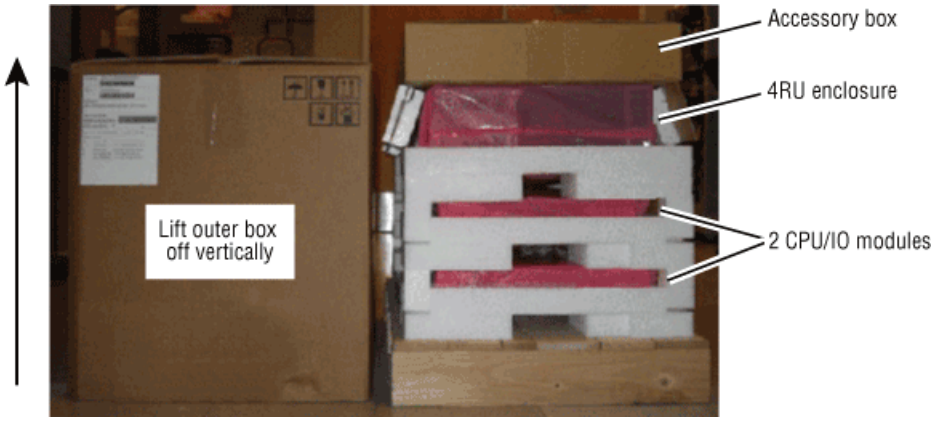
The FT server must be rack-mounted. It is a precision device and should be installed only by qualified maintenance personnel.

Observe the following warning and cautions to unpack, install, and use the FT server safely:

- Read and follow the safety section at the beginning of this manual. Failure to do so can pose a risk of a serious injury, such as a burn, personal injury or damage to physical assets.
- A fully loaded FT server chassis is heavy; have at least two people available for installation.
- This unit may be installed in a standard 19 inch tapped or untapped video rack or a standard 19 inch EIA IT rack.
- Install the product in places designated by the specifications only.
- Do not attempt to assemble or disassemble parts of this device alone.
- Use caution to avoid injury to hands and fingers when installing.

Unpacking

The FT server ships packaged as shown below.



You will need two or three people to unpack and rack the FT server safely.

To unpack the shipping box:

1. Cut the plastic bindings holding the outer box to the pallet and lift the outer box vertically to access the contents.

2. Lift off the accessory box and check for the contents listed below:
   - Assorted hardware for installing enclosure and side brackets
   - CD with OS software
   - Front bezel
   - Rack mount side brackets
3. Remove the 4RU enclosure with backplane and optical drive installed.
4. Remove the two identical CPU I/O modules.
5. Install the brackets and 4RU enclosure, then the CPU/IO modules and front bezel as described in the installation instructions for these items.

Related Topics

Install chassis in rack on page 1660
Install CPU/IO modules on page 1664
Install or remove front bezel on page 1676

Rack types

The FT server can be installed in any of the standard 19 inch video or EIA racks listed below.

- A standard 19 inch video rack with 0.281 round untapped holes with universal spacing requires the installation of a front adapter flange and a front plate included in the accessory kit.
- A standard 19 inch video rack with #10-32UNF tapped holes requires the installation of a front adapter flange and a rear adapter flange included in the accessory kit.
- A standard EIA IT rack with square holes uses threaded core nuts to attach the screws hold to the unit in place. No adapters are required.

Procedures for all three types of rack mounting are described in this manual. Use the procedure that matches your rack type.

Installing rack rail brackets in untapped rack

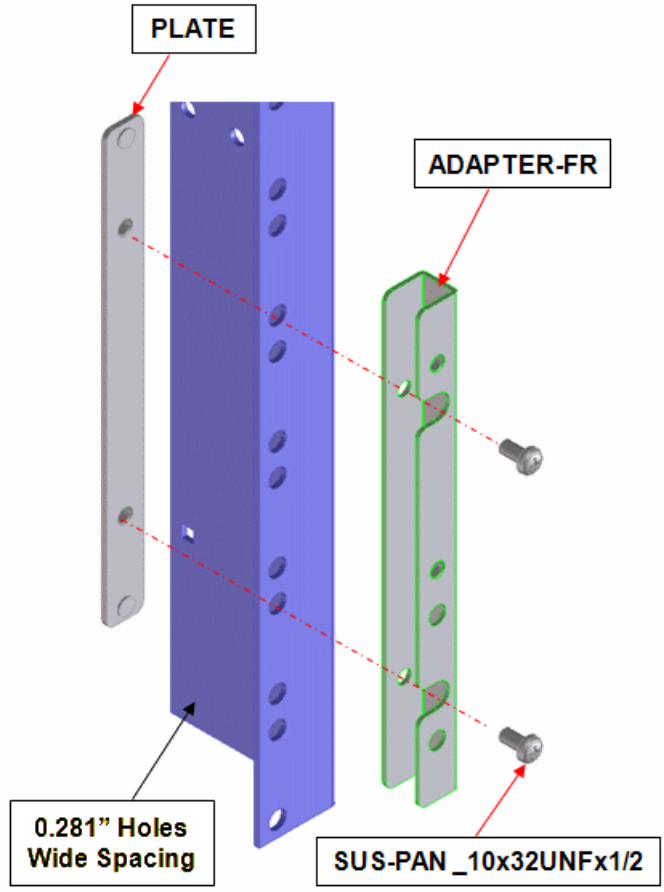
The FT server chassis requires 4RUs of space. Be sure to have another person help you to install the chassis, do not attempt to install it alone.

You will need the following hardware from the accessory kit to install the rack rail brackets to support the chassis in a untapped rack:

- 2 rack rail mounting brackets
- 2 front flange adapters (ADAPTER-FR)
- 2 plate adapters (PLATE)
- 8 panhead screws
- 4 washers

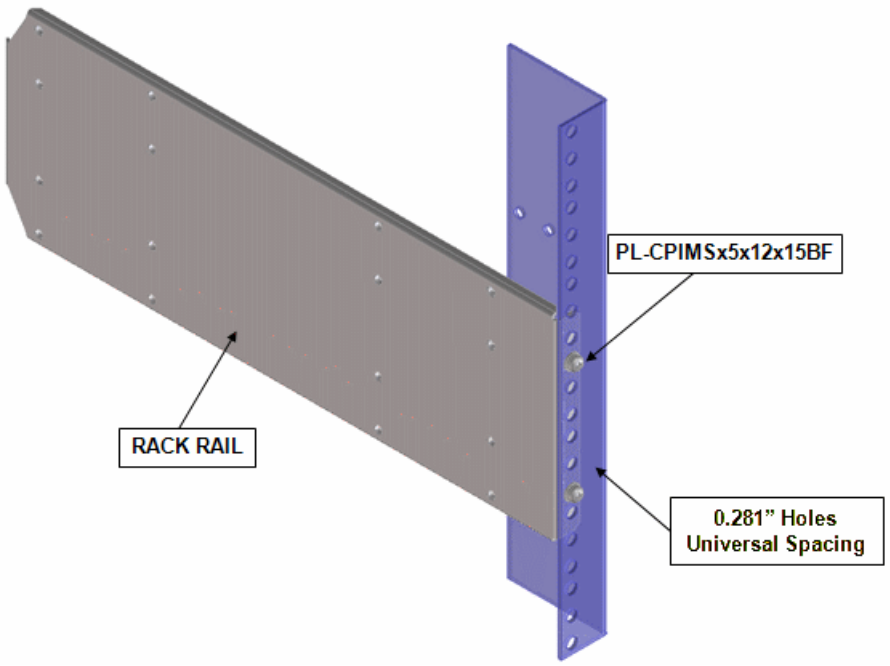
1. Locate the desired positioning of the FT server in the rack.

2. On both sides of the rack, line up the front adapter and plate as shown below.



3. Attach the front adapters and plates to the front of the rack with the panhead screws provided on the left and right sides of the rack front.

4. Now attach the rear of each rack rail bracket to the left and right rear sides of the rack using the 4 remaining panhead screws and washers. No adapters are necessary for this step.



5. Now go to the instructions for installing the FT server chassis.

Installing rack rail brackets in tapped rack

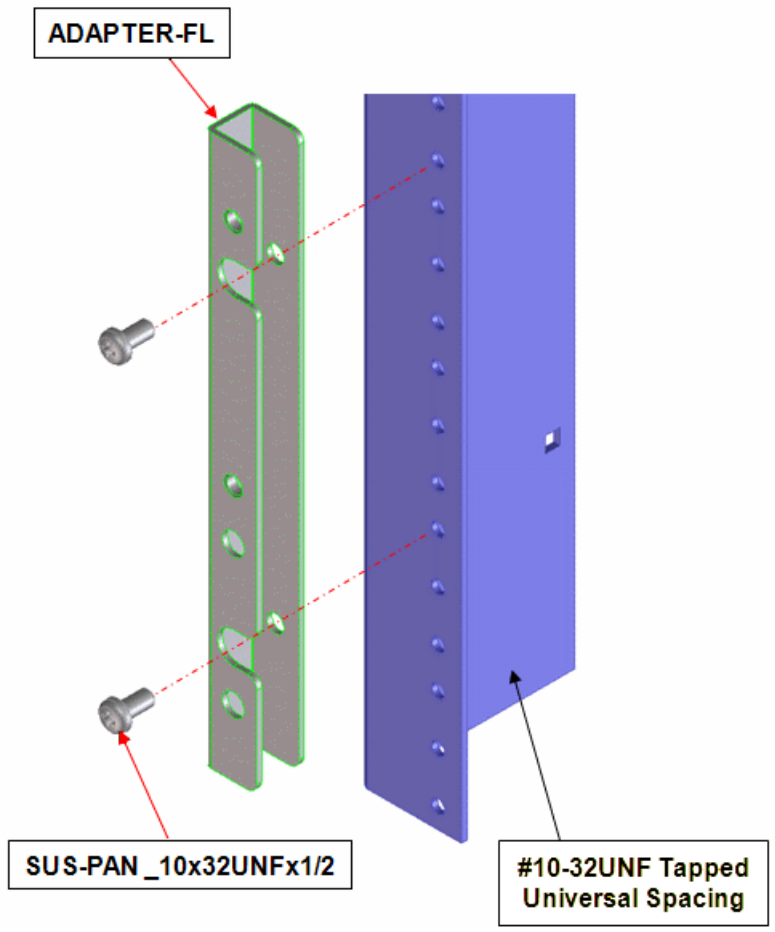
The FT server chassis requires 4RUs of space. Be sure to have another person help you to install the chassis, do not attempt to install it alone.

You will need the following hardware from the accessory kit to install the rack rail brackets to support the chassis in a tapped rack:

- 2 rack rail mounting brackets
- 2 front flange adapters (ADAPTER-FL)
- 2 rear flange adapters (ADAPTER-R)
- 8 panhead screws
- 4 panhead washers

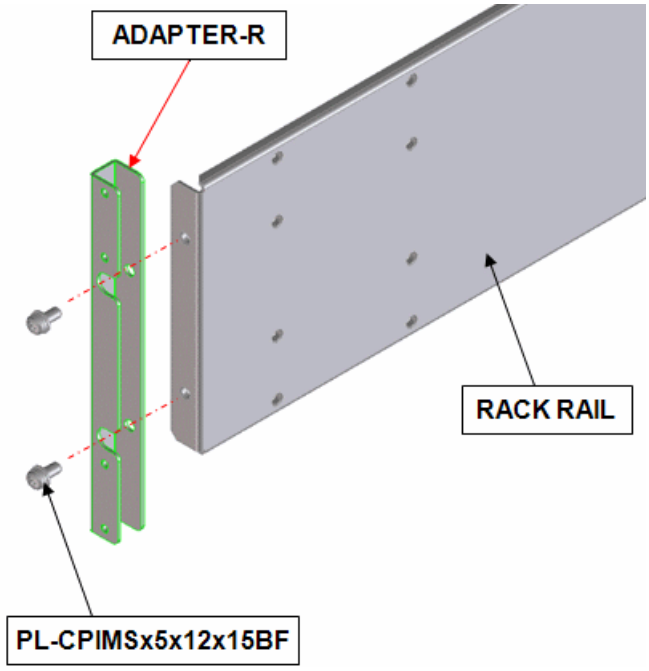
1. Locate the desired positioning of the FT server in the rack.

2. On both sides of the rack front, line up the front adapter as shown below.

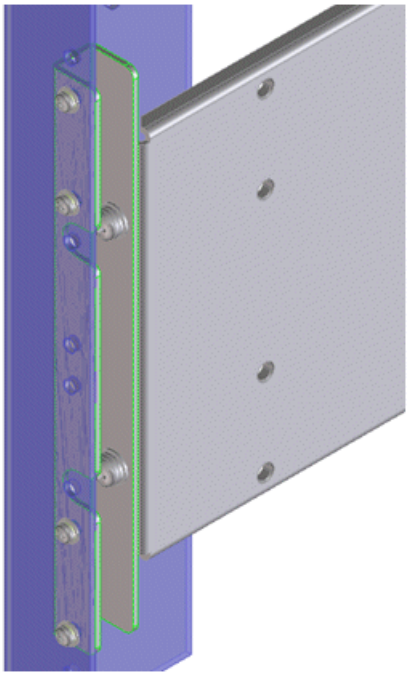


3. Attach the front adapters to the front of the rack with the panhead screws provided on the left and right sides of the rack front.

4. Attach a rear adapter to the rear of each rack rail.



5. Attach the rear of each adapter/rack rail assembly to the left and right rear sides of the rack using the 4 screws and washers.



6. Now go to the instructions for installing the FT serverchassis.

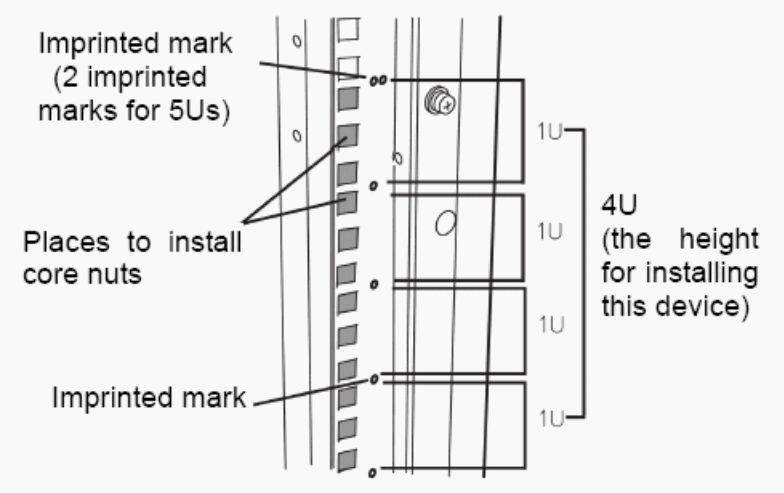
Install rack rail brackets in IT rack

The FT server chassis requires 4RU of space. Be sure to have another person help you to install the chassis, do not attempt to install it alone.

You will need the following hardware from the accessory kit to install the rack rail brackets to support the chassis in an EIA IT rack:

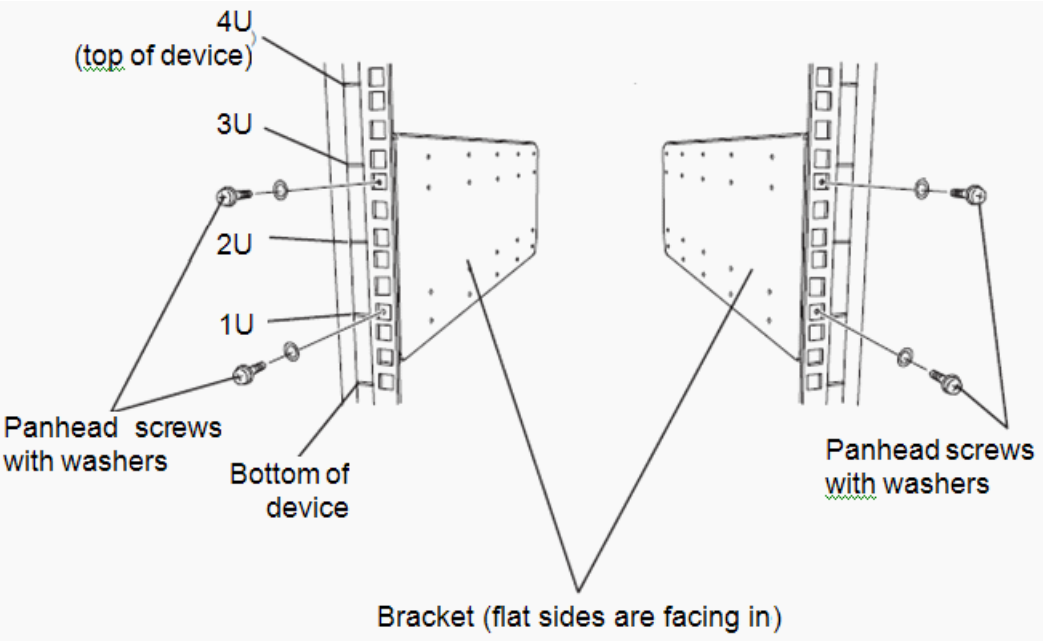
- 2 rack rail mounting brackets
- 4 washers for panhead screws
- 8 plate screws
- 8 panhead screws
- 4 core nuts (not provided)

1. Determine where in the rack you want to install the FT server chassis. If using an empty rack, install it in a lower position near the bottom of the rack rather than at the top to maintain balance.
2. Next to a square hole on the rack, an imprinted mark indicates 1RU. This device is 4RU (about 176 mm), so install it between the imprinted marks that indicate the height of 4RU.

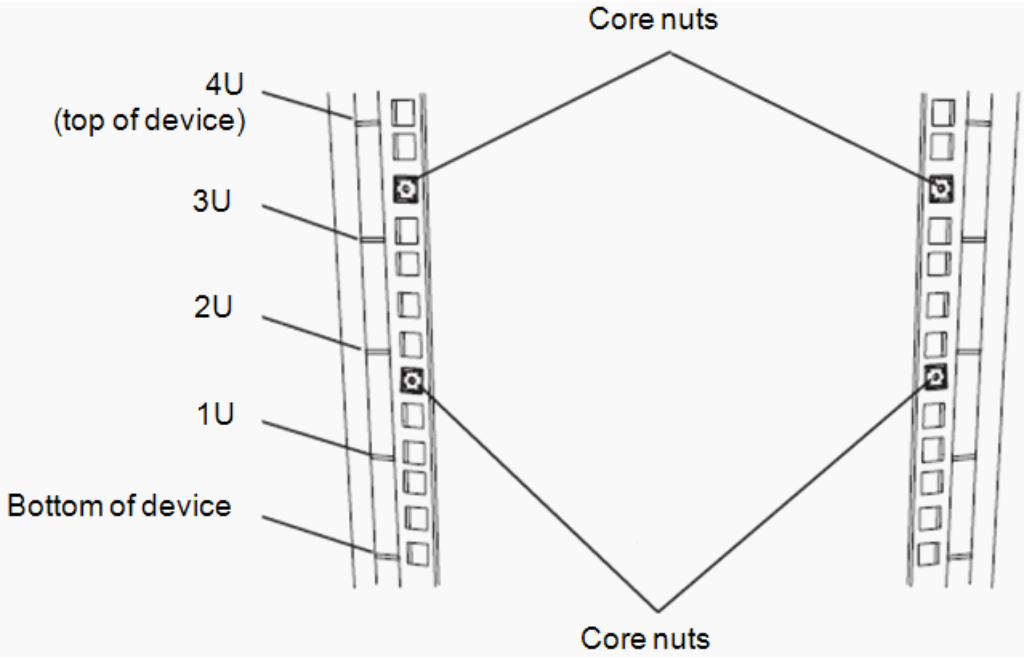


3. If the rack has front and rear doors, read the instruction that comes with the rack, and open them.

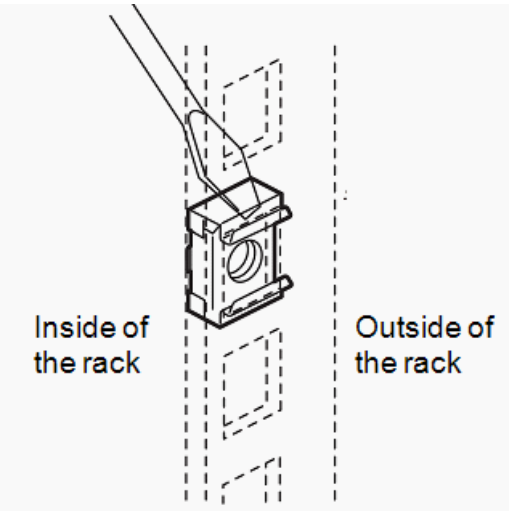
4. Install the rack rail brackets from the rear side of the rack with their flat sides facing in. Attach the brackets to the rack by installing the four panhead screws with washers just above the 1RU mark and just below the 3RU mark as shown below. Fasten the screws just enough to hold the brackets in place. Do not tighten them all the way.



5. Install the four core nuts (not provided) to the front of the rack so the left and right sides are in the same locations as shown below.



6. Install a core nut from inside of the rack. Hook either of the clips of the core nut to a square hole of the rack. then hook the other clip to a hole by a flat-blade screwdriver.



7. Now go to the procedure for installing the FT server chassis.

Temperature requirements for rack installation

The FT server requires good ventilation and proper airflow to operate properly. Make sure you meet the temperature airflow and humidity requirements listed below before installing the FT server in the rack.

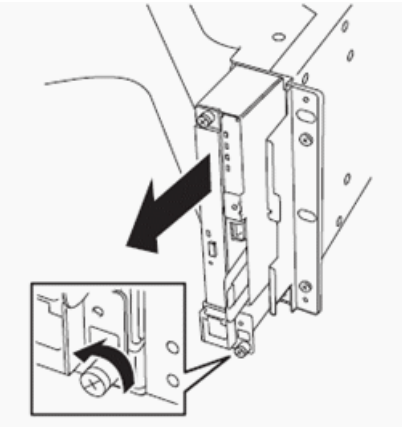
- The operating temperature of the FT server is from 10 degrees C (50 degrees F) to 35 degrees C (95 degrees F). Please take adequate precautions and measures for maintaining the proper airflow inside the rack as well as in the room so that the internal temperature can be kept within this range during operation.
- The recommended operating room temperature range is between 15 degrees C (59 degrees F) and 25 degrees C (77 degrees F).
- Optimum humidity for proper operation should be kept between 20 and 80%.
- Use only the rack installation instructions given in this manual to install the unit and other components as recommended to avoid overheating conditions.

Install chassis in rack

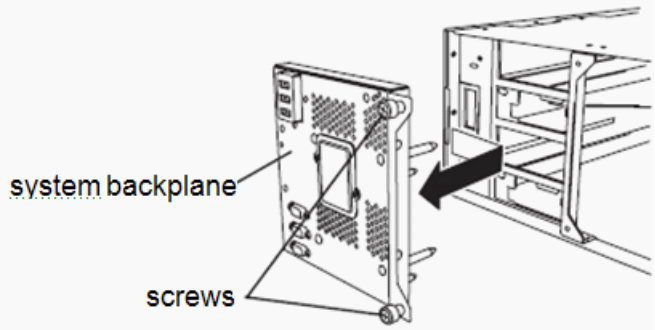
Once you have installed the rack mounting brackets, install the FT server empty chassis enclosure in the rack.

NOTE: Installation will vary slightly according to whether there is an adapter on the front of the rack. A standard EIA IT rack with no adapters is shown.

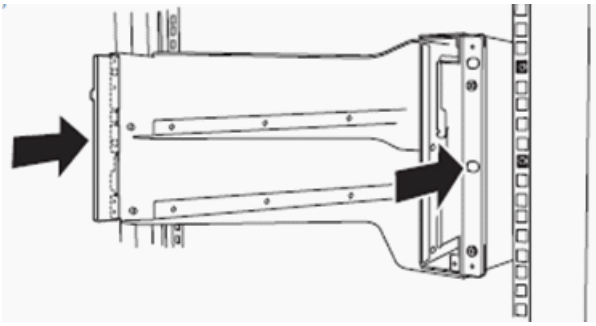
1. Remove the front unit containing the DVD drive and the LED module from the front of the chassis by loosening the screw at the bottom of the unit and pulling it out.



2. At the rear of the chassis, remove the system backplane. Loosen the two thumb screws then move the backplane slightly to the right and pull it straight out from the chassis.

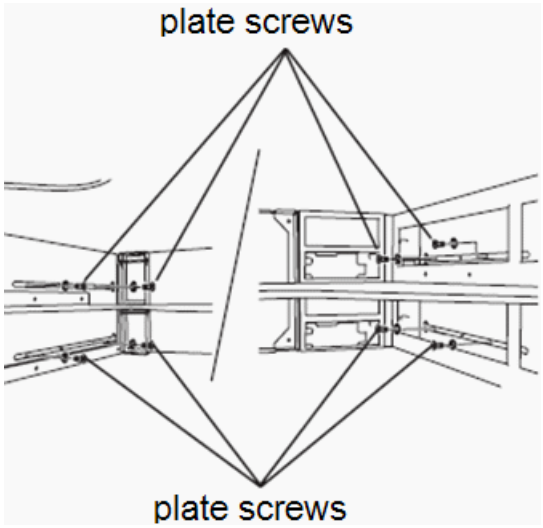


3. Insert the empty chassis into the rack from the front.

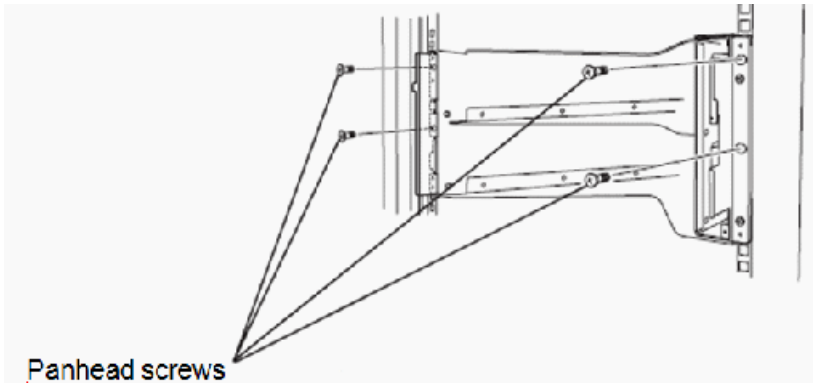


4. Align the empty chassis so it is centered on the side rack mount rails.

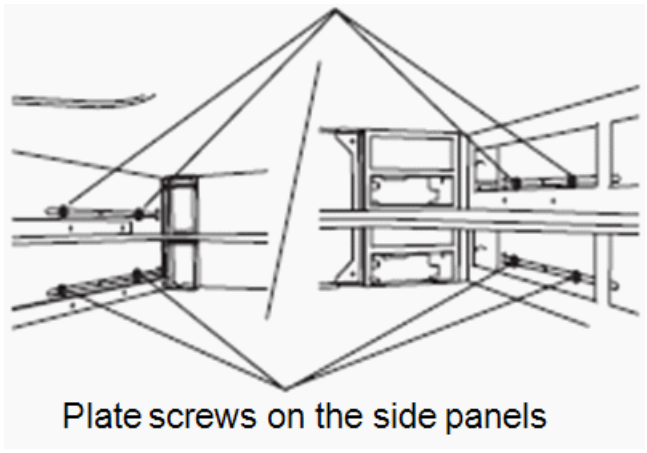
5. Loosely install the 8 plate screws through the holes on the inside of the empty chassis, fastening to the threaded holes in the side rack mount rails, as shown below. Tighten just enough to hold them in place.



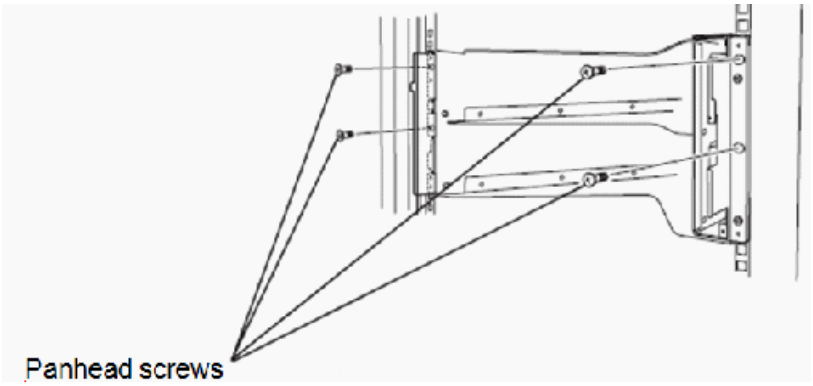
6. Securely attach the front of the chassis to the rack front with 4 panhead screws.



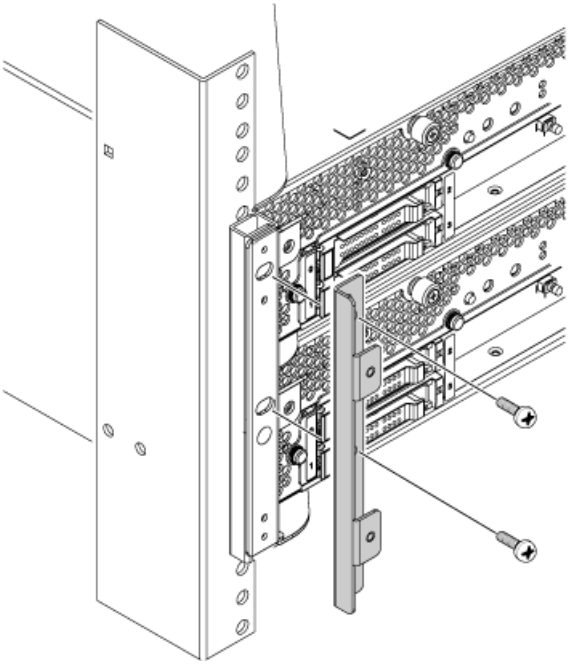
7. Tighten the 8 internal plate screws you installed earlier to secure the chassis to the side rack mount rails.



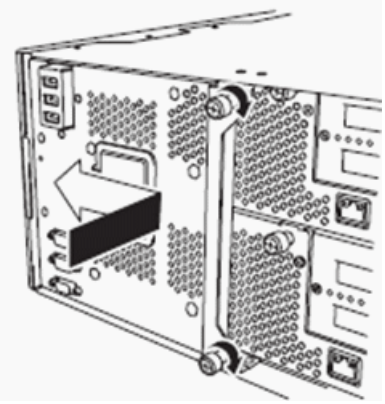
8. Remove the 4 panhead screws you installed earlier.



9. Fasten the bezel brackets to the front of the chassis on each side. Use the 4 panhead screws. Tighten securely.



10. Reinstall the system backplane in the rear of the chassis by inserting it straight into the slot then sliding it all the way to the left. Fasten the thumb screws securely by turning to the right.



11. Reinstall the front unit containing the DVD drive and LED module in the front of the chassis in the reverse order done in Step 1 of this procedure.
12. Now install the two CPU/IO modules as described in the next section.

Install CPU/IO modules

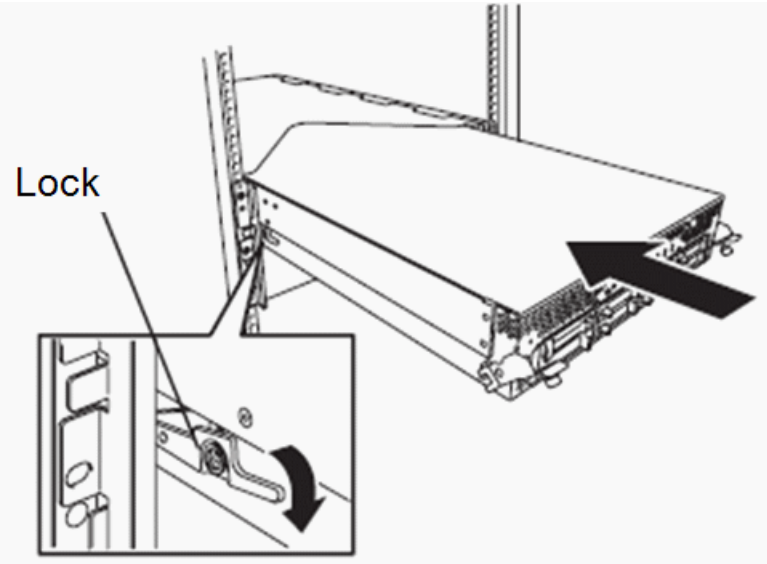
This procedure explains how to install the CPU/IO modules into the chassis enclosure once it is installed in the rack. It is recommended to have two people available to do this procedure.

There are two CPU/IO modules in the system, Module 0 (in the top slot) and Module 1 (in the bottom slot). When you receive these modules from the factory they are identical (mirrored). Either module from the factory may be installed in the top or bottom slot. Both modules have their power supply and all hard drives installed.

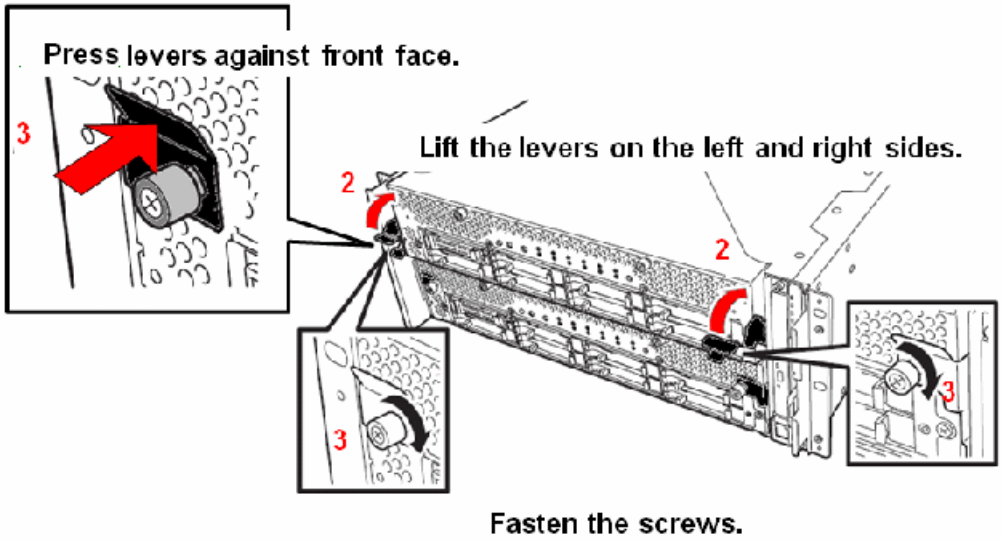
NOTE: Upon power up, the top module will be automatically designated as the Primary and the module in the bottom slot will be designated as the Secondary. All hard drives installed have been

mirrored at the factory. Once you have powered up the system, Primary and Secondary modules or any hard drives should not be swapped.

1. Mount either module into the enclosure by sliding it into the top slot. As you slide the module in, press down on the side locking lever on the left side of the module so the module slides in past the locking mechanism. You will hear a click when the side locking lever engages.

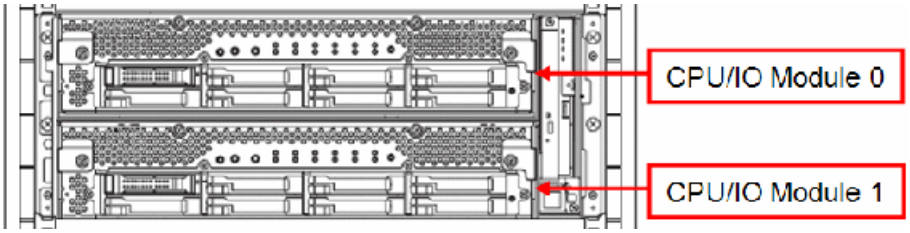


2. Once the module is all the way in, lift the front locking levers into position on both sides of the module up as shown below.
3. Press the side levers firmly against the front face as you turn the screws to the right to secure the module in the frame.



4. Repeat this procedure to install the bottom module.

   The resulting installation should look like the example below from the front.



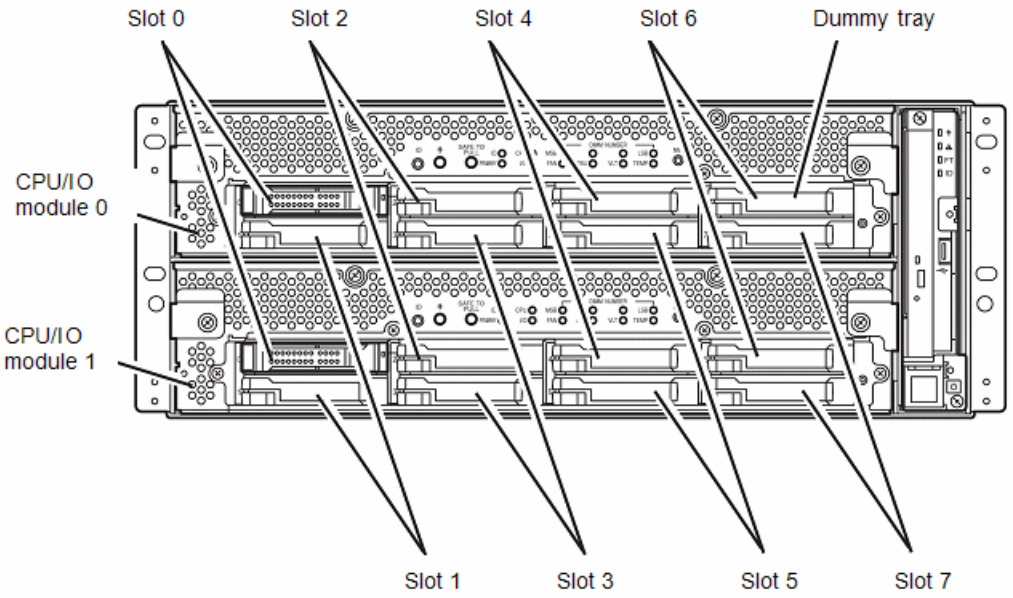
5. Install the front bezel as described in the topic describing this procedure.

2.5 inch hard disk drives

The 2.5-inch hard disk drive bays in front of the FT server can mount up to 16 hard disk drives with the 2.5 inch width exclusive trays. All hard disk drives are installed and mirrored at the factory. Do not swap the positions of any hard disk drives.

The operation is executed on the created mirror volume with installed hard disk drive pairs such as slot 0 on CPU/IO module 0/1, slot 1 on CPU/IO module 0/1, slot 2 on CPU/IO module 0/1. (The OS is installed on the mirror volumes that consist of the hard disks in the slot 0.)

Hard disk drive slot locations are shown below.

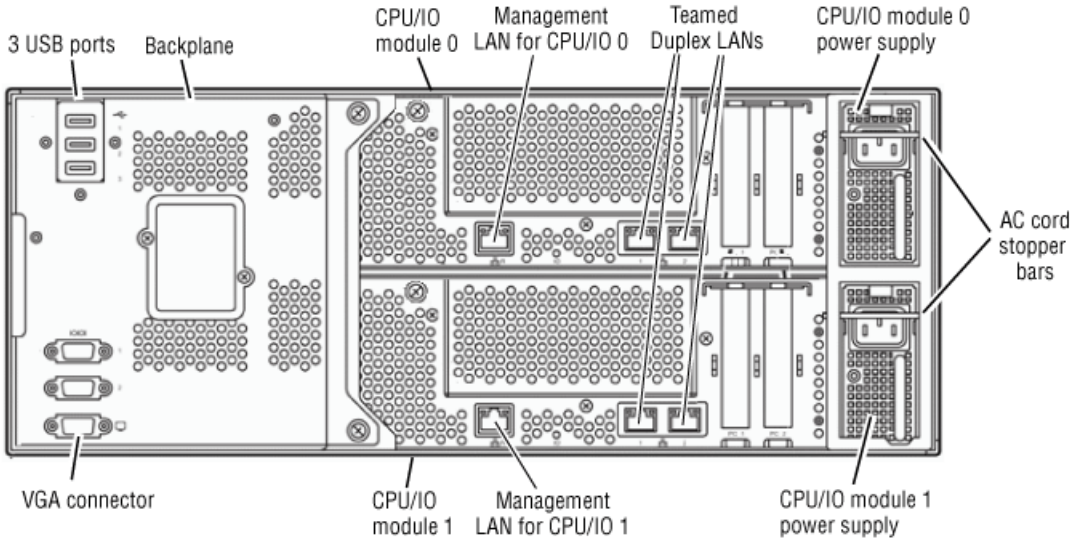


Empty slots in the 2.5-inch hard disk drive bay contain dummy trays. The dummy trays are inserted to improve the cooling effect within the device. Always insert the dummy trays in the slots with no hard disk drives installed.

Cable connections

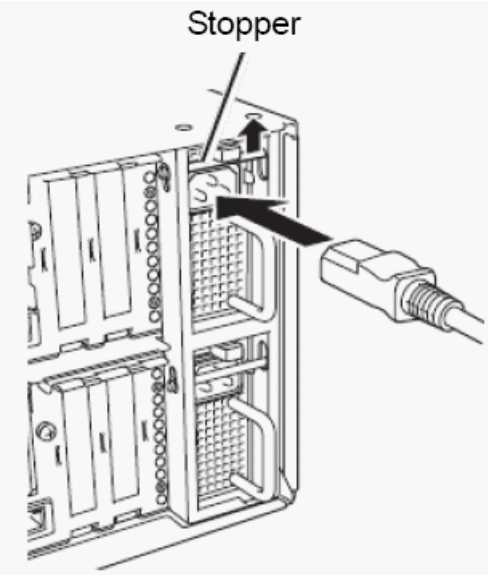
Cable connections to the FT server are made on the rear of the unit to the backplane and to both CPU/IO modules as described here.

Refer to the illustration of the rear module and its cable connections below.



1. Connect a mouse and keyboard to the USB connections on the backplane.
2. Connect a flat screen to the bottom VGA serial connector.
3. Connect the AC cords to each of the CPU/IO AC receptacles but do not power up.

   Notice that when the AC cord is inserted, the AC Stopper bars will engage as shown below. The Stopper bars prevent you from removing a CPU/IO module with the AC cord connected (while powered up).



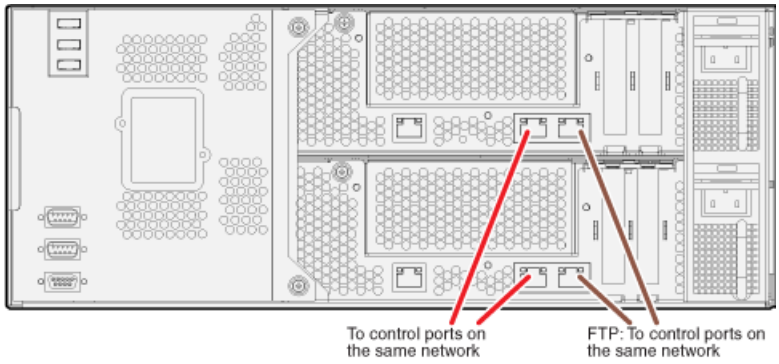
4. The Teamed Duplex LANs connect the FT server to the network as appropriate for the FT server's use as a Grass Valley system device.

STRATUS-CS-FT server: Core (B1, C1)

These cabling instructions apply to GV STRATUS Express server and GV STRATUS Core server, specified as follows:

- Grass Valley FT server with one or more roles from the following list only:
  - GV STRATUS Ingest Services (Required)
  - GV STRATUS Control Panel Service (Required)
  - GV STRATUS Common Services (Required)
  - License Manager (Required)
  - GV STRATUS Data Mover Engine (Required)
  - GV STRATUS Proxy Express Server (Required on Express server)
  - GV STRATUS Control Panel (Required)
  - GV STRATUS Core Services (Required)
  - GV STRATUS Database (Required)
  - GV STRATUS Summit MDI (Required)
  - GV STRATUS Common RESTful Archive MDI (Optional)
  - GV STRATUS Diva MDI (Optional)
  - GV STRATUS FlashNet MDI (Optional)
  - GV STRATUS Masstech MDI (Optional)
  - GV STRATUS Generic FTP MDI (Optional)
  - GV STRATUS Proxy Streaming Service (Optional)
  - GV STRATUS Rules Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV STRATUS Scheduled Transfer Engine (Optional)
  - GV STRATUS Scheduled Ingest Engine (Not used in this GV STRATUS release)
  - GV STRATUS Scheduled Ingest Manager (Not used in this GV STRATUS release)
  - GV STRATUS SocialMedia Engine (Optional)
  - GV STRATUS ExternalMedia Engine (Optional)
  - GV STRATUS Traffic Gateway (Optional)
  - GV STRATUS Topic Service Bus (Not used in this GV STRATUS release)
  - GV STRATUS Web Apps (Required. Must be assigned to Express/Core server to display Statistics panel via Dashboard)
  - GV STRATUS Web Client (Optional)
  - GV STRATUS Workflow Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV STRATUS Xcode Control Engine (Required. Must be assigned to Express/Core server or to dedicated Workflow Server)
  - GV Log Manager (Required)
  - GV Log Viewer (Required)
  - GV STRATUS Rundown Server Components (Optional)
  - GV STRATUS Application (Use for test purposes only)
  - If optionally used as a Render Engine, these additional roles:
    - GV STRATUS Render Engine

These roles require a connection to the control network and the FTP/streaming network.



NOTE: Network ports on CPU/IO module 1 and on CPU/IO 2 both connect to the same network. For example, both control ports connect to the same control network. Do not attempt to connect to different networks.

Related Topics

Devices components: Roles, cab files, services, and licenses on page 444

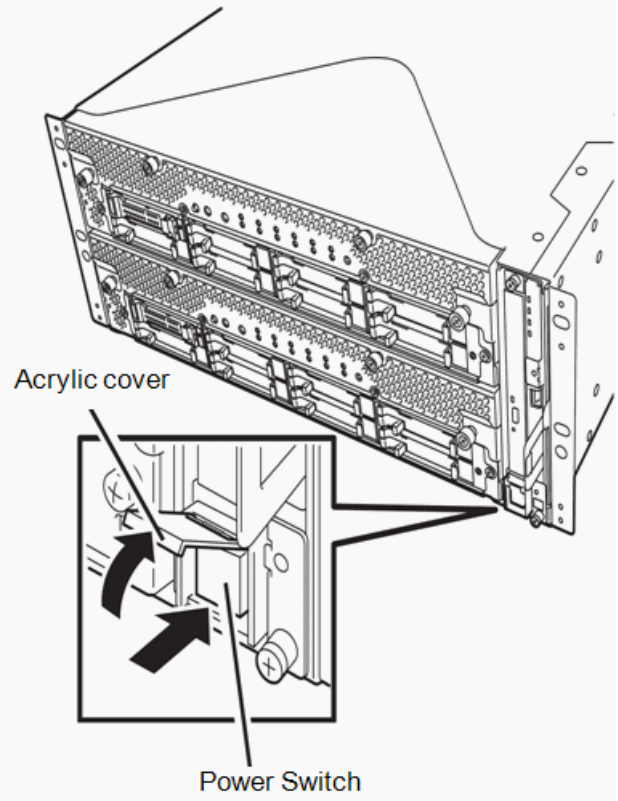
Power up

Power on the display unit and other peripheral devices connected to the server first.

NOTE: If the power code is connected to a power controller like a UPS, ensure that it is powered on.

Follow the steps below to turn on the FT server power.

1. With the front bezel removed, press the power switch located on the front panel. Lift up the acrylic cover in front of the power switch, and press the power switch to turn on the FT server.



2. Once the system has booted up, the GV logo should be displayed on the screen of the display unit. While the GV logo is displayed on the screen, the FT server is performing a power-on self test (POST) to check the unit. Upon the completion of POST, the OS will start.

If the server finds errors during POST (power up self test), it will interrupt POST and display an error message.

CPU/IO module status

The CPU/IO module (0 or 1) that is started first is managed as the primary, and the module started later is managed as the secondary. If one CPU/IO module is disconnected because of a failure, the other module becomes the primary.

The CPU/IO module to be started first is selected depending on the primary/secondary status of modules when the server was shut down the last time.

The following devices are connected to the primary CPU/IO module by the connectors on the system backplane and access both CPU/IO modules 0 and 1. When one CPU/IO module is disconnected because of a failure, those are switched to the other module automatically and continue operating.

- VGA (display)
- USB device (keyboard, mouse, optical disk drive)

NOTE: Both CPU/IO modules 0 and 1 can access the optical disk drive. If one CPU/IO module is isolated because of a failure, only the active (Primary) CPU/IO module can access the drive.

NOTE: The drive letter of the optical disk drive is reallocated automatically. The unused letter is allocated to the drive in the order of D to Z. If you want to set the fixed drive letter to the optical disk drive, specify the letter which is not allocated in the order of D to Z after setting the hard disk drive letter.

POST check

POST (Power-On Self Test) is a self-test function stored on the motherboard of the FT server.

When you power on the server, the POST will start automatically to check the motherboard, ECC memory modules, CPU/IO modules, keyboard, mouse, etc. It also shows startup messages for various BIOS setup utilities.

To view details of the POST, do one of the following:

- While the POST is being performed, press the **Esc** key.
- View the POST details from the beginning without pressing the **ESC** key when the BIOS menu appears. To do this, select **System Configuration**, then **Advanced** and set the **Boot-time Diagnostic Screen** to **Enabled**.
- View the test items and details from a management PC where ESMPRO Manager is installed.

You do not always need to check the POST details. You will need to check messages when one of the following conditions exist:

- Installation of a new FT server.
- A failure is suspected.
- Several beeps occur between the time of the power-on and OS start-up.
- The display unit shows an error message.

POST flow details

This topic walks you through how POST is performed.

1. When you power on the system, one selected CPU/IO module will start up.

   POST will be performed on this selected CPU/IO module.

2. The memory check starts.

   A message appears at the upper left of the screen to show that the basic and expanded memories are being counted. The memory check may take a few minutes to complete depending on the server's memory size. Likewise, it may take about one minute for the screen to appear when the server is rebooted.

3. The server starts the processor check, IO check, and initialization.

   Several messages appear showing the ID of the selected CPU/IO modules, information on the processor, detection of the keyboard and mouse, etc

4. A message appears at the lower left of the screen (shown below), prompting for startup of the BIOS setup utility SETUP.

   ```
   Press <F2> to enter SETUP
   ```

   You will need to start it when you want to modify the configuration for using the server. Unless this message appears together with an error message, you do not need to start the utility to modify the configuration. (If you wait for a few seconds, POST will go on automatically.)

   To start the SETUP utility, press **F2** while the above message is displayed.

   When SETUP is completed, the server will reboot itself automatically and perform POST.

5. A message appears prompting for startup of the SAS BIOS setup utility.

   When a built-in SAS controller is detected, a message will appear prompting for startup of the SAS BIOS setup utility. (If you wait for a few seconds, POST will go on automatically.)

   If you press **Ctrl + A**, the SAS BIOS setup utility will start. However, you usually do not need to use the setup utility. For setting and parameter functions, see the Configuration section of this manual.

   When SETUP is complete, the server will reboot automatically and perform POST from the start again.

6. The screen shows the ID numbers of the connected disk drive.
7. Upon completion of POST, the password entry screen appears prior to OS startup.

   The password entry screen will appear after the normal termination of POST only if you have set a password in the BIOS setup utility SETUP.

   You can enter a password up to three times. If you enter an incorrect password three times, the startup will be unsuccessful. In this case, turn off the power and then turn it on again after waiting 30 seconds to boot the server.

   IMPORTANT: Set a password after the OS installation.

8. Upon completion of POST, the OS will start up.

POST error messages

When the server detects an error during POST, it will notify you of the occurrence in the following manners:

- Displays an error message on the display unit.

Write down the error messages. They will serve as helpful information during maintenance or if you need to contact Customer Service.

POST Message

In a normal situation, the POST Code and BIOS Build Number are displayed on the top side of the Virtual LCD.

The POST running LCD format is shown in the table below.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	X	X	X	X				B	I	O	S	Z	Z	Z	Z	
1																

The POST running LCD format detail is shown in the table below.

Display	Description
XXXX	Normal: Currently executing POST code
ZZZZ	BIOS Build Number

The message displays the state of duplication on the upper row of LCD by software driver after the OS boots.

The Boot message for the Virtual LCD is shown in the table below.

LCD Message	Row	Representation	Comments	Action
CPU broken	Upper	DC ON	If CPU part is broken, LCD is displayed on the broken CPU/IO modules.	The module displayed LCD is broken. Change the broken CPU/IO module.
I/O broken	Upper	DC ON	If IO part is broken, LCD is displayed on the broken CPU/IO modules.	The module displayed LCD is broken. Change the broken CPU/IO module or PCI card.
System Duplex	Upper	DC ON	When the system is under duplex mode, the message is displayed on both CPU/IO modules.	System duplex completed.
System Simplex	Upper	DC ON	When system is not under duplex mode, the message is displayed on the CPU/IO module working normally.	The system is working under simplex mode.

LCD Message	Row	Representation	Comments	Action
Split Mode	Upper	DC ON	The message is displayed on the standby CPU/IO module during Split mode.	Active Upgrade

POST or OS Error behavior

If the POST or OS startup does not finish normally, the server will reboot itself automatically.

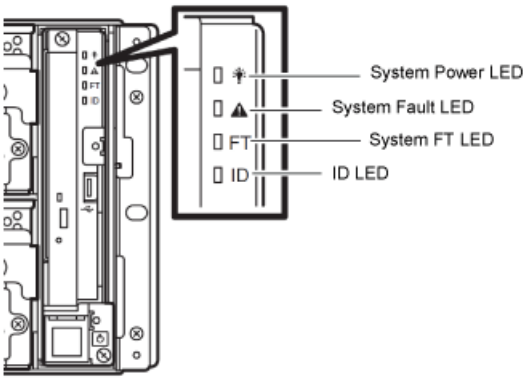
At the time of reboot, it will select the other CPU/IO module and run POST or OS startup.

In this manner, the server retries POST or OS startup with different combinations of CPU/IO modules. If POST does not finish normally with any combinations, the server will stop with the state of DC OFF or POST end with an error message displayed.

While performing retries, the server displays or registers the error types.

Front panel LEDs

On the right side of the front of the unit are four LEDs that show the current system conditions.



The LED meanings are shown in the table below.

LED Name	Function	Description
System Power LED	Indicates Power condition of system.	**Green:** System DC ON. **OFF:** System DC OFF or AC OFF.

LED Name	Function	Description
System Fault LED	LED Amber is on or blinking if either CPU/IO module is broken. When LED is on, detail information is displayed on ExpressScope (LED panel that is visible when front bezel is removed).	**Amber:** Either CPU/IO module has a failure. A CPU/IO module can not be brought up in case that CPU/IO module is not connected to AC. **Amber blinking:** It is difficult to distinguish a faulty CPU/IO module. For example, indicating a loss of synchronization. In this case, it is possible that both CPU/IO modules will need to be replaced. When analyzing Ringbuffer, there is a possibility that the cause and faulty CPU/IO module can be found out.
System FT LED	Indicates system is duplexing.	**Green:** Duplexing **Green blinking:** Split operating by Active Upgrade. **Off:** Running under simplex. **Off:** LAN or FC function is not duplexing.
ID LED	Pushing ID Switch, or demanding ID from remote.	**Blue**: ID switch has been pressed. **Blue blinking**: Demanded ID from remote. **Off:** No demand.

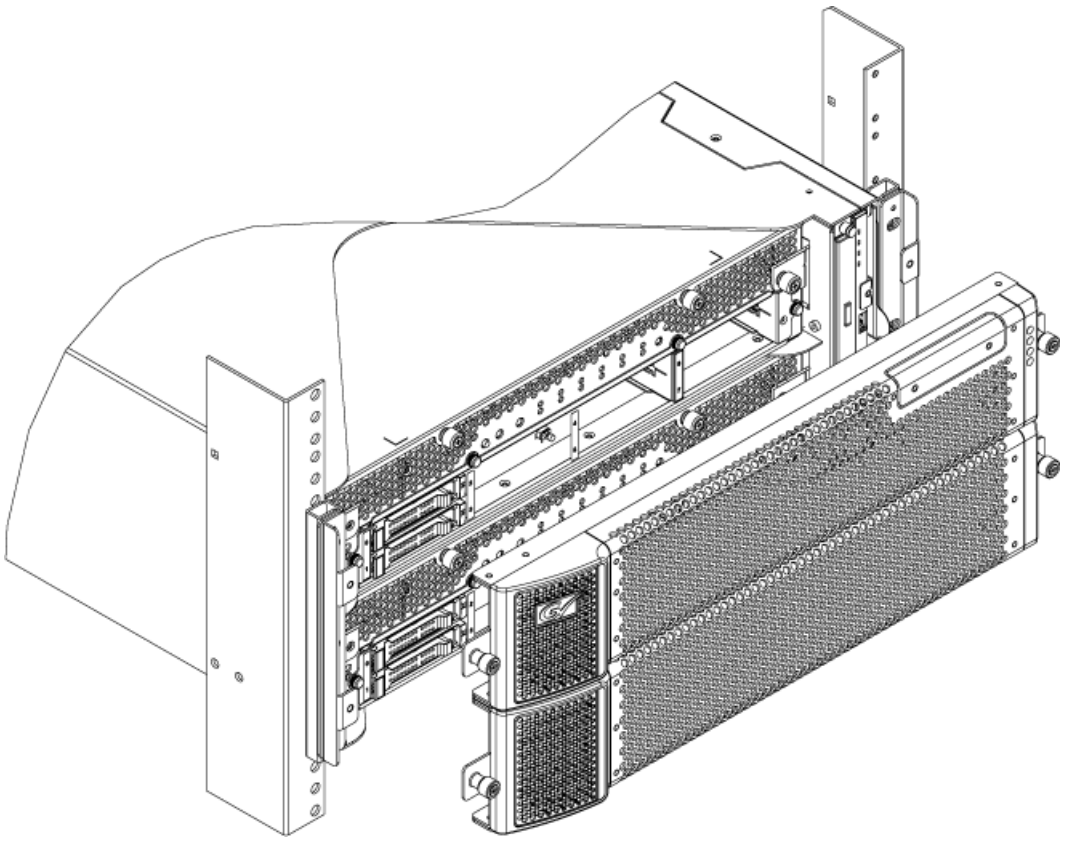
Install or remove front bezel

When your system is up and operating normally, install the front bezel. Mount it on the front of the unit and turn the thumb screws on both sides to the right.

You may remove the front bezel while the unit is powered up to check LED status.

To remove the front bezel:

1. Unscrew the two thumb screws on either side of the front bezel.



2. Remove the front bezel carefully and set in a protected location to prevent damage.

   NOTE: Keep the front bezel installed on the unit during normal operation.

Power off

Follow the steps below to turn off the power. If the FT server is plugged to a UPS (Uninterrupted Power Supply), refer to the manuals included with the UPS or the application that controls the UPS.

1. Perform a normal shutdown from the OS.

   The entire system will be powered off automatically. (Note: the POWER switch on the primary side will remain lit when AC power is supplied.)

2. Power off all peripheral devices.

Configuring the FT Server

Configuration overview

If you have received your FT server from the factory for use in a STRATUS Media Workflow system, it has been configured with all necessary STRATUS software and all server functionality such as duplexed LANs and Rapid Disk Resync (RDR) has been performed at the factory. Once you have installed and powered up your system, refer to the STRATUS documentation for further instructions.

If you have received your FT server from the factory as a replacement for an older server in a STRATUS Media Workflow system, it will require the installation of STRATUS software using SiteConfig. The Discovery Agent utility necessary for SiteConfig has been installed at the factory and all server functionality such as duplexed LANs and Rapid Disk Resync (RDR) has been performed. Once you have installed and powered up your system, refer to the STRATUS Media Workflow documentation for further instructions.

Service Program configuration

The FT server achieves the duplex system using the following service programs which are configured at the factory, in addition to dedicated drivers.

Service program names shown in **Services**:

- ftSys eService (outputs SEL (System Event Log)
- ftSys Maintenance and Diagnostics (MAD) (provides ft control management and diagnostic features)
- ftSys RPC Provider (manages WMI configuration and status)
- Windows Management Instrumentation
- ftSys SSN (contols communication between modules, such as when executing an Active Upgrade)
- SNMP Service
- Alert Manager Main Service
- ESMFSService
- ESMCommonService
- ESRAS Utility Service
- ESMPS
- Virtual Disk Service (vds)
- DHCP Client

The above programs are necessary for the FT server operation. Do not stop these services.

When minimizing the number of operating service programs temporarily is required, the following service programs may be stopped:

- ESRAS Utility Service

Make sure to restart the operations of stopped service programs immediately after the backup processes are completed.

Confirming control software version

This topic describes how to check the version of FT server Control Software, which consists of various types of software for fault tolerance. Perform the procedure when you need to check the FT server Control Software version of the current system before adding units or connecting to other ft servers.

Confirm the version following the steps below:

1. Log on the system as an authorized **Administrator**. Select **ftServer Control Software** from the list of programs to check the Product version.
2. Open **Control Panel** from the **Start** menu.
3. Open **Programs and Features**. If the **Programs and Features** icon is not displayed, open **Programs** and click **Programs and Features**.
4. Select **ftServer Control Software** from the list of programs to check the Product version.

Disk operations

The topics in this section explain disk operation using the RDR (Rapid Disk Resync) function.

The FT server duplicates disks to secure data by using the Rapid Disk Resync (RDR) function. The topics in this section describes operations such as configuration of dual settings to disks and replacement of disks.

Dual disk configuration overview

The FT server secures data by setting the dual disk configuration using the RDR (Rapid Disk Resync) function in the control software. Dual disk configuration procedures differ depending on whether you are configuring the system disk (slot 0) or the data disk (slot 1 to slot 7).

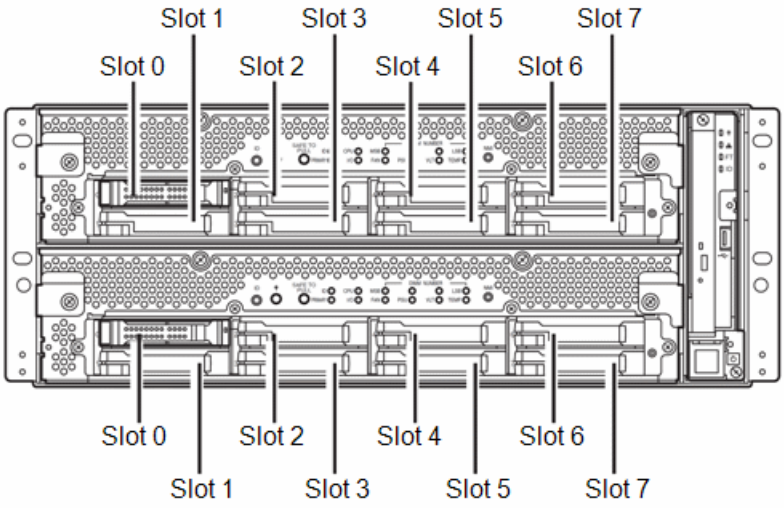
There are two different procedures:

- To configure the dual disk of the system disk, refer to the System Disk Dual Configuration Procedure.
- To configure the dual disk of the data disk, refer to the Data Disk Dual Configuration Procedure.

IMPORTANT: Refer to the following notes:

- The CPU/IO module has a processor function part and an IO function part and monitors and manages each part. The IO function part is referred to as PCI module in this section.
- Hard disk drives mounted in built-in slots need to be duplexed.

By setting RDR, as the following figure and table show, dual configuration is set between the disks of the corresponding slots and then these disks are recognized as one virtual disk by Windows (such as Disk Management and Device Manager).



Slots corresponding to the mirroring process

Corresponding slot
PCI module 10 Slot 0 ⇔ PCI module 11 Slot 0
PCI module 10 Slot 1 ⇔ PCI module 11 Slot 1
PCI module 10 Slot 2 ⇔ PCI module 11 Slot 2
PCI module 10 Slot 3 ⇔ PCI module 11 Slot 3
PCI module 10 Slot 4 ⇔ PCI module 11 Slot 4
PCI module 10 Slot 5 ⇔ PCI module 11 Slot 5
PCI module 10 Slot 6 ⇔ PCI module 11 Slot 6
PCI module 10 Slot 7 ⇔ PCI module 11 Slot 7

* In the table above, PCI module names correspond as follows:
PCI module (for CPU/IO module 0) - PCI module 10
PCI module (for CPU/IO module 1) - PCI module 11

CAUTIONS: Read the following cautions before using the RDR Utility:

- RDR can only be used on the disks inserted into the built-in slots of the FT server. It cannot be used on the dynamic disk.
- Be sure to use a basic disk as the system disk. Only a data disk can be used for a dynamic disk.
- Be sure to specify RDR to all disks inserted in the built-in slots and make duplex settings.
- Be sure to configure the RDR settings in the same way not only when the OS is installed but also when the disk is added to the PCI module.
- RDR can only be used on basic disks. If a span volume or stripe volume is needed, configure RDR to a basic disk and then change the disk to a dynamic disk using **Disk Management**.
- Before performing physical formatting, change **OS Boot Monitoring** to **Disabled** on **Server Monitoring Configuration** in the BIOS setup utility.
- If the system is shut down (or restarted) while the mirror is broken, or a long time (30 minutes or longer) has passed after the mirror is broken, the mirror resynchronization target will be the entire area of the partition existing on the disk. For example, if the mirroring has been broken due to a PCI module failure, when you shut down the system and replace the PCI module in such a state, the entire area of the partition existing on the disk needs to be resynchronized.

- Create a data disk partition after configuring the RDR. If you create a data disk partition before configuring the RDR, the partition's drive letters may be deleted when the RDR is configured.

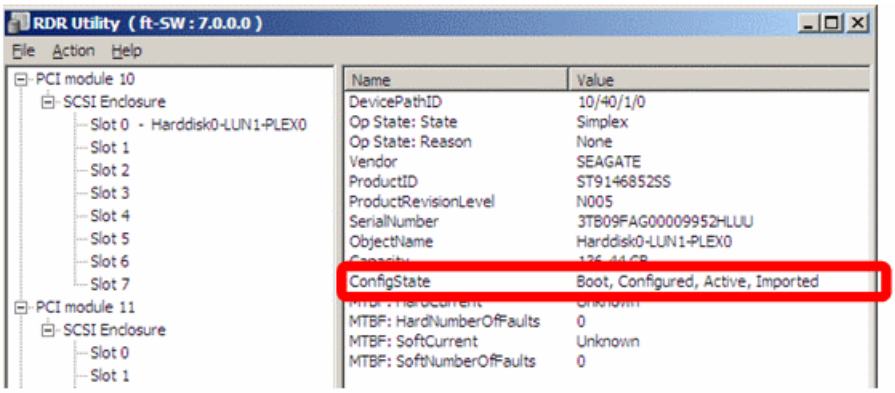
System disk dual configuration procedure

Read the Dual Disk Configuration Overview before performing this procedure.

Configure the dual disk of the system disk with the following procedure.

NOTE: To perform this procedure, you need to log on as an administrator or a member of an administrator group.

1. Go to **Start | All Programs | RDR | RDR Utility** and start the RDR utility. On the left pane of the RDR utility, select **Slot 0** of PCI module 10 under **SCSI Enclosure** and confirm that the **ConfigState** on the right pane reports: **Boot**, **Configured**, **Active**, **Imported**.



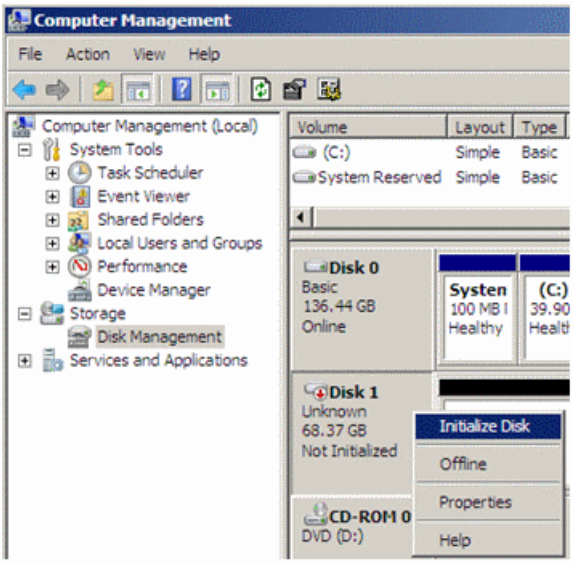
TIPS:

- The RDR Utility display does not refresh automatically. From the menu, go to **Action** and click **Refresh** or press the F5 key every time you conduct disk-related operations such as connecting/disconnecting disks or configuring the RDR.
- On the RDR Utility, PCI module names appear as follows. PCI module (CPU/IO module 0) − PCI module 10 PCI module (CPU/IO module 1) − PCI module 11.

NOTE: Be sure to use new disks or physically formatted ones with the same capacity as the synchronization source disk. If you use other disks, dual configuration will not be correct.

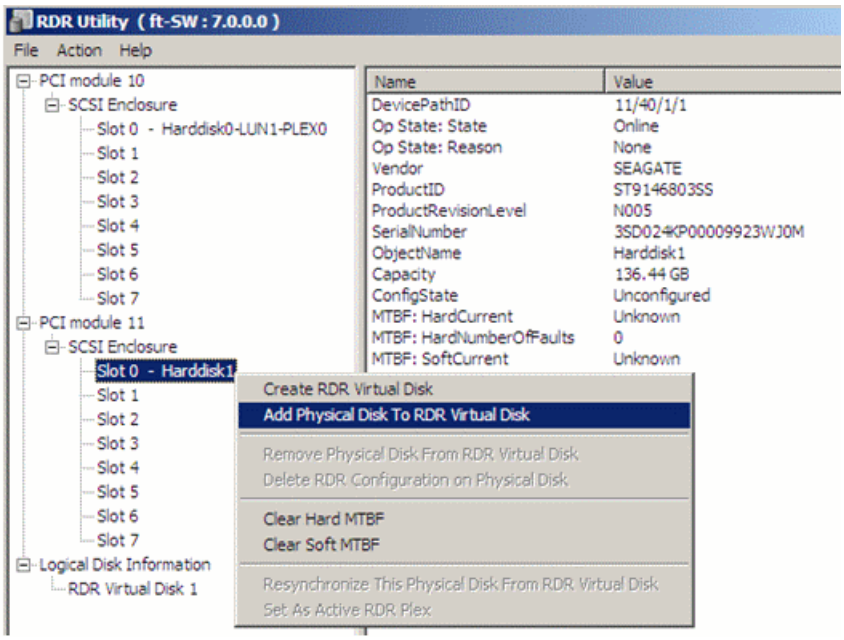
2. Insert the disk for the dual configuration into Slot 0 of PCI Module 11.

3. Start **Computer Management** by going to **Start | Administrative Tools** and select **Disk Management** in the left tree. If the disk reports **Not Initialized** on the right pane, right-click on the relevant disk to initialize.

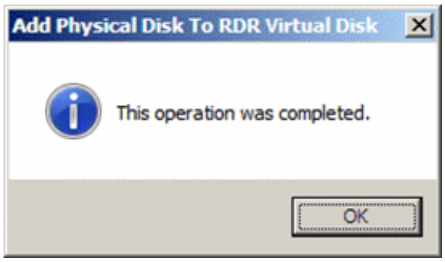


IMPORTANT: A popup window prompting you to reboot appears when inserting or initializing the disk; however, you do not need to reboot the system. Select **Restart Later** to exit the popup window.

4. Right-click on Slot 0 of PCI module 11 from the left pane of the RDR Utility and click **Add Physical Disk To RDR Virtual Disk**.

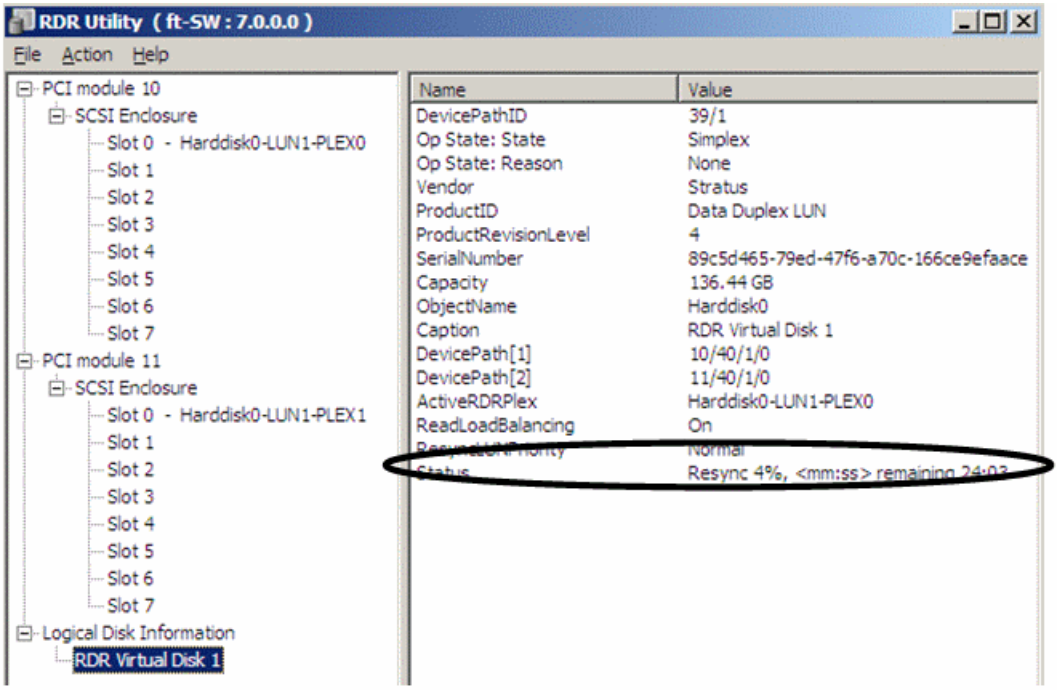


5. Click **OK**.


Add Physical Disk To RDR Virtual Disk
This operation was completed.
OK

6. Verify that disk synchronization has been started and the status of the DISK ACCESS LED and RDR Utility display changes during synchronization as described in the table and RDR Utility screen below:

During synchronization	Disk Access LED	RDR Utility	
Synchronization source disk	Amber and blinking	Condition: Simplex	Status: N/A
Synchronization destination disk	Amber and blinking	Condition: Syncing	Status: N/A
RDR Virtual disk	N/A	Condition: Simplex	Status: Resync x % (x=0, 4, 8,...96



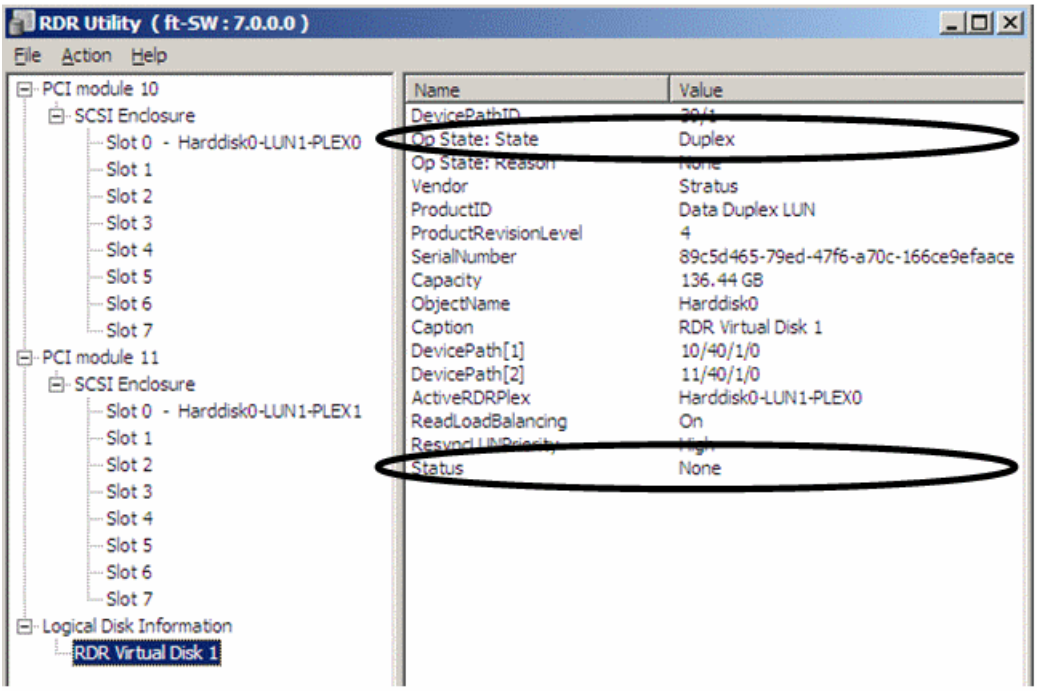
IMPORTANT:

- The time required for synchronization varies depending on the partition size on the disk. For a 40GB partition, it takes about 50 minutes.
- Setting dual disk configuration may not complete if you reboot the system during the synchronization. Do not reboot the system before the synchronization process completes.
- If the system stops by terminating Windows improperly such as pressing the **Power** button, the whole disk area already synchronized will be resynchronized after rebooting the system.

Verify that disk synchronization is complete by noting that the status of the DISK ACCESS LED and RDR Utility display change as described in the table and RDR Utility screen below:

Synchronization completed	Disk Access LED	RDR Utility	
		Condition	**Status**

Synchronization completed	Disk Access LED	RDR Utility	
Synchronization source disk	Green and blinking	Duplex	N/A
Synchronization destination disk	Green and blinking	Duplex	N/A
RDR Virtual disk	N/A	Duplex	None



Data disk dual configuration procedure

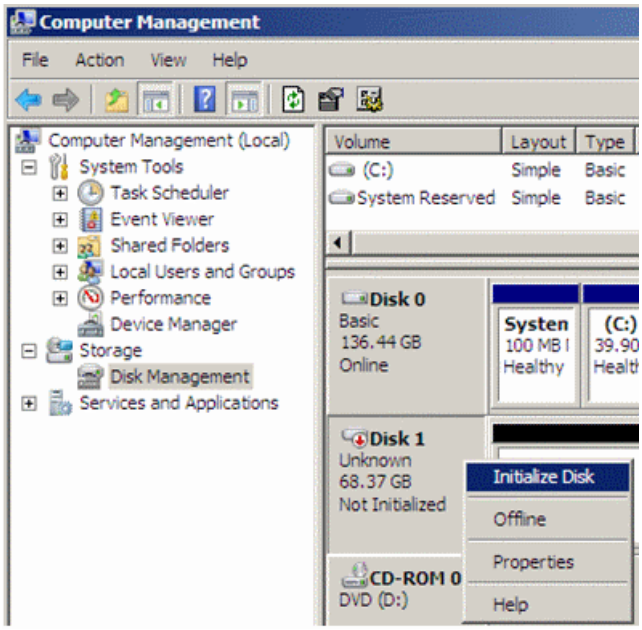
NOTE: Read the Dual Disk Configuration Overview before performing this procedure.

Follow the procedure below to configure dual data disks for slots 1 to 7.

IMPORTANT: The following procedure describes how to configure the dual disk for Slot 1. To configure the dual disks for Slot 2 to Slot 7, follow the same instructions for Slots 2-7 as Slot 1, selecting the proper disk.

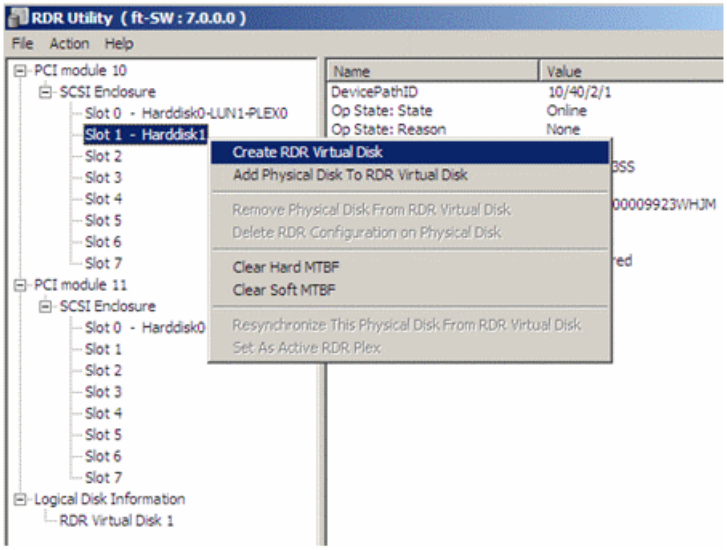
1. Insert a disk for the dual configuration into slot 1 of PCI Module 10. If a disk is already mounted, this procedure is not necessary. Go to step 2.

2. Start **Computer Management** by going to **Start | Control Panel |**, **Administrative Tools**, and select **Disk Management** on the left tree. If the disk which is to be set as dual configuration shows as **Not Initilized** on the right pane, right-click on the relevant disk to initialize.



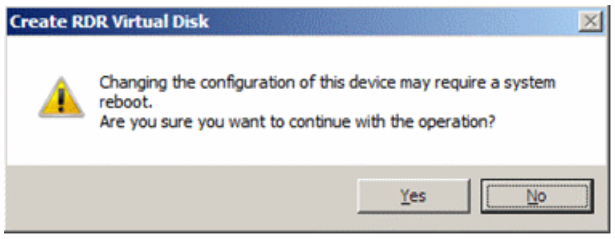
IMPORTANT: A popup window prompting to reboot appears when you insert or initialize the disk; however, you do not need to reboot the system. Select **Restart Later** to exit the popup window

3. Go to **Start | All Programs | RDR | RDR Utility |** and start the RDR Utility. On the left pane of the RDR Utility, right-click on the Slot 1 disk of PCI Module 10 and choose **Create RDR VirtualDisk**.

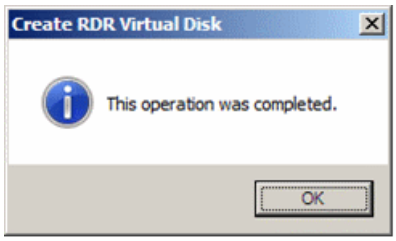


NOTE: Depending on the disk status, it takes time to set RDR, and the RDR Utility may stop for a few minutes. This is not an error. Allow it to finish.

4. When the dialog box shown below comes up asking you to do a system reboot, click **Yes**.



5. Click **OK** when the operation complete dialog box appears.

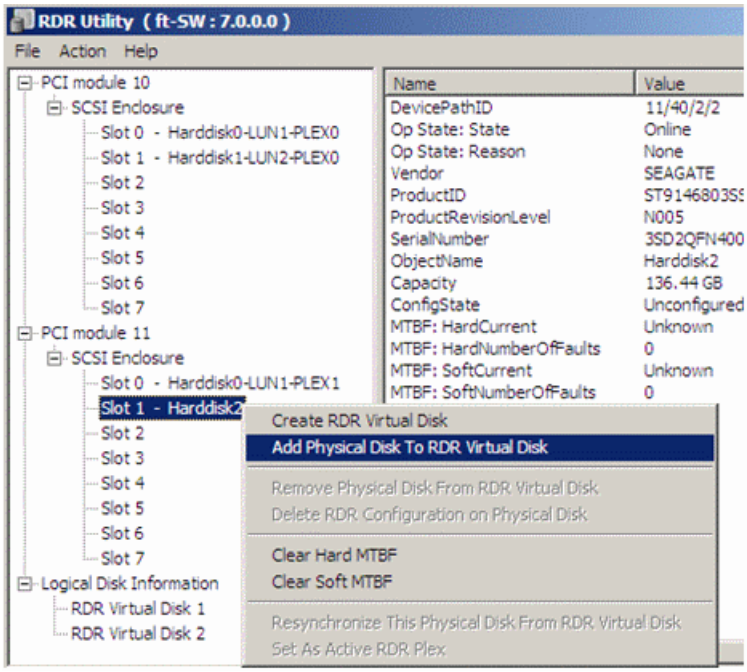


NOTE: If you set RDR on a disk that includes a system partition disabled to mount, a system restart pop-up message appears. The system reboots after 2 minutes after clicking Yes. After rebooting, perform the procedures starting with step 6 below.

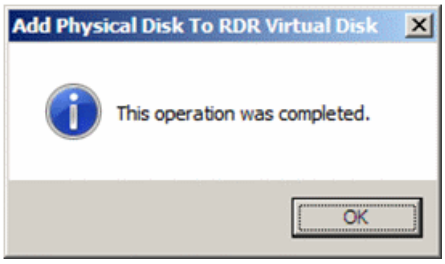
6. Insert the disk to perform dual configuration into the Slot 1 of PCI module 11, and perform the procedure in step 2. If a HDD is already mounted, this procedure is not necessary. Perform the procedure in step 2 only.

   NOTE: Be sure to use new hard drive disks or physically formatted ones with the same capacity as the synchronization source disk. If you use other disks, dual configuration will not work properly.

7. Right-click on Slot 1 of the PCI module 11 from the left pane of the RDR Utility, then click **Add Physical Disk To RDR Virtual Disk**.

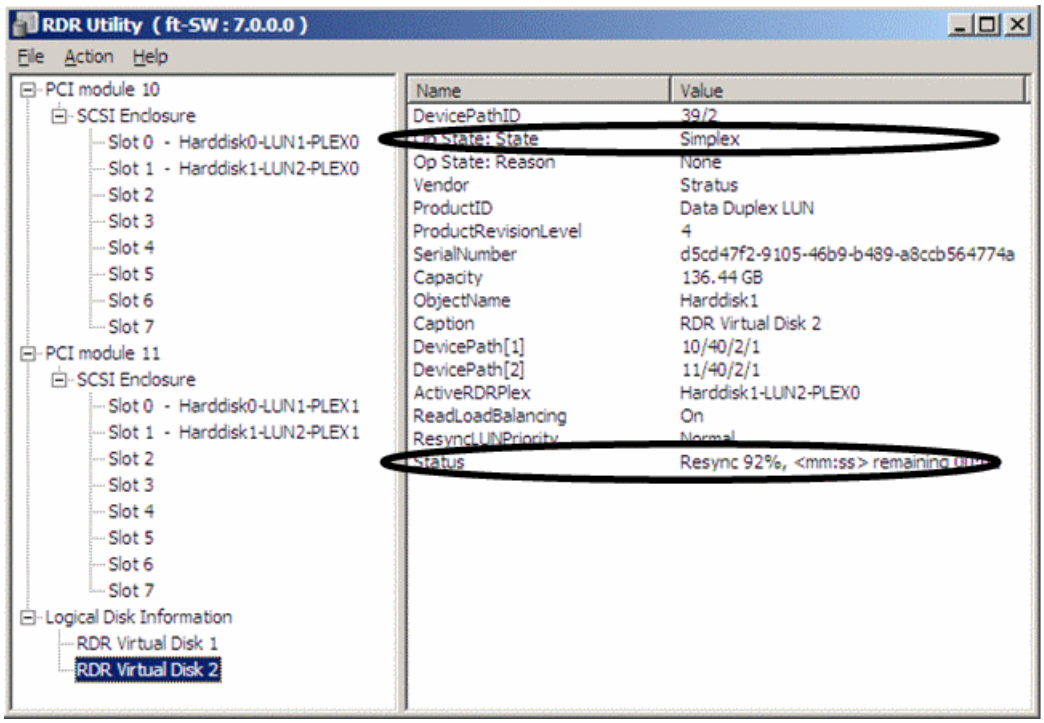


8. Click **OK** in the dialog box that appears.



9. Verify that disk synchronization has started and the status of the DISK ACCESS LED and RDR Utility display changes as shown in the table and the RDR Utility screen below.

During synchronization	DISK ACCESS LED	RDR Utility	
		Condition	**Status**
Synchronization source disk	Green and blinking	Online	N/A
Synchronization destination disk	Amber and blinking	Syncing	N/A
RDR Virtual disk	N/A	Simplex	Resync X % (x = 0, 4, 8, ...96)

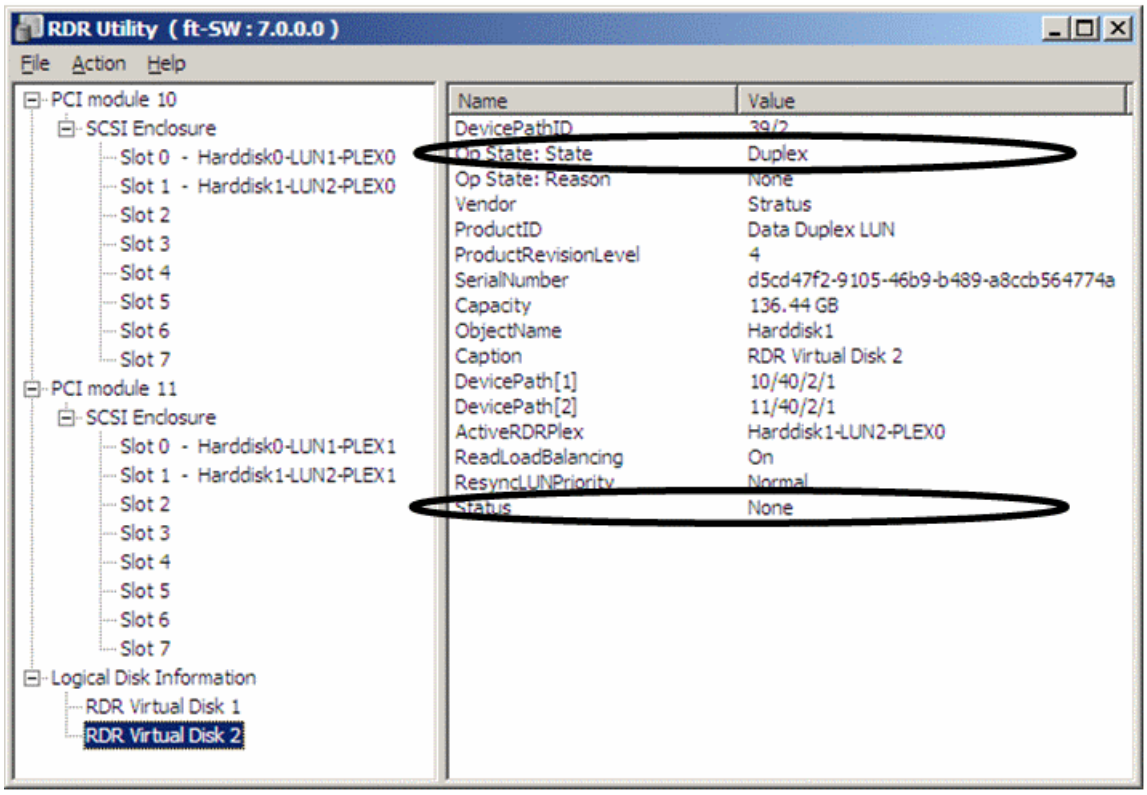


IMPORTANT:

- The time required for synchronization varies depending on the partition size on the disk. For a 73GB partition, it takes about 80 minutes. When the partition does not exist on the disk, the synchronization is completed immediately after the RDR is set, and Op State: State changes to Duplex. However, when the dynamic disk is used, the time required for synchronization depends on the disk size regardless of whether or not the partition exists on the disk.
- Setting dual disk configuration may not complete if you reboot the system during the synchronization. Do not reboot the system before the synchronization process completes.
- If the system stops by improper termination of Windows such as pressing the **Power** button, the entire synchronized disk area will be resynchronized after rebooting the system.

Verify that disk synchronization is complete by noting that the status of the DISK ACCESS LED and RDR Utility display change as described in the table and RDR Utility screen below.

Synchronization completed	Disk Access LED	RDR Utility	
		Condition	**Status**
Synchronization source disk	Green and blinking	Online	N/A
Synchronization destination disk	Green and blinking	Online	N/A
RDR Virtual disk	N/A	Duplex	None



10. Do this procedure for all hard disk drives.

Re-synchronize physical disk from RDR virtual disk

Disks whose synchronization by RDR is cancelled for reasons including a failure can be re-synchronized using the following procedure:

1. Start the RDR Utility and right-click a target disk in the left pane and click **Resynchronize This Physical Disk From RDR Virtual Disk**.
2. In the **Resynchronize This Physical Disk From RDR Virtual Disk** dialog box, click **OK**.

3. Confirm that the re-synchronization starts and the status of disks changes as shown below:

Resynchronizing	**DISK ACCESS LED**	**RDR Utility**	
		Op State: State	**Status**
Source disk	Amber (Blinking)	Simplex	N/A
Destination disk	Amber (Blinking)	Syncing	N/A
RDR Virtual disk	N/A	Simplex	Resync x percent (x=0, 4, 8, ..., 96)

Synchronization completed	**DISK ACCESS LED**	**RDR Utility**	
		Op State: State	**Status**
Source disk	Green (blinking)	Duplex	N/A
Destination disk	Green (blinking)	Duplex	N/A
RDR Virtual disk	N/A	Duplex	None

Set as active RDR plex

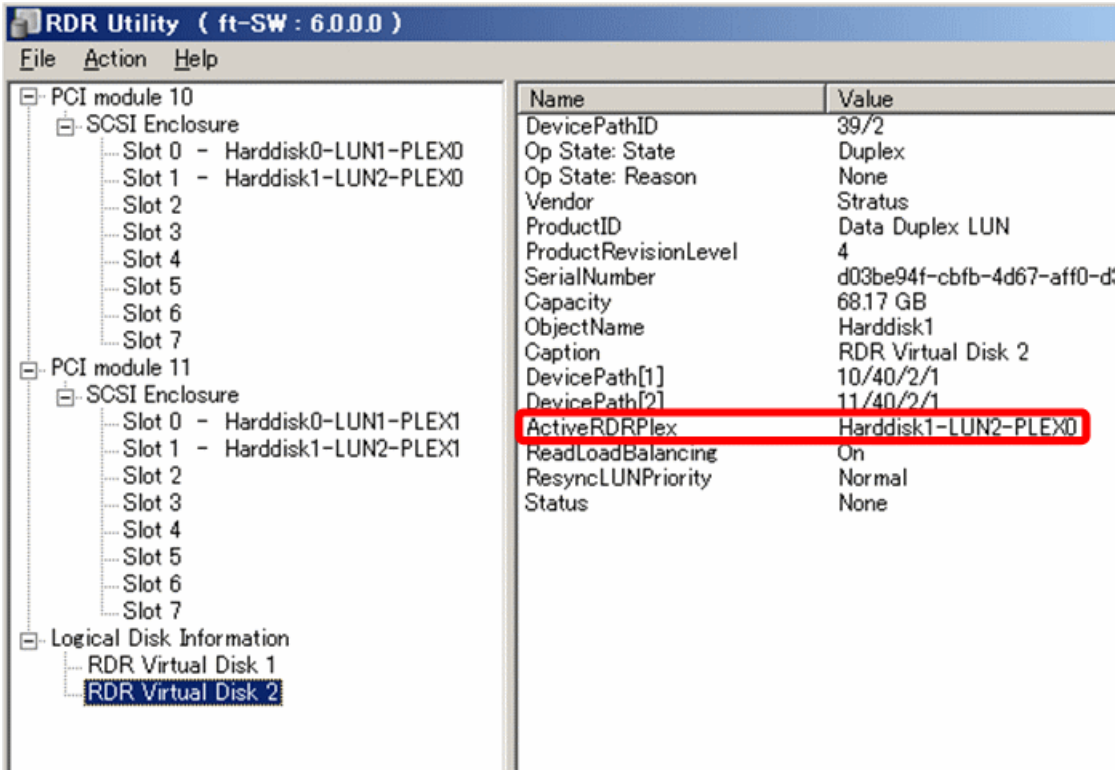
A physical disk can be set as “Active RDR Plex” by a command.

Active RDR Plex is the disk on which the data reading process is performed when Load Balancing of RDR Virtual Disk is off.

1. Start the RDR Utility and right-click a target disk in the left pane and click **Set As Active RDR Disk**.

2. In the **Set As Active RDR Plex** dialog box, click **OK**.

   Active RDR Plex can be viewed from **Active RDR Plex** of the RDR Virtual Disk. (In the image below, the disk in slot 1 of PCI module 10 is set to Active RDR Plex among physical disks constructing RDR Virtual Disk 2.)



Verify RDR virtual disk

To check whether the synchronization by RDR has been performed, use the following steps:

1. Start the RDR Utility and right-click on **RDR Virtual Disk x** in the left pane and click **Verify RDR Virtual Disk**.
2. In the **Verify RDR Virtual Disk** dialog box, click **OK**. The progress of verification can be viewed using the RDR Utility.

	Verifying	Verification completed
Status of RDR Virutal Disk x	Verify x percent (x=0, 4, 8, ..., 96)	None

Tips:

- The verification process is automatically performed every week.
- The time required for verification depends on the disk size and load. For a 73GB disk, it takes about 90 minutes.

Stop verifying RDR virtual disk

Verification of RDR virtual disk in progress can be stopped with the procedure below:

1. Start the RDR Utility and right-click **RDR Virtual Disk x** in the left pane and click **Stop Verify RDR Virtual Disk**.
2. In the **Stop Verify RDR Virtual Disk** dialog box, click **OK**.

Set resync priority

The priority of synchronization by RDR can be specified. By changing the priority, the I/O load during synchronization can be reduced using the following steps:

1. Start the RDR Utility and right-click on **RDR Virtual Disk x** in the left pane then click **Set Resync Priority**.
2. When a dialog box appears, select **Low**, **Normal**, or **High** (the default is **Normal**) and click **OK**.
3. In the **Set Resync Priority** dialog box, click **OK**.

Set LUN load balancing

Load balancing can be specified as on or off.

When the load balancing is on (default), the read process is performed alternately from two physical disks forming the RDR Virtual Disk to improve performance. When it is off, the read process is performed from the physical disk specified as Active RDR Plex. To set the load balancing on or off, use the following procedure.

1. Start the RDR Utility, right-click on **RDR Virtual Disk x** in the left pane to change the priority and click **Set RDR LUN Load Balancing**.
2. When a dialog box appears, select **On** or **Off** (the default is **On**) and click **OK**.
3. In the **Set RDR LUN Load Balancing** dialog box, click **OK**.

Build dynamic disk

Use Windows utilities and build a Dynamic disk with all the disks except for drive 0.

1. From the Windows desktop, right-click **My Computer** and select **Manage**.
2. Change the CD ROM drive letter to `F:\`.
3. Select **Disk Management**.
4. Right-click on one of the unallocated **Disk 1**.
5. Select **New Striped Volume**.
6. Click **Next**.
7. Add disk **2** – **4** to the group in the Selected column.
8. Click **Next**.
9. Assign drive letter **D**.
10. Set file system to **NTFS**.
11. Set Allocation unit size to **default**.

12. Set Volume label to **Data**.
13. Verify that **Perform a quick format** is selected.
14. Click **Finish**.

Duplex LAN configuration overview

The FT server duplex LAN is configured at the factory with Adapter Fault Tolerance (AFT) functionality. This is correct, even for an FT server on a system with multiple control networks, such as a redundant K2 SAN. Since the FT server provides its own "redundancy" it does not participate in the K2 SAN's redundant control networks. AFT is a feature that places more than one LAN controller on the same LAN (same segment), and automatically switches the process of the primary controller to the backup controller when any trouble occurred on the primary.

Instructions are given in this manual for doing the duplex LAN configuration in the unlikely event it is required at the customer site. If you create a system-specific recovery disk image, all server configuration can be restored after a failure.

Set duplex LAN configuration

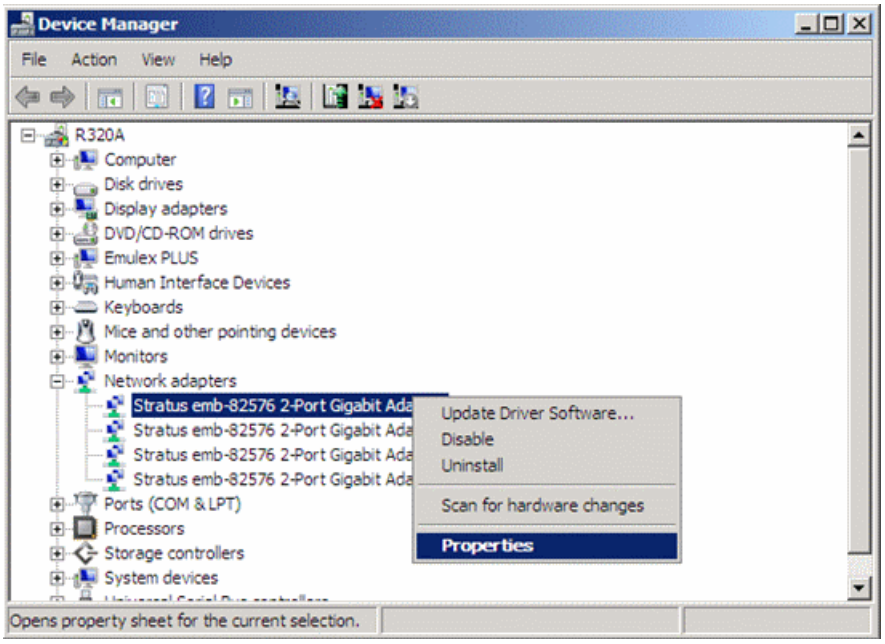
The duplex LAN configuration for the FT server has been done at the factory. There is no need to redo this configuration after installing your server. However, the procedure is provided here in case it is needed on the customer site.

To configure the duplex LAN, log on to the FT server using the factory default login, user **Administrator** and password, or the username and password you have set.

In this task you team network adapters, which correspond to the Ethernet connectors on the CPU/IO module rear panels. One team includes the top module's left-hand connector and the bottom module's left-hand connector. The other team includes the top module's right-hand connector and the bottom module's right-hand connector.

1. Start **Device Manager**.

2. Select a target Network Adapter. Right-click and select **Properties** from the menu displayed to show the Properties dialog box.



IMPORTANT: The display of Network Adapters may be duplicated as shown below, depending on the status at installation.

- Stratus emb-82576 2-Port Gigabit Adapter
- Stratus emb-82576 2-Port Gigabit Adapter
- Stratus emb-82576 2-Port Gigabit Adapter #2
- Stratus emb-82576 2-Port Gigabit Adapter #2

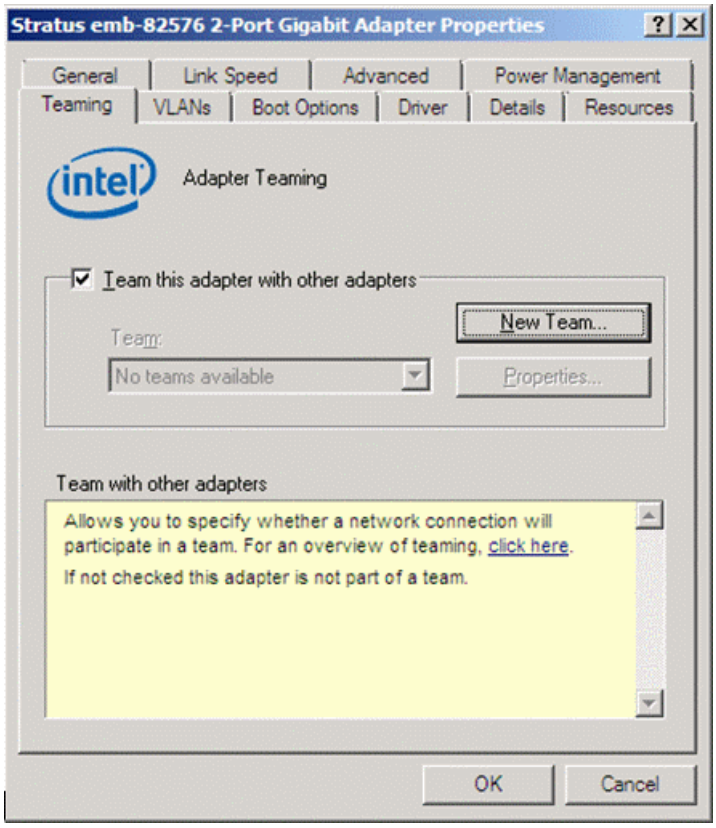
If such a case occurs, perform the following actions:

1. Delete all Network Adaptors from Device Manager.
2. Select **Action Scan for hardware changes**.

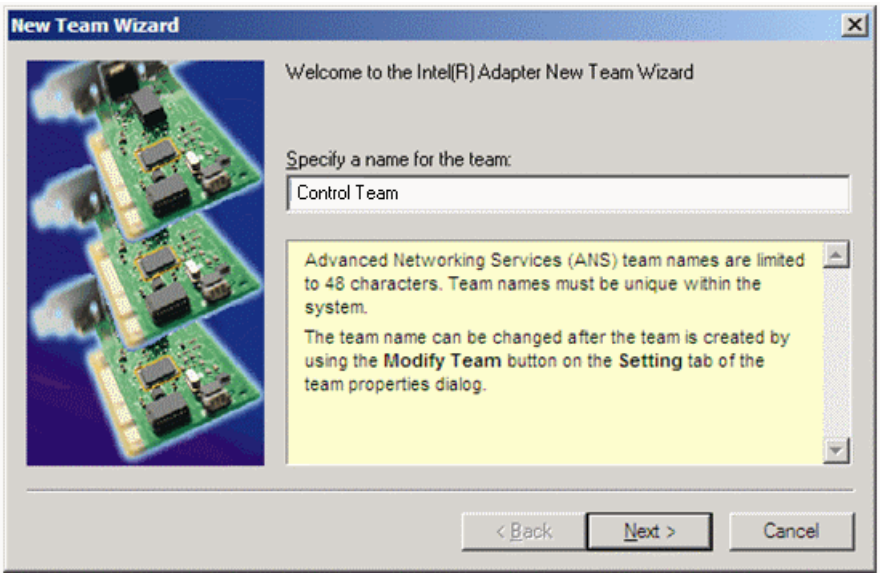
The display will be as follows when the actions are performed properly.

- Stratus emb-82576 2-Port Gigabit Adapter
- Stratus emb-82576 2-Port Gigabit Adapter #2
- Stratus emb-82576 2-Port Gigabit Adapter #3
- Stratus emb-82576 2-Port Gigabit Adapter #4

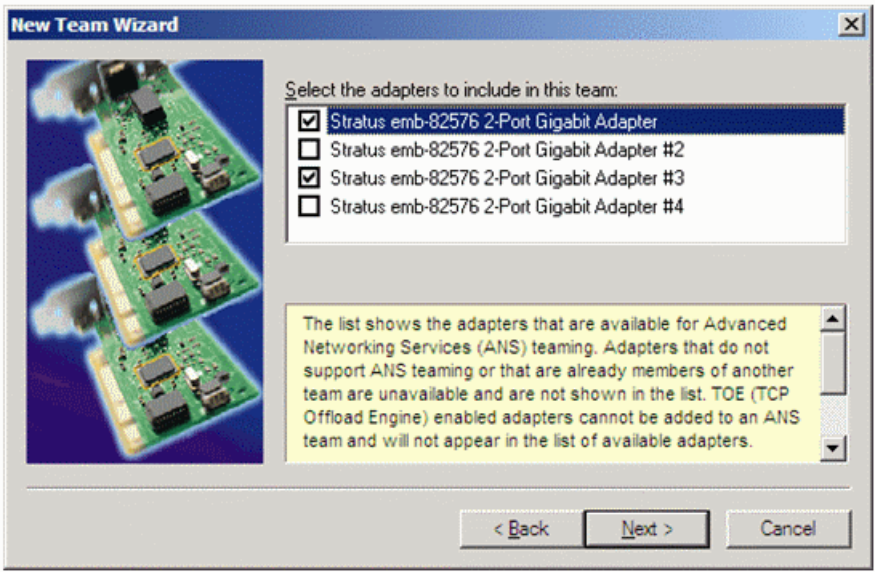
3. Select the **Teaming** tab in the Properties window. Check the **Team with other adapters** button and click **New Team...**.



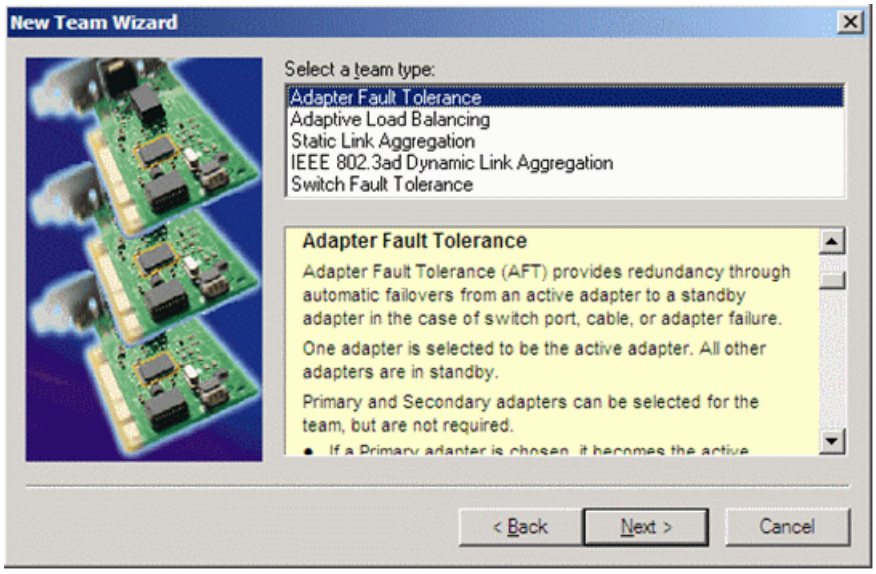
4. Enter team name `Control Team` and click **Next**.



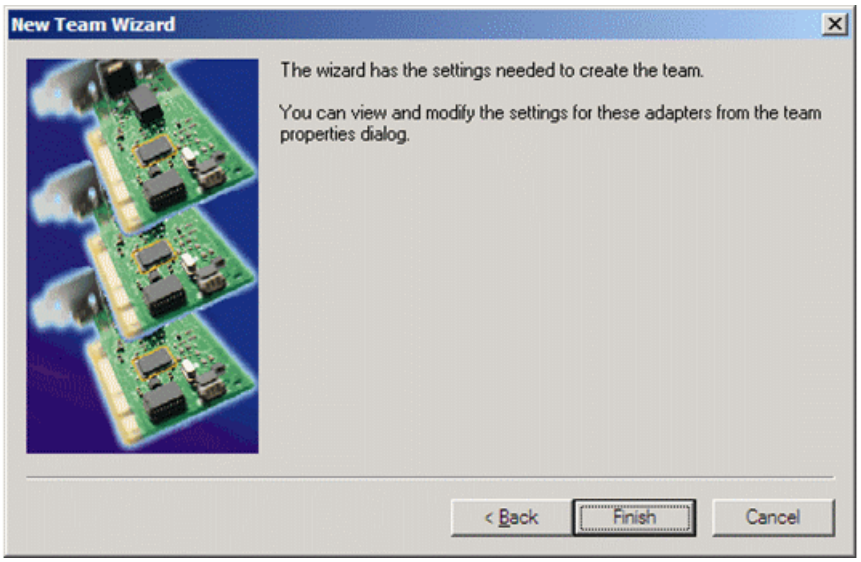
5. Select the adapters that correspond to the two left-hand ports (when facing the rear panel) and click **Next**.



6. Select **Adapter Fault Tolerance** as a team mode. Click **Next**.

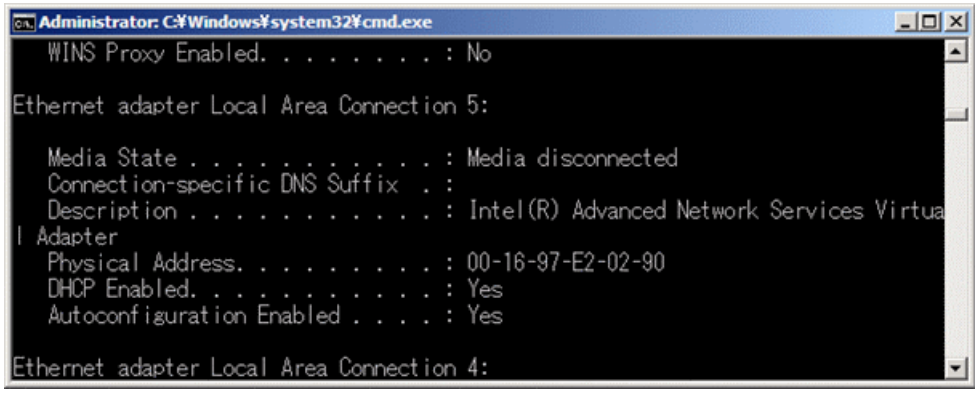


7. Click **Finish**.



8. Open the Modify Team dialog box as follows:
   a) In **Device Manager | Network Adapters**, right-click **Control Team** and select **Properties**.
      The Properties dialog box opens.
   b) Select the **Settings** tab.
   c) Click **Modify Team**.
      A dialog box opens.
9. On the **Adapters** tab, do the following:
   a) Select the adapter in the team that corresponds to port the top CPU/IO module, and click **Set Primary**.
   b) Select the other adapter in the team and click **Set Secondary**.
10. Click **OK** and **OK** to close dialog boxes.
11. Repeat steps to create another team as follows:
    - Name the team `FTP Team`.
    - Team the adapters that correspond to the two right-hand ports (when facing the rear panel) .
    - Make primary and secondary.

12. Start a Command prompt to check the physical MAC address set on ipconfig/all.



Name teams

Before beginning this task, make sure of the following:

- Adapters are named
- The teams are created

1. Open Windows Network Connections.
2. Select adapter names in the “Device Name” column and rename them as follows:
   - Local Area 5: `Control Team`
   - Local Area 6: `FTP Team`

Reorder adapters

Before beginning this task, make sure of the following:

- Teams are created and named

1. Open Windows Network Connections.
2. Select **Advanced**, then **Advanced Settings…**
3. On the **Adapters and Bindings** tab, set the **Control Team** to be the first (top-most) connection and the **FTP Team** to be the second connection.
4. Click **OK** to close and accept the changes.
5. Close Network Connections.

Servicing the FT Server

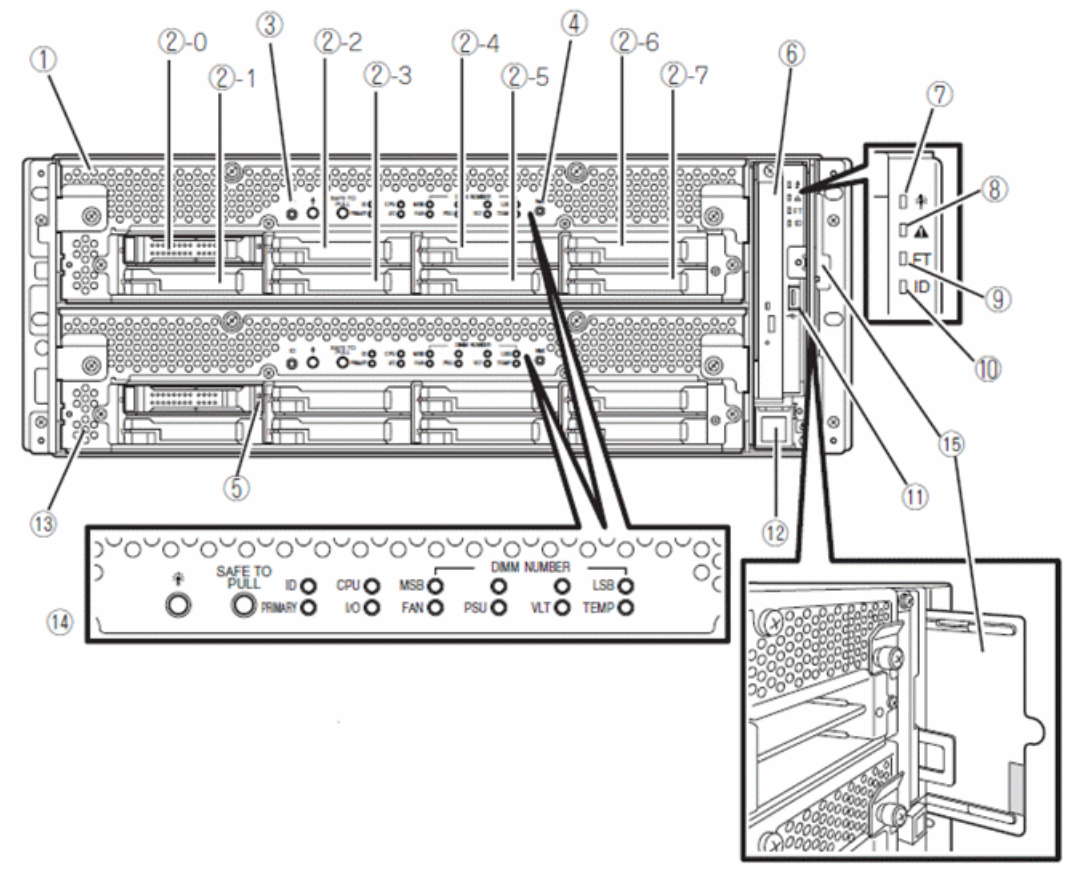
Checking status with LEDs

Use the LED guides in this section to troubleshoot the FT server. All LED indicators are described in detail in this section.

Front status LEDs (bezel removed)

A front view of a fully loaded chassis with two CPU/I/O modules with the front bezel removed is shown below. Numbered pointers indicate the various modules, switches, and LEDs visible when the front bezel is removed.

NOTE: Keep the front bezel installed at all times during normal operation to maintain cooling requirements.



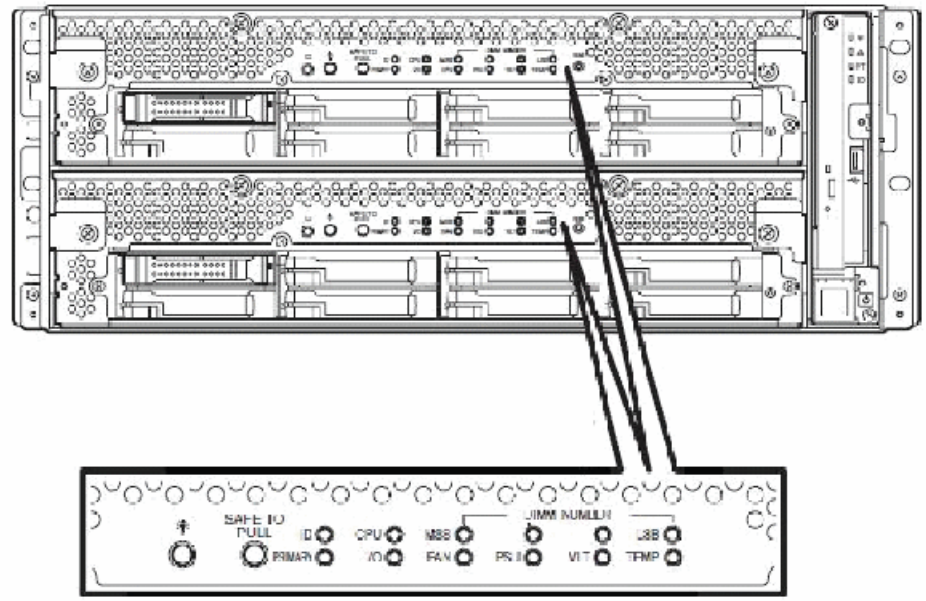
- **(1) CPU/IO module 0**: This is a module with a set of CPU (processor), memory (DIMM), PCI board, cooling fan unit, and hard disk drive components.
- **(2-0, 2-1, 2-2, 2-3, 2-4, 2-5, 2-6, 2-7) Hard disk drive bays**: These are the bays to mount the hard disk drives. The number after the numbers in parentheses indicates a slot number.
- **(3) UID (Unit ID) switch**: Set this switch to ON/OFF to control the UID LED on the front of the device. When processing the switch once, UID LED lights and it goes off when pressing it again.
- **(4) Dump (NMI) switch**: Not used in this application.
- **(5) Disk access LED**: This LED illuminates/blinks while accessing the installed hard disks.
- **(6) Optical disk drive**: This device is used to read data from the disks such as DVDs and CD-ROMs.
- **(7) System POWER LED**: This LED illuminates green when one of the power supplies of the CPU/IO modules is ON. The LED goes off when both power supplies of the CPU/IO module are OFF.
- **(8) System FAULT LED**: When one of the CPU/IO modules has an error, this amber LED lights. Details can be confirmed by checking EXPRESSSCOPE. The amber LED lights when it cannot identify which one of the CPU/IO modules has an error.

- **(9) System FT LED**: This LED displays the device status. This green LED lights when operating under a duplex condition. The LED goes off if it's not duplex. This green LED also lights when executing an Active Upgrade.
- **(10) System ID LED**: The blue system ID LED lights on the front bezel if pressing UID switch when there are multiple devices installed in one rack. This enables the user to identify the device to be maintained. This blue LED blinks when there are remote device identification requests.
- **(11) USB connector**: Connect a device supporting USB interface.
- **(12) Power switch**: Use this switch to turn ON/OFF the power. When pressing it once, the power will be ON. When pressing it again, the power will be OFF. Forced shut down takes place when pressing it for 4 seconds or longer.
- **(13): CPU/IO module 1**: This is a module with a set of CPU (processor), memory (DIMM), PCI board, cooling fan unit, and hard disk drive components identical to CPU/IO module 0.
- **(14) EXPRESSSCOPE various LEDs (green/amber)**: This LED indicates the status of CPU/IO modules.
- **(15) SLIDE-TAG**: A Label where N-Code and Serial number are printed is pasted to this tag.

ExpressScope LEDs

On the front of the FT server with the front bezel removed, the EXPRESSSCOPE LEDs (amber) can be accessed to determine if either CPU/IO module has failures. The LEDs on the upper line correspond to the upper names and the LEDs on the lower line correspond to the lower names.

NOTE: If any component has failed in a CPU/IO module including DIMMs and the power supply, the entire CPU/IO module is replaced. All hard disk drives should be labeled for slot location, then removed from the faulty unit. When a replacement module is received, the hard disk drives should be replaced into the same slots to maintain the mirrored images.



Name	Meaning	Possible Cause	Action
Module Power LED	Indicates Power condition of module.		**Green**: Module DC ON **Green blinking**: Module DC OFF (AC ON) **Off**: Module AC OFF
PRIMARY LED	Indicates Primary state of IO Module.		**Green**: IO part of Module is working on priority. **Off**: Module is working as Secondary.
Module ID LED	Pushing ID Switch, or demanding ID from remote.		**Green**: Pushed ID Switch **Green Blinking**: demanded ID from remote **Off**: No demand
SAFE TO PULL	Showing condition whether a module can be unmounted or not.		**Green**: duplexing System can work even if a module is pulled out. **Green blinking**: Simplexing System can not work if a module is pulled out. **Off**: Some offline parts exist. System can work even if a module is pulled out.
CPU (CPU part error LED)	Amber LED illuminates when a failure occurs in CPU of CPU/IO module.	Processor failure CPU/IO module failure DIMM failure	Replace CPU/IO module.
I/O (I/O part error LED)	Amber LED illuminates when a failure occurs in I/O of CPU/IO module.	CPU/IO module failure PCI Board failure	Replace CPU/IO module.

Name	Meaning	Possible Cause	Action
VLT (Power error LED)	Amber LED illuminates when electric voltage failure occurs in CPU/IO module.	CPU/IO module failure Power Supply Unit failure	Replace CPU/IO module.
MEM NUMBER (Memory slot error LED)	Amber LED illuminates when a failure occurs on the memory of CPU/IO module.	Four LEDs indicate DIMM Slot number. Target DIMM failure CPU/IO Module failure Processor failure	Replace CPU/IO Module.
PSU (Power Supply Unit error LED)	Amber LED illuminates when failure occurs on the power supply unit of CPU/IO module.	Processor failure CPU/IO module failure	Replace CPU/IO module. The LED turns on if DC power is not provided in spite of power on request.
TEMP (Abnormal temperature LED	Amber LED illuminates when temperature in CPU/IO module becomes abnormal.	Cooling problem (Fan Failure) Processor placement Processor failure CPU/IO Module failure	At first, confirm whether event log is registered by Temperature sensor. Replace CPU/IO module. There is a possibility of sensor failure.
FAN (FAN error LED)	Amber LED illuminates when failure occurs on the cooling fan of CPU/IO module.	FAN failure CPU/IO Module failure	At first, confirm whether event log is registered by FAN sensor. Is fan working? Is there a clog of module? Replace CPU/IO module. There is a possibility of sensor failure.

LAN LEDs

The LED indicators on the Ethernet LAN connectors are described below.

- **LINK/ACT LED**:

  The LINK/ACT LED shows the status of a standard network port. It is green if power is supplied to the main unit and hub and they are connected correctly (LINK). It blinks green while the network port sends or receives data (ACT).

  When the LED does not illuminate during LINK, check the condition and connection of network cables. If there is nothing wrong with the cables, a defect is suspected in the network (LAN) controller. In this case, contact Customer Service.

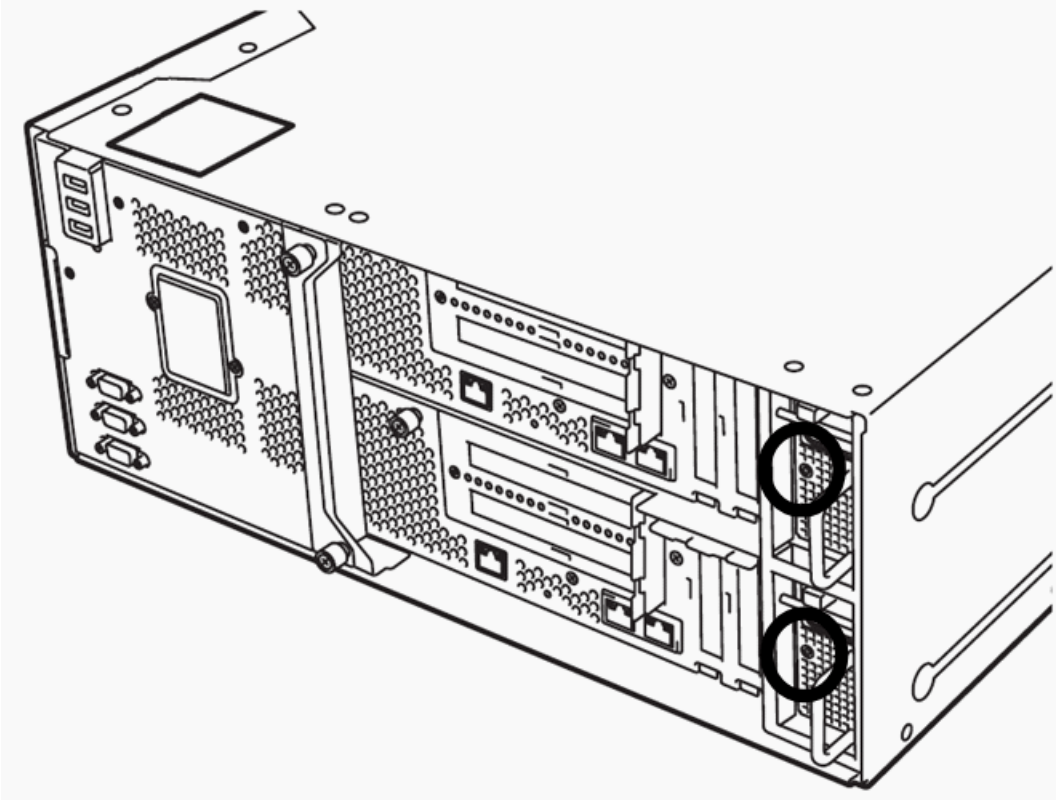
- **Speed LED**:

  This LED indicates the network interface of the communication mode used by a network port.

  1000BASE-T and 100BASE-TX are the supported LAN port types. When this LED illuminates in amber, the port is operating on 1000BASE-T; when in green, 100BASE-TX; and when not illuminate, 10BASE-T.

Power supply unit LED

When the power supply unit has a failure, the amber LED light will light. There are two power supplies per system.



LED Name	Meaning	Cause	Action
Power Supply Unit LED	When power supply unit has a failure, amber LED will light.	Power Supply Unit CPU/IO module	Replace Power Supply Unit. Replace CPU/IO module.

Diagnostics, logs and error messages

The various diagnostics, logs, and error messages available for the FT server are defined in this section in detail. Use these to aid you in determining what failures have occurred in the system.

BIOS error message

The Virtual LCD Display is the function which displays LCD message information in BMC. They are sent via DianaScope.

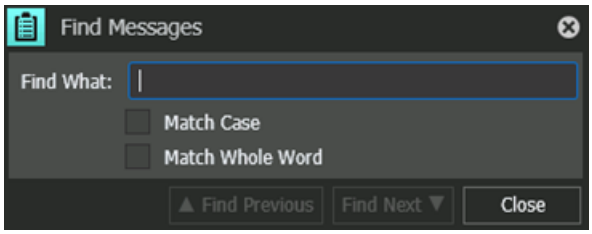
In the case of remote operation, each CPU/IO module has a remote connector. It needs to connected to the CPU/IO module you want to monitor. The Virtual LCD specifications are given in the sections below.

Searching log messages

You can search for specific items in log messages via the Search function or using the Filter in columns.

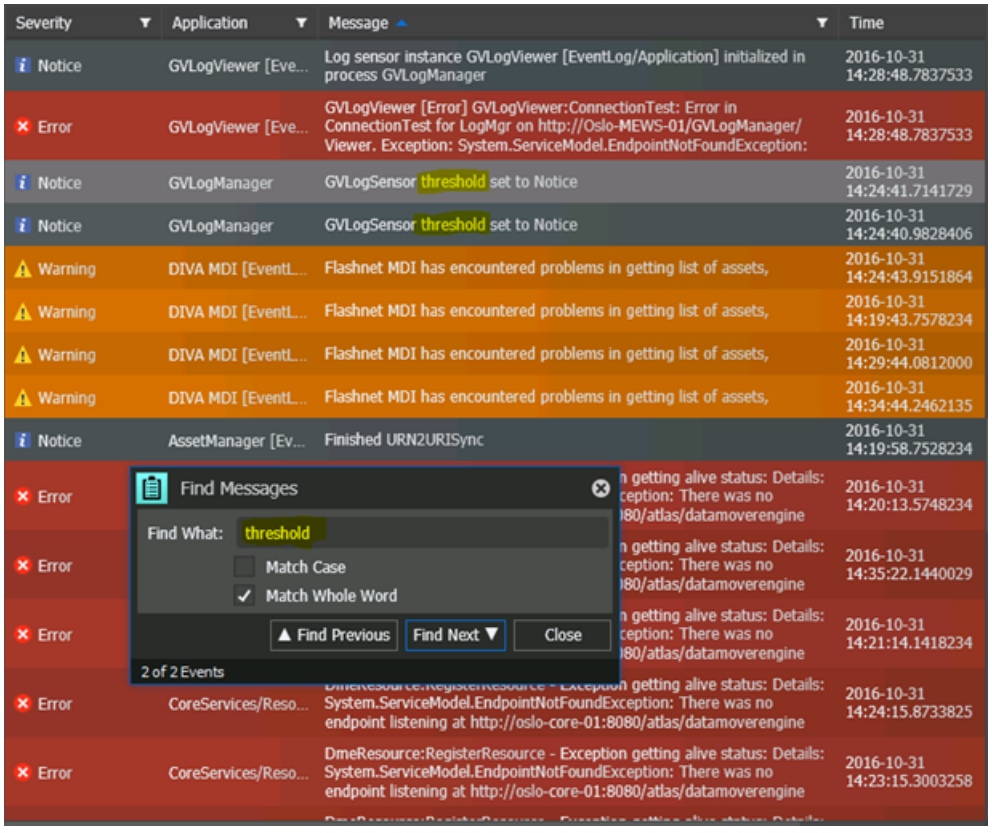
- To search via the Search function, do one from the following options:
  - Click the **Search** button on the toolbar.
  - On the main menu, select **Edit | Find Messages**.
  - Press **Ctrl + F** keys.

  The Find Messages dialog appears.



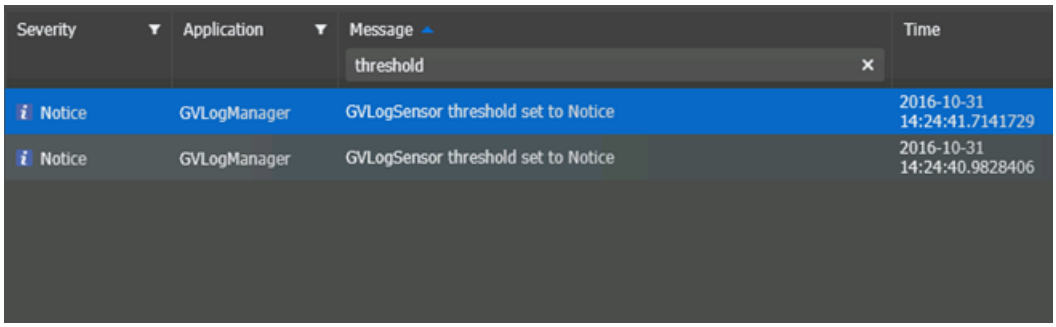
Enter the term that you want to search for, select whether you require the **Match Case** or **Match Whole Word** option, and press **Enter**.

The search results are highlighted in the Message List. Click **Find Next** or **Find Previous** button to keep searching the term throughout your log messages. Click **Close** to close the Find Messages dialog.



- To search via the column filter, click the **Filter** button at the head of a column. Enter the term that you want to search for, and press **Enter**.

  The search results appear in the Message List.



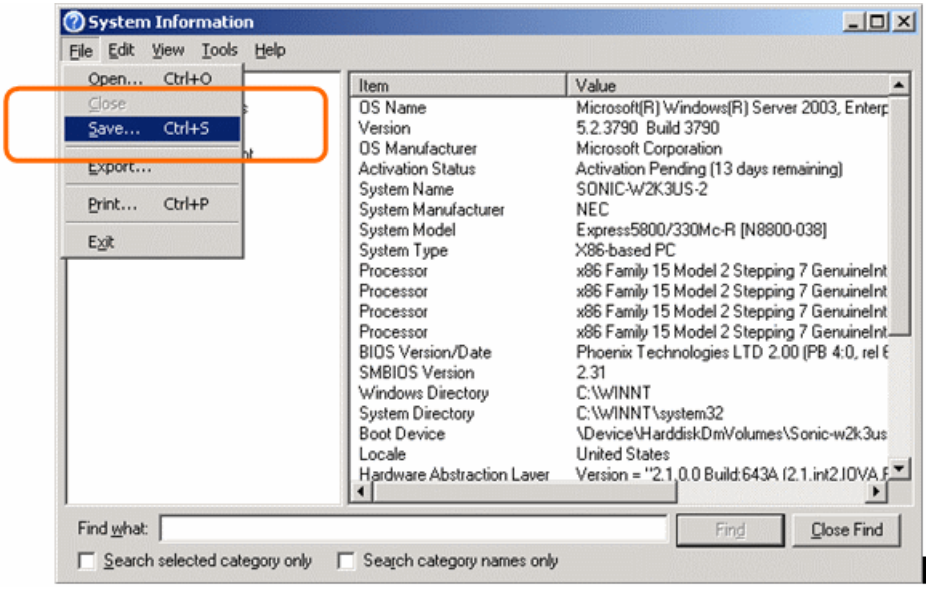
Collecting configuration logs

Collect information such as the hardware configuration and internal setting information for the FT server.

Important: If a STOP error or system error occurs or the system stalls, restart the system, and then start the procedure.

:

1. Click **Start | All Programs | Accessories | System Tools | System Information**.
2. Select **Save...** from the File menu.



3. Enter the name of the target file in the **File name** box.
4. Click **Save**.

Collecting diagnostic information with Dr. Watson

Collect diagnostic information related to application errors by using Dr. Watson. You can designate any destination to save diagnostic information.

For details, see help information. Click **Start | Run..., execute | drwtsn32.exe**, and click **Help** in the **Dr. Watson for Windows** dialog box.

Backup and recovery strategies

On the FT server, there are three partitions to support backup and recovery strategies as follows:

- The C: drive is for the Windows operating system and applications.
- The D: drive is for a database, such as the GV STRATUS system database. This allows you to restore the Windows operating system on the C: drive, yet keep the files on the D: drive intact. Typically the database is backed up and recovered with database-specific processes, rather than with a disk image.
- The E: drive is for storing a system image of the other partitions. From the E: drive you can restore images to the C: and D: drives.

When you receive a FT server from the factory, the machine has a system-specific image on the E: drive. For the highest degree of safety, you should copy this image to a secure location that is not on the FT device itself.

You receive a recovery CD with your server. This recovery CD does not contain a disk image. Rather, the recovery CD is bootable and contains the Acronis True Image software necessary to create and restore a disk image.

After your server is installed, configured, and running in your system environment, you should create new recovery disk images for the machine to capture settings changed from default. These “first birthday” images are the baseline recovery image for the machine in its life in your facility. You should likewise create new recovery disk images after completing any process that changes system software or data, such as a software upgrade. In this way you retain the ability to restore to a recent “last known good” state.

Identifying the FT Server model

FT server platform types are as following:

- Type I (NEC Draco): Released early 2012. Requires Acronis 8162 for recovery disk image process.
- Type II (NEC Cygnus): Released mid-2013. Requires Acronis 11.5 for recovery disk image process.
- Type III (NEC Pegasus): Released mid-2016. Requires Acronis 11.5 for recovery disk image process.

1. On the rear panel, below the PCI card slots, locate the equipment label.
2. Interpret the model number on the label as follows:
   - R320b-M4 = Type I
   - R320c-M4 = Type II
   - R320e-E4 = Type III

Acronis 8162: Creating a recovery disk image for storing on E: Type I

Do the following at the local server to create a disk image of the C: partition and the D: partition and store the image file on the E: partition:

1. Disconnect the AC power cabling from the bottom CPU/IO module.
2. Perform the steps in this procedure on the top CPU/IO module.
3. Make sure that media access is stopped and that the system on which you are working is not being used.
4. Startup and in BIOS setup disable OS Boot Monitoring.

   Refer to related topics in this Topic Library.
5. If you have not already done so, connect keyboard, monitor, and mouse.
6. Do the following:
   a) Insert the Recovery CD.
   b) Restart the machine.

      If there is a problem restarting, hold the standby button down for five seconds to force a hard shutdown. Then press the standby button again to startup.

   The system boots from the Recovery CD.

   The Acronis program loads.
7. At the startup screen, select **True Image Server OEM (Full Version)**.

   The Acronis main window appears.
8. In the Acronis main window, click **Backup**.

   The Create Backup Wizard opens.
9. On the Welcome page, click **Next**.
10. On the Partitions Selection page, do the following:
    a) Select the **(C:)** and the **(D:)** partitions and then click **Next**.
11. On the Backup Archive Location page, do the following:
    a) In the tree view select the **Backup (E:)** partition and enter the name of the image file you are creating.

       Create the file name using the machine hostname and the date. Name the file with the .tib extension.

       For example, if the hostname is MySystem1, in the File name field you enter *E:\MySystem1_20180327.tib*.
    b) Click **Next**.
12. On the Backup Options page, do not change any settings. Click **Next**.
13. On the Archive Comment page, if desired, enter image comments such as the date, time, and software versions contained in the image you are creating. Click **Next**.
14. On the "…ready to proceed…" page, do the following:
    a) Verify that you are creating images from the C: and D: partitions and writing to the E: partition, then click **Proceed**.
15. On the Operation Progress page, observe the progress report.

16. When a message appears indicating a successful backup, click **OK**.
17. Click **Operations | Exit** to exit the Acronis True Image program.

    The machine restarts automatically.
18. Remove the recovery media while the machine is shutting down.
19. Wait until startup processes are complete on the top CPU/IO module. Leave the module running.
20. On the bottom CPU/IO module, connect AC power cabling. The module starts up.
21. Restart and in BIOS setup enable OS Boot Monitoring.

    Refer to related topics in this Topic Library.

Related Topics

Setting OS Boot Monitoring in BIOS on page 1724

Acronis 11.5: Creating a recovery disk image for storing on E: Type II

This task applies to the Type II FT Server model. Do the following at the local server to create a disk image of the C: partition and the D: partition and store the image file on the E: partition:

1. Disconnect the AC power cabling from the bottom CPU/IO module.
2. Perform the steps in this procedure on the top CPU/IO module.
3. Make sure that media access is stopped and that the system on which you are working is not being used.
4. Startup and in BIOS setup disable OS Boot Monitoring.

   Refer to related topics in this Topic Library.
5. Do the following:
   a) Insert the Recovery CD.
   b) Restart the machine.

      If there is a problem restarting, hold the standby button down for five seconds to force a hard shutdown. Then press the standby button again to startup.

   The system boots from the Recovery CD.

   The Acronis program loads.
6. On the Acronis Rescue Media page, do the following:
   a) Use the keyboard arrow keys to select **Acronis Backup and Recovery 11.5 (64-bit...)** and then press **Enter**.
   b) Wait while Acronis fully loads.

      This can take a few minutes. When loaded, the Acronis Backup and Recovery page opens.
7. On the Acronis Backup and Recovery page, select **Back up now**.

   The Back up now page opens.
8. On the Back up now page, under What to back up, select **Item to back up**.

   The Select item to back up dialog box opens.

9. On the Select item to back up dialog box, do the following:
   a) Under Disk 1 select **C** and **D**. Clear other check boxes.
   b) Click **OK**.

   The Select item to back up dialog box closes.
10. On the Back up now page, under Where to back up, select **Location**.

    The Select location back up dialog box opens.
11. On the Select location back up dialog box, do the following:.
    a) Expand the tree-view **Local folders** node and select **E:**.
    b) Enter a name for your backup.
    c) Click **OK**.

    The Select location back up dialog box closes.
12. On the Back up now page, under How to back up, do the following:
    a) Set Backup type to **Full**.
    b) This is recommended for your first backup. For subsequent backups, you can optionally set this to Incremental or Differential.
    c) Set Validation to **Validate a backup as soon as it is created**.
13. On the Back up now page, click **OK**.

    The backup begins and the Backup Details page opens.
14. On the Backup Details page, select the **Progress** tab to view the progress.
15. Verify when the data is successfully backed up.
16. Close all Acronis pages and the Acronis main window.

    The machine restarts automatically.
17. Remove the recovery media while the machine is shutting down.
18. Wait until startup processes are complete on the top CPU/IO module. Leave the module running.
19. On the bottom CPU/IO module, connect AC power cabling. The module starts up.
20. Restart and in BIOS setup enable OS Boot Monitoring.

    Refer to related topics in this Topic Library.

Related Topics

Setting OS Boot Monitoring in BIOS on page 1724

Acronis 11.5: Creating a recovery disk image for storing on E: Type III

This task applies to the Type III FT Server model. Do the following at the local server to create a disk image of the C: partition and the D: partition and store the image file on the E: partition:

1. Disconnect the AC power cabling from the bottom CPU/IO module.
2. Perform the steps in this procedure on the top CPU/IO module.
3. Make sure that media access is stopped and that the system on which you are working is not being used.
4. Startup and in BIOS setup disable OS Boot Monitoring.

   Refer to related topics in this Topic Library.

5. Do the following:
   a) Insert the Acronis 11.5 WinPE Recovery CD.
   b) Restart the machine. The system will reboot a couple of times and the NEC logo will show on the screen.

      If there is a problem restarting, hold the standby button down for five seconds to force a hard shutdown. Then press the standby button again to startup.
6. Press **Enter** when prompted with "Press any key to boot from DVD/CD" on the screen.

   The system boots from the Recovery CD.

   It will take about 3 minutes before the system boots into the Acronis application.

   The Acronis program loads.
7. On the Acronis Rescue Media page, do the following:
   a) Use the keyboard arrow keys to select **Acronis Backup and Recovery 11.5 (64-bit...)** and then press **Enter**.
   b) Wait while Acronis fully loads.

      This can take a few minutes. When loaded, the Acronis Backup and Recovery page opens.
8. On the Acronis Backup and Recovery page, select **Back up now**.

   The Back up now page opens.
9. On the Back up now page, under What to back up, select **Item to back up**.

   The Select item to back up dialog box opens.
10. On the Select item to back up dialog box, do the following:
    a) Under Disk 1 select **C** and **D**. Clear other check boxes.
    b) Click **OK**.

    The Select item to back up dialog box closes.
11. On the Back up now page, under Where to back up, select **Location**.

    The Select location back up dialog box opens.
12. On the Select location back up dialog box, do the following:.
    a) Expand the tree-view **Local folders** node and select **E:**.
    b) Enter a name for your backup.
    c) Click **OK**.

    The Select location back up dialog box closes.
13. On the Back up now page, under How to back up, do the following:
    a) Set Backup type to **Full**.
    b) This is recommended for your first backup. For subsequent backups, you can optionally set this to Incremental or Differential.
    c) Set Validation to **Validate a backup as soon as it is created**.
14. On the Back up now page, click **OK**.

    The backup begins and the Backup Details page opens.
15. On the Backup Details page, select the **Progress** tab to view the progress.
16. Verify when the data is successfully backed up.

17. Close all Acronis pages and the Acronis main window.

    The machine restarts automatically.

18. Remove the recovery media while the machine is shutting down.
19. Wait until startup processes are complete on the top CPU/IO module. Leave the module running.
20. On the bottom CPU/IO module, connect AC power cabling. The module starts up.
21. Restart and in BIOS setup enable OS Boot Monitoring.

    Refer to related topics in this Topic Library.

Acronis 8162: Restoring from a system-specific recovery disk image on E: Type I

Use this task to restore a server using an image made from that particular server. If restoring from a generic factory default image, use the appropriate task.

1. Disconnect the AC power cabling from the bottom CPU/IO module.
2. Perform the steps in this procedure on the top CPU/IO module.
3. Make sure that media access is stopped and that the system on which you are working is not being used.
4. Startup and in BIOS setup disable OS Boot Monitoring.

   Refer to related topics in this Topic Library.

5. If you have not already done so, connect keyboard, monitor, and mouse.
6. Do the following:
   a) Insert the Recovery CD.
   b) Restart the machine.

      If there is a problem restarting, hold the standby button down for five seconds to force a hard shutdown. Then press the standby button again to startup.

   The system boots from the Recovery CD.

   The Acronis program loads.

7. At the startup screen, select **True Image Server OEM (Full Version)**.

   The Acronis main window appears.

8. In the Acronis main window, click **Recovery**.

   The Restore Data Wizard opens.

9. On the Welcome page, click **Next**.
10. On the Backup Archive Selection page, in the tree view expand the node for the E: partition and select the image file, then click **Next**.
11. On the Restoration Type Selection page, select **Restore disks or partitions** and then click **Next**.
12. On the Partition or Disk to Restore page, select **(C:)** and then click **Next**.
13. On the Restored Partition Location page, select **(C:)** and then click **Next**.
14. On the Restored Partition Type page, leave the selection at **Active** and then click **Next**.
15. On the Restored Partition Size page, leave settings at their defaults. The size reported in the upper pane is the size detected of the actual C: partition. This should be the same as that reported in the Partition size field in the middle of the page. Free space before and Free space after should both be reported at 0 bytes. Click **Next**.

16. On the Next Selection page, select **No, I do not** and then click **Next**.
17. On the Restoration Options page, do not make any selections. Click **Next**.
18. On the "…ready to proceed…" page, verify that you are restoring the correct image to the correct location. Click **Proceed**.
19. On the Operation Progress page, observe the progress report.
20. When a message appears indicating a successful recovery, click **OK**.
21. Click **Operations | Exit** to exit the Acronis True Image program.

    The machine restarts automatically.
22. Remove the recovery media while the machine is shutting down.
23. Wait until startup processes are complete on the top CPU/IO module. Leave the module running.
24. On the bottom CPU/IO module, connect AC power cabling. The module starts up.
25. Restart and in BIOS setup enable OS Boot Monitoring.

    Refer to related topics in this Topic Library.

Related Topics

Setting OS Boot Monitoring in BIOS on page 1724

Acronis 11.5: Restoring from a system-specific recovery disk image on E: Type II

This task applies to the Type II FT Server model. Use this task to restore a server using an image made from that particular server. If restoring from a generic factory default image, use the appropriate task.

1. Disconnect the AC power cabling from the bottom CPU/IO module.
2. Perform the steps in this procedure on the top CPU/IO module.
3. Make sure that media access is stopped and that the system on which you are working is not being used.
4. Startup and in BIOS setup disable OS Boot Monitoring.

   Refer to related topics in this Topic Library.
5. Do the following:
   a) Insert the Recovery CD.
   b) Restart the machine.

      If there is a problem restarting, hold the standby button down for five seconds to force a hard shutdown. Then press the standby button again to startup.

   The system boots from the Recovery CD.

   The Acronis program loads.
6. On the Acronis Rescue Media page, do the following:
   a) Use the keyboard arrow keys to select **Acronis Backup and Recovery 11.5 (64-bit...)** and then press **Enter**.
   b) Wait while Acronis fully loads.

      This can take a few minutes. When loaded, the Acronis Backup and Recovery page opens.

7. On the Acronis Backup and Recovery page, select **Recover**.
   The Recover Data page opens.
8. On the Recover Data page, under What to Recover page, select **Select Data**.
   The Data to Recover Selection dialog box opens.
9. On the Data to Recover Selection dialog box, do the following:
   a) Select **Browse**.
   b) In the tree view, expand the **Local Folders** node.
   c) Select the USB drive that contains the NEC-FT disk image.
   d) Click **OK**.
   On the Archive View tab, your backup name is listed.
10. On the Archive View tab, select your backup.
11. Under Backup contents, do the following:
   a) Select **MBR**.
   b) Select **Basic**.
      This selects all drives.
   c) Click **OK**.
   The Data to Recover Selection dialog box closes.
12. On the Recover data page, under Where to recover, verify the following:

Recover to:	Physical machine
	Clear all
Recover the 'NTFS' partition with MB size to...	Properties: System Reserved ..Size:....MB ..Letter: D
	Clear Disk 1/NTFS (D:)
Recover the 'NTFS' partition with GB size to...	Properties: NTFS ..Size:...GB ..Letter: C
	Clear Disk 1/NTFS (C:)

13. On the Recover Data page, click **OK**.
    The restore process begins.
14. On the My Recovery Details page, select the **Progress** tab to view the progress.
    The image loads in approximately 9 minutes.
15. When the data is successfully restored, click **OK**.
16. Close all Acronis pages and the Acronis main window.
    The machine restarts automatically.
17. Remove the recovery media while the machine is shutting down.
18. Wait until startup processes are complete on the top CPU/IO module. Leave the module running.
19. On the bottom CPU/IO module, connect AC power cabling. The module starts up.

20. Restart and in BIOS setup enable OS Boot Monitoring.

    Refer to related topics in this Topic Library.

Related Topics

Setting OS Boot Monitoring in BIOS on page 1724

Acronis 11.5: Restoring from a system-specific recovery disk image on E: Type III

This task applies to the Type III FT Server model. Use this task to restore a server using an image made from that particular server.

1. Disconnect the AC power cabling from the top and bottom CPU/IO module.
2. In top CPU/IO module, leave drive 0 in slot, remove all other drives.
3. Provide AC power to top CPU/IO module.
4. Perform the steps in this procedure on the top CPU/IO module.
5. Make sure that media access is stopped and that the system on which you are working is not being used.
6. Connect the USB flash drive with the NEC-FT image to the USB port.
7. Startup and in BIOS setup disable OS Boot Monitoring.

   Refer to related topics in this Topic Library.

8. Do the following:
   a) Insert the Acronis 11.5 WinPE Recovery CD.
   b) Restart the machine.

      If there is a problem restarting, hold the standby button down for five seconds to force a hard shutdown. Then press the standby button again to startup.

   The system boots from the Recovery CD.

   The Acronis program loads.

9. On the Acronis Rescue Media page, do the following:
   a) Use the keyboard arrow keys to select **Acronis Backup and Recovery 11.5 (64-bit...)** and then press **Enter**.
   b) Wait while Acronis fully loads.
10. On the Acronis Backup and Recovery page, select **Recover**.

    The Recover Data page opens.

11. On the Recover Data page, under What to Recover page, select **Select Data**.

    The Data to Recover Selection dialog box opens.

12. On the Data to Recover Selection dialog box, do the following:
    a) Select **Browse**.
    b) In the tree view, select the USB drive that contains the NEC-FT disk image.
    c) Click **OK**.

    On the Archive View tab, your backup name is listed.

13. On the Archive View tab, select your backup.

14. Under Backup contents, do the following:
    a) Select **MBR**.
    b) Select **Basic**.
       This selects all drives.
    c) Click **OK**.

    The Data to Recover Selection dialog box closes.
15. On the Recover Data page, click **OK**.
    The restore process begins.
16. On the My Recovery Details page, select the **Progress** tab to view the progress.
    The image loads in approximately 9 minutes.
17. When the data is successfully restored, click **OK**.
18. Close all Acronis pages and the Acronis main window.
    The machine restarts automatically.
19. Remove the recovery media while the machine is shutting down.
20. Wait until startup processes are complete on the top CPU/IO module. Leave the module running.
21. On the bottom CPU/IO module, connect AC power cabling. The module starts up.
22. Restart and in BIOS setup enable OS Boot Monitoring.
    Refer to related topics in this Topic Library.

Related Topics

Setting OS Boot Monitoring in BIOS on page 1724

Restoring a GV STRATUS Core Server on a FT Server platform from a generic image

This is the master task that applies to both Type I and Type II FT Server models. As instructed by the steps in this task, use the appropriate Acronis sub-task specified for the Type I or Type II model.

1. Disconnect network cables.
2. Disconnect power cabling from bottom CPU/IO module.
3. In top CPU/IO module, leave drive 0 in slot, remove all other drives.
4. Provide AC power to top CPU/IO module.
5. Provide access to the disk image file to which you are restoring. For example, connect an external drive containing the image.
6. Startup and in BIOS setup disable OS Boot Monitoring.
   Refer to related topics in this Topic Library.
7. Using the Acronis recovery disk image process as appropriate for the FT Server Type I or Type II model, restore the generic disk image to the top CPU/IO module using Acronis.
   The process to boot into Acronis takes several minutes.
   The restore process takes approximately two hours.
   Refer to related topics in this Topic Library.
8. Restart and log in to Windows as Administrator.

9. When prompted, enter Windows operating system product key and activate later.
10. Restart as prompted.
11. Complete items as prompted by the sysprep process, including the following:
    - Time zone
    - Server name
    - Deselect **Automatic Updates**
    - Select **Don't show again at startup**

    The server restarts.
12. If Server Manager opens, select **Don't show again at startup**.
13. In the top CPU/IO module, insert all drives.
14. In the bottom CPU/IO module, insert all drives.
15. Connect power cabling and start up bottom CPU/IO module.
16. Perform dual disk configuration as follows:
    a) In the RDR Utility, create the first Virtual disk.
    b) When prompted to reboot, click **No**.
    c) Manually reboot the system.

    Refer to related topics in this Topic Library.
17. Perform system disk dual configuration as follows:
    a) Right-click on Slot 0 of PCI Module 11 and select **Add Physical Disk To RDR Virtual Disk**.

    Refer to related topics in this Topic Library.
18. Set resync priority as follows:
    a) Set Virtual Disk 0 to high priority In the Logical disk section, highlight **RDR Virtual Disk**, right-click and select **Set Resync Priority**, set to **High** and click **OK**.

       Disk 0 in each chassis blinks rapidly until the initialization is done.

    Refer to related topics in this Topic Library.
19. Repeat steps to create Virtual Disks and map to physical disks.
20. Wait until Disk 0 completes the build process.

    That takes approximately 3 hours.
21. Use Windows utilities and build a Dynamic disk with all other disks, except for drive 0, using the striped mode rather than the span mode.

    Refer to related topics in this Topic Library.
22. Set duplex LAN configuration to team the left NICS in each server and the right NICS in each server.

    Refer to related topics in this Topic Library.
23. Name teams `Control Team` and `FTP Team`.

    Refer to related topics in this Topic Library.
24. Reorder network adapters so the Control Team is first and the FTP Team is second.

    Refer to related topics in this Topic Library.

25. Restart and in BIOS setup enable OS Boot Monitoring.

    Refer to related topics in this Topic Library.

26. Turn off the FT server firewall

    Refer to related topics in this Topic Library.

27. Remove the GVAdmin account from the Deny log on locally list.

    Refer to related topics in this Topic Library.

28. Install SiteConfig Discovery Agent.

    Refer to related topics in this Topic Library.

29. Install SQL.

    Before installing SQL, make sure that you copy the correct `StratusSQLConfigurationFile.ini` file onto the system so that the database is installed on the D:\ partition.

    Refer to related topics in this Topic Library.

30. Activate the Windows operating system.

    Refer to related topics in this Topic Library.

31. Do any Windows High Priority updates that are not already installed.
32. Install GV STRATUS software.
33. If the FT server has a proxy share, on proxy share security settings make sure the local "Everyone" has read permission.
34. If the FT server has a proxy share, add the internal system account, which by default is GVAdmin, to the local Administrators group and on proxy share security settings give that account full permissions.

Related Topics

Setting OS Boot Monitoring in BIOS on page 1724
Acronis 8162: Restoring from the generic recovery disk image Type I on page 1720
Acronis 11.5: Restoring from the generic recovery disk image Type II on page 1721
System disk dual configuration procedure on page 1681
Set resync priority on page 1693
Build dynamic disk on page 1693
Set duplex LAN configuration on page 1694
Name teams on page 1699
Reorder adapters
Turn off FT server firewall on page 1724
Remove GVAdmin account from Deny log on locally list on page 1726
Installing SQL on page 543
Installing the Discovery Agent on a GV STRATUS server on page 544
Activating the Windows operating system on page 544

Acronis 8162: Restoring from the generic recovery disk image Type I

Use this sub-task only as directed by the steps in the master task for restoring from a generic recovery disk image.

This task applies to the Type I FT Server model.

This procedure can be used on a server that needs to be restored to its factory default state. For example, if you neglected to make a first birthday image, you might need to use this procedure. If the image from which you are restoring was made from the specific machine, refer to the appropriate procedure.

NOTE: This procedure restores the server (both C: and D: partitions) to its factory default condition. Passwords and other site-specific configurations are reset to factory defaults.

1. Make sure that media access is stopped and that the system on which you are working is not being used.
2. Disconnect the AC power cabling from the bottom CPU/IO module.
3. Perform the steps in this procedure on the top CPU/IO module.
4. Connect all motherboard NICs to LAN connections.
5. If you have not already done so, connect keyboard, monitor, and mouse.
6. Do the following:
   a) Insert the Recovery CD.
   b) Restart the machine.

      If there is a problem restarting, hold the standby button down for five seconds to force a hard shutdown. Then press the standby button again to startup.

   The system boots from the Recovery CD.

   The Acronis program loads.
7. At the startup screen, select **True Image Server OEM (Full Version)**.

   The Acronis main window appears.
8. In the Acronis main window, click **Recovery**.

   The Restore Data Wizard opens.
9. On the Welcome page, click **Next**.
10. On the Backup Archive Selection page, navigate to and select the image file, then click **Next**.
11. On the Restoration Type Selection page, select **Restore disks or partitions** and then click **Next**.
12. On the Partition or Disk to Restore page, select **(C:)** and then click **Next**.
13. On the Restored Partition Location page, select **(C:)** and then click **Next**.
14. On the Restored Partition Type page, leave the selection at **Active** and then click **Next**.
15. On the Restored Partition Size page, leave settings at their defaults. The size reported in the upper pane is the size detected of the actual C: partition. This should be the same as that reported in the Partition size field in the middle of the page. Free space before and Free space after should both be reported at 0 bytes. Click **Next**.
16. On the Next Selection page, select **Yes, I want to restore another partition or hard disk drive** and then click **Next**.
17. On the Partition or Disk to Restore page, select **(D:)** and then click **Next**.

18. On the Restored Partition Location page, select **(D:)** and then click **Next**.

    opens.

19. On the Restored Partition Type page, leave the selection at **Primary** and then click **Next**.
20. On the Restored Partition Size page, leave settings at their defaults. The size reported in the upper pane is the size detected of the actual D: partition. This should be the same as that reported in the Partition size field in the middle of the page. Free space before and Free space after should both be reported at 0 bytes. Click **Next**.
21. On the Next Selection page, select **No, I do not** and then click **Next**.
22. On the Restoration Options page, do not make any selections. Click **Next**.
23. On the "…ready to proceed…" page, verify that you are restoring the correct image to the correct location. Click **Proceed**.
24. On the Operation Progress page, observe the progress report.
25. When a message appears indicating a successful recovery, click **OK**.
26. Click **Operations | Exit** to exit the Acronis True Image program.

    The machine restarts automatically.

27. Remove the recovery media while the machine is shutting down.
28. Wait until startup processes are complete on the top CPU/IO module. Leave the module running.
29. When prompted, enter the machine name.

    Make sure the name is identical to the name it previously had.

    At first start up after reimage, the system is in Embedded Security Update mode by default.

30. On the bottom CPU/IO module, connect AC power cabling. The module starts up.

Continue with the steps in the master task for restoring from a generic recovery disk image.

Related Topics

Restoring a GV STRATUS Core Server on a FT Server platform from a generic image on page 530

Acronis 11.5: Restoring from the generic recovery disk image Type II

Use this sub-task only as directed by the steps in the master task for restoring from a generic recovery disk image.

This task applies to the Type II FT Server model.

This task restores a server to its factory default state. For example, if you neglected to make a first birthday image, you might need to use this procedure. If the image from which you are restoring was made from the same, specific machine to which it is being restored, do not use this task.

NOTE: This procedure restores the server (C:, D:, and E: partitions) to its factory default condition. Passwords and other site-specific configurations are reset to factory defaults.

1. Make sure that media access is stopped and that the system on which you are working is not being used.
2. Disconnect the AC power cabling from the bottom CPU/IO module.
3. Perform the steps in this procedure on the top CPU/IO module.
4. Connect all motherboard NICs to LAN connections.

5. Manage connections as follows:
   a) Disconnect the mouse from the USB port, if it is currently connected.

      NOTE: A problem with Acronis 11.5 on the FT server requires this workaround. The mouse must be temporarily disconnected before booting into Acronis, then reconnected after Acronis fully loads.

   b) If not already connected, connect keyboard and monitor.
6. Do the following:
   a) Insert the Recovery CD.
   b) Restart the machine.

      If there is a problem restarting, hold the standby button down for five seconds to force a hard shutdown. Then press the standby button again to startup.

   The system boots from the Recovery CD.

   The Acronis program loads.
7. On the Acronis Rescue Media page, do the following:
   a) Use the keyboard arrow keys to select **Acronis Backup and Recovery 11.5 (64-bit...)** and then press **Enter**.
   b) Wait while Acronis fully loads.

      This can take a few minutes. When loaded, the Acronis Backup and Recovery page opens.
8. On the Acronis Backup and Recovery page, select **Recover**.

   The Recover Data page opens.
9. On the Recover Data page, under What to Recover page, select **Select Data**.

   The Data to Recover Selection dialog box opens.
10. On the Data to Recover Selection dialog box, do the following:
    a) Select **Browse**.
    b) In the tree view, select the USB drive that contains the generic recovery disk image.

       Even though your backup is on the drive, it is not yet visible.

    c) Click **OK**.

    On the Archive View tab, your backup name is listed.
11. On the Archive View tab, select your backup.
12. Under Backup contents, do the following:
    a) Select **MBR**.
    b) Select **Basic**.

       This selects all drives.

    c) Click **OK**.

    The Data to Recover Selection dialog box closes.

13. On the Recover data page, under Where to recover, select the correct destination partition for each source partition as follows:
    a) Select **Recover Disk 1 MBR**.
       The MBR Destination dialog box opens.
    b) In the MBR Destination dialog box, select **Disk 1: Seagate SCSI**.
    c) Click **OK**.
    d) Select **Recover System Reserved (C:)**.
       The Volume Selection dialog box opens.
    e) In the Volume Selection dialog box, select **Disk 1: Seagate SCSI**.
    f) Click **OK**.
    g) Select **Recover NTFS (C:)**.
       The Volume Selection dialog box opens.
    h) In the Volume Selection dialog box, select **Disk 1: Seagate SCSI**.
    i) Click **OK**.
    j) Select **Recover NTFS (D:)**.
       The Volume Selection dialog box opens.
    k) In the Volume Selection dialog box, select **Disk 1: Seagate SCSI**.
    l) Click **OK**.
14. On the Recover Data page, click **OK**.
    The restore process begins.
15. On the My Recovery Details page, select the **Progress** tab to view the progress.
    The image loads in approximately 9 minutes.
16. When the data is successfully restored, click **OK**.
17. Close all Acronis pages and the Acronis main window.
    The machine restarts automatically.
18. Remove the recovery media while the machine is shutting down.
19. Wait until startup processes are complete on the top CPU/IO module. Leave the module running.
20. When prompted, enter the machine name.
    Make sure the name is identical to the name it previously had.
    After start up, one or more device discovery windows can open. Allow processes to complete without interference.
    At first start up after reimage, the system is in Embedded Security Update mode by default.
21. On the bottom CPU/IO module, connect AC power cabling. The module starts up.

Continue with the steps in the master task for restoring from a generic recovery disk image.

Related Topics

Restoring a GV STRATUS Core Server on a FT Server platform from a generic image on page 530

Setting OS Boot Monitoring in BIOS

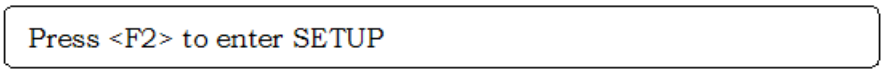
Use this task as directed by other processes, such as the disk image recovery, or as instructed by Grass Valley Support.

- When the FT Server is running the Windows Operating System, OS Boot Monitoring must be enabled to support the primary fault tolerant failover behavior in which one CPU/IO module takes the place of the other CPU/IO module.
- When the FT Server is not running the Windows Operating System, such as when running from Acronis during a disk image recovery process, OS Boot Monitoring must be disabled. If enabled, the FT server continually reboots and disrupts the disk image recovery process.

1. Power on one CPU/IO module.

   POST will be performed on this CPU/IO module.

2. A message appears at the lower left of the screen (shown below), prompting for startup of the BIOS setup utility SETUP.

3. Press **F2** to start the SETUP utility, while the above message is displayed.
4. Select the **Server** tab.
5. Select **Monitoring Configuration** and press **Enter**.
6. Select **OS Boot Monitoring**.
7. Set to Enabled or Disabled, as appropriate.
8. Press **F10** to save and exit.

Turn off FT server firewall

This task applies to the following:

- A GV STRATUS Core server on a FT server platform.

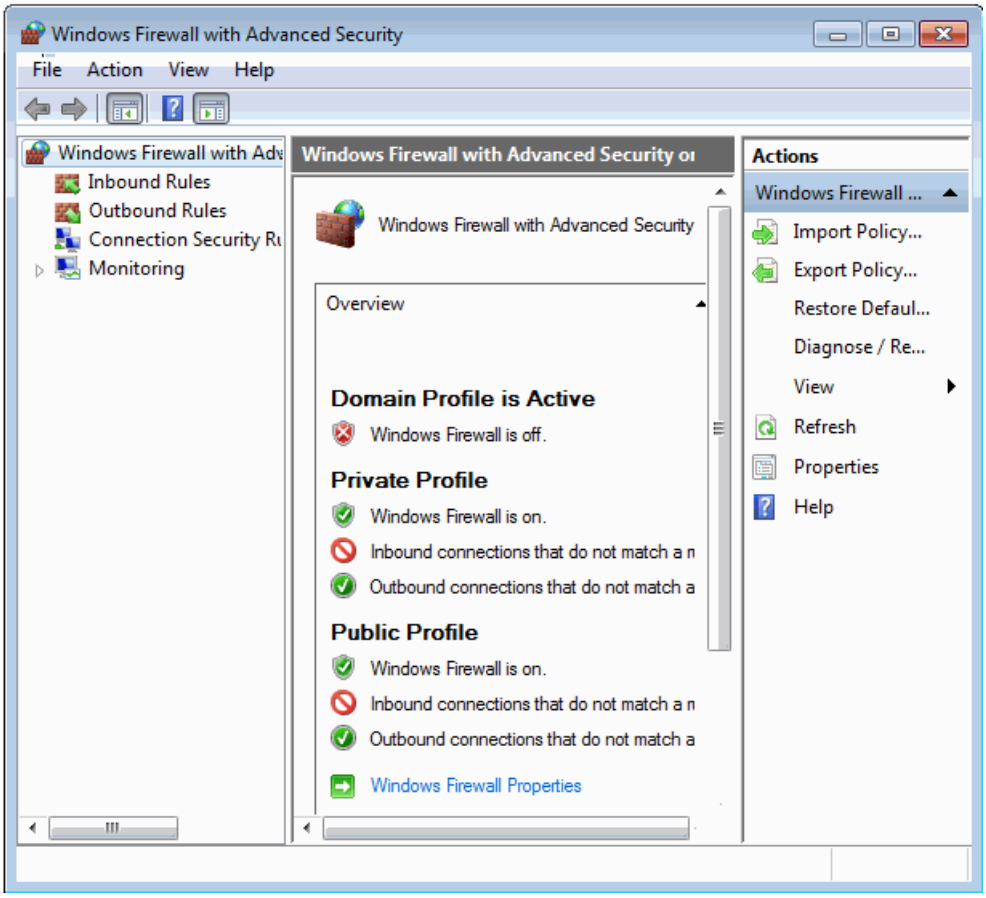
A server must have its firewall disabled for proper K2 system operation. This includes the Windows firewall that has different profiles for workgroup, domain, etc. You must do the following steps to disable the firewall.

1. Log in to the server with Windows administrator privileges.

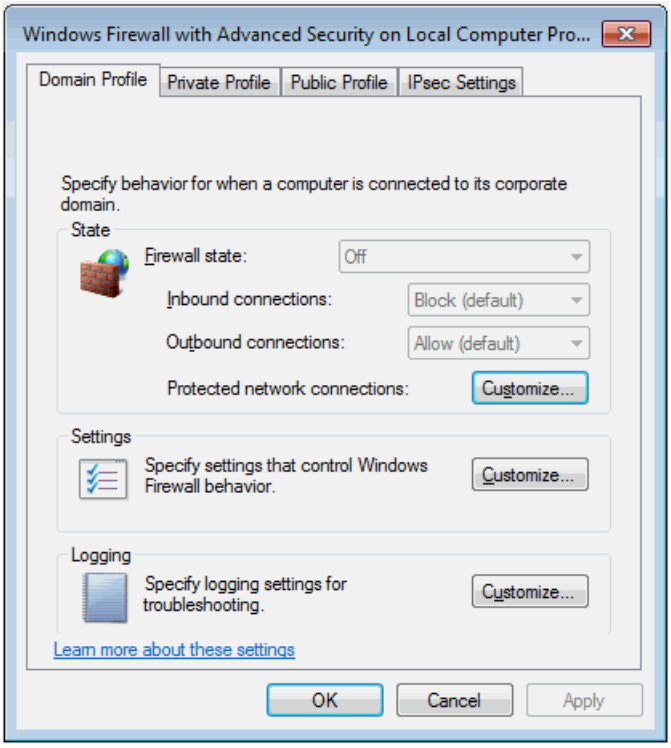
2. From the Windows desktop click **Start** and in the **Search programs and files** box type the following and then press **Enter**.

   ```
   wf.msc
   ```

   The Windows Firewall with Advanced Security window opens.



3. At the bottom of the Overview section, click **Windows Firewall Properties**.
   The Properties dialog box opens.



4. On the **Domain Profile** tab, set **Firewall state** to **Off**.
5. On the **Private Profile** tab, set **Firewall state** to **Off**.
6. On the **Public Profile** tab, set **Firewall state** to **Off**.
7. Click **OK** to save settings and close.

Remove GVAdmin account from Deny log on locally list

1. From the Windows desktop click **Start | Administrative Tools | Local Security Policy**.
   The Local Security Policy window opens.
2. In the tree-view select **Local Policies | User Rights Assignment**.
3. In the Policy list, double-click **Deny log on locally**.
   The Deny log on locally Properties dialog box opens.
4. On the **Local Security Setting** tab, select **GVAdmin** and then click **Remove**.
5. Click **OK** to save settings and close.

Replacing failed components

The components that can be replaced if a failure occurs in the field, FRUs (Field Replaceable Units), are described in this section. Follow instructions replacement for each type of component as given in this section.

Remove a CPU/IO module

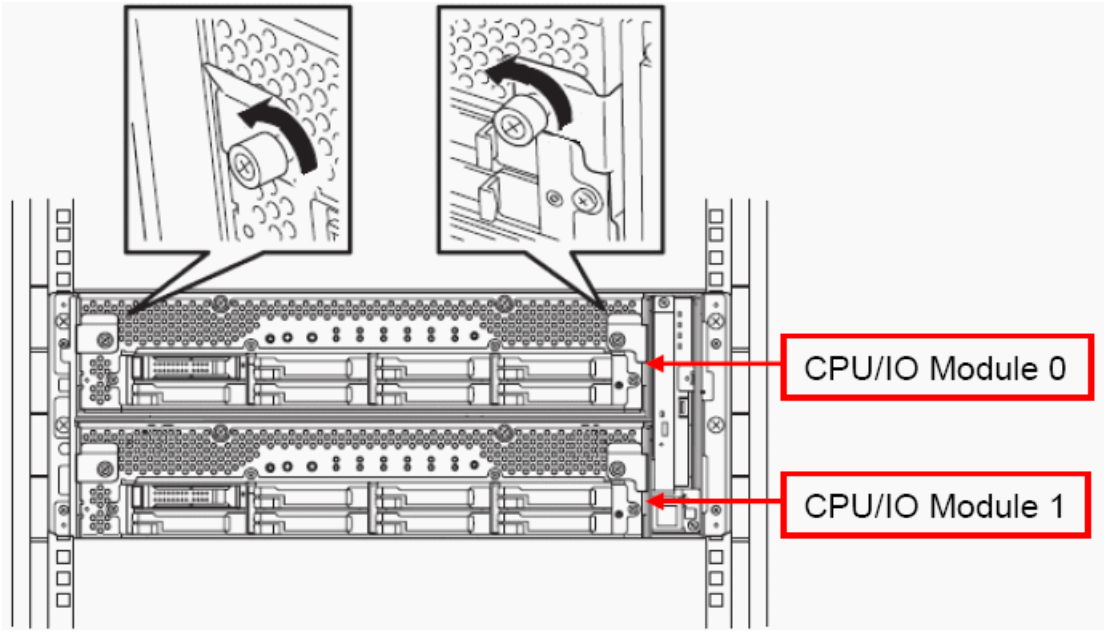
You may remove either CPU/IO module from the rack-mounted enclosure for exchange if required.

Please note the following precautions before doing so:

- Power down the CPU/IO module you are replacing by removing the AC line cord from the rear of that module. When installed, the AC line cords are held in place by stopper bars preventing the removal of the CPU/IO module.
- Have at least two people available to remove a CPU/IO module.
- If you are removing a failed CPU/IO module for exchange, after you have removed the CPU /IO module, you must remove all hard drives in their caddies from the failed module. You must label the hard drives with their drive slot location numbers as you remove them. They must be re-installed in the same hard drive slots when the exchange CPU/IO module is received from the factory. If not, the mirrored hard drives will be out of sync.

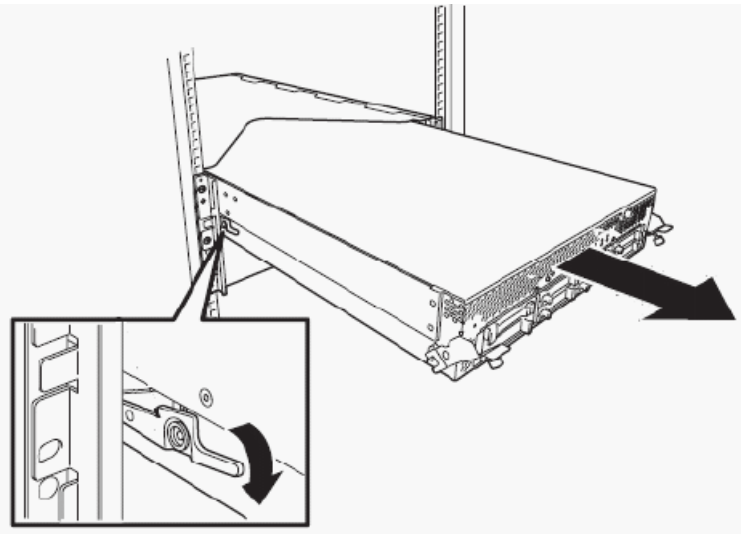
Remove either CPU/IO module as described below.

1. Remove the AC line cord from the module you are removing.
2. Remove the front bezel from the front of the unit by loosening the screws on either side of the bezel.
3. On either side of the module you are removing, loosen the left and right screws to unlock the lock levers holding the module to the sides of the enclosure.



4. Slowly pull out the CPU/IO module until the side lock lever on the left side of the module catches on the lock mechanism.

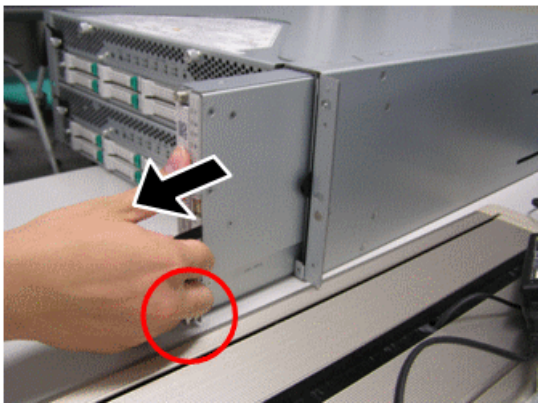
5. Push down on the side lock lever as shown below so it is horizontal and will slide over the lock mechanism, allowing you to pull out the module completely.



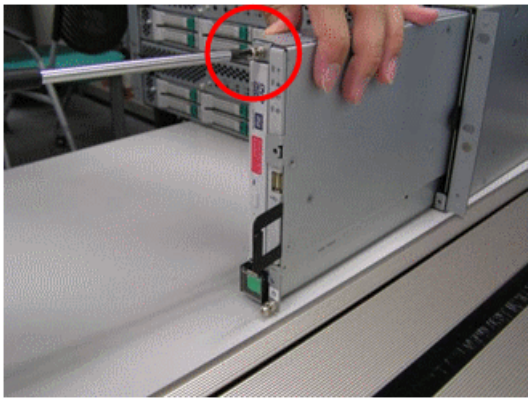
Replacing Optical DVD drive

Use this procedure if you need to replace the optical DVD drive. You may remove this drive while the FT server is powered up.

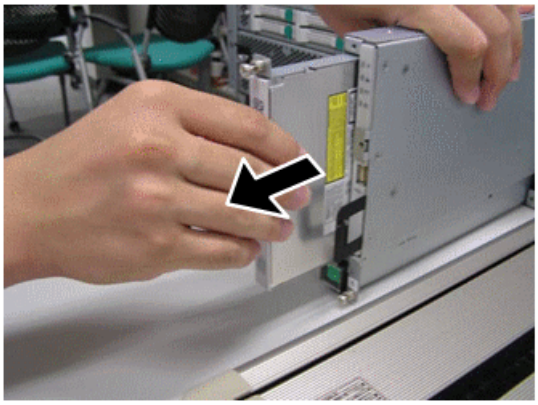
1. Remove the front bezel from the chassis.
2. Remove the entire front unit containing the optical DVD drive by turning the thumb screw on the bottom of the drive unit to the left and pulling out the entire unit.



3. Once the drive unit is free, loosen the top screw holding the DVD drive in the front unit.



4. Pull out the DVD drive.



5. Reverse the steps above to install a replacement DVD drive.

Servicing hard disk drives

The sections given here describe various installation and replacement procedures for the hard disk drives in each CPU/IO module. Refer to the procedure that applies to your condition.

Locating a failed hard drive

Use this procedure to locate a failed hard disk drive. A failed hard disk drive will be indicated by an amber DISK ACCESS LED on the hard drive handle.

To verify a disk failure, do the following:

1. From **Start**, select **All Programs**, **RDR**, and click **RDR Utility** to start the RDR Utility.
2. From the tree on the left pane of the RDR Utility, select each disk and check the values of **MTBF: Current** and **MTBF:NumberOfFaults** in the right pane.

3. Refer to the table below, if either of the values is different from the normal value, the disk has an error.

Property name	Description	Normal value (no error)
MTBF: HardCurrent	Mean time between hardware failures	Unknown
MTBF: SoftCurrent	Mean time between software failures	Unknown

4. If an error is indicated, replace the hard disk drive.

Replacing failed hard drives

Follow the hard disk drive procedures in the order below to replace a failed hard disk drive. The hard disk drive should be replaced with a new device with the server powered on.

1. Locate the failed hard disk. When a hard disk fails, the DISK ACCESS LED on the hard disk drive's handle turns to an amber color.
2. Remove the failed hard drive as described in the related procedure in this manual.
3. Install the new hard drive as described in the related procedure in this manual.
4. Check the following:
   - The hard disk to be installed for replacement must have the same specifications as its mirroring hard disk.
   - Use an unsigned hard disk drive for replacement. To use the signed disk, it is necessary to recover the duplex configuration by referring to Disk Operation in the configuration section of this manual after formatting the disk physically.
   - Before performing physical formatting, change **Option ROM Scan Monitoring** to **Disabled** on **Server Monitoring Configuration** in the BIOS setup utility.
5. Restore the redundant configuration.

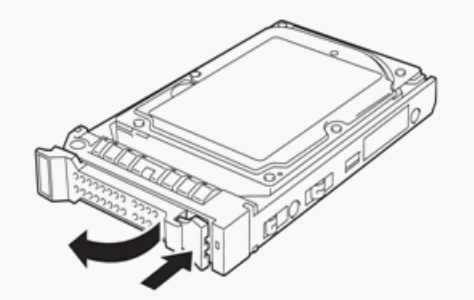
Installing a hard disk drive

Follow the procedure below to install hard disk drives that have been removed from a faulty CPU/IO module and are being installed in the replacement module from the factory.

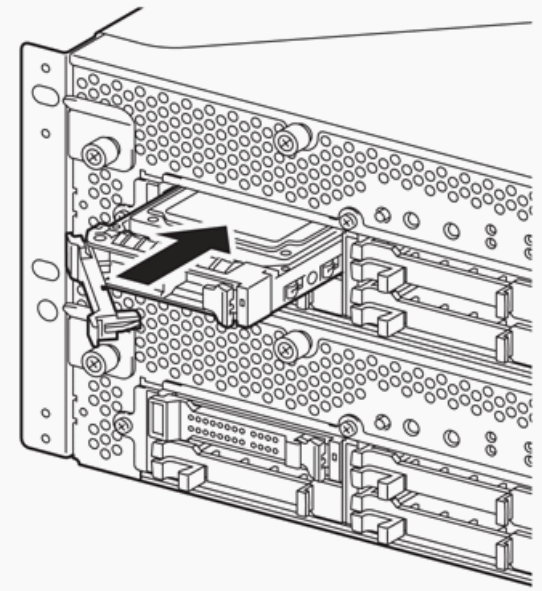
1. Shut down the OS. The system turns off automatically.
2. Remove the front bezel.

   NOTE: When installing hard disk drives into a replacement CPU/IO module, be sure to put the hard disk drive into the same slot that you marked on it when you removed it from the failed CPU/IO module.

3. Unlock the hard disk drive.



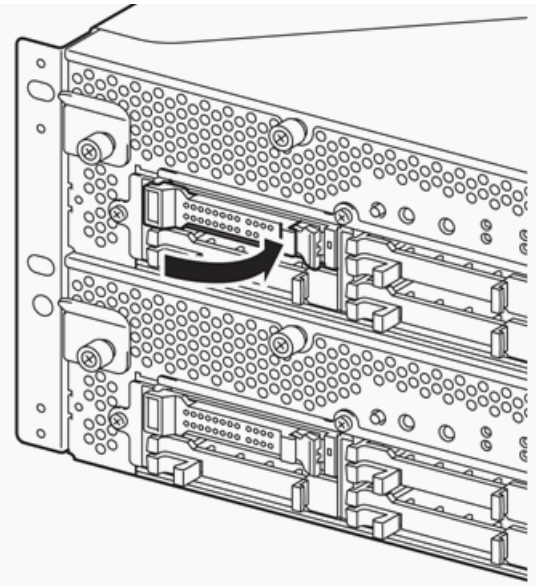
4. Firmly hold the handle of the hard disk drive and insert the drive into the slot.



Follow these tips when installing a hard disk drive. Refer to the illustration above:

- Insert the disk until the lever hook touches the server frame.
- Check the direction of the lever. Insert the hard disk with the lever unlocked.

5. Slowly close the lever. When the lever is locked, you will hear a clicking sound. Check that the hook of the lever is engaged with the frame.



6. Press the POWER switch to power on.

   Original drives installed into a replacement CPU/IO module should require no configuration.

7. Install the front bezel.

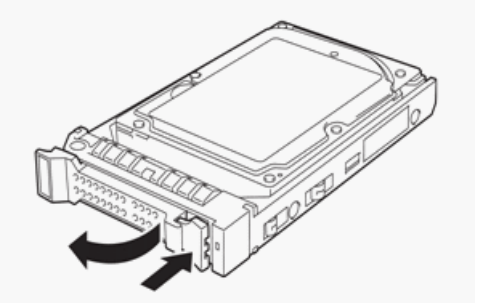
Installing a hard disk drive

Follow the procedure below to install hard disk drives that have been removed from a faulty CPU/IO module and are being installed in the replacement module from the factory.

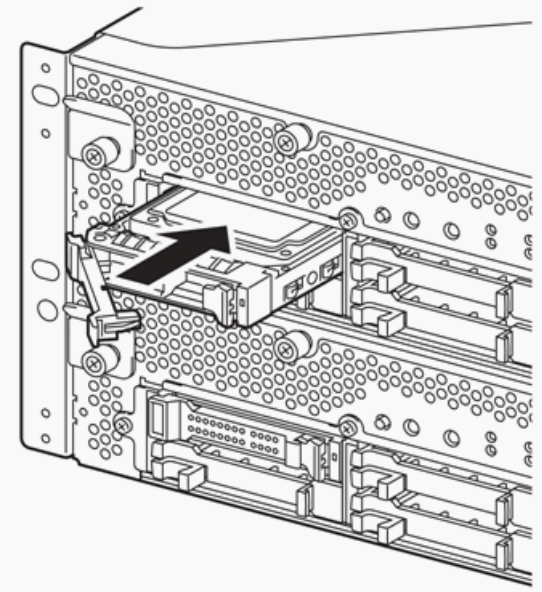
1. Shut down the OS. The system turns off automatically.
2. Remove the front bezel.

   NOTE: When installing hard disk drives into a replacement CPU/IO module, be sure to put the hard disk drive into the same slot that you marked on it when you removed it from the failed CPU/IO module.

3. Unlock the hard disk drive.



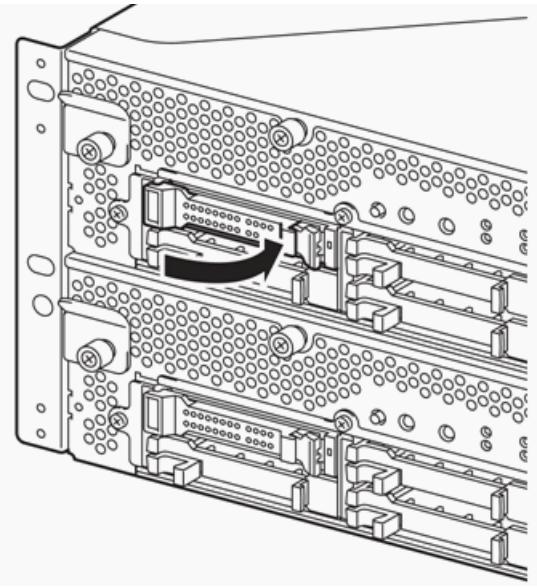
4. Firmly hold the handle of the hard disk drive and insert the drive into the slot.



Follow these tips when installing a hard disk drive. Refer to the illustration above:

- Insert the disk until the lever hook touches the server frame.
- Check the direction of the lever. Insert the hard disk with the lever unlocked.

5. Slowly close the lever. When the lever is locked, you will hear a clicking sound. Check that the hook of the lever is engaged with the frame.



6. Press the POWER switch to power on.
   Original drives installed into a replacement CPU/IO module should require no configuration.
7. Install the front bezel.

Specifications

Storage device specifications

The FT server storage specifications are shown in the tables below:

Hard Disk Drives	Type I and Type II Specification
Type	2.5 inch HDD (SAS 4 8TB, 5 x 600Gbs)
Capacity (maximum)	600GB x 5 in each CPU/IO module. Note that user area is reduced to half of the physical capacity due to software mirroring.
Hot-swappable	Yes
Number of slots	8 (Slots 0-7) per CPU/IO module, 16 total, (number of slots used based on FT server model)
Slot 0, Drive 0	System disk
Slots 1-7, Drives 1-7	Data disks

I/F and RAID	Type I and Type II Specification
Type	SAS 3Gb/s RAID 1 (standard)

Optical Disk Drive	Type I and Type II Specifications
Type	DVD Super Multi x 1

Mechanical specifications

The FT server mechanical specifications are shown in the table below:

Table 21: Mechanical specifications

Characteristic	Type I and Type II Specification
Cabinet Type	Rack-mount
Rack units	4
External Dimensions	483 (w) x 178 (h) x 736 (d) mm, 19.0 in. (w) x 7.0 in. (h) x 28.9 in. (d)
Rack clearance	40 cm or more on top, 1 m or more on the front and rear, 60 cm or more on the right and left.
Weight	Maximum 51.5kg , 113.3 lbs

Power supply specifications

The FT server power supply specifications are shown in the table below:

Table 22: Power specifications

Power Supply	Type I Specifications	Type II Specifications
Type	AC 100V-240V +/- 10%, 50/60Hz +/- 3Hz	AC 100V-240V +/- 10%, 50/60Hz +/- 3Hz
Power Consumption	1400VA, 1390W	1300VA, 1290W

Environmental specifications

The FT server specifications are shown in the following table:

Characteristic	Type I and Type II Specification
Ambient Temperature Non-operating	-10° to +55° C
Ambient Humidity Non-operating	20 to 80% RH (non-condensing)
Ambient Temperature Operating	+10° to +35° C
Ambient Humidity Operating	20 to 80% RH (non-condensing)

Grass Valley Ports

20

TCP: Used by mpgsession.exe, mxfsession.exe, gxfsession.exe, or ftpd.exe for FTP.

21

TCP: Used by ftpd.exe for FTP data.

23

Protocol: TCP. Used by Ignite for Chyron HyperX, CG Graphic Load and Playout.

80

Protocol: TCP. Traffic: HTTP. Used by any GV STRATUS server, MediaFrame server, and Flexera server for EDIUS Workgroup license activation.

81

Protocol: TCP. Used by SNFS for GUI (Java). User starts at port 81, redirected to 443.

137

TCP: Used by SMB. UDP: Used by SiteConfig. File and printer sharing. Used by SMB.

138

UDP: Used by SiteConfig. File and printer sharing. Used by SMB.

139

TCP: Used by SiteConfig. File and printer sharing. Used by SMB.

161

UDP: Used by snmp.exe for SNMP.

162

UDP: Used by snmptrap.exe for SNMP trap.

280

TCP: Used by MediaFrame Server version 6.3 and lower, config.

443

Protocol: TCP. Used by SNFS for GUI (Java). Used by GV STRATUS applications for HTTPS secure communication with GV STRATUS Core Server. Used by EDIUS Workgroup applications for HTTPS secure communication with Flexera server for license activation.

445

Protocol: TCP. Used by SDB and XMOS Server and NAS. Used by SiteConfig. File and printer sharing. Used by SMB.

1050

TCP: Used by Ignite for gvMiniViewSG2, Scriptviewer for Story Copy.

1062

Protocol: TCP. Used by SNFS for Blockpool. Both ports 1062 and 1063 if HA primary.

1063

Protocol: TCP. Used by SNFS for Blockpool. Both ports 1062 and 1063 if HA primary.

1070

Used by SNFS for GUI (Java connection to Linter).

1120

Protocol: TCP. Used by GV STRATUS servers hosting Xcode Control Engine to access the Carbon Server.

1223

TCP: Used by EDIUS XRE Server.

1433

TCP: Used by DSM.

1527

Protocol: TCP. Used by SNFS for GUI (Java connection to derby database).

2000

Protocol: TCP. Used by SDB Server incoming, and by GV STRATUS and GV STRATUS Rundown clients outgoing.

2001

Protocol: TCP. Used by SDB Server incoming, and by GV STRATUS and GV STRATUS Rundown clients outgoing.

2002

Protocol: TCP. Used by backup SDB Server incoming, and by GV STRATUS and GV STRATUS Rundown clients outgoing.

2003

Protocol: TCP. Used by backup SDB Server incoming, and by GV STRATUS and GV STRATUS Rundown clients outgoing.

02050

Protocol: TCP. Used by Ignite for Cambotics, Camera Preset Recall.

2063

TCP: Ingest Compusat port.

2500 - 2509

Protocol: TCP. Ports 2500 to 2509 used by Ignite for Telemetrics, Camera Preset Recall.

3000

Protocol: TCP. Used by XMOS Server incoming, and by GV STRATUS and GV STRATUS Rundown clients outgoing.

3001

Protocol: TCP. Used by XMOS Server incoming, and by GV STRATUS and GV STRATUS Rundown clients outgoing.

3020

TCP/UDP: SMB.

3200

TCP: Used by SDB and XMOS Server Thumbnail Server.

3307

Protocol: TCP. Used by SNFS for GUI (Java connection to MySQL).

3333

TCP: Used by Ingest Server.

3334

TCP: Used by Ingest Server.

3389

TCP: Used by Remote Desktop for use by SiteConfig.

3811

Protocol: TCP. Used by Grass Valley AppService for 3rd party applications to communicate using AMP protocol. Used by SDB Server and GV STRATUS Rundown outgoing AMP communication to control playout channels. Used by Ignite for AMP, Video Server Control.

3838

Protocol: TCP. Used by GV STRATUS Ingest services.

3839

Protocol: TCP. Used by GV STRATUS Ingest services.

5001

Protocol: TCP. Used by Ignite for SDC/HDC Camera, Camera Preset Recall.

5050

Protocol: TCP. Used by Ignite for Tally Expander, Enables GPI/O Relays.

5164

Protocol: TCP. Used by SNFS for fsmpm, IOPS.

5189

Protocol: TCP. Used by SNFS for HA Manager. Symbol HAMGR_DEFAULT_PORT.

7144

Protocol: TCP. Traffic: HTTP. Used by GV STRATUS Router Config service for configuration.

7145

Protocol: TCP. Traffic: HTTP. Used by router config data service.

7213

Protocol: TCP. Used by GV STRATUS Router Controller service.

8000 - 8032

Protocol: TCP. Traffic: HTTP. Port 8000 used as follows: GV STRATUS Common Services, including preferences, licensing, authorization; Proxy config, Web Monitor data service; Ignite for Radamec SCP and Shotoku, IP to 422 Serial Communication (Camera Preset Recall). Ports 8000 to 8032 used by Ignite as follows: Digicart, IP to 422 Serial Communication; MDS-B5 and MDS-E11,

IP to 422 Serial Communication (Audio Deck Control); Chyron Aprisa SSX, Chyron Duet, Inscriber MOS, and Multi Deko, IP to 232 Serial Communication (CG Graphic Load and Playout); GV Cameraman, IP to 232 Serial Communication (Camera Preset Recall); Under Monitor Display, IP to 422 Serial Communication (Sends Clip +/- time to external device); CalrecMixer, IP to 422 or 232 Serial Communication (Audio Mixer Control); VCR (BVW), IP to 422 Serial Communication (Deck Control); VDCP, IP to 422 Serial Communication (Deck/Video Server Control). Ports 8000 - 8032 used by Comtrol Devicemaster RTS.

8080

Protocol: TCP. Traffic: HTTP. Used by GV STRATUS Summit Services. Used by WCF service provided by the GV STRATUS Workflow Engine. Used by WCF service provided by the GV STRATUS Rules Engine.

8081

NET.TCP: Used by WCF service provided by the GV STRATUS Workflow Engine. Used by WCF service provided by the GV STRATUS Rules Engine.

8100

HTTP/TCP: Used by Macintosh systems for the SabreTooth licensing web service to check out licenses

8190

Protocol: TCP. Traffic: HTTP. Used by WCF service provided by DeviceKey Service.

8511

Protocol: TCP. Traffic: HTTP. Used by playout config data service.

8594

Protocol: TCP. Used by Ignite for VizRT, CG Graphic Load and Playout.

8676

Protocol: WCF. Used by GV STRATUS servers hosting Xcode Control Engine to access the Vantage Server.

8732

Protocol: TCP. Traffic: HTTP. Used by Site Config data service .

8733

Protocol: TCP. Traffic: HTTP. Used by K2 Config data service .

8734

Protocol: TCP. Traffic: HTTP. Used by Site Config data service .

8735

Protocol: TCP. Traffic: HTTP. Used by K2 Config data service.

8736

Protocol: TCP. Used by GV STRATUS Control Panel Services for third-party storage configuration.

8737

Protocol: TCP. Traffic: HTTP. Used by GV STRATUS Ingest Config service for configuration. Used by GV STRATUS Control Panel Services for K2 Remote storage configuration. Used by GV STRATUS Core Server.

8740

Protocol: TCP. Traffic: HTTP. Used by general config data service.

8742

Protocol: TCP. Traffic: HTTP. Used by Send destination config data service.

8744

Protocol: TCP. Traffic: HTTP. Used by RMI config data service.

9010

TCP: Used by GV Ask service.

9012

TCP: Used by GV License Manager.

9016

TCP: Used by GV Resolver. Not visible on a configuration page.

9018

TCP: Used by GV RulesWizard. Not visible on a configuration page.

9019

TCP: Used by GV RulesWizard. Not visible on a configuration page.

9020

TCP: Used by GV Transfer Manager.

9024

TCP: Used by GV Subscription Manager.

9090

Protocol: TCP. Used by Ignite for Ross XPression, CG Graphic Load and Playout.

9110

TCP: Used by GV Proxy MDI.

9115

TCP: Used by GV NTFS MDI.

9120

TCP: Used by GV Common RESTful Archive MDI.

9121

TCP: Used by GV Common RESTful Archive MDI.

9122

TCP: Used by GV DIVA MDI.

9124

TCP: Used by GV FlashNet MDI.

9128

TCP: Used by GV FTP MDI in the Aurora workflow, which can use a range of ports, starting with this port number.

9129

TCP: Used by GV Masstech MDI.

9130

TCP: Used by GV Profile MDI. The service manages one host process for each managed Profile. These host processes require ports 9130-9139. Stopping/starting the service stops/starts all of the host processes.

9140

TCP: Used by GV MSeries MDI. The service manages one host process for each managed M-Series iVDR. These host processes require ports 9140 - 9149. Stopping/starting the service stops/starts all of the host processes.

9150

TCP: Used by GV News Share MDI.

9160

TCP: Used by GV K2 MDI and GV K2 Summit MDI Service. The service manages a number of host processes, one for each K2 system that is being managed. These host processes require ports 9160 - 9169. Stopping/starting the service stops/starts all of the host processes.

9170

TCP: Used by GV FTP MDI in the GV STRATUS workflow, which can use a range of ports, starting with this port number.

9230

TCP: Used by GV Aurora Proxy Encoder. Starting range for first control.

10260

Protocol: TCP. Used by Ignite for Pixel Power Clarity, CG Graphic Load and Playout.

10540

TCP: Used by XMOS Server incoming and outgoing MOS communication.

10541

TCP: Used by XMOS Server incoming and outgoing MOS communication.

10543

Protocol: TCP. Used by Ignite for Deko Mos, CG Graphic Load and Playout.

11239

Protocol: TCP. Used by Ignite for Vinten 200, Camera Preset Recall.

12000

Protocol: TCP. Used by Ignite for Miranda Vertigo, CG Graphic Load and Playout.

12345

Protocol: TCP. Used by Ingest Router Port. Used by Ignite for VCP Server (ESPN).

14500

Protocol: TCP. Used by SNFS for snpolicyd.

16210 - 16215

Protocol: TCP. Ports 16210 to 16215 used by GV STRATUS Send Message tool.

18262

TCP: Used by GV ProductFrame Configuration Service, ProductFrame Discovery Agent Service for use by SiteConfig. Used by GV NetConfig Service. gv-pf. UDP: Used by GV NetConfig Service. gv-pf.

18263

UDP: Used by ProductFrame Discovery Agent Service for GV NetConfig Device Broadcast/Unicast Protocol. Used by SiteConfig. Sent by ControlPoint, received by Devices

18264

UDP: Used by ProductFrame Discovery Agent Service for GV NetConfig Controller Protocol. Used by SiteConfig. Sent by Devices, received by ControlPoint

20566

Protocol: TCP. Used by SNFS for MySQL. Only used internally on an MDC.

31820

Protocol: UDP. Used for live streaming from K2 Summit/Solo systems. This is the default base for UDP ports, with the range being 31820 to 31827. Other ranges are possible, depending on the UDP port base configured on the K2 Summit/Solo system.

49152

Protocol: TCP. Used by Ignite for DeviceMgr.

49168

HTTP/TCP: Used by Grass Valley K2 Config for K2Config application connection between a control point PC and the K2 system device configured. Used for most functions.

49169

TCP: Used by Grass Valley K2 Config for K2Config application connection between a control point PC and the K2 system device configured. Used for a few functions that require longer time periods.

49170

HTTP: Used by Grass Valley Transfer Queue Service for Transfer Manager connection between source system and destination system.

49171

TCP: Used by Grass Valley AppService for AppCenter connection between control point PC and K2 client/Solo, and used by GV STRATUS application and services to connect to Grass Valley K2 AppService.

49172

HTTP: Used by Grass Valley Storage Utility Host for connection for Storage Utility between the control point PC and the K2 system being configured.

50872

UDP: Used by K2 Appcenter to discover K2 systems on the network.

52000

Protocol: TCP. Grass Valley recommends port range 52000 to 52100 for use by SNFS, configurable with fsports file. Other ranges are available. Contact Grass Valley Support.

60001

Protocol: TCP. Used by ACSLS Tape Libraries. Related to SNFS.

60002

Protocol: TCP. Used by ACSLS Tape Libraries. Related to SNFS.

62051

Protocol: TCP. Used by Ignite for IQLayer, Internal Port used by Ignite.

62052

Protocol: TCP. Used by Ignite for IQLayer, Internal Port used by Ignite.

Glossary

Advanced Logging
The tool that creates and customizes logging of assets.

Advanced Search
The functionality provided by the Advanced Search tool, which includes the ability to search by multiple criteria.

Application Window
An application's main surrounding window, in which the application's panels are docked.

Asset
A physical or logical entity defined and managed by the Grass Valley system.

Asset List
The panel that displays the list for the item currently selected in the Navigator panel or the search results.

Asset type icon
An icon that indicates the type of asset.

Assignment List
The tool that creates placeholders for clips and coordinates with rundown stories on the Newsroom Computer System and with GV STRATUS Rundown.

Authorization Manager
Settings in the GV STRATUS Control Panel that assign licenses and permissions to users and groups.

Bin
On a K2 system, a folder that contains media.

Button Panel
The panel that creates and assigns logging buttons.

Channel Panel
The tool that includes channels and channel gangs for controlling one or more K2 channels.

Channel Panel configuration
The settings that you configure to create a Channel Panel. When the Channel Panels node is selected under the Tools item in the Navigator, the settings appear as an item in the Asset List.

Clip
A single media asset with video and/or audio, timecode, and associated metadata.

Composite panel
A panel that contains one or more panels.

Control Point PC
A network connected PC that is an optional component of the Grass Valley system. It serves as the central configuration location for the Grass Valley system. It runs applications such as the GV STRATUS Control Panel application, the SiteConfig application, the K2Config application, and an SNMP manager application.

Control Tray
The toolbar that opens on the bottom of a GV STRATUS component that displays video. The Control Tray contains buttons for transport control, markup, and other functions.

Copy
A complete copy of an asset.

Crash Record
Start a recording without specifying a clip name.

Dashboard
The tool that displays a dynamic system overview of the activity on the GV STRATUS system, such as channel usage and storage capacity.

Details view
The list view format that displays each asset as a multi-column row.

Drop target
The graphic that appears when hovering an undocked panel over another panel or over the application window. The graphic indicates the area in which the panel is docked if the panel is dropped on the graphic.

Event (Playlist)
A clip, trigger, or other entity that is one of the items in a playlist.

Event (Scheduler)
An item that marks the time that a recording or other action is scheduled to occur.

Feed Ingest
Operations performed by the Scheduler tool where K2 system channels are configured to record clips.

Focus
The state of a user interface component in which the component is currently receiving the input from the keyboard or mouse.

Folder
A physical or logical container. It can be a physical directory on a computer's file system or a database record managed by a Grass Valley system database.

FT server
The fault tolerant server that provides a platform for Grass Valley system devices, such as the GV STRATUS Core server.

Gang
Two or more channels that can be controlled as a single unit. A channel in a gang is referred to as a ganged channel. A channel that is not in a gang is referred to as a single channel.

Grass Valley system
The applications with their database(s) and supporting infrastructure that manage assets for one or more Grass Valley products.

House Number
The panel that populates the house number list and links assets to house numbers from the traffic system.

Ingest Database
The database for the Scheduler tool.

Inspector
The panel that displays details of the asset currently loaded.

K2Config
Grass Valley's application for configuring the K2 Storage Area Network (SAN).

K2 Media Server
The K2 Media Server product, which is a K2 SAN device. It can have the role of file system manager and other roles.

K2 Nearline SAN
A large pool of offline K2 storage to which files can be saved. Suitable for media file transfer. Does not support record or play.

K2 SAN
The K2 Storage Area Network, including K2 Media Server, K2 RAID, and K2 SAN-attached systems. This term applies to an online or production SAN except if it is specified as a nearline SAN.

K2 Solo system
The K2 Solo Media Server product.

K2 Summit SAN-attached system
A K2 Summit system with media storage on a K2 SAN. Applies to K2 Summit (3G) Production Client and K2 Summit Transmission Client products.

K2 Summit standalone system
A K2 Summit system with internal or direct-connect media storage. Applies to K2 Summit (3G) Production Client and K2 Summit Transmission Server products.

K2 Summit system
A K2 Summit system of any storage type, including standalone internal/direct-connect or SAN-attached shared media storage. Applies to K2 Summit (3G) Production Client and K2 Summit Transmission Server/Client products.

K2 system
K2 product family servers, clients, and SANs, either individually or combined as a system. This includes K2 Media Clients, K2 Summit (3G) Production Clients, K2 Summit Transmission Servers/Clients and K2 Solo Media Servers with standalone, direct-connect, or SAN storage, as appropriate for the product.

Keyword
A section of a clip that has duration, as defined by an in point and an out point, with its associated metadata.

Launch

Opening a tool or other component to expose the controls and functionality that you can use to accomplish a task.

Lease

A license that is checked out to a particular user. For the period of time that the license is checked out to that user, the user has a lease on that license.

License Management Database

The database for the assignment of GV STRATUS licenses and roles to groups and users

Marker Panel

The panel that displays keywords and markers of assets.

Marker

A specific point in a clip, as defined by timecode, with its associated metadata.

MDI

MDI is the acronym for Managed Device Interface. An MDI is a software component that provides an interface for the GV STRATUS database to access a device. Typically these are devices on which media resides, such as K2 systems, NAS devices, and archive devices. Each type of device has its own MDI. For most MDIs, the MDI software component is hosted on the GV STRATUS Core server, rather than being hosted on the same machine that it accesses.

Media ID

Metadata assigned to a disk or directory that contains a group of clips that can be imported via RMI.

MEWS Server

A customer-supplied server dedicated to MEWS functionality. It hosts MewsService, which is a Grass Valley service.

Navigator

The panel that contains the tree-view.

Panel

A UI component that can be undocked and docked in an application window.

Permissions

Access to files or directories that can be assigned to user groups.

Playback

Playing an asset, such as a clip or playlist.

Playlist

An asset type consisting of a series of events. A playlist contains only events, transitions, and other features supported on the K2 system channel.

Playlist Editor

The tool that creates and modifies playlists. This tool uses a K2 channel.

Proxy server

The GV STRATUS server on an online or production K2 SAN that provides access to the low-resolution proxy media stored on the SAN. The server has the role of Proxy K2 SAN Server and SNFS file system client.

Proxy Storage

A K2 Nearline SAN that stores low-resolution proxy media for a GV STRATUS system. A GV STRATUS Core Services server takes the role of file system server for the Proxy Storage.

Proxy Storage file system server

The GV STRATUS server on a dedicated Proxy Storage system that provides access to the low-resolution proxy media stored on the system. The server has the roles of Proxy Storage Server and SNFS file system server for the Proxy Storage system.

Render Engine

A GV STRATUS server that functions as a proxy encoder and as a conform server. As a proxy encoder, the server creates low-resolution proxy assets. If a high-resolution asset does not yet have associated proxy, the server creates it. The software that provides the proxy encoder functionality can run on a dedicated Render Engine server or on a GV STRATUS server that has other roles as well, such as a GV STRATUS Express server. As a conform server, the server hosts the Render Engine Service. The service renders a complex asset, such as a GV STRATUS sequence or a project created in EDIUS, into a simple clip.

RMI

RMI is the acronym for Removable Media Interface. It is the tool that populates and ingests files from multiple removable media devices such as P2 and XDCAM. The RMI tool requires a GV STRATUS client with access to high-resolution assets.

Role

Functionality that can be assigned. In the SiteConfig application, it is software functionality assigned to a device. In the GV STRATUS application, it is licensed functionality assigned to a user or group.

Rules Engine Database

The database for the Rules Engine. Stores the rules and the current state of the active rules. This is a SQL database. The database name is RulesEngine.

Salvo

A pre-defined and re-usable set of clips to load into a specific channel.

Scheduler

The tool that schedules events to be recorded.

Scrub bar

The control that allows you to navigate through a clip using your mouse. The scrub bar slider provides click and drag mouse operations.

SDB

SDB is the acronym for Simple Database, which is the database server component for GV STRATUS Rundown. It provides status on clips and on playlists associated with NCS rundowns.

Section
A panel's subdivision, such as the Explore section of the Navigator panel.

Segmentation Tool
The tool that creates segments from assets.

Segment Template
A collection of metadata properties, as configured in the GV STRATUS Inspector panel, that can be associated with a segment as part of the Digital Media Platform workflow.

Send Message
The tool that sends and receives messages and attachments between users logged on to GV STRATUS applications.

Sequence
An asset consisting of a series of events for EDL exchange with an editor or creating finished stories for playout.

Sequence Viewer
The tool that plays sequences and playlists.

Shortcut
The representation of an asset that operates as a copy of the asset but is actually a reference that points to the original asset.

Show/Hide button
The button that shows or hides an interface component. For example, the Show/Hide button that shows or hides transport controls in a Channel Panel.

Show/Hide tab
The tab that indicates the position of a hidden panel. When the tab is clicked, the panel slides open (shows).

Simple Search
The functionality provided by the Simple Search tool, which is the ability to search by a single search term.

SiteConfig
Grass Valley's application for network configuration and software deployment.

Source Viewer
The tool that plays assets and provides controls for adding markers, keywords, and other features.

Storyboard Editor
The tool that creates and modifies sequences. This tool does not use a K2 channel.

GV STRATUS
Grass Valley's media workflow application framework. Applications include the GV STRATUS application and the GV STRATUS Control Panel.

GV STRATUS Common server

A GV STRATUS server with common roles, excluding the role of Core Server and Proxy Server. This server provides licensing and user preference functionality on typical GV STRATUS systems where there are multiple GV STRATUS servers.

GV STRATUS Control Panel

The GV STRATUS application that provides central configuration of the software components of the GV STRATUS system.

GV STRATUS Core server

A GV STRATUS server that has the role of Core Services on a system with multiple GV STRATUS servers. The server provides media management functionality, including the GV STRATUS database and associated software components.

GV STRATUS Core Services

The software components that provide the underlying functionality to GV STRATUS applications. The components run as services on one or more GV STRATUS Core Services servers.

GV STRATUS Database

The database that provides the core asset management functionality to the GV STRATUS system.

GV STRATUS Express server

A GV STRATUS server with all the roles necessary for a basic GV STRATUS system, including the role of Proxy Express Server. The server has larger drives than other GV STRATUS servers to accommodate the low-resolution proxy media that is stored on the local server. This server is designed for use on smaller GV STRATUS systems where no other GV STRATUS servers or proxy systems are present.

Subclip

A clip created by referencing a portion of media from a parent clip. The subclip does not contain any actual media. Rather, it points to the media in the parent clip.

Tag

A metadata entry that has no timecode information. In the GV STRATUS application this applies to an entire asset rather than to a particular point or section in an asset.

Take control

To take control of a K2 system channel that is currently being controlled by another. This can occur when two people are using the application on different PCs and one person opens or adds a channel that is in use by the other person.

Tally indicator

The colored bar or rectangle that indicates the current status (recording, playing, etc) of a channel gang or an individual channel.

Thumbnails view

The list view format that displays each asset as a small rectangular image.

Tiles view

The list view format that displays each asset as a small rectangular image with asset property information to the right.

Transition

The place between two events in a playlist or sequence. A cut and an effect are examples of a transition.

View Mode

The visual representation of a list of items. Modes include detail, tile, and thumbnail views.

Web Monitor

The tool that displays a web page.

WfPersistence Database

The database for the runtime data of the workflow engine. Stores the current state of running workpackages. This is a SQL database. The database name is WfPersistence.

Workflow Database

The database for the workflow engine. Stores the workflow templates. This is a SQL database. The database name is MediaFlow.

Workflow Server

A GV STRATUS server dedicated to hosting the Workflow Engine Service, the Rules Engine Service, and the Xcode Control Engine Service. These services support rules-based operations.

Working Bin

The bin on a K2 system into which one or more channels record.

Workspace

The layout of docked and undocked panels that are part of an application.

Xcode Control Engine

The service that controls a third-party transcode application to support rules-based transcode operations.

Grass Valley Knowledge Base

Visit the Grass Valley Knowledge Base site for technical articles and FAQs (Frequently Asked Questions) about Grass Valley systems and products.

Grass Valley Knowledge Base

Safety Summary

Safety Summary

Read and follow the important safety information below, noting especially those instructions related to risk of fire, electric shock or injury to persons. Additional specific warnings not listed here may be found throughout the manual.

⚠	***WARNING: Any instructions in this manual that require opening the equipment cover or enclosure are for use by qualified service personnel only. To reduce the risk of electric shock, do not perform any servicing other than that contained in the operating instructions unless you are qualified to do so.***

Safety terms and symbols

Terms in this manual

Safety-related statements may appear in this manual in the following form:

⚠	***WARNING: Warning statements identify conditions or practices that may result in personal injury or loss of life.***
⚠	***CAUTION: Caution statements identify conditions or practices that may result in damage to equipment or other property, or which may cause equipment crucial to your business environment to become temporarily non-operational.***

Terms on the product

These terms may appear on the product:

DANGER — A personal injury hazard is immediately accessible as you read the marking.

WARNING — A personal injury hazard exists but is not immediately accessible as you read the marking.

CAUTION — A hazard to property, product, and other equipment is present.

Symbols on the product

The following symbols may appear on the product:

⚠	Indicates that dangerous high voltage is present within the equipment enclosure that may be of sufficient magnitude to constitute a risk of electric shock.
⚠	Indicates that user, operator or service technician should refer to product manual(s) for important operating, maintenance, or service instructions.
⚠	This is a prompt to note fuse rating when replacing fuse(s). The fuse referenced in the text must be replaced with one having the ratings indicated.
⏚	Identifies a protective grounding terminal which must be connected to earth ground prior to making any other equipment connections.

⏚	Identifies an external protective grounding terminal which may be connected to earth ground as a supplement to an internal grounding terminal.
	Indicates that static sensitive components are present which may be damaged by electrostatic discharge. Use anti-static procedures, equipment and surfaces during servicing.

Warnings

The following warning statements identify conditions or practices that can result in personal injury or loss of life.

Dangerous voltage or current may be present — Disconnect power and remove battery (if applicable) before removing protective panels, soldering, or replacing components.

Do not service alone — Do not internally service this product unless another person capable of rendering first aid and resuscitation is present.

Remove jewelry — Prior to servicing, remove jewelry such as rings, watches, and other metallic objects.

Avoid exposed circuitry — Do not touch exposed connections, components or circuitry when power is present.

Use proper power cord — Use only the power cord supplied or specified for this product.

Ground product — Connect the grounding conductor of the power cord to earth ground.

Operate only with covers and enclosure panels in place — Do not operate this product when covers or enclosure panels are removed.

Use correct fuse — Use only the fuse type and rating specified for this product.

Use only in dry environment — Do not operate in wet or damp conditions.

Use only in non-explosive environment — Do not operate this product in an explosive atmosphere.

High leakage current may be present — Earth connection of product is essential before connecting power.

Dual power supplies may be present — Be certain to plug each power supply cord into a separate branch circuit employing a separate service ground. Disconnect both power supply cords prior to servicing.

Double pole neutral fusing — Disconnect mains power prior to servicing.

Use proper lift points — Do not use door latches to lift or move equipment.

Avoid mechanical hazards — Allow all rotating devices to come to a stop before servicing.

Cautions

The following caution statements identify conditions or practices that can result in damage to equipment or other property

Use correct power source — Do not operate this product from a power source that applies more than the voltage specified for the product.

Use correct voltage setting — If this product lacks auto-ranging power supplies, before applying power ensure that the each power supply is set to match the power source.

Provide proper ventilation — To prevent product overheating, provide equipment ventilation in accordance with installation instructions.

Use anti-static procedures — Static sensitive components are present which may be damaged by electrostatic discharge. Use anti-static procedures, equipment and surfaces during servicing.

Do not operate with suspected equipment failure — If you suspect product damage or equipment failure, have the equipment inspected by qualified service personnel.

Ensure mains disconnect — If mains switch is not provided, the power cord(s) of this equipment provide the means of disconnection. The socket outlet must be installed near the equipment and must be easily accessible. Verify that all mains power is disconnected before installing or removing power supplies and/or options.

Route cable properly — Route power cords and other cables so that they ar not likely to be damaged. Properly support heavy cable bundles to avoid connector damage.

Use correct power supply cords — Power cords for this equipment, if provided, meet all North American electrical codes. Operation of this equipment at voltages exceeding 130 VAC requires power supply cords which comply with NEMA configurations. International power cords, if provided, have the approval of the country of use.

Use correct replacement battery — This product may contain batteries. To reduce the risk of explosion, check polarity and replace only with the same or equivalent type recommended by manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Troubleshoot only to board level — Circuit boards in this product are densely populated with surface mount technology (SMT) components and application specific integrated circuits (ASICS). As a result, circuit board repair at the component level is very difficult in the field, if not impossible. For warranty compliance, do not troubleshoot systems beyond the board level.

Sicherheit – Überblick

Lesen und befolgen Sie die wichtigen Sicherheitsinformationen dieses Abschnitts. Beachten Sie insbesondere die Anweisungen bezüglich

Brand-, Stromschlag- und Verletzungsgefahren. Weitere spezifische, hier nicht aufgeführte Warnungen finden Sie im gesamten Handbuch.

⚠ ***WARNUNG: Alle Anweisungen in diesem Handbuch, die das Abnehmen der Geräteabdeckung oder des Gerätegehäuses erfordern, dürfen nur von qualifiziertem Servicepersonal ausgeführt werden. Um die Stromschlaggefahr zu verringern, führen Sie keine Wartungsarbeiten außer den in den Bedienungsanleitungen genannten Arbeiten aus, es sei denn, Sie besitzen die entsprechende Qualifikationen für diese Arbeiten.***

Sicherheit – Begriffe und Symbole

In diesem Handbuch verwendete Begriffe

Sicherheitsrelevante Hinweise können in diesem Handbuch in der folgenden Form auftauchen:

⚠ ***WARNUNG: Warnungen weisen auf Situationen oder Vorgehensweisen hin, die Verletzungs- oder Lebensgefahr bergen.***

⚠	***VORSICHT: Vorsichtshinweise weisen auf Situationen oder Vorgehensweisen hin, die zu Schäden an Ausrüstungskomponenten oder anderen Gegenständen oder zum zeitweisen Ausfall wichtiger Komponenten in der Arbeitsumgebung führen können.***

Hinweise am Produkt

Die folgenden Hinweise können sich am Produkt befinden:

GEFAHR – Wenn Sie diesen Begriff lesen, besteht ein unmittelbares Verletzungsrisiko.

WARNUNG – Wenn Sie diesen Begriff lesen, besteht ein mittelbares Verletzungsrisiko.

VORSICHT – Es besteht ein Risiko für Objekte in der Umgebung, den Mixer selbst oder andere Ausrüstungskomponenten.

Symbole am Produkt

Die folgenden Symbole können sich am Produkt befinden:

⚠	Weist auf eine gefährliche Hochspannung im Gerätegehäuse hin, die stark genug sein kann, um eine Stromschlaggefahr darzustellen.
⚠	Weist darauf hin, dass der Benutzer, Bediener oder Servicetechniker wichtige Bedienungs-, Wartungs- oder Serviceanweisungen in den Produkthandbüchern lesen sollte.
⚠	Dies ist eine Aufforderung, beim Wechsel von Sicherungen auf deren Nennwert zu achten. Die im Text angegebene Sicherung muss durch eine Sicherung ersetzt werden, die die angegebenen Nennwerte besitzt.
⏚	Weist auf eine Schutzerdungsklemme hin, die mit dem Erdungskontakt verbunden werden muss, bevor weitere Ausrüstungskomponenten angeschlossen werden.
⏚	Weist auf eine externe Schutzerdungsklemme hin, die als Ergänzung zu einem internen Erdungskontakt an die Erde angeschlossen werden kann.
⚡	Weist darauf hin, dass es statisch empfindliche Komponenten gibt, die durch eine elektrostatische Entladung beschädigt werden können. Verwenden Sie antistatische Prozeduren, Ausrüstung und Oberflächen während der Wartung.

Warnungen

Die folgenden Warnungen weisen auf Bedingungen oder Vorgehensweisen hin, die Verletzungs- oder Lebensgefahr bergen:

Gefährliche Spannungen oder Ströme – Schalten Sie den Strom ab, und entfernen Sie ggf. die Batterie, bevor sie Schutzabdeckungen abnehmen, löten oder Komponenten austauschen.

Servicearbeiten nicht alleine ausführen – Führen Sie interne Servicearbeiten nur aus, wenn eine weitere Person anwesend ist, die erste Hilfe leisten und Wiederbelebungsmaßnahmen einleiten kann.

Schmuck abnehmen – Legen Sie vor Servicearbeiten Schmuck wie Ringe, Uhren und andere metallische Objekte ab.

Keine offen liegenden Leiter berühren – Berühren Sie bei eingeschalteter Stromzufuhr keine offen liegenden Leitungen, Komponenten oder Schaltungen.

Richtiges Netzkabel verwenden – Verwenden Sie nur das mitgelieferte Netzkabel oder ein Netzkabel, das den Spezifikationen für dieses Produkt entspricht.

Gerät erden – Schließen Sie den Erdleiter des Netzkabels an den Erdungskontakt an.

Gerät nur mit angebrachten Abdeckungen und Gehäuseseiten betreiben – Schalten Sie dieses Gerät nicht ein, wenn die Abdeckungen oder Gehäuseseiten entfernt wurden.

Richtige Sicherung verwenden – Verwenden Sie nur Sicherungen, deren Typ und Nennwert den Spezifikationen für dieses Produkt entsprechen.

Gerät nur in trockener Umgebung verwenden – Betreiben Sie das Gerät nicht in nassen oder feuchten Umgebungen.

Gerät nur verwenden, wenn keine Explosionsgefahr besteht – Verwenden Sie dieses Produkt nur in Umgebungen, in denen keinerlei Explosionsgefahr besteht.

Hohe Kriechströme – Das Gerät muss vor dem Einschalten unbedingt geerdet werden.

Doppelte Spannungsversorgung kann vorhanden sein – Schließen Sie die beiden Anschlußkabel an getrennte Stromkreise an. Vor Servicearbeiten sind beide Anschlußkabel vom Netz zu trennen.

Zweipolige, neutrale Sicherung – Schalten Sie den Netzstrom ab, bevor Sie mit den Servicearbeiten beginnen.

Fassen Sie das Gerät beim Transport richtig an – Halten Sie das Gerät beim Transport nicht an Türen oder anderen beweglichen Teilen fest.

Gefahr durch mechanische Teile – Warten Sie, bis der Lüfter vollständig zum Halt gekommen ist, bevor Sie mit den Servicearbeiten beginnen.

Vorsicht

Die folgenden Vorsichtshinweise weisen auf Bedingungen oder Vorgehensweisen hin, die zu Schäden an Ausrüstungskomponenten oder anderen Gegenständen führen können:

Gerät nicht öffnen – Durch das unbefugte Öffnen wird die Garantie ungültig.

Richtige Spannungsquelle verwenden – Betreiben Sie das Gerät nicht an einer Spannungsquelle, die eine höhere Spannung liefert als in den Spezifikationen für dieses Produkt angegeben.

Gerät ausreichend belüften – Um eine Überhitzung des Geräts zu vermeiden, müssen die Ausrüstungskomponenten entsprechend den Installationsanweisungen belüftet werden. Legen Sie kein Papier unter das Gerät. Es könnte die Belüftung behindern. Platzieren Sie das Gerät auf einer ebenen Oberfläche.

Antistatische Vorkehrungen treffen – Es gibt statisch empfindliche Komponenten, die durch eine elektrostatische Entladung beschädigt werden können. Verwenden Sie antistatische Prozeduren, Ausrüstung und Oberflächen während der Wartung.

CF-Karte nicht mit einem PC verwenden – Die CF-Karte ist speziell formatiert. Die auf der CF-Karte gespeicherte Software könnte gelöscht werden.

Gerät nicht bei eventuellem Ausrüstungsfehler betreiben – Wenn Sie einen Produktschaden oder Ausrüstungsfehler vermuten, lassen Sie die Komponente von einem qualifizierten Servicetechniker untersuchen.

Kabel richtig verlegen – Verlegen Sie Netzkabel und andere Kabel so, dass Sie nicht beschädigt werden. Stützen Sie schwere Kabelbündel ordnungsgemäß ab, damit die Anschlüsse nicht beschädigt werden.

Richtige Netzkabel verwenden – Wenn Netzkabel mitgeliefert wurden, erfüllen diese alle nationalen elektrischen Normen. Der Betrieb dieses Geräts mit Spannungen über 130 V AC erfordert Netzkabel, die NEMA-Konfigurationen entsprechen. Wenn internationale Netzkabel mitgeliefert wurden, sind diese für das Verwendungsland zugelassen.

Richtige Ersatzbatterie verwenden – Dieses Gerät enthält eine Batterie. Um die Explosionsgefahr zu verringern, prüfen Sie die Polarität und tauschen die Batterie nur gegen eine Batterie desselben Typs oder eines gleichwertigen, vom Hersteller empfohlenen Typs aus. Entsorgen Sie gebrauchte Batterien entsprechend den Anweisungen des Batterieherstellers.

Das Gerät enthält keine Teile, die vom Benutzer gewartet werden können. Wenden Sie sich bei Problemen bitte an den nächsten Händler.

Consignes de sécurité

Il est recommandé de lire, de bien comprendre et surtout de respecter les informations relatives à la sécurité qui sont exposées ci-après, notamment les consignes destinées à prévenir les risques d'incendie, les décharges électriques et les blessures aux personnes. Les avertissements complémentaires, qui ne sont pas nécessairement repris ci-dessous, mais présents dans toutes les sections du manuel, sont également à prendre en considération.

⚠ ***AVERTISSEMENT: Toutes les instructions présentes dans ce manuel qui concernent l'ouverture des capots ou des logements de cet équipement sont destinées exclusivement à des membres qualifiés du personnel de maintenance. Afin de diminuer les risques de décharges électriques, ne procédez à aucune intervention d'entretien autre que celles contenues dans le manuel de l'utilisateur, à moins que vous ne soyez habilité pour le faire.***

Consignes et symboles de sécurité

Termes utilisés dans ce manuel

Les consignes de sécurité présentées dans ce manuel peuvent apparaître sous les formes suivantes :

⚠ ***AVERTISSEMENT: Les avertissements signalent des conditions ou des pratiques susceptibles d'occasionner des blessures graves, voire même fatales.***

⚠ ***MISE EN GARDE: Les mises en garde signalent des conditions ou des pratiques susceptibles d'occasionner un endommagement à l'équipement ou aux installations, ou de rendre l'équipement temporairement non opérationnel, ce qui peut porter préjudice à vos activités.***

Signalétique apposée sur le produit

La signalétique suivante peut être apposée sur le produit :

DANGER — risque de danger imminent pour l'utilisateur.

AVERTISSEMENT — Risque de danger non imminent pour l'utilisateur.

MISE EN GARDE — Risque d'endommagement du produit, des installations ou des autres équipements.

Symboles apposés sur le produit

Les symboles suivants peut être apposés sur le produit :

	Signale la présence d'une tension élevée et dangereuse dans le boîtier de l'équipement ; cette tension peut être suffisante pour constituer un risque de décharge électrique.
	Signale que l'utilisateur, l'opérateur ou le technicien de maintenance doit faire référence au(x) manuel(s) pour prendre connaissance des instructions d'utilisation, de maintenance ou d'entretien.
	Il s'agit d'une invite à prendre note du calibre du fusible lors du remplacement de ce dernier. Le fusible auquel il est fait référence dans le texte doit être remplacé par un fusible du même calibre.
	Identifie une borne de protection de mise à la masse qui doit être raccordée correctement avant de procéder au raccordement des autres équipements.
	I dentifie une borne de protection de mise à la masse qui peut être connectée en tant que borne de mise à la masse supplémentaire.
	Signale la présence de composants sensibles à l'électricité statique et qui sont susceptibles d'être endommagés par une décharge électrostatique. Utilisez des procédures, des équipements et des surfaces antistatiques durant les interventions d'entretien.

Avertissements

Les avertissements suivants signalent des conditions ou des pratiques susceptibles d'occasionner des blessures graves, voire même fatales :

Présence possible de tensions ou de courants dangereux — Mettez hors tension, débranchez et retirez la pile (le cas échéant) avant de déposer les couvercles de protection, de défaire une soudure ou de remplacer des composants.

Ne procédez pas seul à une intervention d'entretien — Ne réalisez pas une intervention d'entretien interne sur ce produit si une personne n'est pas présente pour fournir les premiers soins en cas d'accident.

Retirez tous vos bijoux — Avant de procéder à une intervention d'entretien, retirez tous vos bijoux, notamment les bagues, la montre ou tout autre objet métallique.

Évitez tout contact avec les circuits exposés — Évitez tout contact avec les connexions, les composants ou les circuits exposés s'ils sont sous tension.

Utilisez le cordon d'alimentation approprié — Utilisez exclusivement le cordon d'alimentation fourni avec ce produit ou spécifié pour ce produit.

Raccordez le produit à la masse — Raccordez le conducteur de masse du cordon d'alimentation à la borne de masse de la prise secteur.

Utilisez le produit lorsque les couvercles et les capots sont en place — N'utilisez pas ce produit si les couvercles et les capots sont déposés.

Utilisez le bon fusible — Utilisez exclusivement un fusible du type et du calibre spécifiés pour ce produit.

Utilisez ce produit exclusivement dans un environnement sec — N'utilisez pas ce produit dans un environnement humide.

Utilisez ce produit exclusivement dans un environnement non explosible — N'utilisez pas ce produit dans un environnement dont l'atmosphère est explosible.

Présence possible de courants de fuite — Un raccordement à la masse est indispensable avant la mise sous tension.

Deux alimentations peuvent être présentes dans l'équipement — Assurez vous que chaque cordon d'alimentation est raccordé à des circuits de terre séparés. Débranchez les deux cordons d'alimentation avant toute intervention.

Fusion neutre bipolaire — Débranchez l'alimentation principale avant de procéder à une intervention d'entretien.

Utilisez les points de levage appropriés — Ne pas utiliser les verrous de la porte pour lever ou déplacer l'équipement.

Évitez les dangers mécaniques — Laissez le ventilateur s'arrêter avant de procéder à une intervention d'entretien.

Mises en garde

Les mises en garde suivantes signalent les conditions et les pratiques susceptibles d'occasionner des endommagements à l'équipement et aux installations :

N'ouvrez pas l'appareil — Toute ouverture prohibée de l'appareil aura pour effet d'annuler la garantie.

Utilisez la source d'alimentation adéquate — Ne branchez pas ce produit à une source d'alimentation qui utilise une tension supérieure à la tension nominale spécifiée pour ce produit.

Assurez une ventilation adéquate — Pour éviter toute surchauffe du produit, assurez une ventilation de l'équipement conformément aux instructions d'installation. Ne déposez aucun document sous l'appareil – ils peuvent gêner la ventilation. Placez l'appareil sur une surface plane.

Utilisez des procédures antistatiques - Les composants sensibles à l'électricité statique présents dans l'équipement sont susceptibles d'être endommagés par une décharge électrostatique. Utilisez des procédures, des équipements et des surfaces antistatiques durant les interventions d'entretien.

N'utilisez pas la carte CF avec un PC — La carte CF a été spécialement formatée. Le logiciel enregistré sur la carte CF risque d'être effacé.

N'utilisez pas l'équipement si un dysfonctionnement est suspecté — Si vous suspectez un dysfonctionnement du produit, faites inspecter celui-ci par un membre qualifié du personnel d'entretien.

Acheminez les câbles correctement — Acheminez les câbles d'alimentation et les autres câbles de manière à ce qu'ils ne risquent pas d'être endommagés. Supportez correctement les enroulements de câbles afin de ne pas endommager les connecteurs.

Utilisez les cordons d'alimentation adéquats — Les cordons d'alimentation de cet équipement, s'ils sont fournis, satisfont aux exigences de toutes les réglementations régionales. L'utilisation de cet équipement à des tensions dépassant les 130 V en c.a. requiert des cordons d'alimentation qui satisfont aux exigences des configurations NEMA. Les cordons internationaux, s'ils sont fournis, ont reçu l'approbation du pays dans lequel l'équipement est utilisé.

Utilisez une pile de remplacement adéquate — Ce produit renferme une pile. Pour réduire le risque d'explosion, vérifiez la polarité et ne remplacez la pile que par une pile du même type, recommandée par le fabricant. Mettez les piles usagées au rebut conformément aux instructions du fabricant des piles.

Cette unité ne contient aucune partie qui peut faire l'objet d'un entretien par l'utilisateur. Si un problème survient, veuillez contacter votre distributeur local.

Certifications and compliances

Canadian certified power cords

Canadian approval includes the products and power cords appropriate for use in the North America power network. All other power cords supplied are approved for the country of use.

FCC emission control

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense. Changes or modifications not expressly approved by Grass Valley can affect emission compliance and could void the user's authority to operate this equipment.

Canadian EMC Notice of Compliance

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A préscrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

EN55103 1/2 Class A warning

This product has been evaluated for Electromagnetic Compatibility under the EN 55103-1/2 standards for Emissions and Immunity and meets the requirements for E4 environment.

This product complies with Class A (E4 environment). In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

FCC emission limits

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesirable operation.

Laser compliance

Laser safety requirements

This product may contain a Class 1 certified laser device. Operating this product outside specifications or altering its original design may result in hazardous radiation exposure, and may be considered

an act of modifying or new manufacturing of a laser product under U.S. regulations contained in 21CFR Chapter 1, subchapter J or CENELEC regulations in HD 482 S1. People performing such an act are required by law to recertify and reidentify this product in accordance with provisions of 21CFR subchapter J for distribution within the U.S.A., and in accordance with CENELEC HD 482 S1 for distribution within countries using the IEC 825 standard.

Laser safety

Laser safety in the United States is regulated by the Center for Devices and Radiological Health (CDRH). The laser safety regulations are published in the "Laser Product Performance Standard," Code of Federal Regulation (CFR), Title 21, Subchapter J.

The International Electrotechnical Commission (IEC) Standard 825, "Radiation of Laser Products, Equipment Classification, Requirements and User's Guide," governs laser products outside the United States. Europe and member nations of the European Free Trade Association fall under the jurisdiction of the Comité Européen de Normalization Electrotechnique (CENELEC).

Safety certification

This product has been evaluated and meets the following Safety Certification Standards:

Standard	Designed/tested for compliance with:
ANSI/UL 60950-1	Safety of Information Technology Equipment, including Electrical Business Equipment (Second edition 2007).
IEC 60950-1 with CB cert.	Safety of Information Technology Equipment, including Electrical Business Equipment (Second edition, 2005).
CAN/CSA C22.2 No. 60950-1	Safety of Information Technology Equipment, including Electrical Business Equipment (Second edition 2007).
BS EN 60950-1	Safety of Information Technology Equipment, including Electrical Business Equipment 2006.

ESD Protection

Electronics today are more susceptible to electrostatic discharge (ESD) damage than older equipment. Damage to equipment can occur by ESD fields that are smaller than you can feel. Implementing the information in this section will help you protect the investment that you have made in purchasing Grass Valley equipment. This section contains Grass Valley's recommended ESD guidelines that should be followed when handling electrostatic discharge sensitive (ESDS) items. These minimal recommendations are based on the information in the *Sources of ESD and Risks* on page 1763 area. The information in *Grounding Requirements for Personnel* on page 1763 is provided to assist you in selecting an appropriate grounding method.

Recommended ESD Guidelines

Follow these guidelines when handling Grass Valley equipment:

- Only trained personnel that are connected to a grounding system should handle ESDS items.

- Do not open any protective bag, box, or special shipping packaging until you have been grounded.

  NOTE: When a Personal Grounding strap is unavailable, as an absolute minimum, touch a metal object that is touching the floor (for example, a table, frame, or rack) to discharge any static energy before touching an ESDS item.
- Open the anti-static packaging by slitting any existing adhesive tapes. Do not tear the tapes off.
- Remove the ESDS item by holding it by its edges or by a metal panel.
- Do not touch the components of an ESDS item unless it is absolutely necessary to configure or repair the item.
- Keep the ESDS work area clear of all nonessential items such as coffee cups, pens, wrappers and personal items as these items can discharge static. If you need to set an ESDS item down, place it on an anti-static mat or on the anti-static packaging.

Sources of ESD and Risks

The following information identifies possible sources of electrostatic discharge and can be used to help establish an ESD policy.

Personnel

One of the largest sources of static is personnel. The static can be released from a person's clothing and shoes.

Environment

The environment includes the humidity and floors in a work area. The humidity level must be controlled and should not be allowed to fluctuate over a broad range. Relative humidity (RH) is a major part in determining the level of static that is being generated. For example, at 10% - 20% RH a person walking across a carpeted floor can develop 35kV; yet when the relative humidity is increased to 70% - 80%, the person can only generate 1.5kV.

Static is generated as personnel move (or as equipment is moved) across a floor's surface. Carpeted and waxed vinyl floors contribute to static build up.

Work Surfaces

Painted or vinyl-covered tables, chairs, conveyor belts, racks, carts, anodized surfaces, plexiglass covers, and shelving are all static generators.

Equipment

Any equipment commonly found in an ESD work area, such as solder guns, heat guns, blowers, etc., should be grounded.

Materials

Plastic work holders, foam, plastic tote boxes, pens, packaging containers and other items commonly found at workstations can generate static electricity.

Grounding Requirements for Personnel

The information in this section is provided to assist you in selecting a grounding method. This information is taken from ANSI/ESD S20.20-2007 (Revision of ANSI/ESD S20.20-1999).

Product Qualification

Personnel Grounding Technical Requirement	Test Method	Required Limits
Wrist Strap System*	ANSI/ESD S1.1 (Section 5.11)	< 3.5 x 10^7 ohm
Flooring / Footwear System – Method 1	ANSI/ESD STM97.1	< 3.5 x 10^7 ohm
Flooring / Footwear System – Method 2 (both required)	ANSI/ESD STM97. 1ANSI/ESD STM97.2	< 10^9 ohm
	ANSI/ESD STM97.2	< 100 V

Product qualification is normally conducted during the initial selection of ESD control products and materials. Any of the following methods can be used: product specification review, independent laboratory evaluation, or internal laboratory evaluation.

Compliance Verification

Personnel Grounding Technical Requirement	Test Method	Required Limits
Wrist Strap System*	ESD TR53 Wrist Strap Section	< 3.5 x 10^7 ohm
Flooring / Footwear System – Method 1	ESD TR53 Flooring Section and ESD TR53 Footwear Section	< 3.5 x 10^7 ohm
Flooring / Footwear System – Method 2 (both required)	ESD TR53 Flooring Section and ESD TR53 Footwear Section	< 1.0 x 10^9 ohm

* For situations where an ESD garment is used as part of the wrist strap grounding path, the total system resistance, including the person, garment, and grounding cord, must be less than 3.5 x 10^7 ohm.

Trademarks and Agreements

Trademarks

Belden, Belden Sending All The Right Signals, and the Belden logo are trademarks or registered trademarks of Belden Inc. or its affiliated companies in the United States and other jurisdictions. Grass Valley, GV STRATUS, GV Director, K2, Summit, ChannelFlex, Dyno, Solo, ClipStore, Infinity, Turbo, Profile, Profile XP and NetCentral, are trademarks or registered trademarks of Grass Valley Canada. Belden Inc., Grass Valley Canada and other parties may also have trademark rights in other terms used herein, such as Microsoft® Windows® operating system, Windows Media® player, Internet Explorer® internet browser, and SQL Server™. QuickTime and the QuickTime logo are trademarks or registered trademarks of Apple Computer, Inc., used under license therefrom. Avid DNxHD and Avid are registered trademarks of Avid Technology, Inc., a Delaware corporation.

Patent Information

This product may be protected by one or more patents.

For further information, please visit: *https://www.grassvalley.com/patents/*

JPEG acknowledgment

This software is based in part on the work of the Independent JPEG Group.