

GV STRATUS

Media Workflow Application Framework

Upgrade Instructions

Software Version 3.1

This document contains the most recent information and supersedes previous publications. Check the Grass Valley website at www.grassvalley.com/docs for an updated version that contains additional important information.

Contacting Grass Valley

International Support Center		United States/Canada	+1 800 547 8949 or +1 530 478 4148	
Local Support Centers	N.America	+1 800 547 8949 (Option 2) or +1 530 478 4148		France: +800 80 80 20 20 or +33 1 48 25 20 20
	Asia	Hong Kong, Taiwan, Korea, Macau: +852 2531 3000 India: 1800 200 3432 (within India) Southeast Asia/Malaysia: +603 7492 3033 Southeast Asia/Singapore: +65 6379 1771 China: +86 10 5883 7525		
	Australia: 1300 721 495 New Zealand: 0800 846 676 Outside Australia/New Zealand: +61 3 8540 3650			
	Near East and Africa: +800 8080 2020 or +33 1 48 25 20 20		Central/South America: +55 11 5509 3443	
	Europe	Armenia/Azerbaijan/Belarus/Kazakhstan/Kyrgyzstan/Moldova/Russia/Tajikistan/Turkmenistan/Ukraine/Uzbekistan :+7 495 787 06 55 Turkey: +90 (0) 212 408 22 23 N. Europe: +44 844 338 7007, +44 (0) 20 8867 6305 S. Europe/Italy: +39 06 87 20 35 28 S. Europe/Portugal: +34 91 512 03 58 S. Europe/Spain: +34 91 512 03 50 Belgium/Luxemburg:+32 (0) 2 334 90 30 Netherlands: +31 (0) 76 57 21420 Germany, Austria, Eastern Europe: +49 6150 104 444 UK, Ireland, Israel: +44 844 338 7007		

Copyright © Grass Valley USA, LLC. All rights reserved.
This product may be covered by one or more U.S. and foreign patents.

Grass Valley Web Site

The <http://www.grassvalley.com/support> web site offers the following:

Online User Documentation — Current versions of product catalogs, brochures, data sheets, ordering guides, planning guides, manuals, and release notes in .pdf format can be downloaded.

FAQ Database — Solutions to problems and troubleshooting efforts can be found by searching our Frequently Asked Questions (FAQ) database.

Software Downloads — Download software updates, drivers, and patches.



END-OF-LIFE PRODUCT RECYCLING NOTICE

Grass Valley's innovation and excellence in product design also extends to the programs we've established to manage the recycling of our products. Grass Valley has developed a comprehensive end-of-life product take back program for recycle or disposal of end-of-life products. Our program meets the requirements of the European Union's WEEE Directive, the United States Environmental Protection Agency, and U.S. state and local agencies.

Grass Valley's end-of-life product take back program assures proper disposal by use of Best Available Technology. This program accepts any Grass Valley branded equipment. Upon request, a Certificate of Recycling or a Certificate of Destruction, depending on the ultimate disposition of the product, can be sent to the requester.

Grass Valley will be responsible for all costs associated with recycling and disposal, including freight. However, you are responsible for the removal of the equipment from your facility and packing the equipment to make it ready for pickup.



For further information on the Grass Valley product take back system please contact Grass Valley at + 800 80 80 20 20 or +33 1 48 25 20 20 from most other countries. In the U.S. and Canada please call 800-547-8949, and ask to be connected to the EH&S Department. Additional information concerning the program can be found at: www.grassvalley.com/about/environmental-policy

001187401

Contents

Upgrading GV STRATUS systems.....	5
Summary of upgrade from version 3.0 to version 3.1.....	5
Summary of upgrade from version 2.8 to version 3.1.....	6
Summary of steps for upgrade to version 3.1.....	7
Upgrading from version 3.0 to version 3.1.....	8
Make recovery images of servers.....	8
Prepare for upgrade.....	8
Prepare SiteConfig for software deployment.....	8
Upgrade K2/Summit/SAN systems that are accessed by the GV STRATUS system.....	9
About deploying software for the K2 SAN.....	9
Install High Priority Windows updates (recommended).....	9
Upgrade .NET on GV STRATUS servers and client PCs.....	9
Check all currently installed software on GV STRATUS devices.....	10
Add software package to deployment group for GV STRATUS devices.....	11
Setting deployment options.....	12
Prepare for configuration.....	15
Verify GV STRATUS Engines are running.....	15
Set GV STRATUS client PC to high-resolution.....	16
Upgrade Aurora Payout systems.....	17
Install Grass Valley Prerequisite Files on the SiteConfig PC.....	17
Make recovery images of servers.....	17
Upgrading from version 2.8 to version 3.1.....	18
Make recovery images of servers.....	18
Prepare for upgrade.....	18
Prepare SiteConfig for software deployment.....	18
Upgrade K2/Summit/SAN systems that are accessed by the GV STRATUS system.....	19
About deploying software for the K2 SAN.....	19
Install High Priority Windows updates (recommended).....	19
Upgrade .NET on GV STRATUS servers and client PCs.....	19
Add/remove software roles.....	21
Check all currently installed software on GV STRATUS devices.....	21
Add software package to deployment group for GV STRATUS devices.....	22
Setting deployment options.....	23
Upgrade GV STRATUS Database.....	26
Update SQL.....	26
SabreTooth license process.....	27
Prepare for configuration.....	28
Configure Proxy Config settings.....	28
Verify GV STRATUS Engines are running.....	32
Configure licenses and roles.....	32
Set GV STRATUS client PC to high-resolution.....	33
Upgrade Aurora Payout systems.....	34
Install Grass Valley Prerequisite Files on the SiteConfig PC.....	34
Make recovery images of servers.....	34
Upgrading EDIUS XRE Servers and EDIUS clients.....	35
Uninstall EDIUS Elite and supporting software.....	35
Upgrade .NET on EDIUS XRE Server.....	35
Verify EDIUS software roles.....	36
Add software package to deployment group for EDIUS clients and EDIUS XRE Server.....	36

Upgrade EDIUS software.....	38
Configuring EDIUS XRE Server settings.....	38
Activate EDIUS XRE Server license.....	43
Activate EDIUS XRE Server license online.....	43
Activate EDIUS XRE Server license offline.....	44
If you have trouble launching EDIUS XS.....	47
Upgrade Workflow Server, license, configure Rules.....	49
SiteConfig Workflow Server software install.....	49
Upgrade software on a Workflow Server.....	49
SabreTooth Rules, Xcode license process.....	50
Configuring Rules.....	51
Adding a delete rule.....	51
Adding an export rule.....	53
Adding a transfer rule.....	60
Adding an archive rule.....	63
Adding a restore rule.....	66
Custom rules.....	70
Example rule: Deleting EDIUS XS lock files.....	70
Enabling and disabling rules.....	71
Monitoring rules.....	72
Identifying assets affected by rules.....	73
Adding a thumbnail marker.....	74
Adding a Carbon Coder transcode profile.....	74
Adding a Vantage transcode profile.....	74
Additional Topics.....	76
Complete listing of device types, roles, and software packages for GV STRATUS devices.....	76
Summary of previous upgrades.....	86
Summary of upgrade from version 1 to version 2.....	86
Summary of upgrade from version 1 to version 2.5.....	86
Summary of upgrade from version 2.0 to version 2.5.....	87
Summary of upgrade from version 2.5 to version 2.7.....	88
Summary of upgrade from version 2.5 to version 2.7.5.....	89
Summary of upgrade from version 2.5 to version 2.8.....	89
Summary of upgrade from version 2.7 to version 2.8.....	90
Adding a device to a network with SiteConfig.....	91
Discovering devices with SiteConfig.....	91
Assigning discovered devices.....	92
Modifying managed control network interface.....	93
Making the host name the same as the device name.....	97
Pinging devices from the PC that hosts SiteConfig.....	97
Verify credentials.....	98
Generating host tables using SiteConfig.....	98
Trademarks and Agreements.....	100
Trademarks.....	100
JPEG acknowledgment.....	100

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 2.8. If you have a lower version of software, first follow the 2.8 version of this document and upgrade to version 2.8. 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 upgrade instructions in this document, you use SiteConfig from a network connected control point PC and remotely upgrade software simultaneously on your system devices. This is the recommended process for software upgrades.

Upgrading without using SiteConfig (manual install) is not supported.

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
 - Proxy server (A1)
 - Proxy Storage file system server (B1, C1)
 - Proxy Encoder
 - Conform Server
 - EDIUS XRE Server
 - Workflow 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.

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 "GV STRATUS User Manual".

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 CIFS 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 "GV STRATUS User Manual".

Summary of steps for upgrade to version 3.1

1. Start with one of the following topics to follow the upgrade path appropriate for the version of software from which you are upgrading:
 - [Upgrading from version 3.0 to version 3.1](#) on page 8
 - [Upgrading from version 2.8 to version 3.1](#) on page 18
2. Upgrade Aurora Playout systems, if in your GV STRATUS system.
3. As appropriate for your system design, work through tasks in the following sections:
 - [Upgrade EDIUS XRE Servers and EDIUS clients](#) on page 35
 - [Upgrade Workflow Server, license, configure Rules](#) on page 49
4. Make recovery images of servers.
5. If you have not already done so, upgrade to .NET 4.5 on all GV STRATUS servers and client PCs on which GV STRATUS and/or EDIUS components are installed.

Upgrading from version 3.0 to version 3.1

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

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.*

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.
- Stop all media access on the devices you are upgrading.
- Shut down all applications on the devices you are upgrading.
- Restart all the devices you are upgrading.

Prepare SiteConfig for software deployment

Do the following to prepare SiteConfig for the software upgrade.

If a newer version of SiteConfig is available for upgrade and you have not yet upgraded SiteConfig, do the following:

- a) From Windows Add/Remove programs, uninstall the current version of SiteConfig from the control point PC.
- b) Install the new version of SiteConfig on the control point PC.

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

Prerequisites for this task are as follows:

- You have procured the necessary software and documentation for the upgrade. Go to http://www.grassvalley.com/dl/k2_summit and refer to "K2 Release Notes" to determine the compatible software versions and documentation required.
- All standalone K2 Summit systems must be offline (all media access stopped) or shut down.
- If upgrading a K2 SAN, all SAN clients must be offline (all media access stopped) or shut down. 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.*

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.

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.

Install High Priority Windows updates (recommended)

- Windows "High Priority" updates are recommended, but not required. While you have devices in an offline state to upgrade software, you should check to see if there are any new updates that you need to install. Use standard Windows procedures.

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

NOTE: *Do not install updates KB2859537 or KB2872339 on any Grass Valley system. If this update has been installed on your system, remove the update and restart your system.*

Upgrade .NET on GV STRATUS servers and client PCs

Do not do this task if:

- The GV STRATUS server or client PC has .NET 4.5 installed

Do this task if:

- The GV STRATUS server or client PC does not have .NET 4.5 installed

This task applies to client PCs hosting one or more of the following:

- GV STRATUS
- GV STRATUS Control Panel
- EDIUS XS
- EDIUS Elite

This task also applies to all GV STRATUS servers, as follows:

- GV STRATUS Express server
- GV STRATUS Core server
- Proxy server
- Proxy Storage file system server
- Proxy Encoder
- Conform Server
- EDIUS XRE Server
- Workflow Server

1. On the GV STRATUS server or client PC, check Windows Control Panel **Programs and Features** for currently installed .NET version(s), then proceed as follows:
 - If .NET 4.5 is installed, skip this task.
 - If .NET 4.5 is not installed, continue with this procedure.
2. Procure the .NET 4.5 installation file from the software download page on the Grass Valley website.
3. Run the installation file and install .NET as directed by the installation wizard.

Check all currently installed software on GV STRATUS devices

Check software on GV STRATUS devices.

Prerequisites for this task are as follow:

- The device is assigned in the SiteConfig system description and network connectivity is present.
- SiteConfig is able to log in to the device using the username/password credentials assigned to the device.

- The SiteConfig PC does not have a network drive mapped to an administrative share (such as C\$) on a device on which you are checking software.

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 Grass Valley Embedded Security, 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 76

Add software package to deployment group for GV STRATUS devices

Prerequisites for this task are as follows:

- The GV STRATUS devices to which you are deploying software have their SiteConfig roles correctly configured.
- The GV STRATUS devices to which you are deploying software are in a deployment group.

The following software upgrade cab files apply to GV STRATUS devices.

- *GrassValley_STRATUSClient_X.X.XX.XXXX.cab*
- *GrassValley_CoreServer_X.X.XX.XXXX.cab*
- *GrassValley_K2system_X.X.XX.XXXX.cab*

Refer to release notes for version information.

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 76

Setting deployment options

Pre-requisites for this procedure are as follows:

- A software package has been assigned to the deployment group and applicable deployment tasks are now 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."

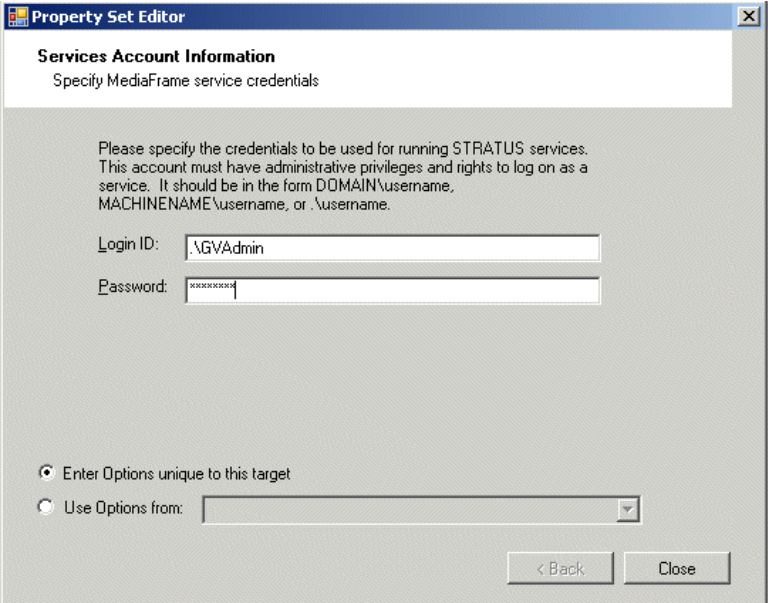
If you select a task that needs to have its deployment options set, the Start Deployment button is disabled and the message is displayed next to the button.

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_ConformService	
GrassValley_STRATUS_CoreServices	
GrassValley_STRATUS_DataMover	
GrassValley_STRATUS_DIVA_MDI	
GrassValley_STRATUS_FlashNet_MDI	
GrassValley_STRATUS_GFTP_MDI	
GrassValley_STRATUS_HttpProxyServer	
GrassValley_STRATUS_MediaFlow	
GrassValley_STRATUS_Proxy_Encoder	
GrassValley_STRATUS_Rules	
GrassValley_STRATUS_Summit_MDI	
GrassValley_STRATUS_TrafficGateway	
GrassValley_STRATUS_Transcode	

The account must be the internal system account, which by default is GVAdmin. It is advisable to enter it as .\accountname where the "." means a local account. Entering the local account in this way allows you to use the **Use options from** feature for all other devices of the same type. Once you enter the local account in 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

Prerequisites for this task are as follows:

- The devices that you are upgrading are in a deployment group.
- For the software you are upgrading, you have added a newer version of that managed software package to the deployment group.
- You have recently done the SiteConfig "Check Software" operation 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.

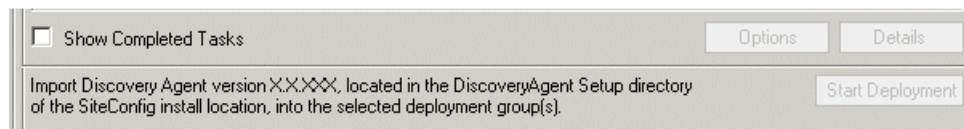
1. In the **Software Deployment | Deployment Groups** tree view, select the device or the group of devices to which you are deploying software.

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

2. For the software you are deploying, 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.

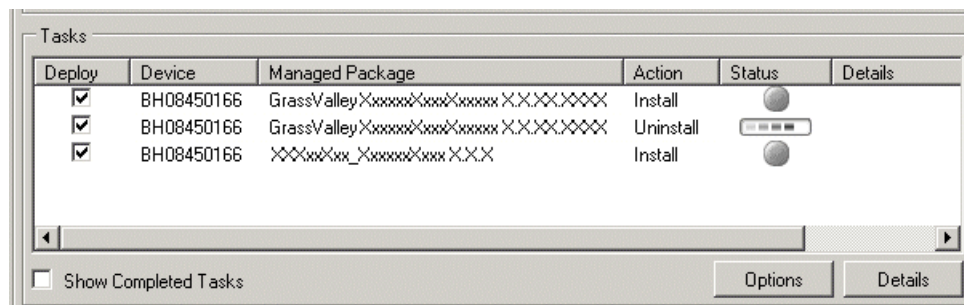
If a WRegMon install task appears, install it as well. It is required to support Grass Valley software installers. There is no uninstall task.

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.

Prepare for configuration

Do the following to verify systems and tools are ready for configuration:

- 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, 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.
- 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.

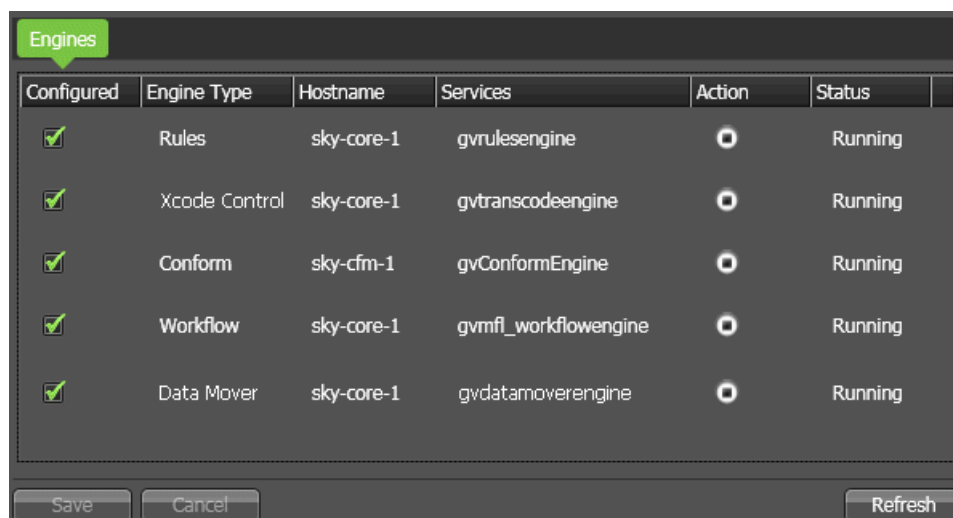
Begin by configuring STRATUS Core Services settings.

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.



Configured	Engine Type	Hostname	Services	Action	Status
<input checked="" type="checkbox"/>	Rules	sky-core-1	gvrulesengine	<input type="radio"/>	Running
<input checked="" type="checkbox"/>	Xcode Control	sky-core-1	gvtranscodeengine	<input type="radio"/>	Running
<input checked="" type="checkbox"/>	Conform	sky-cfm-1	gvConformEngine	<input type="radio"/>	Running
<input checked="" type="checkbox"/>	Workflow	sky-core-1	gvmfl_workflowengine	<input type="radio"/>	Running
<input checked="" type="checkbox"/>	Data Mover	sky-core-1	gvdatamoverengine	<input type="radio"/>	Running

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**.

Set GV STRATUS client PC to high-resolution

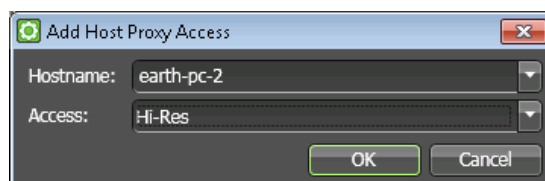
Only systems with GV STRATUS client PCs that use a high-resolution media workflow require this process. Configure the PC in GV STRATUS Control Panel.

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 involve the GV STRATUS RMI tool or that integrate with a high-resolution editor such as EDIUS Elite. 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 CIFS mount access to K2 storage — This setup is for high-resolution workflows, such as those that involve the GV STRATUS RMI tool or that integrate with a high-resolution editor such as EDIUS Elite. The GV STRATUS application accesses the high-resolution assets via a CIFS 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.

Upgrade Aurora Payout systems

Prerequisites for this task are as follows:

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

Upgrade your Aurora Payout systems to the compatible versions of software. Refer to "Aurora Payout Release Notes" for procedures.

Install Grass Valley Prerequisite Files on the SiteConfig PC

Aurora products, including Aurora Payout, 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
All Aurora products	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*.

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 from version 2.8 to version 3.1

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

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.*

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.
- Stop all media access on the devices you are upgrading.
- Shut down all applications on the devices you are upgrading.
- Restart all the devices you are upgrading.

Prepare SiteConfig for software deployment

Do the following to prepare SiteConfig for the software upgrade.

If a newer version of SiteConfig is available for upgrade and you have not yet upgraded SiteConfig, do the following:

- a) From Windows Add/Remove programs, uninstall the current version of SiteConfig from the control point PC.
- b) Install the new version of SiteConfig on the control point PC.

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

Prerequisites for this task are as follows:

- You have procured the necessary software and documentation for the upgrade. Go to http://www.grassvalley.com/dl/k2_summit and refer to "K2 Release Notes" to determine the compatible software versions and documentation required.
- All standalone K2 Summit systems must be offline (all media access stopped) or shut down.
- If upgrading a K2 SAN, all SAN clients must be offline (all media access stopped) or shut down. 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.*

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.

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.

Install High Priority Windows updates (recommended)

- Windows "High Priority" updates are recommended, but not required. While you have devices in an offline state to upgrade software, you should check to see if there are any new updates that you need to install. Use standard Windows procedures.

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

NOTE: *Do not install updates KB2859537 or KB2872339 on any Grass Valley system. If this update has been installed on your system, remove the update and restart your system.*

Upgrade .NET on GV STRATUS servers and client PCs

Do not do this task if:

- The GV STRATUS server or client PC has .NET 4.5 installed

Do this task if:

- The GV STRATUS server or client PC does not have .NET 4.5 installed

This task applies to client PCs hosting one or more of the following:

- GV STRATUS
- GV STRATUS Control Panel
- EDIUS XS
- EDIUS Elite

This task also applies to all GV STRATUS servers, as follows:

- GV STRATUS Express server
- GV STRATUS Core server
- Proxy server
- Proxy Storage file system server
- Proxy Encoder
- Conform Server
- EDIUS XRE Server
- Workflow Server

1. On the GV STRATUS server or client PC, check Windows Control Panel **Programs and Features** for currently installed .NET version(s), then proceed as follows:
 - If .NET 4.5 is installed, skip this task.
 - If .NET 4.5 is not installed, continue with this procedure.
2. Procure the .NET 4.5 installation file from the software download page on the Grass Valley website.
3. Run the installation file and install .NET as directed by the installation wizard.

Add/remove 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 76.

SiteConfig roles are new or require special consideration with this software upgrade.

As appropriate for your system design and licensing, in your SiteConfig system description, configure roles as follows:

- For all GV STRATUS servers, configure roles as follows:
 - Add GV STRATUS Event Viewer role
- For your GV STRATUS Express Server or Core Server, configure roles as follows:
 - For all systems, add the following role:
 - GV STRATUS Data Mover Engine
 - For systems licensed for Rules, verify the following role:
 - GV STRATUS Xcode Control Engine

Even if no XCODECONTROL license is installed and no transcode formats are used, the GV STRATUS Xcode Control Engine is still required to support Export rule functionality.
 - For systems using Segmentation features, add the following role:
 - GV STRATUS Traffic Gateway

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

Related Topics

[Complete listing of device types, roles, and software packages for GV STRATUS devices](#) on page 76

Check all currently installed software on GV STRATUS devices

Check software on GV STRATUS devices.

Prerequisites for this task are as follow:

- The device is assigned in the SiteConfig system description and network connectivity is present.
- SiteConfig is able to log in to the device using the username/password credentials assigned to the device.

- The SiteConfig PC does not have a network drive mapped to an administrative share (such as C\$) on a device on which you are checking software.

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 Grass Valley Embedded Security, 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 76

Add software package to deployment group for GV STRATUS devices

Prerequisites for this task are as follows:

- The GV STRATUS devices to which you are deploying software have their SiteConfig roles correctly configured.
- The GV STRATUS devices to which you are deploying software are in a deployment group.

The following software upgrade cab files apply to GV STRATUS devices.

- *GrassValley_STRATUSClient_X.X.XX.XXXX.cab*
- *GrassValley_CoreServer_X.X.XX.XXXX.cab*
- *GrassValley_K2system_X.X.XX.XXXX.cab*

Refer to release notes for version information.

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 76

Setting deployment options

Pre-requisites for this procedure are as follows:

- A software package has been assigned to the deployment group and applicable deployment tasks are now 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."

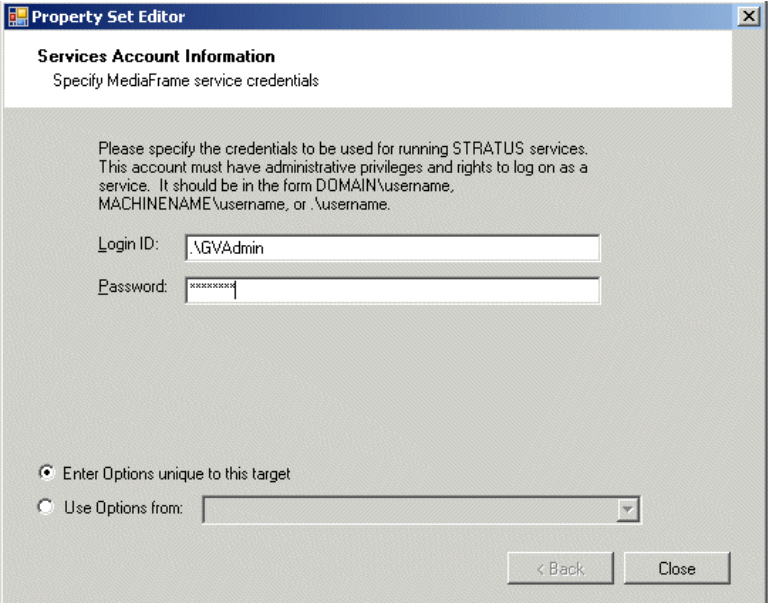
If you select a task that needs to have its deployment options set, the Start Deployment button is disabled and the message is displayed next to the button.

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_ConformService	
GrassValley_STRATUS_CoreServices	
GrassValley_STRATUS_DataMover	
GrassValley_STRATUS_DIVA_MDI	
GrassValley_STRATUS_FlashNet_MDI	
GrassValley_STRATUS_GFTP_MDI	
GrassValley_STRATUS_HttpProxyServer	
GrassValley_STRATUS_MediaFlow	
GrassValley_STRATUS_Proxy_Encoder	
GrassValley_STRATUS_Rules	
GrassValley_STRATUS_Summit_MDI	
GrassValley_STRATUS_TrafficGateway	
GrassValley_STRATUS_Transcode	

The account must be the internal system account, which by default is GVAdmin. It is advisable to enter it as .\accountname where the "." means a local account. Entering the local account in this way allows you to use the **Use options from** feature for all other devices of the same type. Once you enter the local account in 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

Prerequisites for this task are as follows:

- The devices that you are upgrading are in a deployment group.
- For the software you are upgrading, you have added a newer version of that managed software package to the deployment group.
- You have recently done the SiteConfig "Check Software" operation 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.

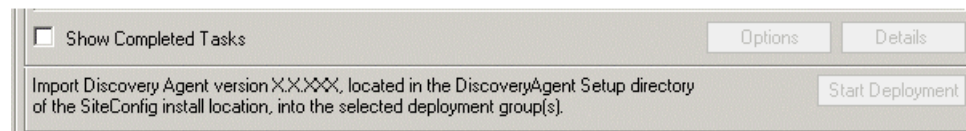
1. In the **Software Deployment | Deployment Groups** tree view, select the device or the group of devices to which you are deploying software.

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

2. For the software you are deploying, 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.

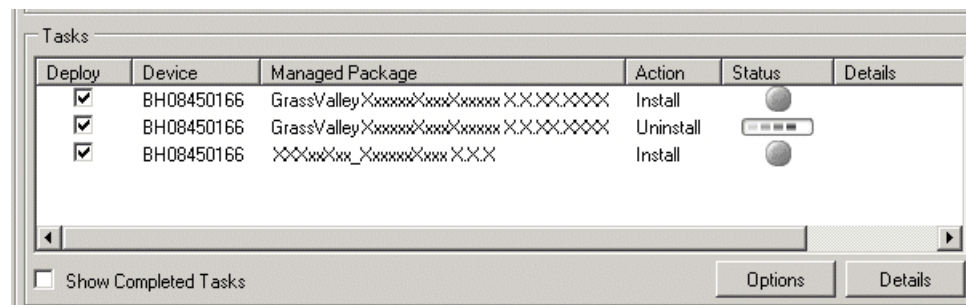
If a WRegMon install task appears, install it as well. It is required to support Grass Valley software installers. There is no uninstall task.

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.

Upgrade GV STRATUS Database

This task applies to the following:

- The GV STRATUS server with the role of GV STRATUS Core Services . Typically this is the GV STRATUS Core server

Before doing this task, do the following:

- Upgrade software on the GV STRATUS server.
- If the server has Embedded Security, make sure it is in Update mode.

This task upgrades the GV STRATUS database.

1. Login to the GV STRATUS server as Administrator.
2. Locate the following file:

C:\Program Files (x86)\Grass Valley\STRATUS Core Services\UpgradeDatabase.exe

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

3. Double-click *UpgradeDatabase.exe* to upgrade the database.

A "The database upgrade completed successfully" message displays.

If the server has Embedded Security, after all installation is complete, leave Update mode.

Update SQL

This task applies to the following:

- Any GV STRATUS server with SQL installed. The following GV STRATUS servers have SQL installed:
 - GV STRATUS Express server
 - GV STRATUS Core server
 - Workflow Server

This includes servers on a Dell platform as well as on the NEC Fault Tolerant platform.

Before doing this task, do the following:

- Upgrade GV STRATUS software on the GV STRATUS server.
- Upgrade the GV STRATUS database.
- If the server has Embedded Security, make sure it is in Update mode.

Microsoft SQL Server 2008 R2 Service Pack 2 is required for compatibility with GV STRATUS version 2.8 and higher. Systems shipping from Grass Valley with GV STRATUS version 2.8 and higher have this SQL version pre-installed.

1. Login to the GV STRATUS server as Administrator.

2. Check the current SQL version to determine if it must be updated, as follows:
 - a) Open SQL Server Management Studio.
 - b) In the **Object Explorer** tree-view, identify the **(local)** node that displays SQL Server version number and proceed as follows:
 - If the version is 10.50.4000.0, your server already has the required version. You do not need to update SQL. Skip the remainder of this task.
 - If the version is 10.50.1600.1, you must update SQL. Proceed with the remainder of this task.
3. Procure the SQL installation file from the Microsoft download page.
<http://www.microsoft.com/en-us/download/details.aspx?id=30437>
The correct version is the 64-bit version, which is
SQLServer2008R2SP2-KB2630458-x64-ENU.exe.
4. On the GV STRATUS server, run the SQL installation file and work through the installation wizard, accepting all defaults.
The installation process at the end of the wizard can take up to 15 minutes.
5. Restart the GV STRATUS server.
6. Open SQL Server Management Studio and make sure the version is 10.50.4000.0, as explained earlier in this task.

If the server has Embedded Security, after all installation is complete, leave Update mode.

SabreTooth license process

Do this task if you are adding any Sabretooth licenses as part of this upgrade.

The following licenses are new with this version of software:

- STRATUS-MULTISITE
- STRATUS-XCODECONTROLVANTAGE

A 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.

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 "GV STRATUS Release Notes" for detailed licensing procedures.
3. When you receive your license file, use SabreTooth License Manager and install it on the server.

Prepare for configuration

Do the following to verify systems and tools are ready for configuration:

- 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, 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.
- 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.

Begin by configuring STRATUS Core Services settings.

Configure 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.*

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

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

The screenshot shows the 'Proxy Settings' window with three tabs: 'Proxy Settings' (selected), 'Proxy Access', and 'Test Connections'. The 'Proxy Settings' tab contains three sections: 'Proxy Server Settings' with dropdowns for 'Location of Proxy Assets:', 'CIFS Server:', and 'HTTP Server:' (all set to 'Demo-cs-1'); 'K2 Summit Settings' with a checked checkbox 'Enable Proxy Creation'; and 'Proxy Encoder Settings' with a checked checkbox 'Enable Proxy Encoders'. At the bottom are 'Save' and 'Cancel' buttons.

NOTE: GV STRATUS versions lower than 3.0 had only one Proxy Server setting. With version 3.0 and higher, the CIFS 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	<p>The name of the system that stores proxy files generated by K2 Summit and GV STRATUS systems, as follows:</p> <ul style="list-style-type: none"> 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.
CIFS Server	<p>The network machine name of the device hosting the server to which proxy files are written, as follows:</p> <ul style="list-style-type: none"> 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	<p>The network machine name of the device hosting the server from which GV STRATUS clients read proxy files. Typically the CIFS Server and the HTTP Server are hosted by the same device.</p> <ul style="list-style-type: none"> 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	<p>The name of the system that stores proxy files generated by K2 Summit and GV STRATUS systems, as follows:</p> <ul style="list-style-type: none"> For proxy stored on the K2 SAN (A1), this is the name of the K2 SAN, as named in K2Config.
CIFS Server	<p>The network machine name of the device hosting the server to which proxy files are written, as follows:</p> <ul style="list-style-type: none"> 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	<p>The network machine name of the device hosting the server from which GV STRATUS clients read proxy files. Typically the CIFS Server and the HTTP Server are hosted by the same device.</p> <ul style="list-style-type: none"> 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	<p>The name of the system that stores proxy files generated by K2 Summit and GV STRATUS systems, as follows:</p> <ul style="list-style-type: none"> For proxy stored on the dedicated Proxy Storage system (B1, C1), this is the name of the Proxy Storage system, as named in K2Config.
CIFS Server	<p>The network machine name of the device hosting the server to which proxy files are written, as follows:</p> <ul style="list-style-type: none"> 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	<p>The network machine name of the device hosting the server from which GV STRATUS clients read proxy files. Typically the CIFS Server and the HTTP Server are hosted by the same device.</p> <ul style="list-style-type: none"> 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.

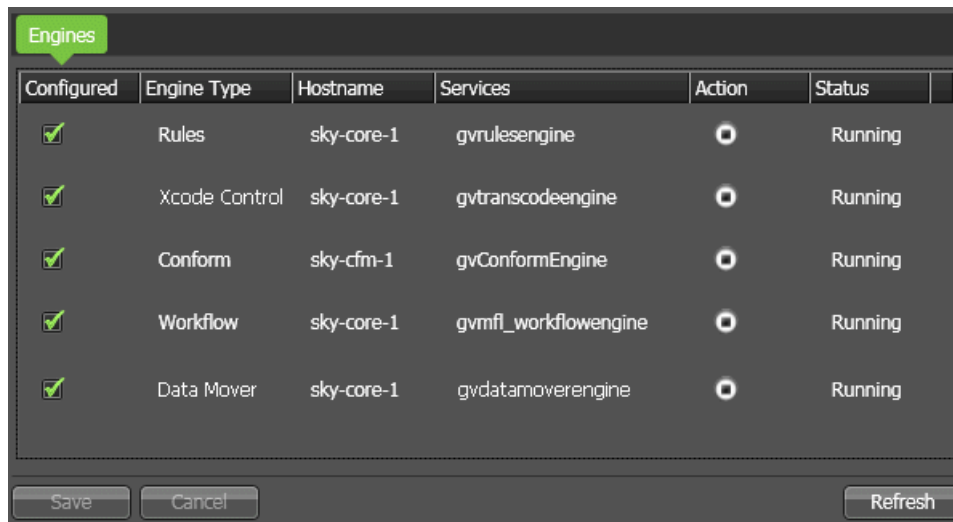
5. On the **Test Connections** tab, click **Test Connections**.
The GV STRATUS system populates a list of K2 Storage devices. Verify that this list is correct.
6. Select **Enable Proxy Creation**.
This allows K2 Summit systems to create proxy assets when high resolution assets are recorded.
7. Select **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.
8. Click **Save**.

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.



Configured	Engine Type	Hostname	Services	Action	Status
<input checked="" type="checkbox"/>	Rules	sky-core-1	gvrulesengine		Running
<input checked="" type="checkbox"/>	Xcode Control	sky-core-1	gvtranscodeengine		Running
<input checked="" type="checkbox"/>	Conform	sky-cfm-1	gvConformEngine		Running
<input checked="" type="checkbox"/>	Workflow	sky-core-1	gvmfl_workflowengine		Running
<input checked="" type="checkbox"/>	Data Mover	sky-core-1	gvdatamoverengine		Running

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**.

Configure licenses and roles

In GV STRATUS Control Panel Authorization Manager settings, configure the following, depending on your site's licensing and workflow requirements.

- Multisite Access
- Trim Rights

Set GV STRATUS client PC to high-resolution

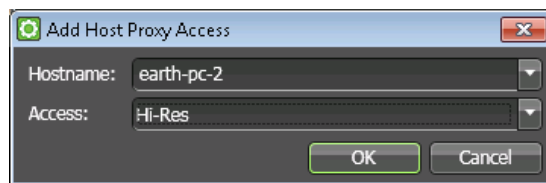
Only systems with GV STRATUS client PCs that use a high-resolution media workflow require this process. Configure the PC in GV STRATUS Control Panel.

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 involve the GV STRATUS RMI tool or that integrate with a high-resolution editor such as EDIUS Elite. 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 CIFS mount access to K2 storage — This setup is for high-resolution workflows, such as those that involve the GV STRATUS RMI tool or that integrate with a high-resolution editor such as EDIUS Elite. The GV STRATUS application accesses the high-resolution assets via a CIFS 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.

Upgrade Aurora Payout systems

Prerequisites for this task are as follows:

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

Upgrade your Aurora Payout systems to the compatible versions of software. Refer to "Aurora Payout Release Notes" for procedures.

Install Grass Valley Prerequisite Files on the SiteConfig PC

Aurora products, including Aurora Payout, 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
All Aurora products	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*.

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 EDIUS XRE Servers and EDIUS clients

Follow the topics in this section to upgrade EDIUS components in your system.

Uninstall EDIUS Elite and supporting software

If you have an EDIUS Elite 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 that you reimage the client PC.

Do not attempt to convert an EDIUS Elite 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.

Upgrade .NET on EDIUS XRE Server

Do not do this task if:

- The EDIUS XRE Server has .NET 4.5 installed

Do this task if:

- The EDIUS XRE Server does not have .NET 4.5 installed
1. On the EDIUS XRE Server, check Windows Control Panel **Programs and Features** for currently installed .NET version(s), then proceed as follows:
 - If .NET 4.5 is installed, skip this task.
 - If .NET 4.5 is not installed, continue with this procedure.
 2. Procure the .NET 4.5 installation file from the software download page on the Grass Valley website.
 3. Run the installation file and install .NET as directed by the installation wizard.

Verify 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 76.

NOTE: *GV STRATUS/EDIUS client PC and EDIUS XRE Server must be in GV STRATUS family, not EDIUS family.*

For upgrading EDIUS 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)

NOTE: *If initial (not upgrade) install, first install GV STRATUS software, then install EDIUS software.*

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

NOTE: *If initial (not upgrade) install, first install GV STRATUS software, then install EDIUS software.*

- EDIUS XRE Server
 - GV STRATUS Application
 - GV STRATUS Event Viewer
 - K2 FTP Server
 - StorNext File System Client
 - XRE Server

NOTE: *If initial (not upgrade) install, first install GV STRATUS software, then install EDIUS software.*

Related Topics

[Complete listing of device types, roles, and software packages for GV STRATUS devices](#) on page 76

Add software package to deployment group for EDIUS clients and EDIUS XRE 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 Grass Valley Embedded Security, 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)

NOTE: If initial (not upgrade) install, first install GV STRATUS software, then install EDIUS software.

The following software upgrade cab files apply to GV STRATUS/EDIUS Elite (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*
 - *GenericISCI_x64_x.x.x.cab*
 - *SNFS_nonK2_x64_x.x.x.cab*
- *EDIUS_x.x.x.cab* (Required for EDIUS Elite).

NOTE: If initial (not upgrade) install, first install GV STRATUS software, then install EDIUS software.

The following software upgrade cab files apply to EDIUS XRE Servers.

- *XREServer_x.x.x.cab*
- *GrassValley_K2system_x.x.x.cab*, which contains the following cab files that apply to this device:
 - *GrassValleyK2Server_x64_x.x.x.cab*
 - *SNFS_x64_x.x.x.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_GVEventViewer_x.x.x.cab*

NOTE: If initial (not upgrade) install, first install GV STRATUS software, then install EDIUS software.

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 76

Upgrade EDIUS software

Prerequisites for this task are as follows:

- If installing to an EDIUS Elite client PC on which you have previously installed EDIUS manually (not with SiteConfig), EDIUS Elite and supporting software must first be uninstalled manually, before attempting to install with SiteConfig.
- If installing EDIUS for the first time (not upgrade), GV STRATUS application software must be installed first before installing EDIUS application or EDIUS XRE software.

NOTE: Expect long deployment times when installing EDIUS software. EDIUS software can take over 15 minutes and EDIUS XRE software can take over 30 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 EDIUS XRE Server. Use SiteConfig for software deployment.

1. If you are upgrading from an EDIUS 6.x version to an EDIUS 7.x version, first uninstall software as follows:
 - a) In one SiteConfig deployment session, uninstall EDIUS/XRE software and GVG_Mlib software.
 - b) Restart the device from which you uninstalled the software.
 - c) In one SiteConfig deployment session, uninstall GV STRATUS software.

NOTE: Use separate deployment sessions to uninstall software. Do not uninstall and install in the same deployment session.

2. Install software as follows:

This step applies if upgrading from an EDIUS 7.x version. It also applies if upgrading from an EDIUS 6.x version, but if upgrading from an EDIUS 6.x version, you must first uninstall as specified in the previous step.

- a) In one SiteConfig deployment session, install GV STRATUS software, and other software, as appropriate for the roles assigned to the device.
- b) Restart the device to which you installed the software.
- c) In one SiteConfig deployment session, install EDIUS/XRE software.
- d) Restart the device to which you installed the software.

Next, if you are upgrading from an EDIUS 6.x version to an EDIUS 7.x version, re-license EDIUS software. This is required to support EDIUS version 7.

Configuring EDIUS XRE Server settings

Only systems with an EDIUS XRE Server require this process.

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

Refer to "EDIUS XRE User Guide" for related detailed information.

If you have one EDIUS XRE Server, configure XRE Management Server, XRE Monitor, and XRE Node settings on the server.

If you have multiple EDIUS XRE Servers, configure XRE Management Server, XRE Monitor, and XRE Node settings on your first server. This first server is then your XRE Management Server, which means it manages all your XRE Nodes. Configure XRE Node settings only on your other EDIUS XRE Servers. Then all your servers are XRE Nodes and available to render EDIUS projects.

1. Configure XRE Management Server settings as follows:

- a) From the Windows desktop, click **Start | All Programs | Grass Valley | XREManagementServer**.
- b) From the Windows desktop system tray, right-click **XREManagementServer** and select **Settings**.

If system tray icons are not present, verify that EDIUS licensing is complete. Missing icons can indicate the software is not licensed.

The **XREManagementServer setting** dialog box opens.

- c) Click **Select** and make settings as follows.

Table 1: XRE Management Server settings

Setting	Value
Project folder	The default location for your EDIUS XS projects, as specified in GV STRATUS Control Panel EDIUS Settings. This is a shared folder on K2 storage, for example <code>\\k2-san-fsm\EDIUS_Projects</code> . Make sure this path uses the standard convention of UNC path with hostname (not drive letter or IP address) for EDIUS access to K2 storage. NOTE: You must click <i>Select</i>, browse through the network to the K2 storage device (FSM), and select the folder in order to enter the path in the standard convention.
Port	The port assigned for communication with the EDIUS XRE Server, as specified in GV STRATUS Control Panel EDIUS Settings. The default port number is 1223.
Days to keep jobs in history	As desired, the number of days to retain information about EDIUS XRE jobs. For example, enter 30 to specify 30 days.

- d) Click **OK** to save settings and close.

2. Configure XRE Monitor settings as follows:
 - a) From the Windows desktop, click **Start | All Programs | Grass Valley | XREMonitor**.
The **XREMonitor** window opens.
 - b) Click **Setting**.
The **Settings** dialog box opens.
 - c) In the tree view, click **Settings | Server settings**.
 - d) Click **Add**.
The **Server setting** dialog box opens.
 - e) Make XRE Monitor settings, as follows.

Table 2: XRE Monitor settings

Setting	Value
Server setting	<p>Name: The XRE Server name. It is recommended that you enter the machine name.</p> <p>Address: The XRE Server IP address.</p> <p>Port: The port assigned for communication with the EDIUS XRE Server, as specified in GV STRATUS Control Panel EDIUS Settings. The default port number is 1223.</p>

- f) Click **OK** and **Apply** to save settings and close.

3. Configure XRE Node settings as follows:
 - a) From the Windows desktop, click **Start | All Programs | Grass Valley | XRENode**.
 - b) From the Windows desktop system tray, right-click **XRENode** and select **Settings**.
If system tray icons are not present, verify that EDIUS licensing is complete. Missing icons can indicate the software is not licensed.
The **XRENode setting** dialog box opens.
 - c) For **Node name** enter the name of the XRE Node, as specified below.
For **Server setting**, the computer name is present by default.
 - d) Click **Setting**.
The **Settings** dialog box opens.
 - e) In the tree view, click **Settings | Server settings**.
 - f) Click **Add**.
The **Server setting** dialog box opens.
 - g) Make XRE Node settings, as follows.

Table 3: XRE Node settings

Setting	Value
Node name	As desired, enter a name for the XRE node.
Server setting	<p>Name: The local XRE Server name. It is recommended that you enter the machine name.</p> <p>Address: The local XRE Server IP address.</p> <p>Port: The port assigned for communication with the EDIUS XRE Server, as specified in GV STRATUS Control Panel EDIUS Settings. The default port number is 1223.</p>

- h) Click **OK** to save settings and close.

4. If you have EDIUS Elite workstations, on the EDIUS XRE Server configure EDIUS Plug-in settings as follows:

These settings must be the same as those on your EDIUS Elite workstations. 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 Windows desktop system tray, right-click **XRENode** and select **EDIUS Plug-in Settings**.

If system tray icons are not present, verify that EDIUS licensing is complete. Missing icons can indicate the software is not licensed.

The **Settings** dialog box opens.

- b) In the Importer/Exporter tree-view, click **K2 (SAN)**.

Server settings open.

- c) In **Server** settings, click **Add**.

The **Server Settings** dialog box opens.

- d) Select **Configure automatically** to have settings automatically populated.

This automatic configuration requires that the K2 storage location be available as a drive on the local system.

- e) Verify or make settings as follows.

Table 4: 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.
5. If you have multiple EDIUS XRE Servers, repeat the previous step only on each of your additional servers, to configure them as XRE Node Servers. Do not configure the additional servers as XRE Management Servers.

Related Topics

[Access K2 storage for EDIUS using standard convention](#)

Activate EDIUS XRE Server license

Only the EDIUS XRE Server requires this process.

This is an EDIUS license. You install it on the EDIUS XRE 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. Activate the EDIUS XRE Server license in one of the following ways:
 - If the EDIUS XRE Server is connected to the Internet, use online activation.
 - If the EDIUS XRE Server is not connected to the Internet, use offline activation.
2. Follow tasks in this section as appropriate for your choice of online or offline activation.

Activate EDIUS XRE Server license online

Only the EDIUS XRE Server requires this process.

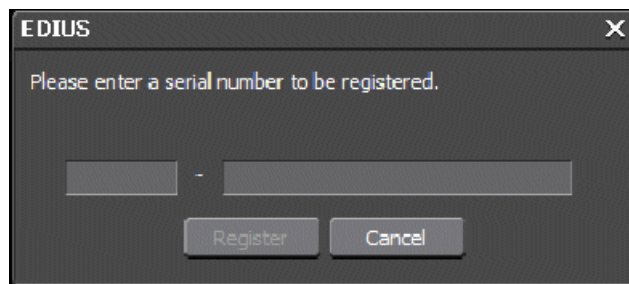
Before doing this task, verify the following:

- XRE Management Server/XRE Node and XRE Monitor (management mode) is completely installed.
- The EDIUS XRE Server has a connection to the Internet.

This is an EDIUS license. You install it on the EDIUS XRE 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. On the Windows desktop, click **Start | All Programs | Grass Valley | Serial number registration**.



2. Enter a serial number and click **Register**.

Activation is complete.

Activate EDIUS XRE Server license offline

Only the EDIUS XRE Server requires this process.

Before doing this task, verify the following:

- XRE Management Server/XRE Node and XRE Monitor (management mode) is completely installed.

This is an EDIUS license. You install it on the EDIUS XRE Server. If you use offline activation, then you must use offline deactivation if you deactivate your license in the future.

If you received your system pre-configured from Grass Valley, licenses are already installed, so you can skip these tasks. Otherwise, do the tasks in this section as follows:

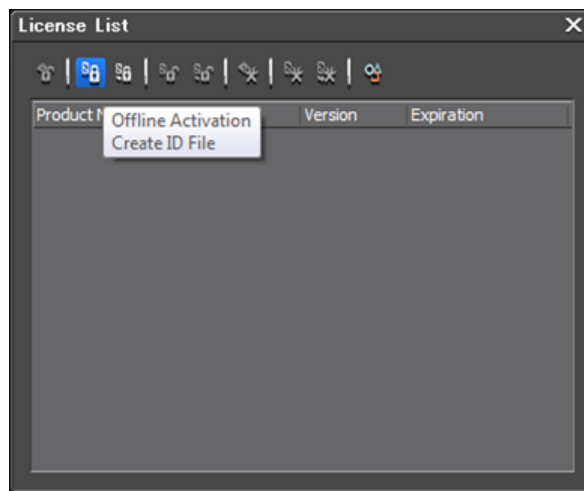
1. Create ID and Activation Agent files on the EDIUS XRE Server.
2. Copy the files to an Internet-connected PC.
3. Run EDIUS Activation Agent and generate a license file on the Internet-connected PC.
4. Copy the file to the EDIUS XRE Server.
5. Activate the software on the EDIUS XRE Server.

Create ID files

Before doing this task, verify the following:

- XRE Management Server/XRE Node and XRE Monitor (management mode) is completely installed.

1. On the EDIUS XRE Server, open **GV License Manager**.



2. Click **Offline Activation - Create ID File**.
The **Serial Input** dialog box opens.
3. Enter the serial number for activation.
The **Folder Selection** dialog box opens.

4. Select a location in which to create files.

The recommend location is `C:\XREactivate`. Create this directory if it is not already created.

The activation process creates the following files in the selected location.

- `ID.key`
- `GV ActivationServer.url`
- `EDIUSLicenseInfo.key`
- `EDIUSActivation.exe`

5. Copy the files to a removable drive.

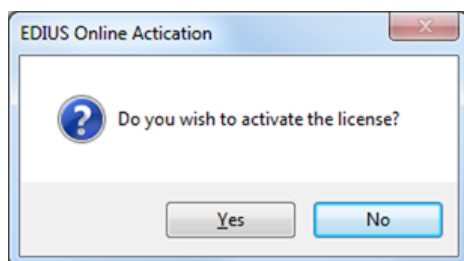
Next, run EDIUS Activation Agent.

Run EDIUS Activation Agent

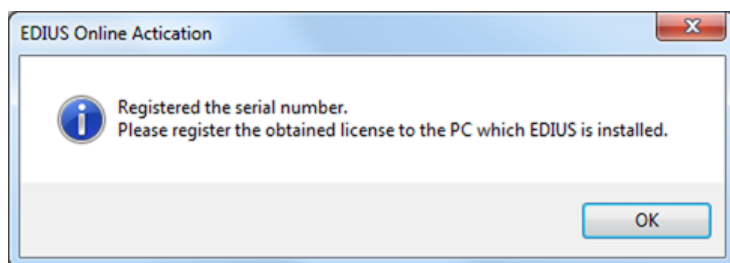
Before doing this task, you must have ID and Activation Agent files from the EDIUS XRE Server that you are activating.

1. From the removable drive, copy the files to a PC that is connected to the Internet.
2. Double-click to run `EDIUSActivation.exe`.

The **EDIUS Online Activation** dialog box opens.



3. Click **Yes** to continue.
4. When the process completes successfully, a `responseXML.xml` file is created in the same folder and a message opens.



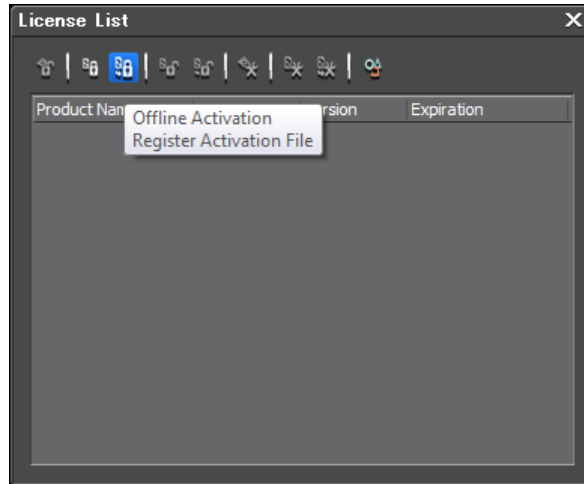
5. Copy the `responseXML.xml` file to a removable drive.

Next, active the software.

Activate the software

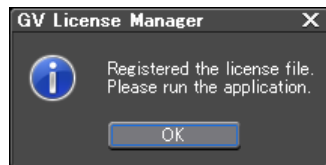
Before doing this task, you must have the *responseXML.xml* file for the EDIUS XRE Server that you are activating.

1. From the removable drive, copy the *responseXML.xml* file to *C:\XREactivate* on the EDIUS XRE Server.
2. On the EDIUS XRE Server, open **GV License Manager**.



3. Click **Offline Activation - Register Activation File**.
4. Select the *responseXML.xml* file.

The following message opens.



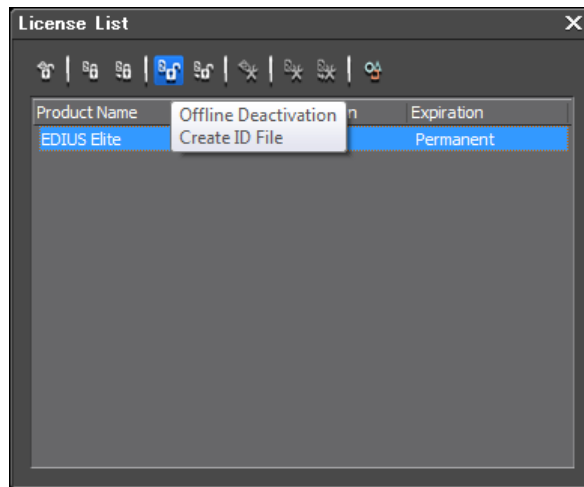
Activation is complete.

Grass Valley recommends that you copy all the files from *C:\XREactivate* to a similar folder on the Control Point PC, in case you need to re-license in the future.

Deactivate EDIUS XRE Server offline

If necessary, you can deactivate an EDIUS XRE Server that is currently activated.

1. On the EDIUS XRE Server, open **GV License Manager**.



2. Click **Offline Deactivation - Create ID File**.

The deactivation process creates the following ID files in the selected location.

- *ID.key*
- *EDIUSLicenseInfo.key*
- *EDIUSDeactivation.exe*


3. Follow a process similar to the activation steps, as follows:
 - a) Copy the ID files to a PC that is connected to the Internet.
 - b) Run *EDIUSDeactivation.exe* to create the *responseXML.xml* file.
 - c) Copy the *responseXML.xml* file to the EDIUS XRE Server you are deactivating.
 - d) Open **GV License Manager**.
 - e) Click **Offline Deactivation - Register Activation File** and select the *responseXML.xml* file.

Deactivation is complete.

If you have trouble launching EDIUS XS

Confusion about EDIUS XS and EDIUS Elite licensing can cause problems.

The following is required in order to launch 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 XS must not be licensed for EDIUS Elite.
- When launching, you must use the **EDIUS STRATUS** icon . If there is an **EDIUS** icon shortcut present, do not use it.

There are two types of EDIUS applications, as follows:

- **EDIUS XS:** This is the application that uses GV STRATUS low-resolution proxy for editing. A connection to the K2 media (iSCSI) network is not required. Its license is on the GV STRATUS Core server.
- **EDIUS Elite:** This is the application that edits K2 system high-resolution assets. The PC hosting EDIUS Elite must have its proxy access set to high resolution in GV STRATUS Control Panel and have the v: drive properly configured to access high resolution assets. Its license is on the EDIUS client PC.

Both of these applications can launch from the **EDIUS STRATUS** icon .

The same EDIUS software installation package is used to install both types of EDIUS 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 application, it detects the licensing on the client PC. If licensed for EDIUS Elite, you are prompted to logon and the EDIUS Elite application always launches. You cannot launch EDIUS XS. If not licensed for EDIUS Elite you are prompted to logon. Based on your logon, the application checks licensing on the GV STRATUS Core server. If the license includes EDIUS XS, EDIUS XS launches. Therefore, if you have ever licensed the client PC for EDIUS Elite, 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.

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 Event Viewer
 - GV STRATUS Workflow Engine
 - GV STRATUS Rules Engine
 - GV STRATUS Xcode Control Engine
 - GV STRATUS Control Panel
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_GVEventViewer_x.x.x.cab*
 - *GrassValley_STRATUS_Mediaflow_Engine_x.x.x.cab*
 - *GrassValley_STRATUS_Rules_Engine_x.x.x.cab*
 - *GrassValley_STRATUS_Transcode_Engine_x.x.x.cab*
 - *GrassValley_STRATUS_TrafficGateway_x.x.x.cab*
 - *GrassValley_Sabretooth_Application_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*

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 Grass Valley Embedded Security, put Embedded Security in Update mode.*

5. Verify that deployment tasks are set to **Install** for the files listed above.

If a WRegMon 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, 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. For transcode functionality, you can optionally install a license to control a third-party transcode application. To control the Harmonic ProMedia™ Carbon (formerly Carbon Coder™) application, install a STRATUS-XCODECONTROLCARBONCODER license. To control the Telestream Vantage™ application, install a STRATUS-XCODECONTROLVANTAGE license.

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 "GV STRATUS Release Notes" for detailed licensing procedures.
3. When you receive your license file, use SabreTooth License Manager and install it on the server.

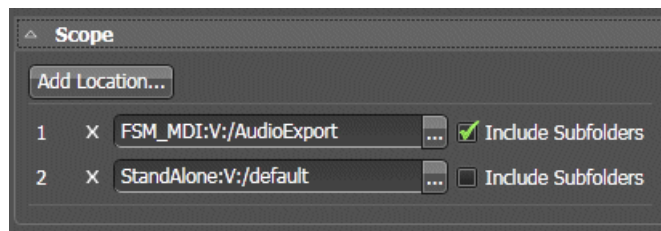
Configuring Rules


The topics in this section provide instructions for configuring GV STRATUS system rules.

Adding a delete rule

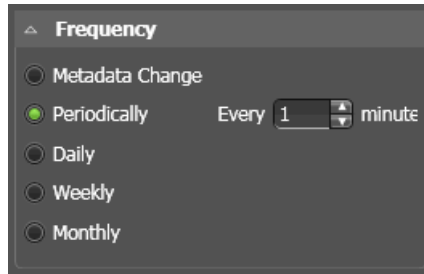
The GV STRATUS Rules Engine can watch a location and delete assets that match your criteria.

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**.
Rules 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**.
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) 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.

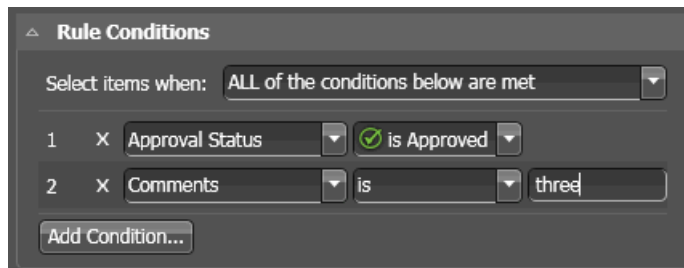


- a) Select one of the following options:

- **Metadata Change:** The rule is constantly monitoring assets in the "Scope" location.
- **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.

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, and proxy.
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.

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.

If the rule applies to newly created assets, such as those created by a scheduled record, configure **Duration | is greater than | 00:00:00.00**. This ensures the asset is ready to transfer.

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.

Adding an export rule

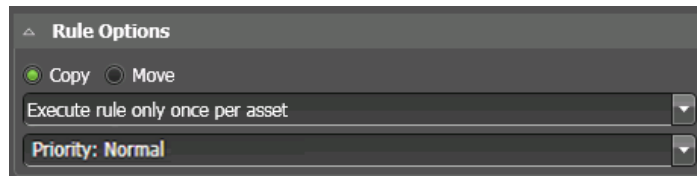
The GV STRATUS Rules Engine can watch a location that is in the GV STRATUS system and export assets that match your criteria to a location that is external to the GV STRATUS system. An export rule can export clips, subclips, and playlists. For playlists, a conform job is automatically triggered to render the complex asset as a simple clip. The Rules Engine exports the assets to the destination that you configure. If an asset already exists at the destination location, the Rules Engine appends a suffix to the asset file name so that the export can succeed without overwriting the existing asset. 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**.

Rules Editor settings open.

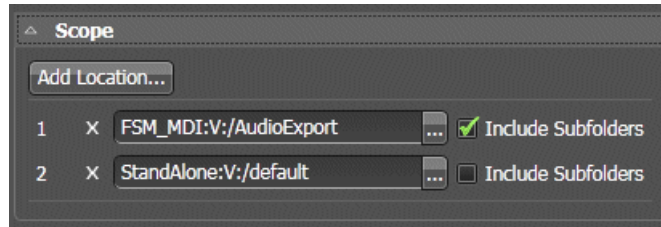
4. In the **Rule Type** drop-down list select **Export**.
5. In the **Name** field type in a name for the rule you are configuring.
6. In the **Description** field type in a description for the rule you are configuring.

7. In **Rule Options** settings, specify the rule behavior.

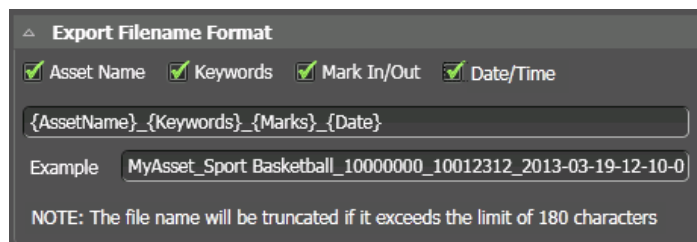


- a) Select whether the rule copies or moves the asset.
- If you select move, after the rule exports the asset, it removes the source asset from the GV STRATUS system.
- b) Select when the rule is applied each asset.
- **Execute rule only once per asset:** The rule is applied once per asset. The Rules 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.
- 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.

8. In **Scope** settings, specify the location or locations in which the rule operates.

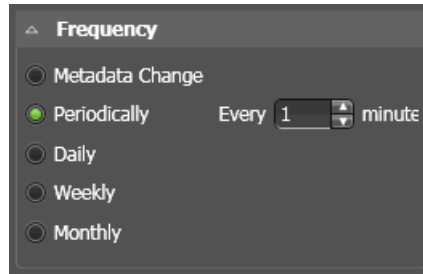


- a) Click **Add location**.
The **Location Selection** dialog box opens.
 - b) Navigate to and select the desired location.
This is the location that contains the files on which the rule operates. Every time the rule runs, it looks in this location to determine if there are any assets that match the 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 **Export Filename Format** settings, set the convention for the name of the exported file.



Asset Name is set by default, as the exported file or files must have a name.

10. In **Frequency** settings, specify how often the Rules Engine triggers the rule.

A screenshot of a software dialog box titled "Frequency". It contains five radio button options: "Metadata Change", "Periodically", "Daily", "Weekly", and "Monthly". The "Periodically" option is selected, indicated by a green dot. To the right of the "Periodically" option, there is a text label "Every" followed by a small numeric input field containing the value "1", and then the word "minute".

- a) Select one of the following options:

- **Metadata Change:** The rule is constantly monitoring assets in the "Scope" location.
- **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.

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 **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**, select as follows:

- **None**: The exported file is the same format as the source on the K2 storage system.
- **<format>**: The exported file is in the selected format.

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 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. Set all other Export Options to None to export metadata only.

d) For **Thumbnails - Marker**, select as follows:

- **None**: The export does not contain thumbnails.
- **Quality - High**: High: The export contains a full-resolution JPG thumbnail with no compression (100%).
- **Quality - Medium**: The export contains a full-resolution JPG thumbnail compressed 85%.
- **Quality - Low**: Low: The export contains a 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.

e) For **Closed Caption Format**, select as follows to additionally export a Close Caption file:

- **None**: No additional Close Caption file is exported.
- **TTML**: Close Caption information is exported to a file in TTML format.

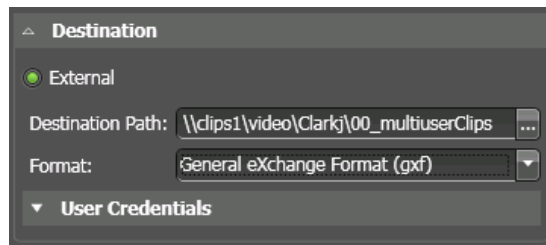
If you select a Closed Caption format, the **CC-Destination Path** field is enabled.

f) 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.


g) If you entered a **CC-Destination Path**, configure **User Credentials** for that destination.

12. 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. For an FTP path, use a `ftp://server/path` convention. For a UNC path, use a `\\server\share\path` convention.

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**.

13. 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.

14. Configure **Format** settings to select the export container format as follows:

- If in **Export Options** settings you selected a **Transcode Format**, you cannot configure **Format** settings. The selected transcode profile specifies the export container format.
- If in **Export Options** settings you set **Transcode Format** to **None**, you can configure **Format** settings as follows:
 - **None**: No video/audio assets are exported, but metadata, CC, or thumbnails are exported, as configured in Export Options.
 - **General eXchange Format (gxf)**
 - **Material eXchange Format (mxf)**
 - **QuickTime Movie (mov)**
 - **QuickTime Reference Movie (mov)**

15. 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.

16. In **Rule Conditions** settings, specify the conditions the Rules Engine looks for to qualify an asset.

17. 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.

18. 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.

If the rule applies to newly created assets, such as those created by a scheduled record, configure **Duration** | **is greater than** | **00:00:00.00**. This ensures the asset is ready to transfer.

If a newly created custom metadata field is not available in the **Add Condition** dialog, restart the GV STRATUS Control Panel application.

19. Click **Save**.

Next, enable the rule.

Related Topics

[Adding a Carbon Coder transcode profile](#) on page 74

Adding a transfer rule

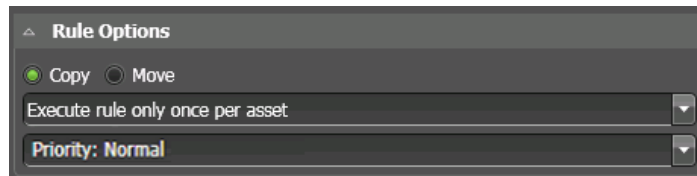
The GV STRATUS Rules Engine can watch a source location that is in the GV STRATUS system and transfer assets that match your criteria to a destination location that is also in the GV STRATUS system. The Rules Engine transfers the assets to the destination that you configure. For playlists, a conform job is automatically triggered to render the complex asset as a simple clip at the destination. If an asset already exists at the destination location, the Rules Engine appends a suffix to the asset file name so that the transfer can succeed without overwriting the existing asset.

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**.

Rules Editor settings open.

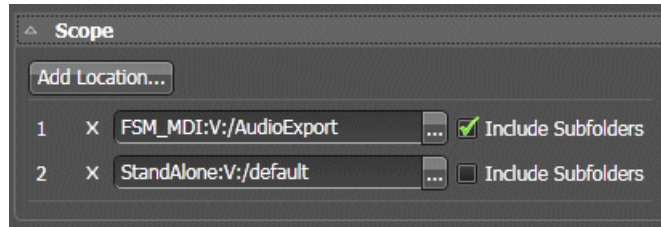
4. In the **Rule Type** drop-down list select **Transfer**.
5. In the **Name** field type in a name for the rule you are configuring.
6. In the **Description** field type in a description for the rule you are configuring.


7. In **Rule Options** settings, specify the rule behavior.

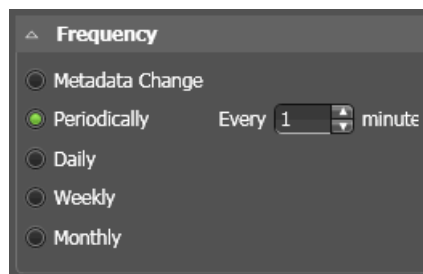


- a) Select whether the rule copies or moves the asset.
If you select move, after the rule transfers the asset, it removes the source asset from the GV STRATUS system.
- b) Select when the rule is applied each asset.
 - **Execute rule only once per asset:** The rule is applied once per asset. The Rules 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.
- 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.

8. In **Scope** settings, specify the location or locations in which the rule operates.



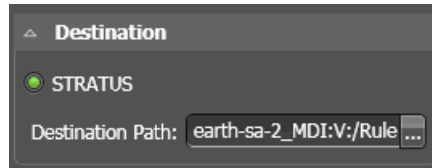
- a) Click **Add location**.
The **Location Selection** dialog box opens.
 - b) Navigate to and select the desired location.
This is the location that contains the files on which the rule operates. Every time the rule runs, it looks in this location to determine if there are any assets that match the 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 assets in the "Scope" location.
 - **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.

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.



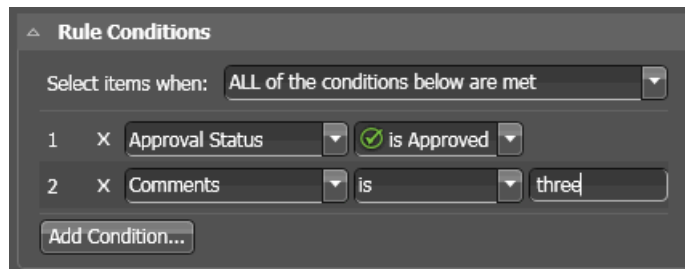
For Transfer rules, the destination must be a location in the GV STRATUS system. This is a location that is in the GV STRATUS application Navigator panel under the Locations node.

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.

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.

If the rule applies to newly created assets, such as those created by a scheduled record, configure **Duration** **I is greater than** **1 00:00:00.00**. This ensures the asset is ready to transfer.

If a newly created custom metadata field is not available in the **Add Condition** dialog, restart the GV STRATUS Control Panel application.

16. Click **Save**.

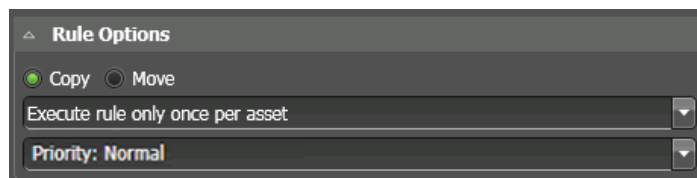
Next, enable the rule.

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.

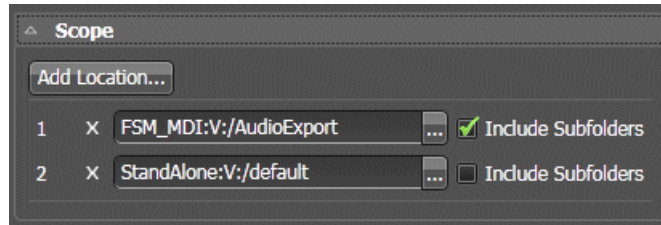
If an asset already exists at the archive destination location, the Rules Engine appends a suffix to the asset file name so that the transfer can succeed without overwriting the existing asset.

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**.
Rules 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 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.
- b) 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.
- 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.

8. 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.

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**.

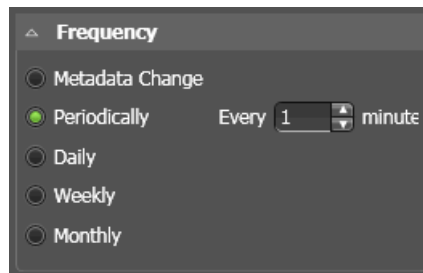
When this is selected, if there are multiple directories under the selected location, the rule operates in each of the sub-directories.

- 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.

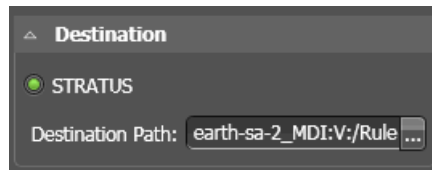


- a) Select one of the following options:

- **Metadata Change:** The rule is constantly monitoring assets in the "Scope" location.
- **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.

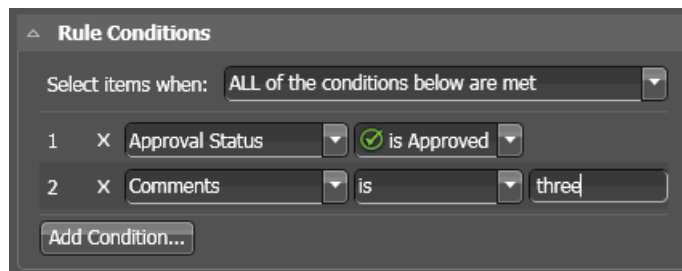
For Daily, Weekly, and Monthly options, a **Start Time** setting opens. Set the day and time the rule is triggered for the first time.

10. In **Destination** settings, specify the destination of the assets on which the rule operates.



For archive rules, only valid archive locations are available.

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.
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.

If the rule applies to newly created assets, such as those created by a scheduled record, configure **Duration** **I is greater than** **1 00:00:00.00**. This ensures the asset is ready to transfer.

If a newly created custom metadata field is not available in the **Add Condition** dialog, restart the GV STRATUS Control Panel application.

16. Click **Save**.

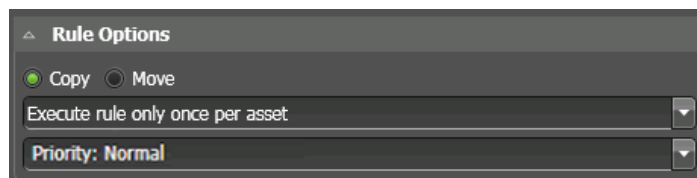
Next, enable the rule.

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. If an asset already exists at the destination

location, the Rules Engine appends a suffix to the asset file name so that the transfer can succeed without overwriting the existing asset.

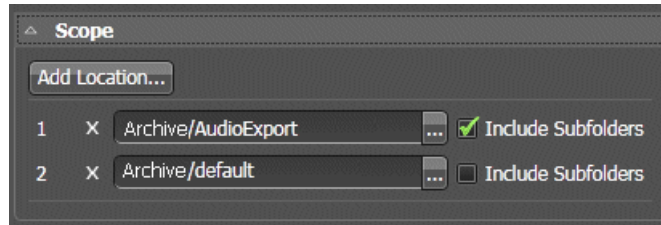
1. Log in to the GV STRATUS Control Panel application with administrator privileges.
2. In the GV STRATUS Control Panel application, click **General | Rules**.
3. Click **Add**.
Rules Editor settings open.
4. In the **Rule Type** drop-down list select **Restore**.
5. In the **Name** field type in a name 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.

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.

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**.

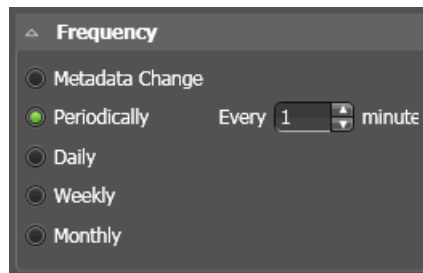
When this is selected, if there are multiple directories under the selected location, the rule operates in each of the sub-directories.

- 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.

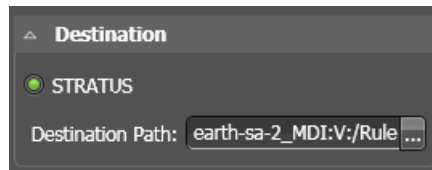


- a) Select one of the following options:


- **Metadata Change**: The rule is constantly monitoring assets in the "Scope" location.
- **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.

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.



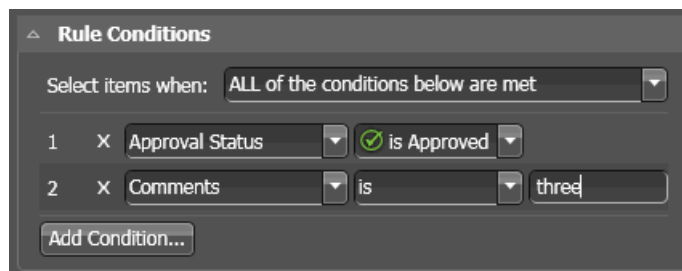
For restore rules, the destination must be a K2 system location. Assets cannot be restored to other GV STRATUS system locations.

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.

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.

If a newly created custom metadata field is not available in the **Add Condition** dialog, restart the GV STRATUS Control Panel application.

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.

If the rule applies to newly created assets, such as those created by a scheduled record, configure **Duration** | **is greater than** | **00:00:00.00**. This ensures the asset is ready to transfer.

If a newly created custom metadata field is not available in the **Add Condition** dialog, restart the GV STRATUS Control Panel application.

17. 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.

Example rule: Deleting EDIUS XS lock files

You can create a rule that periodically deletes EDIUS XS lock files. This removes the lock from assets that were a part of an EDIUS XS project, so that you can access the asset after the EDIUS XS project is done. This is an example of a typical rule.

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**.
Rules Editor settings open.
4. In the **Rule Type** drop-down list select **Delete**.
5. In the **Name** field type in `EDIUS_LOCK_DELETE` as the 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 in which the rule operates.
 - a) Click **Add location**.
The **Location Selection** dialog box opens.
 - b) Navigate to the `EDIUS_LOCK` bin on the K2 system, select the bin, and click **OK**.
The location is added to the **Scope** list.
 - c) 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.
8. In **Frequency** settings, specify how often the Rules Engine triggers the rule.
 - a) Select the following option:
 - **Daily**: Sets the number of days.A **Start Time** setting opens. Enter a time during which the system is not used, such as 3:00 AM.
9. In **Rule Options** settings, specify how the asset is deleted. Select the following option:
 - **Delete Entire Asset**: Deletes online material, archived material, and proxy.

10. In **Rule Conditions** settings, specify the conditions the Rules Engine looks for to qualify an asset.
 - a) In the **Select items when** drop down list, select the following:

- **ALL of the conditions below are met:** Assets that match all conditions.

Conditions and custom expressions are similar to those in GV STRATUS Advanced Search.

- b) For each condition (1, 2, 3, 4, etc) click the **Add Condition** button and select from lists to define the condition, as follows.

1 [Asset Type] [is List]

2 [Modified] [is before] [48 hours ago]

11. Click **Save**.

This creates a rule that runs every day at 3:00 am. The rule searches in the *EDIUS_LOCK* bin and deletes any file that was modified more than 48 hours ago.

You have now created the rule, but the rule does not run until you enable it.

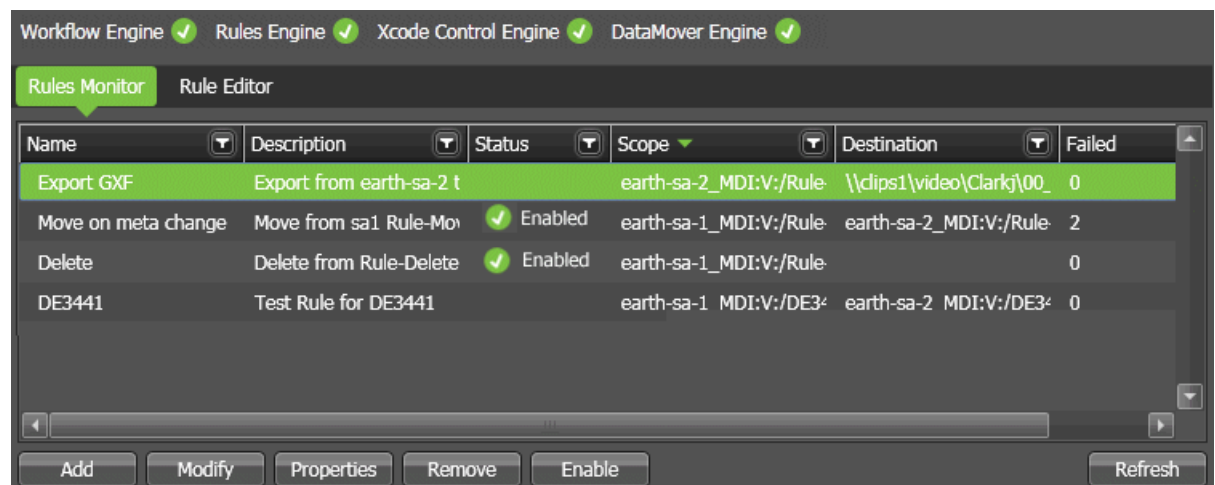
Next, enable the rule.

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 Rule Monitor list is displayed.

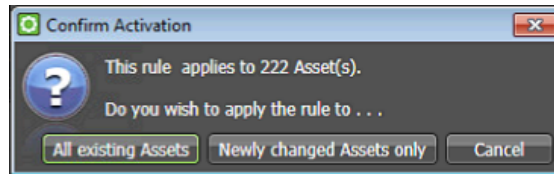


4. To disable a rule, select a rule with a Status that reports Enabled and click **Disable**.
The button toggles between Enable and Disable, depending on the status of the selected rule.

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 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.*

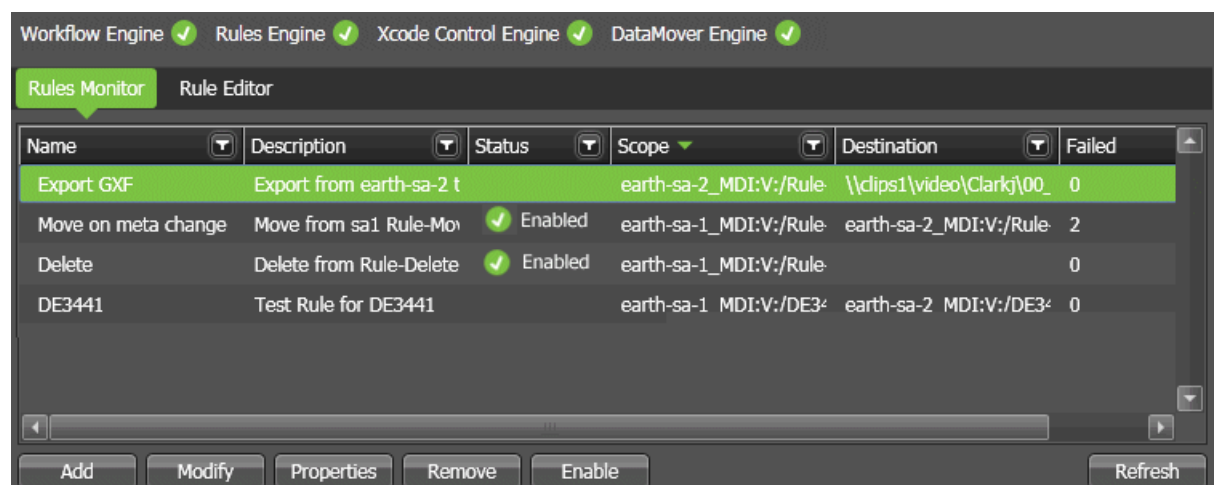
- **Newly changed Assets only:** The rule is enabled but it does not take action on existing assets. Rather, it waits until an asset changes and then evaluates the asset to take action.
- **Cancel:** The rule is not enabled.

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.

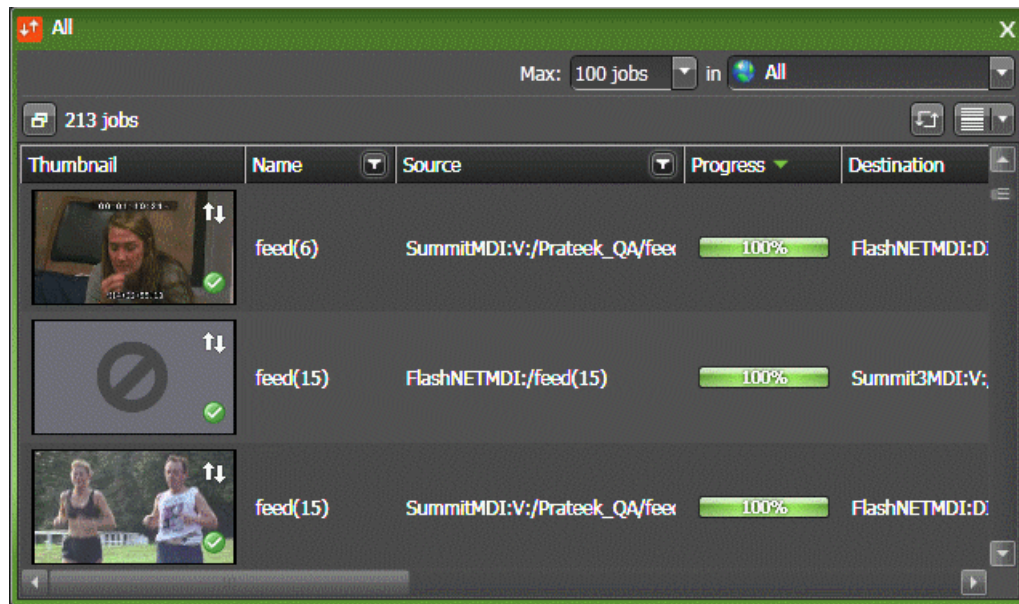
Monitoring rules

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.



2. In the GV STRATUS application, in the Navigator, 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 | 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.

3. Right-click an upcoming job and select **Cancel** to stop the GV STRATUS system from running the job.
4. Right-click completed job and select **Delete** to remove it from the list of jobs.
5. Click the **Refresh** button  if the Jobs List is not updated.

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 that have been 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 thumbnails 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 the thumbnail `tn`.

The thumbnail at the marker is exported by the export rule.

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.

At the time of this writing, the following formats are supported as source formats for transcoding by the Harmonic ProMedia™ Carbon (formerly Carbon Coder™) application:

- DV25/50
- DVCAM
- MPEG I-frame
- MPEG long GoP
- DVCPRO HD
- MPEG XDCAM
- AVC-Intra
- DNxHD

These formats are supported in PAL and NTSC. This list can change with ongoing product development. Refer to the manufacturer's product information for updates.

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.
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.

The transcode profile is added in GV STRATUS Control Panel at **General | Rules** in **Export Options** settings as a **Transcode Format**.

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.

The following formats are supported as source formats for transcoding by the Telestream Vantage™ application:

- DV25/50
- DVCAM
- MPEG I-frame
- MPEG long GoP
- DVCPRO HD
- MPEG XDCAM
- AVC-Intra
- DNxHD

These formats are supported in PAL and NTSC.

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.
 - 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 workflow.
 - 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 Vantage workflow as a transcode profile.

The transcode profile is added in GV STRATUS Control Panel at **General | Rules** in **Export Options** settings as a **Transcode Format**.

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)
NOTE: If initial (not upgrade) install, first install GV STRATUS software, then install EDIUS software.
- 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)
NOTE: If initial (not upgrade) install, first install GV STRATUS software, then install EDIUS software.

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 Elite)
- SiteConfig Roles:
 - GV STRATUS Application
 - StorNext File System Client
 - Generic iSCSI Client (non K2 only)
 - EDIUS (Required for EDIUS Elite)**NOTE: If initial (not upgrade) install, first install GV STRATUS software, then install EDIUS software.**
- 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*
 - *GenericISCI_x64_x.x.x.cab*
 - *SNFS_nonK2_x64_x.x.x.cab*
 - *EDIUS_x.x.x.cab* (Required for EDIUS Elite).**NOTE: If initial (not upgrade) install, first install GV STRATUS software, then install EDIUS software.**

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 Summit MDI (Required)
 - GV STRATUS Diva MDI (Optional)
 - GV STRATUS Event Viewer
 - GV STRATUS FlashNet MDI (Optional)
 - GV STRATUS Generic FTP MDI (Optional)
 - GV STRATUS Proxy Encoder (Optional)
 - GV STRATUS Workflow Engine (Optional)
 - GV STRATUS Rules Engine (Optional)
 - GV STRATUS Xcode Control Engine (Required only on systems with GV STRATUS Rules Engine)
 - GV STRATUS Traffic Gateway (Optional)
 - Aurora Playout 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_HttpProxyServer_x.x.x.cab*
 - *GrassValley_STRATUS_DataMover_x.x.x.cab*
 - *GrassValley_STRATUS_DIVA_MDI_x.x.x.cab*
 - *GrassValley_STRATUS_GVEventViewer_x.x.x.cab*
 - *GrassValley_STRATUS_FlashNet_MDI_x.x.x.cab*
 - *GrassValley_STRATUS_GFTP_MDI_x.x.x.cab*
 - *GrassValley_STRATUS_Summit_MDI_x.x.x.cab*
 - *GrassValley_STRATUS_Proxy_Encoder_x.x.x.cab*
 - *GrassValley_STRATUS_Mediaflow_Engine_x.x.x.cab*
 - *GrassValley_STRATUS_Rules_Engine_x.x.x.cab*
 - *GrassValley_STRATUS_Transcode_Engine_x.x.x.cab*
 - *GrassValley_STRATUS_TrafficGateway_x.x.x.cab*
 - *GrassValley_Sabretooth_Application_x.x.x.cab*
 - *AuroraPlayout_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)
 - X

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 Data Mover Engine (Required)
 - GV STRATUS Summit MDI (Required)
 - GV STRATUS Diva MDI (Optional)
 - GV STRATUS Event Viewer
 - GV STRATUS FlashNet MDI (Optional)
 - GV STRATUS Generic FTP MDI (Optional)
 - GV STRATUS Workflow Engine (Optional)
 - GV STRATUS Rules Engine (Optional)
 - GV STRATUS Xcode Control Engine (Required only on systems with GV STRATUS Rules Engine)
 - GV STRATUS Traffic Gateway (Optional)
 - Aurora Playout 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_DataMover_x.x.x.cab*
 - *GrassValley_STRATUS_DIVA_MDI_x.x.x.cab*
 - *GrassValley_STRATUS_GVEventViewer_x.x.x.cab*
 - *GrassValley_STRATUS_FlashNet_MDI_x.x.x.cab*
 - *GrassValley_STRATUS_GFTP_MDI_x.x.x.cab*
 - *GrassValley_STRATUS_Summit_MDI_x.x.x.cab*
 - *GrassValley_STRATUS_Proxy_Encoder_x.x.x.cab*
 - *GrassValley_STRATUS_Mediaflow_Engine_x.x.x.cab*
 - *GrassValley_STRATUS_Rules_Engine_x.x.x.cab*
 - *GrassValley_STRATUS_Transcode_Engine_x.x.x.cab*
 - *GrassValley_STRATUS_TrafficGateway_x.x.x.cab*
 - *GrassValley_Sabretooth_Application_x.x.x.cab*
 - *AuroraPlayout_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)

GV STRATUS Proxy server:

- SiteConfig "Add Device":
 - Family: GV STRATUS
 - Device Type: GV STRATUS Server
 - Model: GV STRATUS Proxy Server
- SiteConfig Roles:
 - GV STRATUS Event Viewer
 - GV STRATUS Proxy K2 SAN Server
 - StorNext File System Client

- Software packages:
 - *GrassValley_K2system_x.x.x.cab*, which contains the following cab files that apply to this device:
 - *GrassValleyK2Server_x64_x.x.x.cab*
 - *SNFS_x64_x.x.x.cab*
 - *GrassValley_STRATUS_GVEventViewer_x.x.x.cab*
 - *GrassValley_STRATUS_HttpProxyServer_x.x.x.cab*

The *GrassValley_CoreServer_x.x.x.cab* is not deployed.

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 Event Viewer
 - GV STRATUS Proxy Storage Server
 - StorNext File System Server
 - StorNext File System Client
- Software packages:
 - *GrassValley_K2system_x.x.x.cab*, which contains the following cab files that apply to this device:
 - *GrassValleyK2Server_x64_x.x.x.cab*
 - *SNFS_x64_x.x.x.cab*
 - *GrassValley_STRATUS_GVEventViewer_x.x.x.cab*
 - *GrassValley_STRATUS_HttpProxyServer_x.x.x.cab*

The *GrassValley_CoreServer_x.x.x.cab* is not deployed.

GV STRATUS Proxy Encoder:

- SiteConfig "Add Device":
 - Family: GV STRATUS
 - Device Type: GV STRATUS Server
 - Model: GV STRATUS Proxy Encoder or GV STRATUS Proxy Encoder (Redundant iSCSI)

- SiteConfig Roles:
 - GV STRATUS Event Viewer
 - GV STRATUS Proxy Encoder
 - StorNext File System Client
 - K2 FTP Server
 - License Manager
- Software packages:
 - *GrassValley_K2system_x.x.x.cab*, which contains the following cab files that apply to this device:
 - *GrassValleyK2Server_x64_x.x.x.cab*
 - *SNFS_x64_x.x.x.cab*
 - *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
 - *GrassValley_STRATUS_GVEventViewer_x.x.x.cab*
 - *GrassValley_STRATUS_Proxy_Encoder_x.x.x.cab*
 - *GrassValley_Sabretooth_Application_x.x.x.cab*

GV STRATUS Conform Server:

- SiteConfig "Add Device":
 - Family: GV STRATUS
 - Device Type: GV STRATUS Server
 - Model: GV STRATUS Conform Server or GV STRATUS Conform Server (Redundant iSCSI)
- SiteConfig Roles:
 - GV STRATUS Event Viewer
 - GV STRATUS Conform Engine
 - StorNext File System Client
 - K2 FTP Server
 - GV STRATUS Control Panel

- Software packages:
 - *GrassValley_K2system_x.x.x.cab*, which contains the following cab files that apply to this device:
 - *GrassValleyK2Server_x64_x.x.x.cab*
 - *SNFS_x64_x.x.x.cab*
 - *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
 - *GrassValley_STRATUS_Conform_Engine_x.x.x.cab*
 - *GrassValley_Sabretooth_Application_x.x.x.cab*
 - *GrassValley_STRATUS_GVEventViewer_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*

EDIUS XRE Server:

- SiteConfig "Add Device":
 - Family: GV STRATUS
 - NOTE: Do not select the EDIUS family.***
 - Device Type: GV STRATUS Server
 - Model: GV STRATUS EDIUS XRE Server
- SiteConfig Roles:
 - GV STRATUS Application
 - GV STRATUS Event Viewer
 - K2 FTP Server
 - StorNext File System Client
 - XRE Server

NOTE: If initial (not upgrade) install, first install GV STRATUS software, then install EDIUS software.

- Software packages:
 - *XREServer_x.x.x.cab*
 - *GrassValley_K2system_x.x.x.cab*, which contains the following cab files that apply to this device:
 - *GrassValleyK2Server_x64_x.x.x.cab*
 - *SNFS_x64_x.x.x.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_GVEventViewer_x.x.x.cab*

NOTE: If initial (not upgrade) install, first install GV STRATUS software, then install EDIUS software.

GV STRATUS Workflow Server:

- SiteConfig "Add Device":
 - Family: GV STRATUS
 - Device Type: GV STRATUS Server
 - Model: GV STRATUS Workflow Server
- SiteConfig Roles:
 - GV STRATUS Event Viewer
 - GV STRATUS Workflow Engine
 - GV STRATUS Rules Engine
 - GV STRATUS Xcode Control Engine
 - GV STRATUS Control Panel
- Software packages:
 - *GrassValley_CoreServer_x.x.x.cab*, which contains the following cab files that apply to this device:
 - *GrassValley_STRATUS_GVEventViewer_x.x.x.cab*
 - *GrassValley_STRATUS_Mediaflow_Engine_x.x.x.cab*
 - *GrassValley_STRATUS_Rules_Engine_x.x.x.cab*
 - *GrassValley_STRATUS_Transcode_Engine_x.x.x.cab*
 - *GrassValley_STRATUS_TrafficGateway_x.x.x.cab*
 - *GrassValley_Sabretooth_Application_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*

Summary of previous 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

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

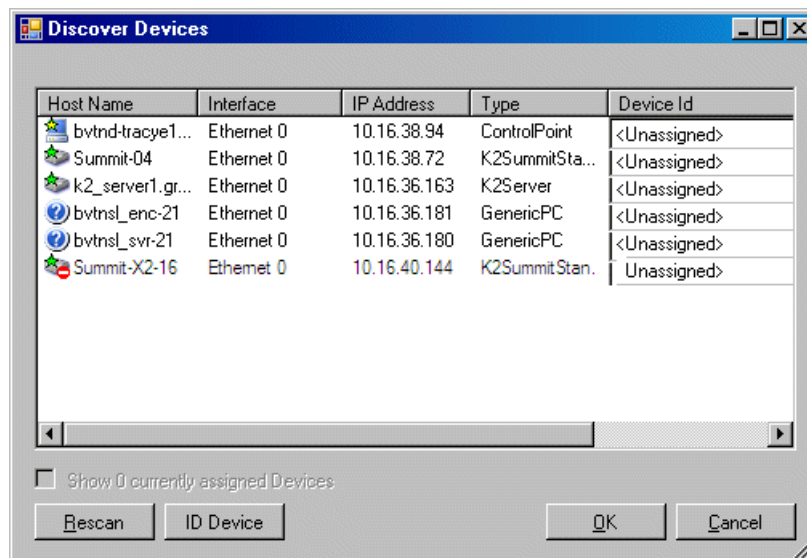
Prerequisites for this task are as follows:

- The Ethernet switch or switches that support the control network are configured and operational. If multiple switches, ISLs are connected and trunks configured.
- The PC that hosts SiteConfig is communicating on the control network.
- There are no routers between the PC that hosts SiteConfig and the devices to be discovered.
- Devices to be discovered are Windows operating system devices, with SiteConfig support installed.
- Devices are cabled for control network connections.
- If discovering a device with Microsoft Windows Server 2008 operating system, the device must have an IP address, either static or DHCP supplied.

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

Prerequisites for this task are as follows:

- Devices have been discovered by SiteConfig
- Discovered devices are not yet assigned to a device in the system description
- The system description has 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

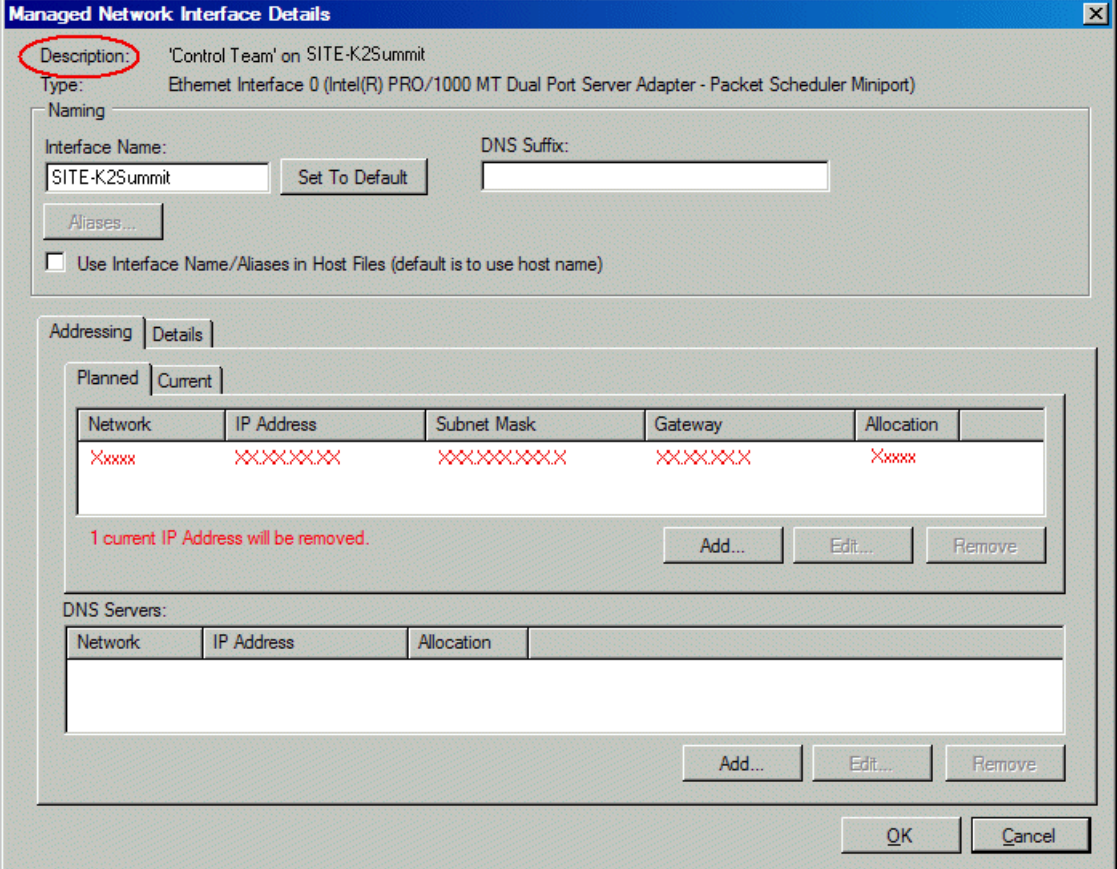
Prerequisites for this task are as follows:

- The physical device you are configuring has been discovered and is assigned to a device in the SiteConfig system description.
- SiteConfig has communication with the device.
- The device is 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.



The dialog box is titled "Managed Network Interface Details". It has a blue title bar with a close button. The main content area is divided into several sections:

- Description:** A red circle highlights the "Description:" label. The text next to it is "'Control Team' on SITE-K2Summit".
- Type:** The text next to it is "Ethernet Interface 0 (Intel(R) PRO/1000 MT Dual Port Server Adapter - Packet Scheduler Miniport)".
- Naming:**
 - Interface Name:** A text box containing "SITE-K2Summit". To its right is a "Set To Default" button.
 - DNS Suffix:** An empty text box.
 - Aliases...** A button below the Interface Name field.
 - ☐ Use Interface Name/Aliases in Host Files (default is to use host name)
- Addressing:** A tabbed section with "Planned" and "Current" tabs.
 - Planned:** A table with columns: Network, IP Address, Subnet Mask, Gateway, Allocation. The first row contains red "X" placeholders.

Network	IP Address	Subnet Mask	Gateway	Allocation
Xxxxx	XXXXXXXX	XXXXXXXX	XXXXXXXX	Xxxxx
 - Current:** A red message says "1 current IP Address will be removed." Below this are "Add...", "Edit...", and "Remove" buttons.
- DNS Servers:** A table with columns: Network, IP Address, Allocation. It is currently empty.

Network	IP Address	Allocation
---------	------------	------------

At the bottom right are "Add...", "Edit...", and "Remove" buttons for the DNS Servers table. At the very bottom are "OK" and "Cancel" buttons.

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.

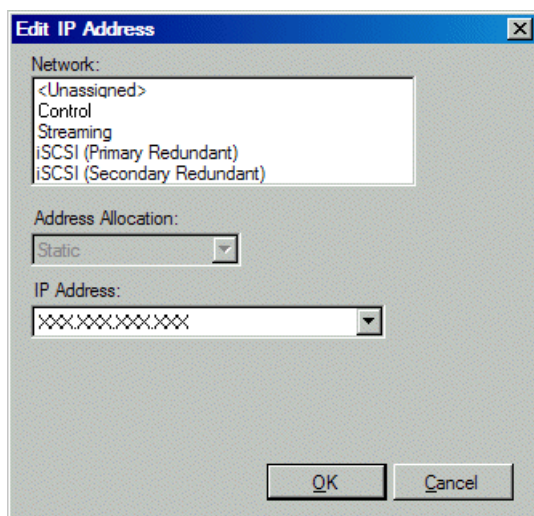
5. Configure naming settings as follows:

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	<i>Unselected</i> 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	<i>Control</i> is required
Address Allocation	<i>Static</i> 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

Prerequisites:

- The devices you are pinging are 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

Prerequisites:

- The device you are verifying is in the SiteConfig system description and is 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.

Generating host tables using SiteConfig

Prerequisites for this task are as follows:

- Planned control network settings are applied to control network interfaces and devices are 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, have settings applied and are communicating.
- You have viewed host names, as currently defined in the system description, and determined that they are correct.
- The SiteConfig PC is 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.

Trademarks and Agreements

Trademarks

Grass Valley, GV STRATUS, GV Director, K2, Aurora, Summit, ChannelFlex, Dyno, Solo, ClipStore, Infinity, Turbo, Profile, Profile XP, NetCentral, NewsBrowse, NewsEdit, NewsQ, NewsShare, NewsQ Pro, and Media Manager are either registered trademarks or trademarks of Grass Valley USA, LLC. in the United States and/or other countries. GRASS VALLEY® is a registered trademark. Grass Valley USA, LLC. products are covered by U.S. and foreign patents, issued and pending. Additional information regarding Grass Valley USA, LLC. trademarks and other proprietary rights may be found at www.grassvalley.com. Other trademarks and logos used in this document are either registered trademarks or trademarks of the manufacturers or vendors of the associated products, 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. AVCHD and the AVCHD logo are trademarks of Panasonic Corporation and Sony Corporation. Avid DNxHD is a registered trademark of Avid Technology, Inc., a Delaware corporation.



JPEG acknowledgment

This software is based in part on the work of the Independent JPEG Group.