

# **K2 Summit Production Client and K2 SAN Version 7.0.13 Release Notes & Upgrade Instructions**

These release notes contain the most recent information and supersede previous publications, as of 13 October 2009. Check the Grass Valley website at [www.grassvalley.com/docs](http://www.grassvalley.com/docs) for an updated version that contains additional important information.

These release notes contain information for the following:

- K2 Summit Production Clients with internal storage
- K2 Summit Production Clients with direct-connect storage
- The K2 Storage Area Network (SAN) with connected shared storage K2 Summit Production Clients

## **Documentation path to install K2 client with internal storage**



## **Documentation path to install K2 client with shared or direct-connect storage**



\*Cabling Guide packed with RAID primary chassis

Copyright © Grass Valley, Inc. All rights reserved. Printed in the United States of America. Portions of software © 2000 – 2009, Microsoft Corporation. All rights reserved. This document may not be copied in whole or in part, or otherwise reproduced except as specifically permitted under U.S. copyright law, without the prior written consent of Grass Valley, Inc., P.O. Box 59900, Nevada City, California 95959-7900. This product may be covered by one or more U.S. and foreign patents.

Product options and specifications subject to change without notice. The information in this manual is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Grass Valley, Inc. Grass Valley, Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in this publication.

Grass Valley, K2, Aurora, Summit, Solo, Dyno, Turbo, M-Series, Profile, Profile XP, NetCentral, NewsBrowse, NewsEdit, NewsQ, NewsShare, NewsQ Pro, and Media Manager are either registered trademarks or trademarks of Grass Valley, Inc. in the United States and/or other countries. Grass Valley, Inc. products are covered by U.S. and foreign patents, issued and pending. Additional information regarding Grass Valley, Inc.'s trademarks and other proprietary rights may be found at [www.grassvalley.com](http://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.

# Contents

Grass Valley Product Support.....	4
Release note revisions for this release.....	6
Release Summary.....	7
Version compatibility.....	9
Compatible K2 Summit Production Client components.....	9
Compatible K2 Media Server components.....	10
Compatible K2 Control Point PC components.....	10
Compatible HP ProCurve GigE switch components.....	11
Compatible K2 Lx0 RAID components.....	11
Compatible K2 Lx0 RAID disk drive microcode.....	13
Compatible Grass Valley products.....	14
Compatible K2 FCP Connect components.....	15
Compatible recovery applications.....	15
Upgrading K2 systems.....	16
Upgrading a K2 SAN.....	16
About upgrading the K2 SAN with SiteConfig.....	16
Make recovery images.....	16
Prepare SiteConfig for software deployment to K2 SAN devices.....	17
Deploy control point PC software.....	17
Take SAN clients offline.....	18
Manage multiple K2 Media Servers.....	19
Upgrade K2 Media Server.....	19
Upgrade K2 client.....	25
Upgrade Aurora Edit, Ingest, and Playout systems.....	29
Upgrade NAS systems.....	29
Upgrade Browse and MediaFrame systems.....	30
Upgrade other SAN clients.....	30
Make recovery images.....	30
Managing stand-alone K2 clients with SiteConfig.....	31
SiteConfig and stand-alone K2 clients checklist.....	31
System requirements for SiteConfig control point PC.....	32
About installing SiteConfig.....	33
Installing/upgrading SiteConfig.....	33
Creating a system description for stand-alone K2 clients.....	35
Creating the control network for stand-alone K2 clients.....	36
Creating the FTP/streaming network for stand-alone K2 clients (optional).....	38
Adding a group.....	39
Adding stand-alone K2 clients to the system description.....	39
Modifying stand-alone K2 client unassigned (unmanaged) interfaces.....	40
Discovering devices with SiteConfig.....	42
Assigning discovered devices.....	43
Modifying stand-alone K2 client managed network interfaces.....	44
Adding a control point PC placeholder device to the system description.....	49
Assigning the control point PC.....	50
Making the host name the same as the device name.....	51
Pinging devices from the control point PC.....	51
About hosts files and SiteConfig.....	51
Generating host tables for devices with SiteConfig.....	52

Configuring deployment groups.....	53
About deploying software for stand-alone K2 clients.....	54
Upgrading stand-alone K2 clients with SiteConfig.....	54
About upgrading stand-alone K2 clients with SiteConfig.....	55
Make recovery images.....	55
Prepare for K2 client upgrade.....	56
Configure SNFS default.cfg file on K2 client.....	56
Prepare SiteConfig for software deployment to stand-alone K2 clients.....	57
Check all currently installed software on stand-alone K2 clients.....	57
Add software package to deployment group for stand-alone K2 clients.....	58
Unlock K2 Summit Production Clients.....	59
Upgrade software on stand-alone K2 clients.....	59
Upgrade K2 Dyno Server software.....	61
Lock K2 Summit Production Clients.....	62
Upgrade K2 Dyno Controller.....	63
Make recovery images.....	64
Deploy control point PC software.....	64
Upgrading stand-alone K2 clients without SiteConfig.....	64
Make recovery images.....	65
Prepare for K2 client upgrade.....	65
Disable write filter.....	65
Configure SNFS default.cfg file on K2 client.....	66
Uninstall K2 software from K2 Client.....	67
Install K2 software.....	67
Verify upgraded software.....	70
Upgrade K2 Dyno Server software.....	70
Upgrade remaining K2 clients.....	71
Enable write filter.....	71
Upgrade K2 Dyno Controller.....	72
Make recovery images.....	73
Licensing K2 products.....	73
Additional notes.....	78
Managing the write filter.....	78
Passwords and security on K2 systems.....	80
Running Check Disk.....	82
Running diagnostics for K2 Summit Production Client.....	82
K2 FCP Connect.....	84
About K2 FCP Connect.....	84
Install and configure Macintosh Final Cut Pro systems on a K2 SAN.....	84
Using Final Cut Pro on a K2 SAN.....	106
Maintaining K2 FCP Connect.....	107
Operation considerations.....	110
Known Problems.....	111

# Grass Valley Product Support

To get technical assistance, check on the status of a question, or to report a new issues, contact Grass Valley Product Support via e-mail, the Web, or by phone or fax.

## Web Technical Support

To access support information on the Web, visit the product support Web page on the Grass Valley Web site. You can download software or find solutions to problems.

**World Wide Web:** <http://www.grassvalley.com/support/>

**Technical Support E-mail Address:** [gvgtechsupport@grassvalley.com](mailto:gvgtechsupport@grassvalley.com)

## Telephone Support

Use the following information to contact Product Support by phone.

## International Support Centers

Our international support centers are available 24 hours a day, 7 days a week.

Support Center	Toll free	In country
France	+800 80 80 20 20	+33 1 48 25 20 20
United States	+1 800 547 8949	+1 530 478 4148

## Authorized Local Support Representative

A local support representative may be available in your country. To locate a support center during normal local business hours, refer to the following list. This list is regularly updated on the website for Grass Valley Product Support

(<http://www.grassvalley.com/support/contact/phone/>)

After-hours local phone support is also available for warranty and contract customers.

Region	County	Telephone
Asia	China	+86 10 5883 7575
	Hong Kong, Taiwan, Korea, Macau	+852 2531 3058
	Japan	+81 3 6848 5561
	Southeast Asia - Malaysia	+603 7492 3303

<b>Region</b>	<b>County</b>	<b>Telephone</b>
	Southeast Asia - Singapore	+65 6379 1769
	Indian Subcontinent	+91 11 515 282 502; +91 11 515 282 504
Pacific	Australia, New Zealand	+61 1300 721 495
Central America, South America	All	+55 11 5509 3440
North America	North America, Mexico, Caribbean	+1 800 547 8949; +1 530 478 4148
Europe	UK, Ireland, Israel	+44 118 923 0499
	Benelux – Netherlands	+31 (0) 35 62 38 421
	Benelux – Belgium	+32 (0) 2 334 90 30
	France	+800 80 80 20 20; +33 1 48 25 20 20
	Germany, Austria, Eastern Europe	+49 6150 104 444
	Belarus, Russia, Tadzhikistan, Ukraine, Uzbekistan	+7 095 258 09 20; +33 (0) 2 334 90 30
	Nordics (Norway, Sweden, Finland, Denmark, Iceland)	+45 40 47 22 37
	Southern Europe – Italy	+39 02 24 13 16 01; +39 06 87 20 35 42
	Southern Europe – Spain	+34 91 512 03 50
Middle East, Near East, Africa	Middle East	+971 4 299 64 40
	Near East and Africa	+800 80 80 20 20; +33 1 48 25 20 20

## Release note revisions for this release

This release of software has multiple versions of release notes, as follows:

Part number	Description
071-8630-02	Initial release notes for K2 7.0.13 software
071-8630-03	K2 FCP Connect topics added/modified, with the following changes: <ul style="list-style-type: none"><li>• <a href="#">Final Cut Pro on K2 SAN quick start installation checklist</a> on page 84 updated with additional steps. This topic replaces the document "K2 Final Cut Pro Connect Quick Start Guide".</li><li>• <a href="#">Configure Macintosh hosts files</a> on page 88 updated with Apple host file requirements.</li><li>• Topics <a href="#">Compatible K2 FCP Connect components</a> on page 15, <a href="#">Configure Macintosh systems for Active Directory Domain</a> on page 90, <a href="#">Enable Access Control Lists on the K2 Media Server (FSM)</a> on page 96, <a href="#">Verify bandwidth of SAN connection</a> on page 101, <a href="#">Verify Access Control Lists</a> on page 102, and <a href="#">Connecting via SAMBA/CIFS</a> on page 104 added. These topics replace the document "Enabling Cross Platform ACL support for Windows and Mac Active Directory Users".</li></ul> <p><a href="#">Known Problems</a> on page 111 updated with CR105208, CR106979, and CR101794. CR106071 removed.</p>

---

# Release Summary

## What's new in version 7.0.13

### Version 7.0.13

- **K2 Media Servers** — Dell PowerEdge R710 and R610 are supported as K2 Media Server platforms.
- **Live Production option** — In K2Config, you can now create a Live Production K2 SAN. This type of SAN has a shorter minimum delay between start record and start playout when the record and play are on different SAN K2 Summit Production Clients. To support this feature, the K2 SAN must be sized for increased bandwidth. Contact your Grass Valley representative for specifications relative to your needs.

## Feature limitations in this release

- Security on AppCenter bins is not implemented.
- No nested bin support with Aurora applications.
- Mix effects (an AppCenter Pro feature) are supported as follows:
  - Supported between like formats: DV-to-DV, MPEG-to-MPEG, etc. Not supported between different formats.
  - Not supported for MPEG long GoP.
- There is no centralized logging of the K2 SAN. Logs are stored on each individual device.

## Not supported in this release

The following devices and functionality are not supported in this release.

- K2 Media Client
- AVC-Intra

## Changes and features in previous releases

The following sections describe changes and features in past releases.

### Version 7.0.12

- **K2 Dyno Reply Controller** — For live event replay, the K2 Dyno Replay System includes a K2 Dyno Controller and a K2 Summit Product Client.
- **Final Cut Pro support** — K2 FCP Connect is a licensable feature that allows your Macintosh Final Cut Pro system to become a K2 SAN iSCSI client. This enables edit in place functionality for K2 media via QuickTime reference files. Supports DV, IMX, HD, and XDCAM formats. Refer to the section later in these release notes for more information.

### Version 7.0.11

- **K2 Summit Production Client** — This new product is a SD/HD K2 client for replay in sports, news, live, and live-to-tape applications. Its features are similar to the current K2 Media Client. New or modified features are documented in these release notes.
  - **Live Play** — Extremely fast record-to-plaintext performance. Also known as Chase Play. Playout to within ½ second of record point.
  - **DV formats** — Supports the DV25, DV50, and DV100 (DVCPROHD) P2 acquisition formats natively. Does not support MPEG.
  - **Transition effects** — Dissolves and audio fades can be assigned to clip playout transitions. This is an AppCenter Pro feature.
  - **Graphical User Interface design** — AppCenter has a gray/brown color scheme with improved buttons and fonts.
  - **Media file system** — The file system with this release allows nested bins for better media management and is supported on the K2 Summit Production Client only. It is not supported on the K2 Media Client.
  - **Write filter** — A file-based write filter prevents accidental or unintended changes. It must be disabled before changes are made and enabled after changes are made.
  - **Metadata server role** — The role of metadata server replaces the role of media database server for a K2 Media Server. The metadata server role is required to support the media file system with this release.
  - **AppCenter Video Monitor** — Active video is provided on a locally connected VGA monitor for AppCenter channels. You can also select the AppCenter view to display a four pane active video monitor of all four channels. This is an AppCenter Pro feature.
  - **Modular channels** — Codec and real-time functionality is combined on a two channel module, allowing for two and four channel options.
  - **CompactFlash** — The system drive is CompactFlash.



# Version compatibility

Versions qualified for compatibility with this version 7.0.13 release of K2 software are summarized in the following sections.

## Compatible K2 Summit Production Client components

The following components reside on the K2 Summit Production Client and are compatible with this release of K2 software as listed in the following table. Compatible versions are pre-installed on the K2 Summit Production Client when you receive it new from Grass Valley.

Component	Version	Comments
GrassValley K2 Client software	7.0.13	Includes AppCenter
Media File System (SNFS)	3.1.2.RC25225.6138	—
SiteConfig Discovery Agent, also known as SiteConfig	1.0.8	This version is still compatible
Network Configuration Connect Kit	1.1 and higher	Upgrade to this version is enforced when deploying software with SiteConfig version 1.1 and higher
Windows Operating System	Windows XP embedded 2002 SP3	—
Microsoft .NET Framework	2.0 SP2, 3.0 SP2, 3.5 SP1	—
QuickTime	7.0 and higher	—
Intel Graphics Media Accelerator Driver	—	—
Intel Network Connections	13.3	—
MegaRAID Storage Manager	2.35-01	—
Microsoft iSCSI Initiator	—	—
MS XML	4.0 SP2 6.0	—

## Compatible K2 Media Server components

The following components reside on the K2 Media Server and are compatible with this release of K2 software as listed in the following table. Compatible versions are pre-installed on the K2 Media Server when you receive it new from Grass Valley.

Component	Version	Comments
Grass Valley K2 Server software	7.0.13	—
Media File System (SNFS)	3.1.2.RC25225.6138	—
SiteConfig Discovery Agent, also known as SiteConfig	1.0.8	This version is still compatible
Network Configuration Connect Kit	1.1 and higher	Upgrade to this version is enforced when deploying software with SiteConfig version 1.1 and higher
Windows Operating System	Windows 2003 Server	With the latest update
Microsoft .NET Framework	2.0 SP2, 3.0 SP2, 3.5 SP1	—
QuickTime	7.0 and higher	—
Adobe Acrobat Reader	7.0 and higher	—
ATI Display Driver	8.24.3.0	—
Dell OpenManage	5.3.0	—
J2SE Runtime Environment	6, Update 3	—
MSXML	4.0 and higher	—

## Compatible K2 Control Point PC components

The following components reside on the K2 Control Point PC and are compatible with this release of K2 software as listed in the following table. Compatible versions are pre-installed on the K2 Control Point PC when you receive it new from Grass Valley.

Software	Version	Comments
K2 control point	7.0.13	—
Windows operating system	Server 2003 SP 1	—
NetCentral	5.0	—
SQL Server Express	2005	—
.NET Framework	1.1, 1.1 Hotfix, 3.5 SP1	—

Software	Version	Comments
QuickTime	7	—
MS XML	4.0	—
Windows Installer	3.1	—
SiteConfig Discovery Agent, also known as SiteConfig Network Configuration Connect Kit	1.0.8	This version is still compatible
	1.1 and higher	Upgrade to this version is enforced when deploying software with SiteConfig version 1.1 and higher
7-ZIP	—	—
Adobe Reader	9.0	—

## Compatible HP ProCurve GigE switch components

Components that reside on the the HP ProCurve 3400cl series GigE switch and the HP ProCurve 29xx series GigE switch are compatible with this release of K2 software as follows:

Product	Version	Comments
HP ProCurve 3400cl series firmware	M.08.66	This older version is still compatible
	M.08.86	Upgrade to this version is recommended
HP ProCurve 2900 series firmware	T.11.12	This older version is still compatible
	T.13.23	Upgrade to this version is recommended

## Compatible K2 Lx0 RAID components

This compatibility specification applies to the K2 RAID device on a Level 10, Level 20, Level 30 and Level 35 (both basic and redundant) K2 SAN. RAID firmware is compatible with this release of K2 software as follows:

Component	Version	File Name	Comments
Level 10/20 controller firmware for primary chassis with 15K SAS	07VS	D1_07VS.BIN	This version is still compatible
	07VV	D1_07VV.BIN	Upgrade to this version is recommended

---

## Version compatibility

Component	Version	File Name	Comments
drives or SATA drives			
Level 10/20 controller firmware for expansion chassis with 15K SAS drives or SATA drives	030F	ENCL_030F.BIN	This version is still compatible
	050B	ENCL_050B.BIN	Upgrade to this version is recommended
Level 10/20 controller firmware for primary chassis with 7.2K SAS drives	07VV	D1_07VV.BIN	7.2K SAS drives are used in K2 Production Storage and K2 Nearline Storage.
Level 10/20 controller firmware for expansion chassis with 7.2K SAS drives	050B	ENCL_050B.BIN	
Level 30/35 controller firmware for primary chassis with 15K SAS drives or SATA drives	07VS	D3_07VS.BIN	This version is still compatible
	07VV	D3_07VV.BIN	Upgrade to this version is recommended
Level 30/35 controller firmware for expansion chassis with 15K SAS drives or SATA drives	030F	ENCL_030F.BIN	This version is still compatible
	050B	ENCL_050B.BIN	Upgrade to this version is recommended
Level 30/35 controller firmware for primary chassis with 7.2K SAS drives	07VV	D3_07VV.BIN	7.2K SAS drives are used in K2 Production Storage and K2 Nearline Storage.
Level 30/35 controller firmware for expansion chassis	050B	ENCL_050B.BIN	

Component	Version	File Name	Comments
with 7.2K SAS drives			

Find firmware on the K2 client (for direct-connect storage) or the K2 Media Server (for shared storage) at `C:\profile\microcode\NEC\Condor`.

## Compatible K2 Lx0 RAID disk drive microcode

This compatibility specification applies to the K2 RAID device on a Level 10, Level 20, Level 30 and Level 35 K2 SAN. Disk drive microcode is compatible with this release of K2 software as summarized in the following table:

Disk Drive	Microcode Type	Microcode Version	Microcode File Name	Comments
73G 15K SAS	Interface	0002	CT15K5SAS.01_	—
	Servo	0002	CT15K5SAS_73_1	
146G 15K SAS	Interface	0002	CT15K5SAS.01_	—
	Servo	0002	CT15K5SAS_146_1	
300G 15K SAS	Interface	0002	CT15K5SAS.01_	—
	Servo	0002	CT15K5SAS_300_1	
450G 15K SAS <sup>1</sup>	—	0004	CH_15K6_SAS.0004	This version is still compatible.
	—	N005	CH_15K6_SAS.N005	Upgrade to this version is recommended.
500G 7.2K SAS	Interface	N001	BA_7K_ Interface.N001	—
	Servo	N001	BA_7K_ ST3500620SS_ Servo.C30D	
1TB 7.2K SAS	Interface	N001	BA_7K_ Interface.N001	—
	Servo	N001	BA_7K_ ST31000640SS_ Servo.B30D	

Be aware that Storage Utility can report inconsistent disk drive microcode versions. This can be a normal condition, since the RAID system supports multiple drive

<sup>1</sup> This type of microcode has a single microcode file, rather than separate Interface and Servo files.

capacities and microcode versions. Be sure to compare the version numbers with this table, and update only as required.

Be aware that Storage Utility can report inconsistent disk drive microcode versions. This can be a normal condition, since the RAID system supports multiple drive capacities and microcode versions. Be sure to compare the version numbers with this table, and update only as required.

Find microcode on the K2 client (for direct-connect storage) or the K2 Media Server (for shared storage) at `C:\profile\microcode\NEC\Seagate`.

## Compatible Grass Valley products

Grass Valley products are compatible with this version 7.0.13 release of K2 software as follows:

Product	Version	Comments
K2 Dyno Replay Controller	1.1.0	—
Aurora Browse	6.5.1 or 6.5.2	Check with your Grass Valley representative for version availability
Aurora Edit	6.5.1 or 6.5.2	
Aurora Ingest	6.5.1 or 6.5.2	
Aurora Payout	6.5.1 or 6.5.2	
Profile XP Media Platform	5.4.8 or higher	Media assets can be transferred to/from a Profile XP system.
NetCentral	5.0.0	—
SiteConfig application	1.1 or higher	—
UIM	2.1.1	—
K2 InSync	4.0.2	Check with your Grass Valley representative for version availability
K2 Avid plug-in	1.0.0	On the Avid Editor install the <i>K2AvidIngest</i> module and on the device that runs the Avid Transfer Manager/Interplay Engine install the <i>K2AvidDhm</i> module.
K2 FCP Connect	3.3.0	—

## Compatible K2 FCP Connect components

The following components are compatible when integrating K2 systems and Macintosh systems using K2 FCP Connect.

Component	Product/Version	Comments
K2 software	7.0.12 or higher	—
K2 Media File System (SNFS) software	3.1.2.RC25225.6138	—
K2 RAID	K2 Lx0 RAID (Condor)	Level 2 and Level 3 K2 RAID not supported.
Macintosh system	Mac Pro with Intel Processor, two GigE ports	—
Macintosh operating system	OS X 10.5.6	—
Final Cut Pro software	6.0.5 or higher	—
Apple Xsan software	2.1	—

## Compatible recovery applications

To create a recovery image of a K2 device, use compatible versions of the recovery application, as follows:

Product	Recovery application and version	Comments
K2 Summit Production Client	Recovery Flash Drive part number 86205900	Use the Recovery Flash Drive that you received with the product. It is identified with the product's serial number and is to be used on that specific K2 Summit Production Client only.
K2 Media Server	Recovery CD part number 063-8246-04	—
Grass Valley Control Point PC	Recovery CD part number 063-8246-04	—

# Upgrading K2 systems

This section contains the tasks necessary for the upgrade to this release of software.

## Upgrading a K2 SAN

This section contains the tasks necessary to upgrade a K2 SAN to this release of K2 software. Work through the tasks sequentially to complete the upgrade.

**NOTE:** *These upgrade instructions assume that the current K2 software is at version 7.0.11 or 7.0.12 and that you are upgrading to a higher version of 7.0.x software. If the current K2 software is a 7.x version lower than 7.0.11, contact Grass Valley Support before upgrading. If a K2 Media Client or any K2 device with current K2 software at a 3.x version, do not upgrade, as version 7.x is not supported on these devices*

## About upgrading the K2 SAN with SiteConfig

These topics apply to K2 SANs with instructions to upgrade software on the following K2 SAN devices.

- K2 Media Servers

With these upgrade instructions, you use SiteConfig from a network connected control point PC and remotely upgrade software simultaneously on multiple K2 devices. This is the required process for software upgrades. Do not upgrade software on a K2 SAN locally at each device or via any other process.

**NOTE:** *Do not attempt to upgrade software incrementally across the devices of a K2 SAN while media access is underway. Online software upgrading is not supported.*

The following installation tasks provide information specifically for the upgrade to this 7.0.13 version of software. Read the information in these sections carefully before attempting any upgrade to software on any of the devices of a K2 SAN, including K2 systems, Aurora Edit systems, or other clients.

## Make recovery images

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.

Refer to the K2 product's *Service Manual* for recovery image procedures.

**⚠ CAUTION:** *If you upgrade and then decide you do not want to stay with this version of K2 system software, you must use the recovery disk image process to downgrade to your previous version.*

## Prepare SiteConfig for software deployment to K2 SAN devices

Do the following to prepare SiteConfig for the software upgrade.

1. Make the following files accessible to the SiteConfig control point PC:
  - K2 Media Server software installation (\*.cab) file.
  - Control Point software installation (\*.cab) file.
2. If a newer version of SiteConfig is available for upgrade and you have not yet upgraded SiteConfig, do the following:
  - a) From Windows 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.
3. If not already present in the SiteConfig system description, configure deployment groups as follows:
  - A deployment group that contains your SAN K2 clients
  - A deployment group that contains your K2 Media Servers
  - A deployment group that contains your control point PC

## Deploy control point PC software

Use SiteConfig to upgrade control point software on the K2 control point PC. In most cases, the K2 control point PC is also the SiteConfig control point PC, so you are in effect using SiteConfig to upgrade software on its own local system.

For this release of K2 software, the install task identifies the control point software in the Managed Package column as follows:

- GrassValleyControlPoint 7.0.13.xxxx

The software deployment process for the control point PC is similar to that used to upgrade software on other K2 devices. Use similar procedures and adjust accordingly to do the following:

1. Add the K2 control point software package to the deployment group that contains the control point PC.
2. Check software on the control point PC.

3. Configure and run deployment tasks to upgrade software.

## Unlock K2 Summit Production Clients

This task disables the write filter on a K2 Summit Production Client or on a group of K2 Summit Production Clients.

Prerequisites for this task are as follows:

- The device or all the devices in the group are communicating correctly in SiteConfig. This is indicated by the green star icon overlay.
  - The device or all the devices in the group are currently locked. This is indicated by the gray lock icon overlay.
1. If you have not already done so, stop all media access on the K2 clients. This includes record, play, and transfer operations.
  2. In either the **Network Configuration | Devices** tree view or the **Software Deployment | Deployment Groups** tree view, identify the device or the group of devices that you intend to unlock.
  3. Right-click the device or the group and select **Unlock**.  
A "...may require restart..." message appears.
  4. Click **Yes** to allow SiteConfig to restart the device or devices.  
  
The Set Administrative Credentials dialog box opens.
  5. Enter a username and password with administrator level privileges on the device or devices and click **OK**.  
  
The Unlocking Devices window opens and displays progress.
  6. When the Unlocking Devices window reports that the unlock process completed successfully, click **Close**.

The device or devices are now unlocked. For K2 Summit Production Clients, this also disables the write filter, which enforces the restart.

## Take SAN clients offline

When upgrading software on a K2 SAN, you upgrade software on K2 Media Servers before you upgrade software on the connected SAN clients. This includes K2 clients, K2 appliances, Aurora clients, and generic clients. While you are upgrading software on K2 Media Servers you must keep all connected client devices offline (all media access stopped) or shut down. Do not power up or start media access on connected devices until the upgrade on K2 Media Servers is complete and the media file system/database server is fully operational.

1. If you have not already done so, stop all media access on SAN clients. This includes all record, play, and transfer operations
2. Shutdown all the SAN K2 clients on the SAN. To do this in SiteConfig, right-click a client device in the tree view and select **Shutdown**.

Next upgrade K2 Media Servers. If you have multiple K2 Media Servers you must manage them properly for the upgrade process.

## Manage multiple K2 Media Servers

Do not do this task if:

- You are upgrading a K2 SAN with only one K2 Media Server. Skip ahead and begin upgrading your K2 Media Server.

Do this task if:

- You are upgrading a basic (non-redundant) K2 SAN with multiple servers. This means you have just one K2 Media Server that takes the role of media file system/database server and one or more other K2 Media Servers dedicated to other roles, such as FTP server.
- You are upgrading a redundant K2 SAN. This means you have two K2 Media Servers (primary and backup) that take the role of media file system/database server.

**NOTE:** *If the K2 SAN has multiple K2 Media Servers, you must upgrade all to the same version.*

### If you are upgrading a basic K2 SAN with multiple servers:

1. Upgrade the server that takes the role of media file system/database server first.
2. After the media file system/database server is upgraded and when instructed to do so in a later task, upgrade your other servers.

### If you are upgrading a redundant K2 SAN:

Use the following steps to manage primary/backup roles and upgrade your two media file system/database servers in the proper sequence. This avoids triggering a failover event.

1. Determine the current primary/backup roles of the servers. You can use Server Control Panel (via the K2 System Configuration application or on the local K2 Media Server) or NetCentral to make this determination.
2. Shut down the backup server.
3. Upgrade the primary server.
4. Continue with tasks on your two K2 Media Servers that take the role of media file system/database server. If you have additional servers, upgrade them later, when instructed to do so in a later task.

## Upgrade K2 Media Server

Prerequisites for the upgrade are as follows:

- You have access to the software installation files for this release. Procure the files via the appropriate distribution method, such as download, CD-ROM, network drive, or external drive.

**Configure SNFS default.cfg file on K2 Media Servers**

In this task you open the media file system (SNFS) configuration file and verify/modify settings.

Do not do this task if:

- The K2 system was installed new with the following K2 software version:
  - A 7.x version higher than 7.0.11  
At these versions, K2 tools (Storage Utility and K2Config) automatically configure settings as required.
  - — OR —
  - You have already modified the configuration file with the required settings.

Do this task if:

- You are upgrading from a current version of K2 software as follows:
  - Version 7.0.11
  - — OR —
  - You are not sure if the configuration file has already been modified with the required settings.

In this task you manually modify or add values to the media file system (SNFS) configuration file. Doing so keeps your media file system intact. However, if you need to make a new file system after upgrading K2 software, the values are set automatically by the upgraded version of Storage Utility. This task applies to the following devices:

- K2 Media Servers with role of file system server. If a redundant SAN, you must do this task on both primary and backup K2 Media Server.
1. Using Notepad, open the media file system (SNFS) configuration file:  
On a K2 Media Server, open `D:\SNFS\config\default.cfg`.
  2. On a K2 Media Server, verify, and if necessary modify, settings for required values as follows:

```
# *****  
# A global section for defining file system-wide parameters  
# *****  
GlobalSuperUser Yes  
.  
.  
.  
.  
.
```

```

.
InodeDeleteMax 1000
.
BufferCacheSize 64M
.
.
.
InodeCacheSize 32K

```

3. Close, and if necessary save, the `default.cfg` file.

If you made changes, SNFS services must be restarted for the changes to take effect.

As part of the upgrade procedure, SNFS services are restarted when you restart the K2 device.

### Check all currently installed software on K2 Media Servers

Prerequisites for this task are as follows:

- 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 control point 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 K2 Media Servers that you are upgrading.

1. In the **Software Deployment | Deployment Groups** tree view, right-click the top-most node for the group or any individual device and select **Check Software**.

**NOTE:** *If you have access problems, verify that the administrator account on the device has credentials as currently configured in SiteConfig. By default credentials on the device should be administrator/adminGV! for Aurora devices and Administrator/adminK2 for K2 devices.*

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 for the selected device or devices, 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 Links

[About installing SiteConfig](#) on page 33

### Add software package to deployment group for K2 Media Servers

Prerequisites for this task are as follows:

- You can access the software package file from the SiteConfig control point PC.
- The K2 Media Servers to which you are deploying software are in a deployment group.

Use the following procedure to add one or more software packages to the deployment group that contains your K2 Media Servers. For this release of K2 software, identify and add software installation files as follows:

Software	File name
K2 Server software	<i>GrassValleyK2Server_7.0.13.xxxx.cab</i>

SNFS software is bundled with the K2 software cab file.

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

The Add Package(s) dialog box opens.

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

SiteConfig adds the package to the deployment group.

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

### Upgrade software on K2 Media Servers

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.

When you upgrade software, SiteConfig enforces an uninstall of the current version of software before installing the upgrade version. SiteConfig can do the uninstall/install in a single deployment session. If you are upgrading multiple software components, SiteConfig enforces any dependencies by sequencing deployment tasks. SiteConfig

provides uninstall deployment tasks and install deployment tasks to indicate the taskflow.

1. In the **Software Deployment | Deployment Groups** tree view, select the device or the group of devices for which you are upgrading software.  
The corresponding software deployment tasks are displayed in the Tasks list view.
2. For the software you are uninstalling, select the **Deploy** check box in the row for the uninstall task.
3. For the software you are installing, select the **Deploy** check box in the row for the install task.

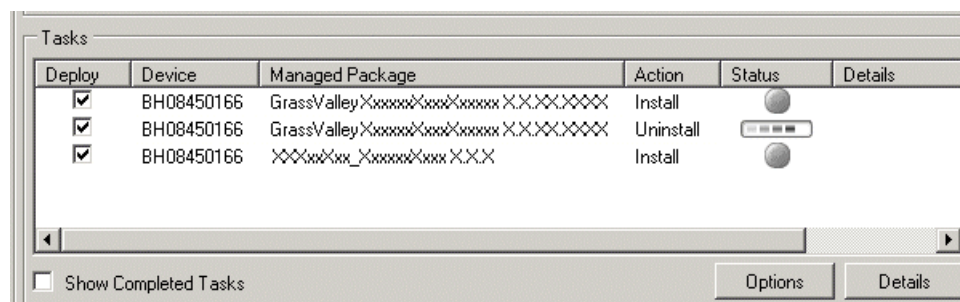
For upgrading a K2 Media Server to this release, deploy the following tasks:

Deploy	Managed Package	Action
✓	GrassValleyK2Server xxxx.xxxx	Uninstall
✓	GrassValleyK2Server 7.0.13.xxxx	Install

If a message instructs you to upgrade the Discovery Agent, on the control point PC go to the directory to which SiteConfig is installed and in the *Discovery Agent Setup* directory find the *DiscoveryAgent\_x.x.x.x.cab* file. Add it to the deployment group and deploy the Discovery Agent software as well.

**NOTE: If there are dependencies, SiteConfig can enforce that some tasks be deployed together.**

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



Deployment tasks run and software is uninstalled. Progress is reported and next steps are indicated in both the Status and Details columns.

5. When the Status or Details columns indicate next steps, proceed as follows:
  - When Details displays a **Restart required** link, click the link and when prompted "...are you sure...", click **Yes**.

The K2 Media Server restarts. This restart is required by the K2 software uninstall.

Deployment tasks run and software is installed. Progress is reported and next steps are indicated in both the Status and Details columns.

6. When the Status or Details columns indicate next steps, proceed as follows:
  - When Details displays a **Restart required** link, click the link and when prompted "...are you sure...", click **Yes**.

The K2 Media Server restarts. This restart is required by the K2 software install.

7. Monitor progress as indicated by both the Status and Details column. When finished, the Status column indicates complete.

#### **Manage redundancy on K2 Media Servers**

Do not do this task if:

- You are upgrading a basic (non-redundant) K2 SAN. This means you have just one K2 Media Server that takes the role of media file system/database server. Skip ahead and begin upgrading your other K2 Media Servers or SAN K2 clients.

Do this task if:

- You are upgrading a redundant K2 SAN. To prevent triggering failover mechanisms, you must manage primary/backup roles as instructed.

#### **If primary upgrade only is complete**

If you have completed the upgrade to the primary server but you have not yet upgraded the backup server, do the following:

1. Make sure the backup server is still shut down.
2. Put the primary server in service as follows:
  - a) On the primary server, run Server Control Panel. You can do this at the local server or through the K2 System Configuration application.
  - b) Use the **Start** button on Server Control Panel. This makes the primary server qualified to take the role of media file system/database server.
  - c) Make sure that Server Control Panel shows green LEDs and that the server on which you have upgraded software is indeed the current primary server.
3. Power up the backup server. Wait until startup processes complete before continuing.

The Failover Monitor should currently be off, as this is the normal state of the service at system startup.

Next upgrade the backup server. Perform all K2 Media Server upgrade tasks on the backup server.

#### **If primary and backup upgrades are complete**

If you have completed the upgrade to both the primary and backup servers, do the following:



1. Make sure the primary server is powered up.
2. Run Server Control Panel. You can do this at the local server or through the K2 System Configuration application. Make sure Server Control Panel shows green LEDs and that the first server on which you upgraded software is still the current primary server.
3. Put the backup server in service as follows:
  - a) Run Server Control Panel. You can do this at the local server or through the K2 System Configuration application.

The Failover Monitor should currently be off on the backup server, as this is the normal state of the service at system startup.
  - b) Use the **Start** button on Server Control Panel. This makes the backup server qualified to take the role of media file system/database server.
  - c) Make sure that Server Control Panel shows green LEDs and that servers are correctly taking primary/backup roles.

Next upgrade any remaining K2 Media Servers.

#### **Upgrade remaining K2 Media Servers**

Do not do this task if:

- All the K2 Media Servers on the K2 SAN have been upgraded.

Do this task if:

- There are K2 Media Servers that do not take the role of media file system/database server on the K2 SAN that have not yet been upgraded.

Perform all upgrade tasks on the remaining K2 Media Servers.

When all the K2 Media Servers on the K2 SAN have been upgraded, next upgrade connected K2 clients.

#### **Upgrade K2 client**

Work through the following topics sequentially to upgrade K2 clients.

##### **Prepare for K2 client upgrade**

Before upgrading K2 clients, do the following:

- Procure the software installation files for this release via the appropriate distribution method, such as download, CD-ROM, network drive, or external drive.
- Start up the K2 clients you are upgrading, if they are not already started.
- Stop all media access on K2 clients.
- Shut down all applications on K2 clients.

### Check all currently installed software on SAN K2 clients

Prerequisites for this task are as follows:

- 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 control point 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 SAN K2 clients that you are upgrading.

1. In the **Software Deployment | Deployment Groups** tree view, right-click the top-most node for the group or any individual device and select **Check Software**.

**NOTE:** *If you have access problems, verify that the administrator account on the device has credentials as currently configured in SiteConfig. By default credentials on the device should be administrator/adminGV! for Aurora devices and Administrator/adminK2 for K2 devices.*

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 for the selected device or devices, 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 Links

[About installing SiteConfig](#) on page 33

### Add software package to deployment group for SAN K2 clients

Prerequisites for this task are as follows:

- You can access the software package file from the SiteConfig control point PC.
- The SAN K2 clients to which you are deploying software are in a deployment group.

Use the following procedure to add one or more software packages to the deployment group that contains your SAN K2 clients. For this release of K2 software, identify and add software installation files as follows:

Software	File name
K2 Client software	7.0.13.xxxx.cab

SNFS software is bundled with the K2 software cab file.

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

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

#### Upgrade software on SAN K2 clients

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.

When you upgrade software, SiteConfig enforces an uninstall of the current version of software before installing the upgrade version. SiteConfig can do the uninstall/install in a single deployment session. If you are upgrading multiple software components, SiteConfig enforces any dependencies by sequencing deployment tasks. SiteConfig provides uninstall deployment tasks and install deployment tasks to indicate the taskflow.

1. In the **Software Deployment | Deployment Groups** tree view, select the device or the group of devices for which you are upgrading software.  
The corresponding software deployment tasks are displayed in the Tasks list view.
2. For the software you are uninstalling, select the **Deploy** check box in the row for the uninstall task.
3. For the software you are installing, select the **Deploy** check box in the row for the install task.

For upgrading SAN K2 clients to this release, deploy the following tasks:

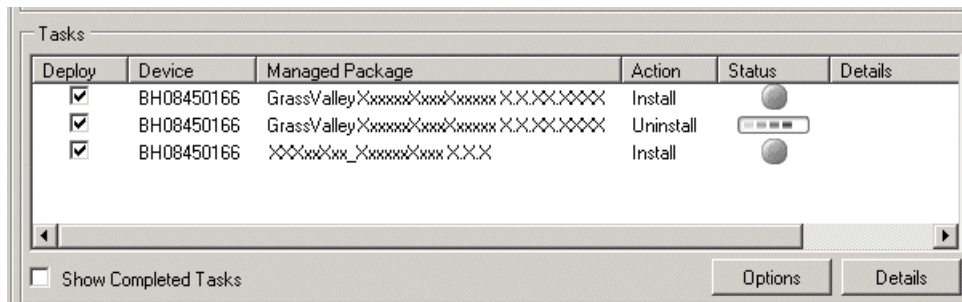
Deploy	Managed Package	Action
✓	GrassValleyK2SummitSANClient xxxx.xxxx	Uninstall

Deploy	Managed Package	Action
✓	GrassValleyK2SummitSANClient 7.0.13.xxxx	Install
✓	WRegMon_SummitSANClient x.x.x	Install (there is no uninstall task for this software)

If a message instructs you to upgrade the Discovery Agent, on the control point PC go to the directory to which SiteConfig is installed and in the *Discovery Agent Setup* directory find the *DiscoveryAgent\_x.x.x.x.cab* file. Add it to the deployment group and deploy the Discovery Agent software as well.

**NOTE: If there are dependencies, SiteConfig can enforce that some tasks be deployed together.**

- 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.

- When the Status or Details columns indicate next steps, proceed as follows:
  - When Details displays a **Restart required** link, click the link and when prompted "...are you sure...", click **Yes**.

The K2 client restarts. This restart is required by the K2 software uninstall. Deployment tasks run and software is installed. Progress is reported and next steps are indicated in both the Status and Details columns.

- When the Status or Details columns indicate next steps, proceed as follows:
  - When Details displays a **Restart required** link, click the link and when prompted "...are you sure...", click **Yes**.

The K2 client restarts. This restart is required by the K2 software install.

- Monitor progress as indicated by both the Status and Details column. When finished, the Status column indicates complete.

### Lock K2 Summit Production Clients

This task enables the write filter on a K2 Summit Production Client or on a group of K2 Summit Production Clients.

Prerequisites for this task are as follows:

- The device or all the devices in the group are communicating correctly in SiteConfig. This is indicated by the green star icon overlay.
- The device or all the devices in the group are currently unlocked. This is indicated by the red lock icon overlay.

1. In the **Network Configuration | Devices** tree view or the **Software Deployment | Deployment Groups** tree view, identify the device or the group of devices that you intend to lock.
2. Right-click the device or the group and select **Lock**.  
A "...may require restart..." message appears.
3. Click **Yes** to allow SiteConfig to restart the device or devices.

The Locking Devices window opens and displays progress.

4. When the Locking Devices window reports that the lock process completed successfully, click **Close**.

The device or devices are now locked. For K2 Summit Production Clients, this also enables the write filter, which enforces the restart.

### Upgrade Aurora Edit, Ingest, and Playout systems

Prerequisites for this task are as follows:

- K2 systems are upgraded to the compatible version of K2 system software.
- All Aurora Browse and MediaFrame devices are offline (all media access stopped) or shut down.

Upgrade your Aurora Edit, Ingest, and Playout systems to the compatible versions of software. Refer to each Aurora product's release notes for procedures.

### Upgrade NAS systems

Prerequisites for this task are as follows:

- K2 systems are upgraded to the compatible version of K2 system software.
- Aurora Edit, Ingest, and Playout systems are upgraded to the compatible versions of software.

Upgrade the MediaFrame Proxy NAS (K2 Nearline SAN) to the compatible version of K2 software. Use SiteConfig and deploy software, using steps similar to those for other systems.

- a) Check software on the Nearline SAN's K2 Media Servers.

- b) Add software \*.cab file to the deployment group that contains the K2 Media Servers.
- c) Upgrade software on K2 Media Servers via a SiteConfig deployment session.

## Upgrade Browse and MediaFrame systems

Prerequisites for this task are as follows:

- K2 systems are upgraded to the compatible version of K2 system software.
- Aurora Edit, Ingest, and Playout systems are upgraded to the compatible versions of software.
- K2 Nearline SAN (NAS) systems are upgraded to the compatible version of K2 system software.

Upgrade your Browse and MediaFrame systems to the compatible versions of software. Refer to *Aurora Browse Release Notes* for procedures.

## Upgrade other SAN clients

Do this task if:

- You have clients on the K2 SAN that have not yet been upgraded. This is the case if you have K2 appliances or other products that use the shared storage of the K2 SAN.

Prerequisites for this task are as follows:

- You have access to the software installation files for this release. Procure the files via the appropriate distribution method, such as download, CD-ROM, network drive, or external drive.

Refer to upgrade procedures for K2 clients and similarly upgrade all remaining client devices on the K2 SAN.

**NOTE:** *You must restart after installing K2 software.*

## Make recovery images

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 events 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.

## Managing stand-alone K2 clients with SiteConfig

The topics in this section apply to the following K2 client products:

- K2 Summit Production Client with internal storage
- K2 Summit Production Client with direct-connect storage

Work through the topics sequentially to get SiteConfig set up to remotely configure and manage one or more K2 clients. Then you can use SiteConfig for software upgrades and other management tasks.

### SiteConfig and stand-alone K2 clients checklist

Use the following sequence of tasks as a guideline to set up SiteConfig and do your initial configuration for one or more stand-alone K2 clients. This checklist outlines the recommended workflow for a new system.

Task	Comment
<input type="checkbox"/> Select a PC to use as the SiteConfig control point PC	Review system requirements and network access requirements about installing SiteConfig.
<input type="checkbox"/> Install SiteConfig on the control point PC	—
<input type="checkbox"/> Create a system description and add a custom site to the system description	If you already have a SiteConfig system description managing other devices in your facility, you can use that system description also for your stand-alone K2 clients, rather than creating a new system description.
<input type="checkbox"/> Add a control network to the site. You can also add a FTP/streaming network if desired	—
<input type="checkbox"/> Add a group for your K2 clients to the system description	—
<input type="checkbox"/> Add a placeholder K2 client to the system description for each of your actual K2 clients	—
<input type="checkbox"/> Configure the names of the placeholder K2 clients	—
<input type="checkbox"/> Configure the network interfaces of the placeholder K2 clients	Specify IP address ranges and other network details
<input type="checkbox"/> Discover your K2 clients	—
<input type="checkbox"/> Assign each discovered K2 client to its placeholder K2 client	—

Task	Comment
<input type="checkbox"/> For each discovered and assigned K2 client, edit each network interface. Specify network settings and apply them to the K2 client.	On each K2 client, set the control network interface IP address first, then the FTP/streaming network interface, if present. Also set the hostname.
<input type="checkbox"/> Add a control point PC placeholder device to the system description	—
<input type="checkbox"/> Discover the control point PC and assign it to the placeholder control point PC	—
<input type="checkbox"/> If not already set correctly, set the hostname of discovered devices	Make sure the device name is correct, then make the hostname the same as the device name.
<input type="checkbox"/> Ping each K2 client and the control point PC to test network communication	—
<input type="checkbox"/> Generate host table information and distribute to hosts files on each K2 client and on the control point PC	Make sure you have completed network configuration of all network interfaces across all devices to ensure complete and valid host table information. You can use SiteConfig to copy hosts files to devices, or you can manage hosts files yourself.
<input type="checkbox"/> Create a deployment group	—
<input type="checkbox"/> Add stand-alone K2 clients to the deployment group	—

## System requirements for SiteConfig control point PC

The PC on which SiteConfig is installed must meet the following requirements:

Requirements	Comments
Operating system	Microsoft Windows (Must be a U.S. version): XP Professional Service Pack 2, Server 2003, or Vista Enterprise Service Pack 1.
RAM	Minimum 512 MB, 1 GB recommended
Graphics acceleration	Must have at least 128 MB memory
Processor	Pentium 4 or higher class, 2 GHz or greater
Hard disk space	400 MB
Microsoft .NET Framework	Version 2.0
Java JRE	1.3.1_12 and 1.4.2_05 or higher. Required for the HP Ethernet Switch configuration



Requirements	Comments
	interface, which is used for K2 Storage Systems (shared storage).
XML	Microsoft XML 4 Service Pack 2 is required. You can install it from the msxml4sp2 file on the K2 System Software CD.

## About installing SiteConfig

SiteConfig uses a protocol that involves sending Ethernet broadcast messages to discover and configure devices. To enable this protocol to work correctly, there must be unrestricted network access between the control point PC and the devices to be discovered.

This is achieved if control network interfaces are all connected to the same switch or to multiple switches interconnected with ISLs/trunks. If your site requires that other switches and/or routers be in the network path, you must make sure that no restrictions are in place that block SiteConfig protocols.

Also, do not install SiteConfig on a PC on which a drive from a managed device is mapped as an administrative share (C\$). For example, if you have a PC set up to run anti-virus software and for this purpose you have network drives set up on the PC mapped to C\$ shares on devices, then do not use that PC as the SiteConfig control point PC that manages those devices.

## Installing/upgrading SiteConfig

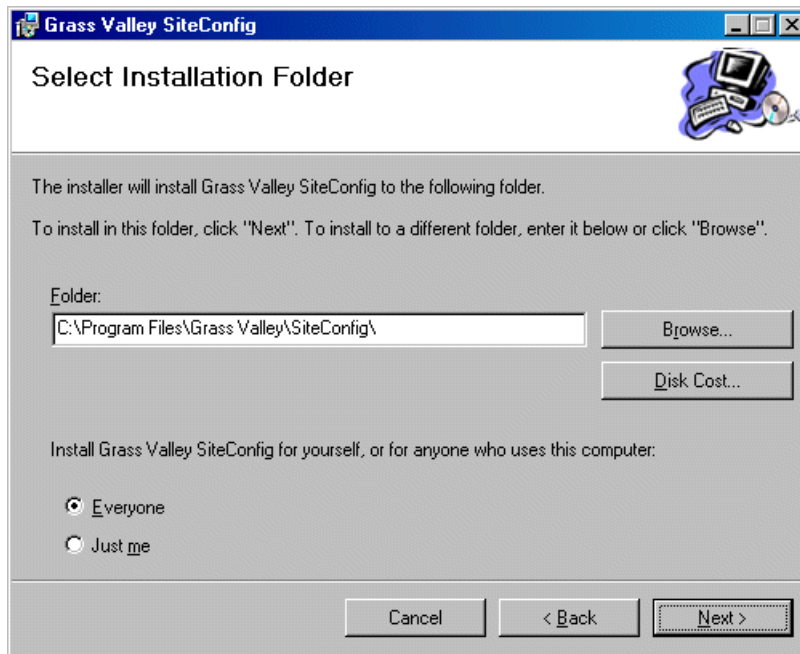
Connect a PC with the appropriate system requirements to the LAN on which all the devices to be managed are connected. Take into consideration the requirement that there be no routed paths to the devices.

1. Procure SiteConfig installation files from the Grass Valley website or from the SiteConfig CD.

The following directory and files are required to install SiteConfig:

- *DotNetFx* directory
- *ProductFrameUISetup.msi*
- *setup.exe*

2. If you already have a version of SiteConfig installed, go to Windows **Add/Remove Programs** and uninstall it.
3. Double-click *setup.exe*.  
The installation wizard opens.
4. Work through the wizard pages, clicking **Next** and **Finish**.



If the PC does not have the appropriate version of Microsoft .NET, the SiteConfig installation programs installs it.

5. Open the Windows operating system Services control panel on your Control Point PC and look for an entry called " ProductFrame Discovery Agent".  
The Discovery Agent is also known as the Network Configuration Connect Kit. The Discovery Agent must be installed on the control point PC so that the control point PC can be discovered by SiteConfig and added to the system description as a managed device. This is necessary to ensure name resolution in SiteConfig's hosts file.
6. Proceed as follows:
  - If the Discovery Agent is not installed, navigate to the SiteConfig install location's Discovery Agent Setup subdirectory and double-click the *DiscoveryAgentServiceSetup.msi* file. This launches the setup program and installs the Discovery Agent. Follow the setup wizard to complete installation. A restart is required after installation. Then continue with the next step in this procedure.
  - If the Discovery Agent is already installed, continue with the next step in this procedure.
7. If not already configured, configure the control point PC with a valid Ethernet IP address for the LAN using Windows Network Connections.
8. If you are not going to be using SiteConfig to manage system hosts files, put the system hosts file on the control point PC.

## Creating a system description for stand-alone K2 clients

Do not do this task if:

- You already have or are developing a SiteConfig system description managing other devices in your facility and that system description has the correct networks and connectivity for your stand-alone K2 clients. In this case, skip ahead to the task in which you add a group to the system description for your stand-alone K2 clients.

Do this task if:

- You do not yet have a system description appropriate for managing your stand-alone K2 clients.
1. Open SiteConfig and proceed as follows:
    - If a dialog box opens that gives you the choice of creating or importing a system description, it means SiteConfig does not have access to a system description file. Click **Create**.
    - If the SiteConfig main window opens, click **File | New**.

The Create New System Description dialog box opens.

2. In the Create New System Description dialog box, enter the name of the file for the system description you are creating.

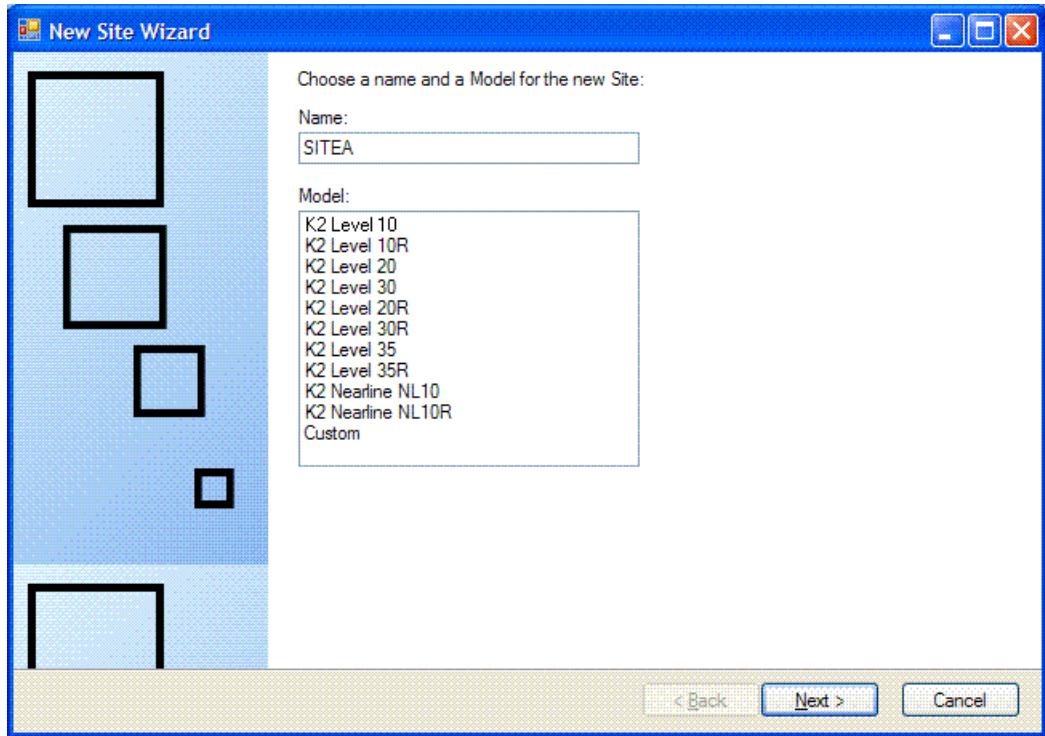
It is recommended that you store the system description file in the default location, rather than browsing to store the file in a different location. SiteConfig always accesses the default location.

3. Click **OK**.

A blank system description loads, which displays just the top-level System node in the tree view.

4. In the **Network Configuration | Devices** tree view, right-click the **System** node or a **Site** node and select **Add Site**.

The New Site Wizard opens.



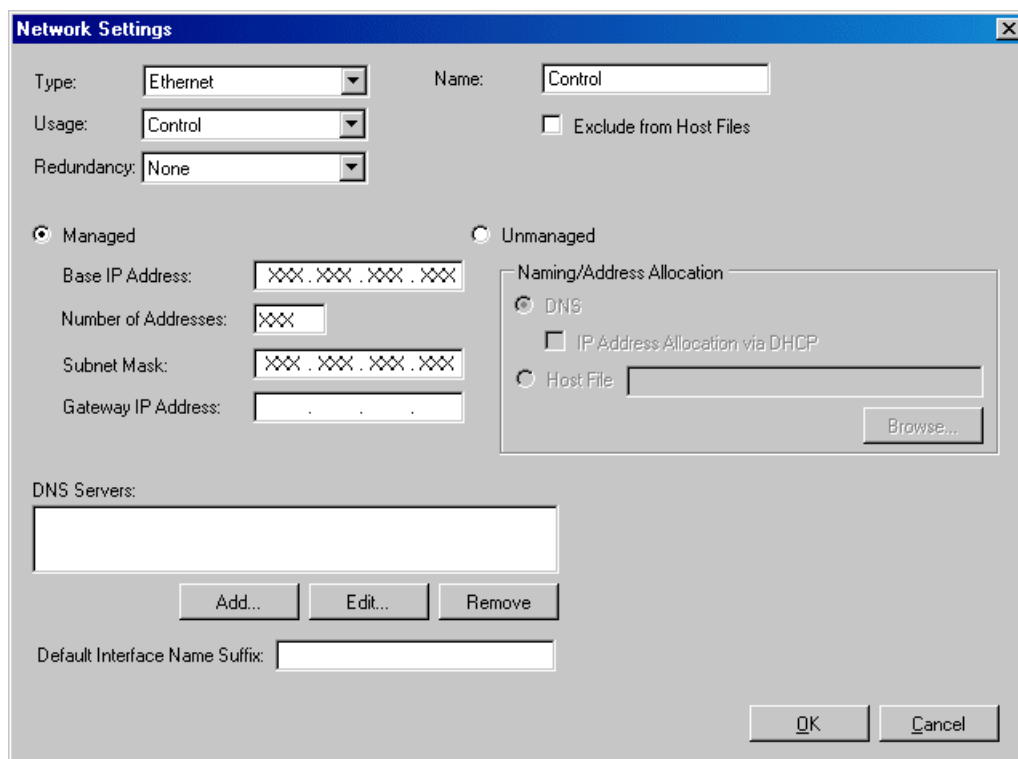
5. Enter a name for the site you are creating, considering the following:
  - Keep the site name short, as it becomes the root identifier that is the default prefix for device and network names.
  - Sites in the tree view are automatically sorted alphabetically.
6. Select **Custom** and click **Next**.
7. Click **Finish** to create the site.

The site is displayed in SiteConfig in the tree view with groups and device placeholders displayed under the site node. New networks are displayed in the tree view of networks in the Networks tab.

### Creating the control network for stand-alone K2 clients

1. In the **Network Configuration | Networks** tree view, select a System node or a Site node.
2. Proceed as follows:
  - To add a network under the currently selected node, in the tree view right-click the node and select **Add Network**.

The Network Settings dialog box opens.



3. Configure the settings for the network as follows:

Setting...	For control network
Type	<i>Ethernet</i> is required
Usage	<i>Control</i> is required
Redundancy	<i>None</i> is required. This is true even on a redundant K2 SAN. (Only the iSCSI network is redundant on a redundant K2 SAN.)
Name	<i>Control</i> is recommended
Exclude from Host Files	<i>Unselected</i> is required
Managed	<i>Selected</i> is required
Base IP Address	The first (lowest) IP address in the range of IP addresses managed by SiteConfig. Required.
Number of Addresses	The number of IP addresses in the range managed by SiteConfig. Required.
Subnet Mask	The network's subnet mask. Required.
Gateway IP Address	Additional network settings managed by SiteConfig. Allowed.

Setting...	For control network
Unmanaged	<i>Unselected</i> is required. Related settings are disabled.
DNS Servers	Servers providing DNS for name resolution. Allowed.
Default Interface Name Suffix	Not allowed

4. Click **OK** to save settings and close.

### Creating the FTP/streaming network for stand-alone K2 clients (optional)

If you transfer media to/from the stand-alone K2 client, create a FTP/streaming network.

1. In the **Network Configuration | Networks** tree view, select a System node or a Site node.
2. Proceed as follows:
  - To add a network under the currently selected node, in the tree view right-click the node and select **Add Network**.

The Network Settings dialog box opens.

3. Configure the settings for the network as follows:

Setting...	For FTP/streaming network
Type	<i>Ethernet</i> is required
Usage	<i>FileTransfer</i> is required
Redundancy	<i>None</i> is required. This is true even on a redundant K2 SAN. (Only the iSCSI network is redundant on a redundant K2 SAN.)
Name	<i>Streaming</i> is recommended
Exclude from Host Files	<i>Unselected</i> is required
Managed	<i>Selected</i> is required
Base IP Address	The first (lowest) IP address in the range of IP addresses managed by SiteConfig. Required.
Number of Addresses	The number of IP addresses in the range managed by SiteConfig. Required.
Subnet Mask	The network's subnet mask. Required.
Gateway IP Address	Additional network settings managed by SiteConfig. Allowed.
Unmanaged	<i>Unselected</i> is required. Related settings are disabled.

Setting...	For FTP/streaming network
DNS Servers	Servers providing DNS for name resolution. Allowed.
Default Interface	_he0 is required
Name Suffix	

4. Click **OK** to save settings and close.

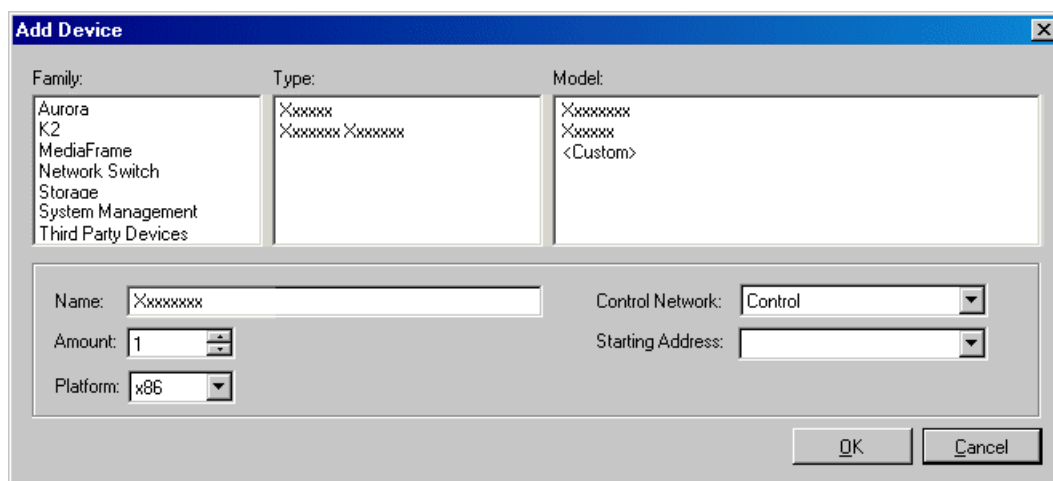
## Adding a group

1. In the **Network Configuration | Networks** tree view, right-click a site node and select **Add Group**.  
The group appears in the tree view.
2. Right-click the group and select **Rename**.
3. Enter the desired name for the group.

## Adding stand-alone K2 clients to the system description

Prerequisites for this task are as follows:

- The system description contains a group.
1. In the **Network Configuration | Devices** tree view, right-click a group and select **Add Device**.



The Add Device dialog box opens.

2. Configure settings for the device you are adding as follows:
  - Family – Select **K2**.

- Type – Select the appropriate type of K2 client as follows:
    - K2 Summit Client - Standalone
  - Model – Select the model with the appropriate storage as follows:
    - K2 Summit Standalone Client (Internal Storage)OR
    - K2 Summit Standalone Client (Direct Connect Storage)
  - Name – This is the device name, as displayed in the SiteConfig device tree view and device list view. This name can be different than the host name (network name). You can accept the default name or enter a name of your choice. Devices in the tree view are sorted alphabetically.
  - Amount – You can add multiple devices, as currently defined by your settings in the Add Device dialog box. An enumerator is added to the name to create a unique name for each device added.
  - Control network – Select the control network.
  - Starting Address – Select from the list of available addresses on the selected control network. If adding multiple devices, this is the starting address, with addresses assigned sequentially to each device added.
3. Click **OK** to save settings and close.
  4. Repeat these steps for each of your stand-alone K2 clients.

### **Modifying stand-alone K2 client unassigned (unmanaged) interfaces**

Prerequisites for this task are as follows:

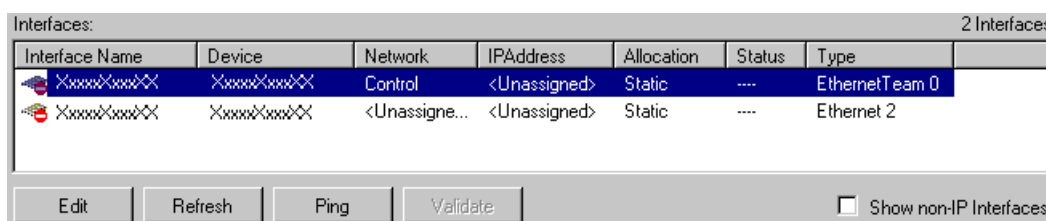
- The system description has a stand-alone K2 client that is a placeholder device.
- The placeholder device has a one or more unmanaged network interfaces.

Use this task to modify unmanaged network interfaces on a standalone K2 client as follows:

- K2 Summit Production Client
1. In the **Network Configuration | Devices** tree view, select a stand-alone K2 client placeholder device.

The interfaces for that device are displayed in the interfaces list view.

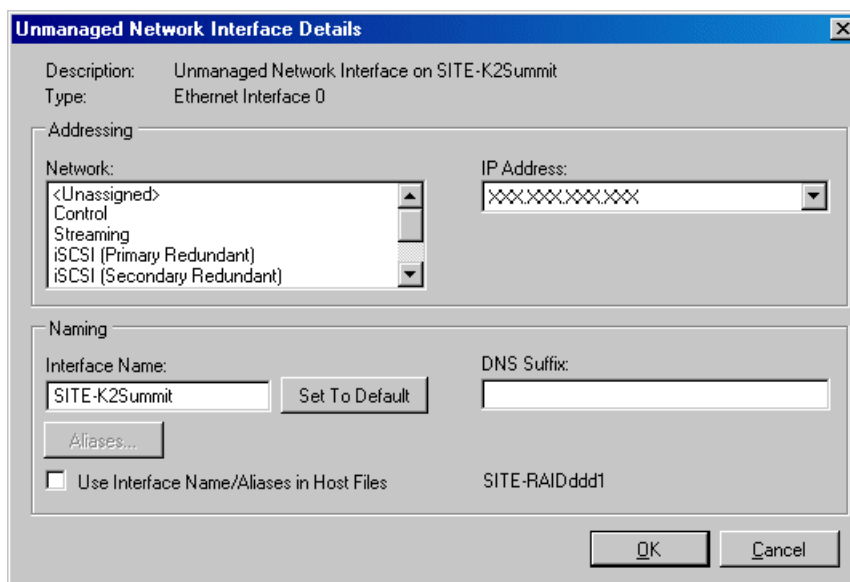




Edit the control network interface first.

2. In the interfaces list view, right-click an interface and select **Edit**.

The Unmanaged Network Interface Details dialog box opens.



3. Configure the settings for the interface as follows:

Setting...	For control network interface
Network	<i>Control</i> is required
IP Address	The IP address for this interface on the network. Required.
Interface Name	The device host name. Required.
Set to Default	Not recommended. Sets the interface name to SiteConfig default convention, based on the root Site name and device-type.
Use Interface Name/Aliases in Host Files	<i>Unselected</i> is required. Since not selected, the default behavior occurs, which is to use the device host name in the hosts file.
Aliases	Not allowed

Setting...	For control network interface
DNS Suffix	Allowed, if applicable to the network. The DNS suffix is added to the interface name.

- Click **OK** to save settings and close.
- If you have a FTP/streaming network, repeat these steps but select the stand-alone K2 client's other network interface and configure settings as follows.


Setting...	For FTP/streaming network interface
Network	<i>Streaming</i> is required
IP Address	The IP address for this interface on the network. Required.
Interface Name	The device host name with the "_he0" suffix added is required. For example, if the host name is <i>K2prod01</i> , then <i>K2prod01_he0</i> is required here.
Set to Default	Not recommended. Sets the interface name to SiteConfig default convention, based on the root Site name and device-type.
Use Interface Name/Aliases in Host Files	<i>Selected</i> is required
Aliases	Not allowed
DNS Suffix	Allowed, if applicable to the network. The DNS suffix is added to the interface name.

- Click **OK** to save settings and close.
- Repeat this procedure for each of your stand-alone K2 client placeholder devices.

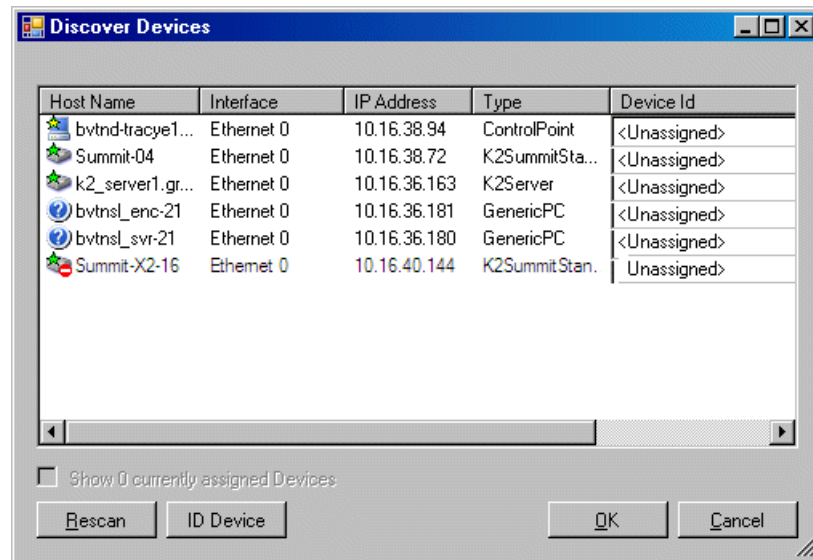
## Discovering devices with SiteConfig

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 control point PC is communicating on the control network.
- There are no routers between the control point PC 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.

- Open SiteConfig on the control point PC.
- 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.


#### Related Links

[About installing SiteConfig](#) on page 33

## 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 stand-alone K2 client managed network interfaces

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 network interfaces on stand-alone K2 client models as follows:

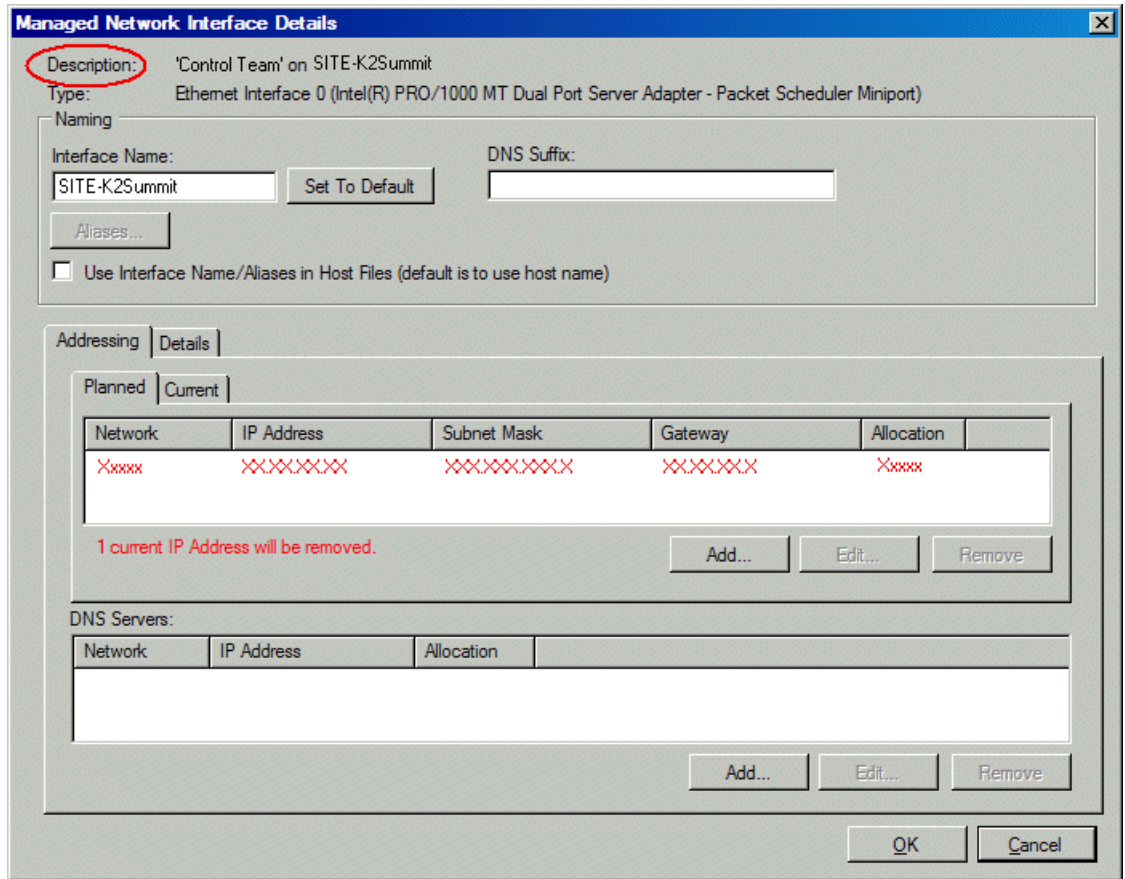
- K2 Summit Production Client
1. In the tree view select a K2 client, then in the Interfaces list view, identify interfaces as follows:
    - For a stand-alone K2 Summit Production Client, the control network interface is a team. Modify the control team interface first. The control team is comprised of two individual interfaces, one for Control Connection #1 and one for Control Connection # 2. If these individual interfaces are displayed, do not modify them.
    - A stand-alone K2 client's other interface is for FTP/streaming. If you have a FTP/streaming network, you can configure and use this interface if desired.

2. 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.
  - Configure the control network interface first before configuring any of the other interfaces.
  - After you have successfully configured the control network interface, return to this step to configure each remaining interface.
3. 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.

***NOTE: For the K2 Summit Production Client, make sure that the device is unlocked in SiteConfig before proceeding. This disables the write filter.***
4. In the Interfaces list view, right-click the interface you are configuring and select **Edit**.

The Managed Network Interface Details dialog box opens.



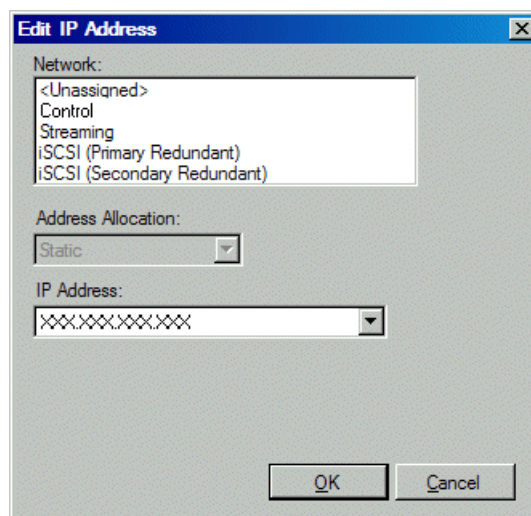
5. Identify the interface on the discovered device that you are configuring.
  - Identify Ethernet LAN adapters by their "Description" name. This is the Windows connection name. SiteConfig reads this name from the device and displays it at the top of this dialog box. This is the most accurate way to identify the network adapter on the discovered device that you are configuring.
  - For a K2 Summit Production Client, when you configure its first interface, make sure you are configuring the 'Control Team' interface.
6. Configure naming settings as follows:

Setting...	For network interface Control Team
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

Setting...	For network interface Control Team
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.

7. 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.
  - Refer to SiteConfig Help Topics for information about planned and current IP configuration.
8. 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 Control Team
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.

9. 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.

10. 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.

11. If you have a FTP/streaming network, repeat steps but select the stand-alone K2 client's other network interface. Open the Managed Network Interface Details dialog box and configure the interface for the FTP/streaming network.

12. Identify the interface on the discovered device that you are configuring.

- On any stand-alone K2 client, for the FTP/streaming network, configure Media Connection #1.

13. Configure naming settings as follows:

Setting...	For network interface Media Connection #1
Interface Name	The device host name with the "_he0" suffix added is 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>Selected</i> is required



- As in steps earlier in this procedure, reconcile planned and current settings. If you must edit the IP address, make settings as follows:

Setting...	For network interface Media Connection#1
Network	Streaming is required
Address Allocation	Static is required.
IP Address	The IP address for this interface on the network. Required.

- When you have verified that the planned settings are correct, click **OK**, then **Yes** to apply settings to the device and close.

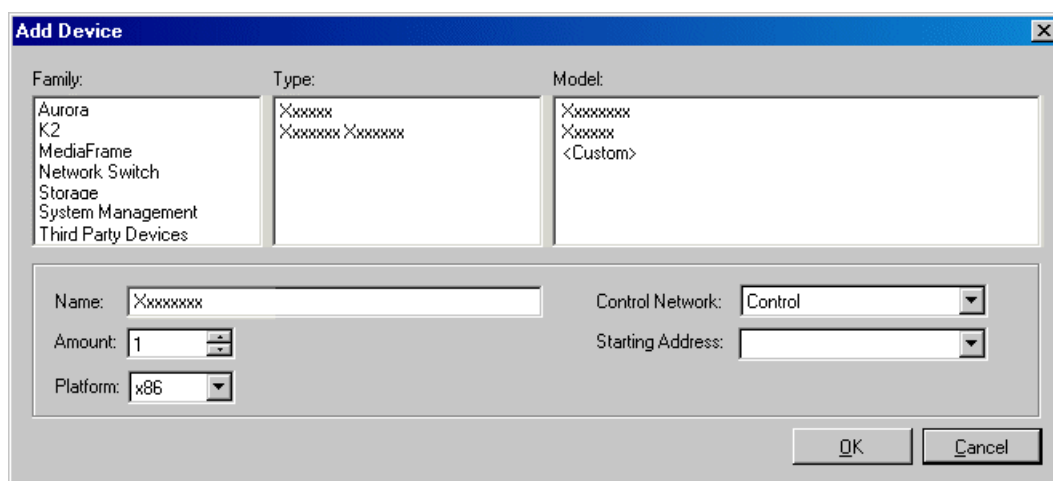
A Contacting Device message box reports progress.

**NOTE: For the K2 Summit Production Client, when configuration is complete, make sure you lock the device in SiteConfig. This enables the write filter.**

## Adding a control point PC placeholder device to the system description

Prerequisites for this task are as follows:

- The system description contains a group.
- In the **Network Configuration | Devices** tree view, right-click a group and select **Add Device**.



The Add Device dialog box opens.

- Configure settings for the device you are adding as follows:
  - Family – Select **System Management**.

- Type – Select **ControlPoint PC**.
  - Model – Select **Control Point PC**.
  - Name - This is the device name, as displayed in the SiteConfig device tree view and device list view. You must configure this name to be the same as the host name on the actual control point PC.
  - Amount – Leave this setting at 1. Do not attempt to configure multiple control point PC simultaneously.
  - Control Network – Select the control network.
  - Starting Address – Select the IP address that is the address currently configured on the actual control point PC.
3. Click **OK** to save settings and close.

Verify that IP settings for the placeholder device's control network interface are identical to those on the actual control point PC before using SiteConfig to discover the control point PC on the control network.

## Assigning the control point PC

Prerequisites for this task are as follows:

- The SiteConfig control point PC has the "SiteConfig Network Configuration Connect Kit" installed.
- The system description contains a control point PC placeholder device.
- The placeholder's control network interface is configured with the control network IP address that is currently on the actual control point PC.
- The device name of the control point PC placeholder is same as the host name of the actual control point PC.

In this procedure you discover the physical control point PC and assign it to the placeholder control point PC in the system description.

1. Open SiteConfig on the control point PC.
2. Discover devices and identify the control point PC discovered device.
3. Assign the discovered device to the control point PC placeholder.
4. In the **Network Configuration | Devices** tree view, select the control point PC.
5. In the Interfaces list view, right-click the control network interface and select **Edit**.

The Managed Network Interface Details dialog box opens.

6. Evaluate IP settings as follows:
  - If only Current settings are displayed (the Planned tab is not displayed), it means the planned settings you configured on the placeholder device are identical to those on the actual control point PC. If this is the case, no further configuration is required.
  - If both a Current tab and a Planned tab are displayed, it means the planned settings you configured on the placeholder device are not identical to those on

the actual control point PC. If this is the case, do not apply planned settings. Doing so overwrites IP settings on the actual control point PC, which stops network communication. Instead, select the **Planned** tab and click **Remove**.

**NOTE: Do not click OK if planned settings (red text) are displayed.**

7. When you are sure that only Current settings are displayed and that those are the current valid settings for the control point PC, click **Apply**, then **OK** to save settings and close.

## 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. If the host name is currently different than the device name, click **Set to Device Name**.

This changes the host name to be the same as the device name.

4. Click **OK**.

## Pinging devices from the control point PC

You can send the ping command to one or more devices in the system description over the network to which the control point 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.

## About hosts files and SiteConfig

SiteConfig uses the network information in the system description to define a hosts file and allows you to view the hosts file. SiteConfig can manage this hosts file on Windows operating system devices that are in the system description and that are part of a SiteConfig managed network.

When you have successfully assigned devices and applied planned network settings to interfaces, it is an indication that host table information, as currently captured in the system description, is valid and that you are ready to have SiteConfig assemble the host table information into a hosts file. Your options for placing this host table information on devices are as follows:

- If you do not want SiteConfig to manage your host table information, you can manage it yourself. This is typically the case if your facility has an existing hosts file that contains host table information for devices that are not in the SiteConfig system description. In this case, you can have SiteConfig generate a single hosts file that contains the host table information for the devices in the system description. You can then copy the desired host table information out of the SiteConfig hosts file and copy it into your facility hosts file. You must then distribute your facility hosts file to devices using your own mechanisms.
- If you want SiteConfig to manage all information in hosts files on devices, you can have SiteConfig copy its hosts file to devices. In so doing, SiteConfig overwrites the existing hosts files on devices. Therefore, this requires that all devices that have name resolution through the hosts file be configured accordingly in the SiteConfig system description.

If you choose to have SiteConfig write hosts files to devices, the process consumes system resource and network bandwidth. Therefore you should wait until you have verified the information for all devices/interfaces in the host file, rather than updating hosts files incrementally as you discover/assign devices.

SiteConfig does not automatically deploy hosts files to managed devices as you add or remove devices. If you add or remove devices from the system description, you must re-deploy the modified hosts file to all devices.

## Generating host tables for devices with 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 control point PC is added to the system description so that it is included in the host tables generated by SiteConfig.

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.

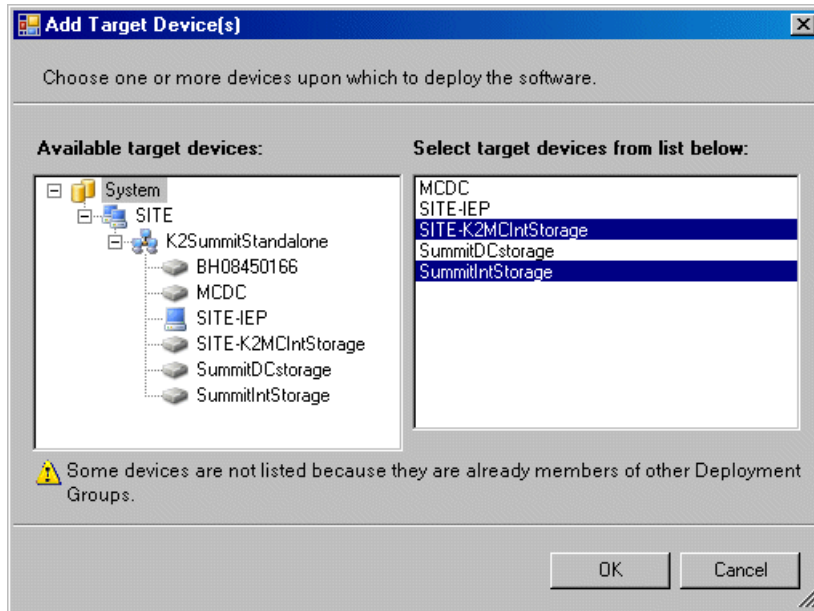
- b) Verify that there is no information that you want to retain in the device's current hosts file that is not also in the hosts file as currently defined in the system description. If you need to save the device's current hosts file, click **Save As** and save to a different location.
- c) In the **Network 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.

## Configuring deployment groups

Prerequisites for this procedure are as follows:

- The device is assigned in the SiteConfig system description and network connectivity is present.
1. In the **Software Deployment | Deployment Groups** tree view, right-click the top node and select **Add Deployment Group**.  
A deployment group appears in the tree view.
  2. Right-click the deployment group, select **Rename**, and enter a name for the deployment group.
  3. Right-click the deployment group and select **Add Target Device**.  
The Add Target Device(s) wizard opens.



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

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

### About deploying software for stand-alone K2 clients

You must control the sequence of software deployment tasks and device restarts as you upgrade software. The exact steps can vary from software version to version. Make sure you follow the documented task flow in the release notes for the version of software to which you are upgrading.

### Upgrading stand-alone K2 clients with SiteConfig

This section contains the tasks for using SiteConfig to upgrade stand-alone K2 clients to this release of K2 software. Work through the tasks sequentially to complete the upgrade.

**NOTE:** These upgrade instructions assume that the current K2 software is at version 7.0.11 or 7.0.12 and that you are upgrading to a higher version of 7.0.x software. If the current K2 software is a 7.x version lower than 7.0.11, contact Grass Valley Support before upgrading. If a K2 Media Client or any K2 device with current K2 software at a 3.x version, do not upgrade, as version 7.x is not supported on these devices

## About upgrading stand-alone K2 clients with SiteConfig

These upgrade instructions apply to stand-alone K2 clients as follows:

With these upgrade instructions, you use SiteConfig from a network connected control point PC and remotely upgrade software simultaneously on multiple K2 clients.

**NOTE:** A control point PC is required.

This is the recommended process for software upgrades. If you choose to upgrade manually instead, you can go to each local K2 client and use keyboard, monitor, and mouse to upgrade software. You can find instructions for a manual upgrade without SiteConfig elsewhere in these release notes.

The following installation tasks provide information specifically for the upgrade to this version of 7.0.13 software. Read the information in these sections carefully before attempting any upgrade to software on a stand-alone K2 client.

### Related Links

[Upgrading stand-alone K2 clients without SiteConfig](#) on page 64

[Managing stand-alone K2 clients with SiteConfig](#) on page 31

## Make recovery images

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.

Refer to the K2 product's *Service Manual* for recovery image procedures.

**⚠ CAUTION:** If you upgrade and then decide you do not want to stay with this version of K2 system software, you must use the recovery disk image process to downgrade to your previous version.

## Prepare for K2 client upgrade

Before upgrading K2 clients, do the following:

- Procure the software installation files for this release via the appropriate distribution method, such as download, CD-ROM, network drive, or external drive.
- Start up the K2 clients you are upgrading, if they are not already started.
- Stop all media access on K2 clients.
- Shut down all applications on K2 clients.

## Configure SNFS default.cfg file on K2 client

In this task you open the media file system (SNFS) configuration file and verify/modify settings.

Do not do this task if:

- The K2 system was installed new with the following K2 software version:
  - A 7.x version higher than 7.0.11At these versions, K2 tools (Storage Utility and K2Config) automatically configure settings as required.
- — OR —
- You have already modified the configuration file with the required settings.

Do this task if:

- You are upgrading from a current version of K2 software as follows:
  - Version 7.0.11
  - — OR —
- You are not sure if the configuration file has already been modified with the required settings.

In this task you manually modify or add values to the media file system (SNFS) configuration file. Doing so keeps your media file system intact. However, if you need to make a new file system after upgrading K2 software, the values are set automatically by the upgraded version of Storage Utility. This task applies to the following devices:

1. Using Notepad, open the media file system (SNFS) configuration file:
2. On a stand-alone K2 client, verify, and if necessary modify, settings for required values as follows:

```
# *****  
# A global section for defining file system-wide parameters  
# *****  
GlobalSuperUser Yes  
.  
.
```



.  
.  
.  
.

InodeDeleteMax 1000

3. Close, and if necessary save, the `default.cfg` file.

If you made changes, SNFS services must be restarted for the changes to take effect.

As part of the upgrade procedure, SNFS services are restarted when you restart the K2 device.

### Prepare SiteConfig for software deployment to stand-alone K2 clients

Do the following to prepare SiteConfig for the software upgrade.

1. Make the following files accessible to the SiteConfig control point PC:
2. 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.
3. If not already present in the SiteConfig system description, configure deployment groups as follows:
  - A deployment group that contains your stand-alone K2 clients
  - A deployment group that contains your control point PC

### Check all currently installed software on stand-alone K2 clients

Prerequisites for this task are as follows:

- 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 control point 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 stand-alone K2 clients that you are upgrading.

1. In the **Software Deployment | Deployment Groups** tree view, right-click the top-most node for the group or any individual device and select **Check Software**.

**NOTE:** *If you have access problems, verify that the administrator account on the device has credentials as currently configured in SiteConfig. By default*

*credentials on the device should be administrator/adminGV! for Aurora devices and Administrator/adminK2 for K2 devices.*

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 for the selected device or devices, 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 Links**

[About installing SiteConfig](#) on page 33

## Add software package to deployment group for stand-alone K2 clients

Prerequisites for this task are as follows:

- You can access the software package file or files from the SiteConfig control point PC.
- The stand-alone K2 clients to which you are deploying software are in a deployment group.

Use the following procedure to add one or more software packages to the deployment group that contains your stand-alone K2 clients. For this release of K2 software, identify and add software installation files as follows:

Software	File name
K2 Client software	7.0.13.xxxx.cab

SNFS software is bundled with the K2 software cab file.

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.

## Unlock K2 Summit Production Clients

This task disables the write filter on a K2 Summit Production Client or on a group of K2 Summit Production Clients.

Prerequisites for this task are as follows:

- The device or all the devices in the group are communicating correctly in SiteConfig. This is indicated by the green star icon overlay.
  - The device or all the devices in the group are currently locked. This is indicated by the gray lock icon overlay.
1. If you have not already done so, stop all media access on the K2 clients. This includes record, play, and transfer operations.
  2. In either the **Network Configuration | Devices** tree view or the **Software Deployment | Deployment Groups** tree view, identify the device or the group of devices that you intend to unlock.
  3. Right-click the device or the group and select **Unlock**.  
A "...may require restart..." message appears.
  4. Click **Yes** to allow SiteConfig to restart the device or devices.  
  
The Set Administrative Credentials dialog box opens.
  5. Enter a username and password with administrator level privileges on the device or devices and click **OK**.  
  
The Unlocking Devices window opens and displays progress.
  6. When the Unlocking Devices window reports that the unlock process completed successfully, click **Close**.

The device or devices are now unlocked. For K2 Summit Production Clients, this also disables the write filter, which enforces the restart.

## Upgrade software on stand-alone K2 clients

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.

When you upgrade software, SiteConfig enforces an uninstall of the current version of software before installing the upgrade version. SiteConfig can do the uninstall/install in a single deployment session. If you are upgrading multiple software components, SiteConfig enforces any dependencies by sequencing deployment tasks. SiteConfig

provides uninstall deployment tasks and install deployment tasks to indicate the taskflow.

1. In the **Software Deployment | Deployment Groups** tree view, select the device or the group of devices for which you are upgrading software.  
The corresponding software deployment tasks are displayed in the Tasks list view.
2. For the software you are uninstalling, select the **Deploy** check box in the row for the uninstall task.
3. For the software you are installing, select the **Deploy** check box in the row for the install task.

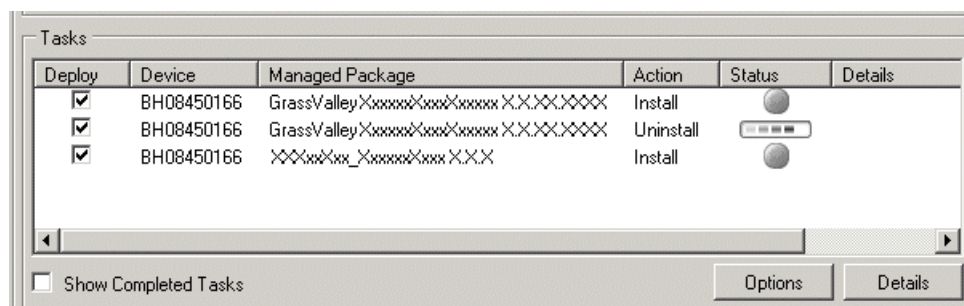
For upgrading stand-alone K2 clients to this release, deploy the following tasks:

Deploy	Managed Package	Action
✓	GrassValleyK2SummitStandalone xxxx.xxxx	Uninstall
✓	GrassValleyK2SummitStandalone 7.0.13.xxxx	Install
✓	WRegMon_SummitStandalone x.x.x	Install (there is no uninstall task for this software)

If a message instructs you to upgrade the Discovery Agent, on the control point PC go to the directory to which SiteConfig is installed and in the *Discovery Agent Setup* directory find the *DiscoveryAgent\_x.x.x.x.cab* file. Add it to the deployment group and deploy the Discovery Agent software as well.

**NOTE: If there are dependencies, SiteConfig can enforce that some tasks be deployed together.**

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



Deployment tasks run and software is uninstalled. Progress is reported and next steps are indicated in both the Status and Details columns.

5. When the Status or Details columns indicate next steps, proceed as follows:

- When Details displays a **Restart required** link, click the link and when prompted "...are you sure...", click **Yes**.

The K2 client restarts. This restart is required by the K2 software uninstall. Deployment tasks run and software is installed. Progress is reported and next steps are indicated in both the Status and Details columns.

6. When the Status or Details columns indicate next steps, proceed as follows:

- When Details displays a **Restart required** link, click the link and when prompted "...are you sure...", click **Yes**.

The K2 client restarts. This restart is required by the K2 software install.

7. Monitor progress as indicated by both the Status and Details column. When finished, the Status column indicates complete.

## Upgrade K2 Dyno Server software

Do not do the tasks in this section if:

- The K2 Summit Production Client is not controlled by a K2 Dyno Controller and therefore K2 Dyno Server software is not installed.

Do the tasks in this section if:

- The K2 Summit Production Client is controlled by a K2 Dyno Controller and you need to upgrade the K2 Dyno Server software, as indicated by compatibility information elsewhere in these release notes.

Check the K2 Dyno Controller release notes for any updated information regarding the upgrade process, then proceed with the tasks in this section.

### Related Links

[About K2 Dyno software](#) on page 61

### About K2 Dyno software

There are two software components in the K2 Dyno Replay system, as follows:

- K2 Dyno Server software – This software runs on the K2 Summit Production Client that is controlled by the K2 Dyno Controller.
- K2 Dyno Client software – This software runs on the K2 Dyno Controller.

When upgrading K2 Dyno software you must upgrade both components: one on the K2 Summit Production Client and one on the K2 Dyno Controller.

### Uninstall K2 Dyno Server software

If you have not already done so, disable the write filter on the K2 Summit Production Client.

On the K2 Summit Production Client, use the Windows **Add/Remove Programs** control panel and uninstall K2 Dyno Server software.

The display name of the software is **K2 Dyno**.

Do not restart the K2 Summit Production Client.

### Install K2 Dyno Server software

If you have not already done so, disable the write filter on the K2 Summit Production Client.

You must uninstall K2 Dyno Server software before you use these steps to install K2 Dyno Server software.

1. From the K2 Summit Production Client, access the K2 Dyno Server software installation files.
2. In the Server directory, locate and open the following file:  
`setup.exe`
3. Follow the onscreen instructions, and work through each page.
4. Click **Next** and **Finish** to complete the installation.
5. Restart the K2 Summit Production Client.

### Lock K2 Summit Production Clients

This task enables the write filter on a K2 Summit Production Client or on a group of K2 Summit Production Clients.

Prerequisites for this task are as follows:

- The device or all the devices in the group are communicating correctly in SiteConfig. This is indicated by the green star icon overlay.
- The device or all the devices in the group are currently unlocked. This is indicated by the red lock icon overlay.

1. In the **Network Configuration | Devices** tree view or the **Software Deployment | Deployment Groups** tree view, identify the device or the group of devices that you intend to lock.
2. Right-click the device or the group and select **Lock**.  
A "...may require restart..." message appears.
3. Click **Yes** to allow SiteConfig to restart the device or devices.

The Locking Devices window opens and displays progress.

4. When the Locking Devices window reports that the lock process completed successfully, click **Close**.

The device or devices are now locked. For K2 Summit Production Clients, this also enables the write filter, which enforces the restart.

## Upgrade K2 Dyno Controller

Do not do the tasks in this section if:

- The K2 Summit Production Client is not controlled by a K2 Dyno Controller.

Do the tasks in this section if:

- The K2 Summit Production Client is controlled by a K2 Dyno Controller and you need to upgrade software on the K2 Dyno Controller, as indicated by compatibility information elsewhere in these release notes.

Before upgrading a K2 Dyno Controller, verify the following:

- You have access to the software installation files for this release. Procure the files via the appropriate distribution method, such as download, CD-ROM, network drive, or external drive.
- You have a recovery image for the K2 Dyno Controller at the current software version.
- Media access is stopped.

### Related Links

[About K2 Dyno software](#) on page 61

### Uninstall K2 Dyno Controller Client software

1. On the K2 Dyno Controller, switch to the Windows operating system as follows:
  - a) At the startup screen, press the **Shift** button and then touch **SHUTDOWN**.
  - b) Touch **MAINTENANCE MODE**.

The K2 Dyno Client software closes and the Windows OS desktop is displayed after a restart.

2. Use the Windows **Add/Remove Programs** control panel and uninstall K2 Dyno Controller Client software.  
The display name of the software is **1.1.0.xx**.
3. Restart the K2 Dyno Controller.

### Install software on K2 Dyno Controller

You must uninstall K2 Dyno Client software before you use these steps to install K2 Dyno Client software.

1. Copy the directory that contains the K2 Dyno Client software onto a portable USB drive, such as a Flash drive.
2. Connect the USB drive to the K2 Dyno Controller and copy the Client directory to the K2 Dyno Controller desktop.
3. In the Client directory, locate and open the following file:

*setup.exe*

4. Follow the onscreen instructions, and work through each page.
5. Click **Next** and **Finish** to complete the installation.
6. When prompted, restart the machine.

## Make recovery images

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 events 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.

## Deploy control point PC software

Use SiteConfig to upgrade control point software on the K2 control point PC. In most cases, the K2 control point PC is also the SiteConfig control point PC, so you are in effect using SiteConfig to upgrade software on its own local system.

For this release of K2 software, the install task identifies the control point software in the Managed Package column as follows:

- GrassValleyControlPoint 7.0.13.xxxx

The software deployment process for the control point PC is similar to that used to upgrade software on other K2 devices. Use similar procedures and adjust accordingly to do the following:

1. Add the K2 control point software package to the deployment group that contains the control point PC.
2. Check software on the control point PC.
3. Configure and run deployment tasks to upgrade software.

## Upgrading stand-alone K2 clients without SiteConfig

This section contains the tasks for upgrading stand-alone K2 clients to this release of K2 software. With these instructions you go to each local K2 client and upgrade software using locally connected keyboard, monitor, and mouse. Work through the tasks sequentially to complete the upgrade.

**NOTE:** *These upgrade instructions assume that the current K2 software is at version 7.0.11 or 7.0.12 and that you are upgrading to a higher version of 7.0.x software. If the current K2 software is a 7.x version lower than 7.0.11, contact Grass Valley Support before upgrading. If a K2 Media Client or any K2 device with current K2 software at a 3.x version, do not upgrade, as version 7.x is not supported on these devices*

### Related Links

[About upgrading stand-alone K2 clients with SiteConfig](#) on page 55



## Make recovery images

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.

Refer to the K2 product's *Service Manual* for recovery image procedures.

**⚠ CAUTION:** *If you upgrade and then decide you do not want to stay with this version of K2 system software, you must use the recovery disk image process to downgrade to your previous version.*

## Prepare for K2 client upgrade

Before upgrading K2 clients, do the following:

- Procure the software installation files for this release via the appropriate distribution method, such as download, CD-ROM, network drive, or external drive.
- Start up the K2 clients you are upgrading, if they are not already started.
- Stop all media access on K2 clients.
- Shut down all applications on K2 clients.

## Disable write filter

Prerequisite:

- K2 software must be installed on the K2 Summit Production Client
1. If you have not already done so, log on to the K2 Summit Production Client with Windows administrator privileges.
  2. From the Windows desktop, click **Start | All Programs | Grass Valley | Write Filter Utility**.  
FBWF Manager opens.
  3. Under Filter Settings, set Filter to **Disable**.
  4. Click **OK**.
  5. When prompted, restart the K2 Summit Production Client.

## Configure SNFS default.cfg file on K2 client

In this task you open the media file system (SNFS) configuration file and verify/modify settings.

Do not do this task if:

- The K2 system was installed new with the following K2 software version:
  - A 7.x version higher than 7.0.11At these versions, K2 tools (Storage Utility and K2Config) automatically configure settings as required.
- — OR —
- You have already modified the configuration file with the required settings.

Do this task if:

- You are upgrading from a current version of K2 software as follows:
  - Version 7.0.11
  - — OR —
- You are not sure if the configuration file has already been modified with the required settings.

In this task you manually modify or add values to the media file system (SNFS) configuration file. Doing so keeps your media file system intact. However, if you need to make a new file system after upgrading K2 software, the values are set automatically by the upgraded version of Storage Utility. This task applies to the following devices:

1. Using Notepad, open the media file system (SNFS) configuration file:
2. On a stand-alone K2 client, verify, and if necessary modify, settings for required values as follows:

```
# *****  
# A global section for defining file system-wide parameters  
# *****  
GlobalSuperUser Yes  
.  
.  
.  
.  
.  
  
InodeDeleteMax 1000
```

3. Close, and if necessary save, the *default.cfg* file.

If you made changes, SNFS services must be restarted for the changes to take effect.

As part of the upgrade procedure, SNFS services are restarted when you restart the K2 device.

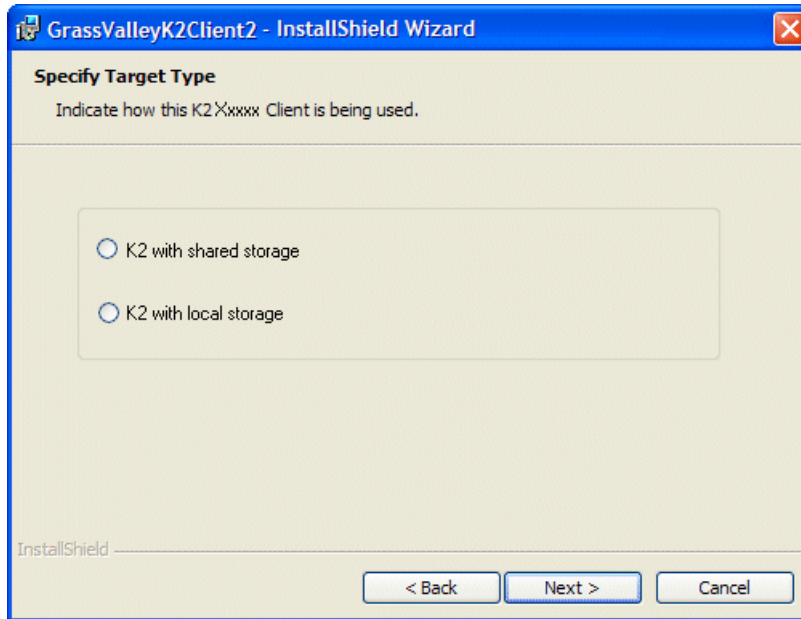
## Uninstall K2 software from K2 Client

1. Open the Windows **Add/Remove Programs** control panel.
2. Select **GrassValleyK2Client**, and click **Remove**.
3. When prompted "Are you sure...?", click **Yes**.
4. When prompted to restart, do not restart.  
While a restart is required after installing K2 Client software, you can delay the restart until after other tasks are complete.
5. Manage the required restart as follows:

## Install K2 software

Prerequisites for this task are as follows:

- If you uninstalled the previous version of K2 software, you must restart the K2 client at least once before installing the new version of K2 software.
1. Log in with a local administrator account. This is required to support K2 System Software licensing.  
***NOTE: When installing K2 system software, you must be logged in with a local administrator account. Do not install software using a domain account.***
  2. Access the installation files.
  3. Locate and open the following file:
  4. Follow the install wizard onscreen instructions, and work through each page.



5. When you arrive at the Specify Target Type page, select the option as follows:

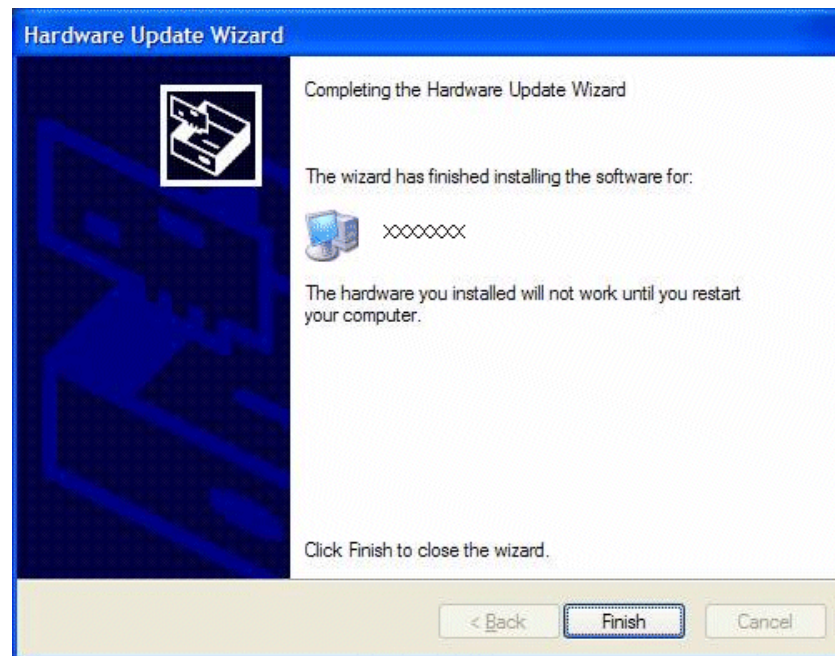
Option	Description
<b>K2 with local storage</b>	For installing on an internal storage K2 client or on a direct-connect storage K2 client.

6. Depending on the state of the system when upgrading, you might see one or more of the following screens or messages as you work through the installation wizard. Proceed as instructed, and then continue with this procedure:
- a) If one or more messages appear referring to "...has not passed Windows logo testing...", you can safely continue. This is a normal part of the upgrade.



Click **Yes** or Continue... to allow the installation to progress.

- b) If installation progress stops after about a minute and does not proceed, look in the Windows taskbar for a Hardware Update Wizard window that has opened.



Click **Finish** on the Hardware Update Wizard to continue installation. If multiple Hardware Update Wizards open, finish them similarly.

7. Click **Next** and **Finish** to complete the installation.
8. When prompted to restart, proceed as follows:
  - Restart now.

## Verify upgraded software

When the K2 client starts up, you can verify that the correct versions of software are installed as follows:

1. Log on to AppCenter.
2. In AppCenter click **Help | About**.

The About dialog box opens.

3. Identify versions as follows

System Version	7.0.13	These should both report the same version number. This is the K2 System Software version number.
RTS Version	7.0.13	
Media File System	3.1.2.RC25225.6138	This is the SNFS version.

## Upgrade K2 Dyno Server software

Do not do the tasks in this section if:

- The K2 Summit Production Client is not controlled by a K2 Dyno Controller and therefore K2 Dyno Server software is not installed.

Do the tasks in this section if:

- The K2 Summit Production Client is controlled by a K2 Dyno Controller and you need to upgrade the K2 Dyno Server software, as indicated by compatibility information elsewhere in these release notes.

Check the K2 Dyno Controller release notes for any updated information regarding the upgrade process, then proceed with the tasks in this section.

### Related Links

[About K2 Dyno software](#) on page 61

### Disable write filter

Prerequisite:

- K2 software must be installed on the K2 Summit Production Client
1. If you have not already done so, log on to the K2 Summit Production Client with Windows administrator privileges.
  2. From the Windows desktop, click **Start | All Programs | Grass Valley | Write Filter Utility**.  
FBWF Manager opens.
  3. Under Filter Settings, set Filter to **Disable**.

4. Click **OK**.
5. When prompted, restart the K2 Summit Production Client.

### Uninstall K2 Dyno Server software

If you have not already done so, disable the write filter on the K2 Summit Production Client.

On the K2 Summit Production Client, use the Windows **Add/Remove Programs** control panel and uninstall K2 Dyno Server software.

The display name of the software is **K2 Dyno**.

Do not restart the K2 Summit Production Client.

### Install K2 Dyno Server software

If you have not already done so, disable the write filter on the K2 Summit Production Client.

You must uninstall K2 Dyno Server software before you use these steps to install K2 Dyno Server software.

1. From the K2 Summit Production Client, access the K2 Dyno Server software installation files.
2. In the Server directory, locate and open the following file:  
*setup.exe*
3. Follow the onscreen instructions, and work through each page.
4. Click **Next** and **Finish** to complete the installation.
5. Restart the K2 Summit Production Client.

## Upgrade remaining K2 clients

For stand-alone storage K2 clients, repeat the previous steps to upgrade your remaining stand-alone storage K2 clients.

### Enable write filter

Prerequisite:

- K2 software must be installed on the K2 Summit Production Client
1. If you have not already done so, log on to the K2 Summit Production Client with Windows administrator privileges.
  2. From the Windows desktop, click **Start | All Programs | Grass Valley | Write Filter Utility**.

FBWF Manager opens.

3. Under Filter Settings, set Filter to **Enable**.
4. Under Protected Volumes, set C: to **Protected**.
5. Click **OK**.
6. When prompted, restart the K2 Summit Production Client.

## Upgrade K2 Dyno Controller

Do not do the tasks in this section if:

- The K2 Summit Production Client is not controlled by a K2 Dyno Controller.

Do the tasks in this section if:

- The K2 Summit Production Client is controlled by a K2 Dyno Controller and you need to upgrade software on the K2 Dyno Controller, as indicated by compatibility information elsewhere in these release notes.

Before upgrading a K2 Dyno Controller, verify the following:

- You have access to the software installation files for this release. Procure the files via the appropriate distribution method, such as download, CD-ROM, network drive, or external drive.
- You have a recovery image for the K2 Dyno Controller at the current software version.
- Media access is stopped.

### Related Links

[About K2 Dyno software](#) on page 61

### Uninstall K2 Dyno Controller Client software

1. On the K2 Dyno Controller, switch to the Windows operating system as follows:
  - a) At the startup screen, press the **Shift** button and then touch **SHUTDOWN**.
  - b) Touch **MAINTENANCE MODE**.

The K2 Dyno Client software closes and the Windows OS desktop is displayed after a restart.

2. Use the Windows **Add/Remove Programs** control panel and uninstall K2 Dyno Controller Client software.

The display name of the software is **1.1.0.xx**.

3. Restart the K2 Dyno Controller.

### Install software on K2 Dyno Controller

You must uninstall K2 Dyno Client software before you use these steps to install K2 Dyno Client software.



1. Copy the directory that contains the K2 Dyno Client software onto a portable USB drive, such as a Flash drive.
2. Connect the USB drive to the K2 Dyno Controller and copy the Client directory to the K2 Dyno Controller desktop.
3. in the Client directory, locate and open the following file:  
`setup.exe`
4. Follow the onscreen instructions, and work through each page.
5. Click **Next** and **Finish** to complete the installation.
6. When prompted, restart the machine.

## Make recovery images

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 events 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.

## Licensing K2 products

The following sections contain instructions for managing K2 product licenses.

### About K2 software licensing

K2 system software version 7.0.13 requires a license from Grass Valley. Licensing is enforced at the , so every K2 client running version 7.0.13 must have a valid license in place. No license is required on the K2 Media Server or on the control point PC.

K2 clients shipping new from the factory have version 7.0.13 pre-installed with a permanent license in place, so no licensing tasks are required unless you want to add optional features such as AppCenter Pro.

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

License information is stored in text files that you can manage just like any other file on your system. Licenses are unique to the system for which they are requested and cannot be used on any other machine. You should back up the license text files to a separate drive or as part of a recovery image.

Licenses are based on your system's unique identifier, which is partially derived from your system's Media Access Control (MAC) address. If you change your system's

MAC address by performing operations such as changing the System Processor card, you must obtain a new license based on the new MAC address.

#### After temporary licenses expire

After the temporary license expires, if you have not yet obtained a permanent license, the following occurs:

- The K2 system software temporary license will expire. You will not be able to start AppCenter once the license has expired. If running, AppCenter will not stop working, and any remote control protocols will continue to function. However, you will not be able to make any changes in AppCenter, such as altering the configuration.
- The AppCenter Pro temporary license will expire and the AppCenter Pro features will stop functioning.

### Requesting a license

Software licenses are unique to the system for which they are purchased. They cannot be used on any other system. This requires that you provide a generated unique ID for the desired system to Grass Valley, which is then used to create your unique license.

1. Log on to the device that you want to license.

You must log in as a Windows administrator with a local account, not a domain account.

2. Open the License Request Wizard.

Find the License Request Wizard shortcut on the Windows desktop.

The License Request Wizard displays.

3. Read the on-screen instructions, then click **Next**.

The Customer dialog box displays.

4. Enter the information requested on this page then click **Next**.

You must provide a valid email address to receive your license file.

The Sales Number dialog box displays.

5. Enter the Sales Order Number in the field then click **Next**.

Typically the Sales Order Number is found on the Software License sheet that you received with your Grass Valley product.

The Summary dialog box displays.

6. Review the License Request information and click **Finish**.

A License Request text file, *License\_Request\_<SalesNumber>.txt*, is generated and saved to the Windows Desktop.

**NOTE:** *If you are requesting licenses for more than one application, be sure to modify the name of the first License Request text file before saving it to your desktop. (In Notepad, use the Save As command.) Otherwise, the second License Request text file will overwrite it.*

7. If a K2 Summit Production Client or K2 Solo Media Server and if the write filter is currently enabled, be aware that files on the desktop are lost on restart. Therefore do one of the following:
  - Save the License Request text file(s) to a different location.
  - Keep the K2 system running (do not restart) until after you have requested the license(s).
8. Do one of the following:
  - Attach the License Request text file to an email.
  - Paste the text directly into an email message.

You might want to keep a copy of the message for your records.

9. Send the email as instructed by the License Request Wizard.

An email will be sent from Grass Valley to the return email address you specified; your SabreTooth software license will be provided as a text file.

10. Save this email in case you ever need to re-image this machine.

Next add the license to the SabreTooth License Manager.

#### **If you encounter difficulties when requesting a license**

If you encounter difficulties running the License wizard, try this alternate method:

1. Generate a unique ID of the device where you will install software, as follows:
  - a) Click on the License Manager icon on the Windows Desktop.

The SabreTooth License Manager opens.
  - b) Choose **File | Generate Unique Id** in the License Manager.
  - c) Click **Copy to clipboard** to copy the generated ID, and **OK** to exit.
2. Prepare an email that includes the following information:
  - Customer Name
  - Customer Email
  - Sales Order Number
  - Unique ID of the device where you will install software.

3. Send the email to [K2License@grassvalley.com](mailto:K2License@grassvalley.com).

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

## Adding a license

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

1. Click on the License Manager icon on the Windows Desktop. The SabreTooth License Manager opens.

The SabreTooth License Manager opens.

2. Do one of the following:
  - Choose **File | Import License** and navigate to the file location to open the text file.
  - Drag and drop the text file onto the License Manager.

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

You should save the permanent license to a backup system.

### Related Links

[Disable write filter](#) on page 79

[Enable write filter](#) on page 80

## Deleting licenses

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

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

### Related Links

[Disable write filter](#) on page 79

[Enable write filter](#) on page 80

## Archiving licenses

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

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

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

## **K2 licenses**

The Grass Valley licenses available at the time of this writing that can be installed on a K2 product are as follows. Contact your Grass Valley representative for more information about licenses.

# ***Additional notes***

The following sections contain additional information about this release

## **Managing the write filter**

The following topics describe the K2 Summit Production Client write filter.

### **About the write filter**

The K2 Summit Production Client has a file-based write filter, which is a feature of the Windows embedded operating system. With the write filter enabled, files can be created, modified, and deleted, but these changes are held in a memory cache. When the K2 Summit Production Client restarts, these changes are lost and the K2 Summit Production Client returns to its original state. This protects the K2 Summit Production Client from changes and increases on-air reliability. For any system configuration change the write filter must be disabled otherwise changes are lost at the next restart.

Some directories, such as *C:\logs*, *C:\Profile\config*, and *C:\Profile\ChannelSuites*, are excluded from write filter protection, so that channel configuration and logs are saved. Do not attempt to alter this list of excluded directories. If you suspect that write filter configuration has been altered, use the recovery image process to restore to the default configuration.

To enable the write filter, the K2 Summit Production Client must be restarted. Likewise, to disable the write filter, the K2 Summit Production Client must be restarted. You can enable/disable the write filter remotely using the SiteConfig lock/unlock feature on one K2 Summit Production Client at a time or on a group of K2 Summit Production Clients all at once. You can also enable/disable the write filter from a local K2 Summit Production Client, but if you use the local method, do not also use the SiteConfig method. If you enable/disable the write filter locally, the change is not automatically sent to SiteConfig, so SiteConfig can not reliably indicate the current lock/unlock state.

### **Local software installation and the write filter**

When you manually install K2 client software at the local K2 Summit Production Client, the installation program helps you manage the write filter. Both the uninstall program and the install program have the same behavior. When you run either the uninstall or the install program, the program behaves as follows:

- If the write filter is enabled, the program notifies you and sets the writer filter to disabled, then prompts you to restart. To continue the uninstall or install process,

you must restart and then run the program again, this time with the write filter disabled.

- If the write filter is disabled, the program sets it to be enabled so that after next restart the K2 Summit Client starts up with the write filter enabled.

In this way the write filter is disabled while software is installed. Changes made to system settings or to the system drive before the restart following an install are preserved.

Once you have uninstalled or installed K2 Client software, at the next restart the write filter is enabled. If you want to keep the write filter disabled after an install, run the Write Filter Utility and disable the write filter before restarting.

### **SiteConfig software installation and the write filter**

When you use SiteConfig to install K2 client software on a K2 Summit Production Client, SiteConfig helps you manage the write filter. The SiteConfig "Lock" feature enables the write filter and the "Unlock" feature disables the write filter. In addition, both uninstall deployment tasks and install deployment tasks behave the same way in how they manage the write filter, as follows:

- If the write filter is enabled (the K2 Summit Production Client is locked), SiteConfig does not allow the task to be deployed. To deploy software, you must first disable (unlock) the write filter on the K2 Summit Production Client.
- If the write filter is disabled (the K2 Summit Production Client is unlocked), when the deployment task completes SiteConfig keeps the write filter disabled. If you then restart the K2 Summit Production Client, the write filter is still disabled after the restart. This allows you to deploy additional software.

When you are finished deploying software, use SiteConfig to enable (lock) the write filter on the K2 Summit Production Client.

### **Disable write filter**

Prerequisite:

- K2 software must be installed on the K2 Summit Production Client
1. If you have not already done so, log on to the K2 Summit Production Client with Windows administrator privileges.
  2. From the Windows desktop, click **Start | All Programs | Grass Valley | Write Filter Utility**.  
FBWF Manager opens.
  3. Under Filter Settings, set Filter to **Disable**.
  4. Click **OK**.
  5. When prompted, restart the K2 Summit Production Client.

## Enable write filter

Prerequisite:

- K2 software must be installed on the K2 Summit Production Client
1. If you have not already done so, log on to the K2 Summit Production Client with Windows administrator privileges.
  2. From the Windows desktop, click **Start | All Programs | Grass Valley | Write Filter Utility**.  
FBWF Manager opens.
  3. Under Filter Settings, set Filter to **Enable**.
  4. Under Protected Volumes, set C: to **Protected**.
  5. Click **OK**.
  6. When prompted, restart the K2 Summit Production Client.

## Passwords and security on K2 systems

To provide a basic level of security, K2 systems recognize four different security levels based on Windows users and groups, and the systems ship from the factory with accounts pre-configured accordingly. To access the system you must login with the username and password for one of the pre-configured accounts.

The following table shows the different types of K2 users and their privileges. Passwords are case sensitive. The term “unknown user” applies to any user who logs in to the K2 System without using the Windows administrator, K2 administrator, or K2 user login and password

	<b>Windows administrator</b>	<b>K2 administrator</b>	<b>K2 user</b>	<b>Unknown user</b>
Login	Administrator	K2Admin	K2User	N/A <sup>2</sup>
Password	adminK2	K2admin	K2user	N/A
AppCenter Configuration Manager	Full access	Full access	Can view	Can't access
AppCenter	Full access	Full access	Full access; requires an account on the K2 Media Client(s)	Can view channel suites, channel status, on-line help and System Status

---

<sup>2</sup> The unknown user, like all others who access the K2 system, must have a valid Windows login for the K2 client or the control point PC through which the K2 system is being accessed.



	Windows administrator	K2 administrator	K2 user	Unknown user
				pane. Can export logs.
Storage Utility	Full access	Full access	Can't access	Can't access
K2Config	Full access	Full access	Can't access	Can't access
Windows Operating System	Full access	Limited access (based on Windows login privileges)	Limited access (based on Windows login privileges)	Limited access (based on Windows login privileges)

For more information about Storage Utility or K2 System Configuration application security, see the *K2 SAN Installation and Service Manual*.

To support FTP security features, K2 clients have *movie* and *mxmovie* accounts.

When using K2 with NetCentral, keep in mind that NetCentral has its own levels of security. Grass Valley recommends mapping the NetCentral administrator with the K2 administrator level. If you are using the Grass Valley Control Point PC, this mapping is already done for you at the factory, so you can log on to NetCentral as administrator using the K2 administrator (K2Admin/K2admin) logon. You can also assign other NetCentral groups to users, as necessary for your site's security policies. You need Windows administrator privileges to add or modify a user's privileges.

For information on mapping a NetCentral administrator to the K2 administrator level, see the *K2 System Guide*. For more information on NetCentral security, see the *NetCentral User Guide*.

## About credentials in SiteConfig

SiteConfig requires administrative privileges on devices in order to perform most of the network configuration and deployment tasks. If you add a device based on a known device type, SiteConfig knows the default administrator login and password to use. Then, when you use remote desktop or perform software deployment to the device, SiteConfig automatically uses these credentials. These credentials are called "global" credentials for the device since the same credentials are used on all devices of that type in the system.

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

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

## Running Check Disk

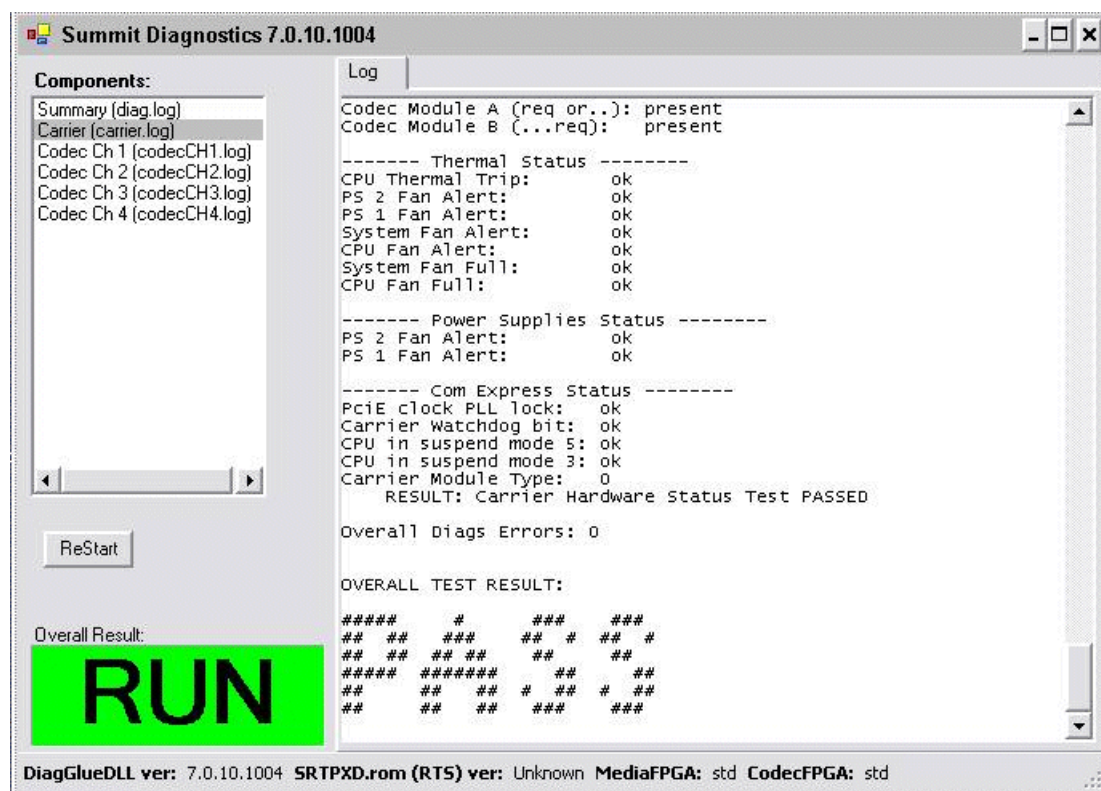
If your K2 Summit Production Client has a critical system fault, you should run Check Disk to identify and remove any corrupted files.

1. Make sure the K2 Summit Production Client has no media access currently underway.
2. At the MS-DOS command prompt, enter the following and press **Enter**.  
`chkdsk`  
Check Disk reports file system information and lists any problem found.
3. Do one of the following:
  - If Check Disk does not report any problems, close the command prompt window. Do not complete the remaining steps of this procedure.
  - If Check Disk reports a problem and prompts you to repair, continue with this procedure.
4. When prompted to repair problems, do the following:
  - a) Press the **Y** key and then press **Enter**.
  - b) Enter the following and press **Enter**.  
`chkdsk /F`  
The screen displays a message similar to the following:  
`The type of the file system is FAT32.  
Cannot lock current drive.  
Chkdsk cannot run because the volume is in use by another  
process. Would you like to schedule this volume to be  
checked the next time the system restarts? (Y/N)`
  - c) Press the **Y** key and then press **Enter**.
5. Restart the K2 Summit Production Client.

## Running diagnostics for K2 Summit Production Client

If you suspect a problem with K2 Summit Production Client hardware, you can run diagnostics and check for errors.

1. Make sure all media access is stopped on the K2 Summit Production Client. Also make sure that there is nothing preventing a restart, as it is required after you run diagnostics.
2. From the Windows desktop, click **Start | All Programs | Grass Valley | Diagnostics**. The Summit Diagnostics application opens.
3. Click **Start**.  
The Overall Result indicator displays RUN while diagnostics are underway.



When diagnostics complete, the Overall Result indicator reports results as follows:

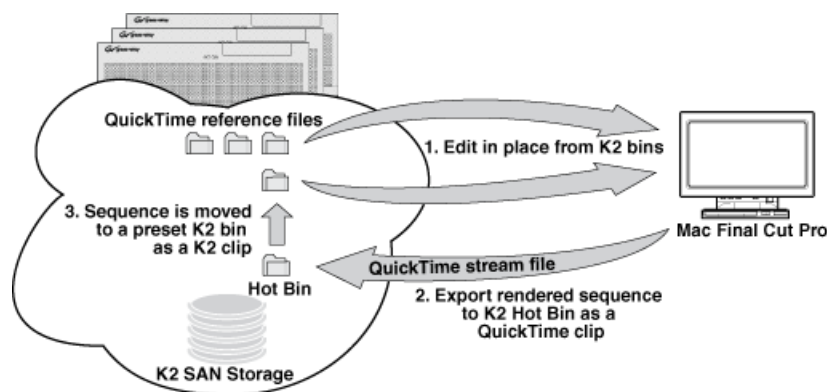
- PASS – There are no problems reported in the diagnostic logs.
  - FAIL – There are one or more problems reported in one or more diagnostic logs.
4. To view a diagnostic log, in the Components list, select a log. The log's contents appear in the Log pane.
  5. To close the Summit Diagnostics application, allow any currently running diagnostics to complete, then click the window close button (X) in the upper right corner of the application window. A "...should be restarted..." message appears.
  6. Click **OK** and then restart the K2 Summit Production Client. You must restart before you can use the K2 Summit Production Client. Running diagnostics puts the real time processor and other services in a non-production state.

## K2 FCP Connect

### About K2 FCP Connect

K2 FCP Connect enables an efficient workflow. You can quickly and easily locate QuickTime files on the K2 SAN and then edit the QuickTime files from the K2 SAN without a file transfer. This capability is called Edit in Place.

The workflow is illustrated as follows:



The K2 FCP Connect product has the following features:

- Seamless browsing of K2 content
- Support growing files editing
- Export/render/flattening of Final Cut Pro finished sequences on the K2 SAN for sharing or playout
- Final Cut Pro and Aurora sequence sharing

It is also possible to use a subset of the K2 FCP Connect features via CIFS mount to a stand-alone K2 client or a K2 Nearline SAN, but this is not the configuration that Grass Valley recommends. Contact your Grass Valley representative to evaluate your needs if you require a CIFS mount.

### Install and configure Macintosh Final Cut Pro systems on a K2 SAN

Read the following topics to get systems connected and file interchange operational.

#### Final Cut Pro on K2 SAN quick start installation checklist

Use the following sequence of tasks to set up Final Cut Pro on a K2 SAN. This checklist assumes that the K2 SAN has been installed/commissioned and is fully operational.

**Prerequisites**

Task	Comment
<input type="checkbox"/> Verify K2 SAN and Macintosh system requirements.	—

**On all Macintosh client computers**

Task	Comment
<input type="checkbox"/> Install Final Cut Pro, if not already installed.	—
<input type="checkbox"/> Install Xsan software, if not already installed.	Xsan must be installed before K2 FCP Connect.
<input type="checkbox"/> Install K2 FCP Connect software.	The software install file is <i>K2FCPConnect.pkg</i> .
<input type="checkbox"/> Cable network connections.	—
<input type="checkbox"/> Configure for control network, if not already done.	—
<input type="checkbox"/> Configure the hosts file for networking.	Copy in host table information from the K2 SAN's hosts file.
<input type="checkbox"/> Configure Active Directory Domain, if desired.	This is optional. If you do this task, you must also enable Access Control Lists on the K2 Media Server (FSM).

**On the K2 Media Server (FSM)**

Task	Comment
<input type="checkbox"/> Request a K2 FCP Connect license from Grass Valley for each K2 Media Server with role of media file system server (FSM) on the SAN.	Make the license request early to ensure that the license file is received and installed before configuring the Mac Client in K2Config.
<input type="checkbox"/> When the license XML is received, install it on the K2 Media Server (FSM).	—
<input type="checkbox"/> Configure hosts files on SAN devices.	Enter Macintosh devices in hosts files.
<input type="checkbox"/> Enable Access Control Lists, if desired.	This is optional. If you do this task, you must also configure Active Directory Domain on the Macintosh systems.

**On the Control Point PC**

Task	Comment
<input type="checkbox"/> Configure hosts file.	Enter Macintosh devices in hosts file.

Task	Comment
<input type="checkbox"/> In K2Config, add and configure Mac Client(s) onto K2 SAN.	The K2 FCP Connect license must be installed on K2 Media Server(s). K2Config can not proceed if the license is not installed.

#### On selected Macintosh computer(s)

Task	Comment
<input type="checkbox"/> Test access to K2 SAN storage.	From the Macintosh system, create, modify, delete a text file.
<input type="checkbox"/> Verify bandwidth of SAN connection	—

#### Final tasks

Task	Comment
<input type="checkbox"/> If used, verify Access Control Lists.	—
<input type="checkbox"/> If desired, configure K2 SAN HotBin to receive finished Final Cut Pro files.	Refer to the <i>K2 System Guide</i> .

### K2 SAN System Requirements

To support K2 FCP Connect, your K2 SAN must meet requirements as follows. Products and versions listed are compatible at the time of this writing. Refer to compatibility information in release notes for updates.

- K2 SAN devices have K2 software version 3.3 or higher. Refer to your K2 product release notes for specific version compatibility information.
- On K2 SAN K2 Media Servers (FSMs), the SNFS configuration file is configured to *GlobalSuperUser Yes*.
- The K2 SAN has unused iSCSI (TOE) bandwidth sufficient to support the Mac clients.
- Storage is K2 Lx0 RAID (Condor). Level 1 and Level 2 RAID not supported.

### Macintosh System Requirements

To support K2 FCP Connect for iSCSI connection to a K2 SAN, your Final Cut Pro Macintosh systems must meet the requirements as follows. Products and versions listed are compatible at the time of this writing. Refer to compatibility information in release notes for updates.

- Mac Pro
- Intel processor
- Two GigE ports
- Mac OS X 10.5.6

- Final Cut Pro version 6.0.5 or higher
- Apple Xsan 2.1

### Install Xsan software

If you have not already done so, install Xsan software on each Macintosh system.

### Install K2 FCP Connect software on Macintosh systems

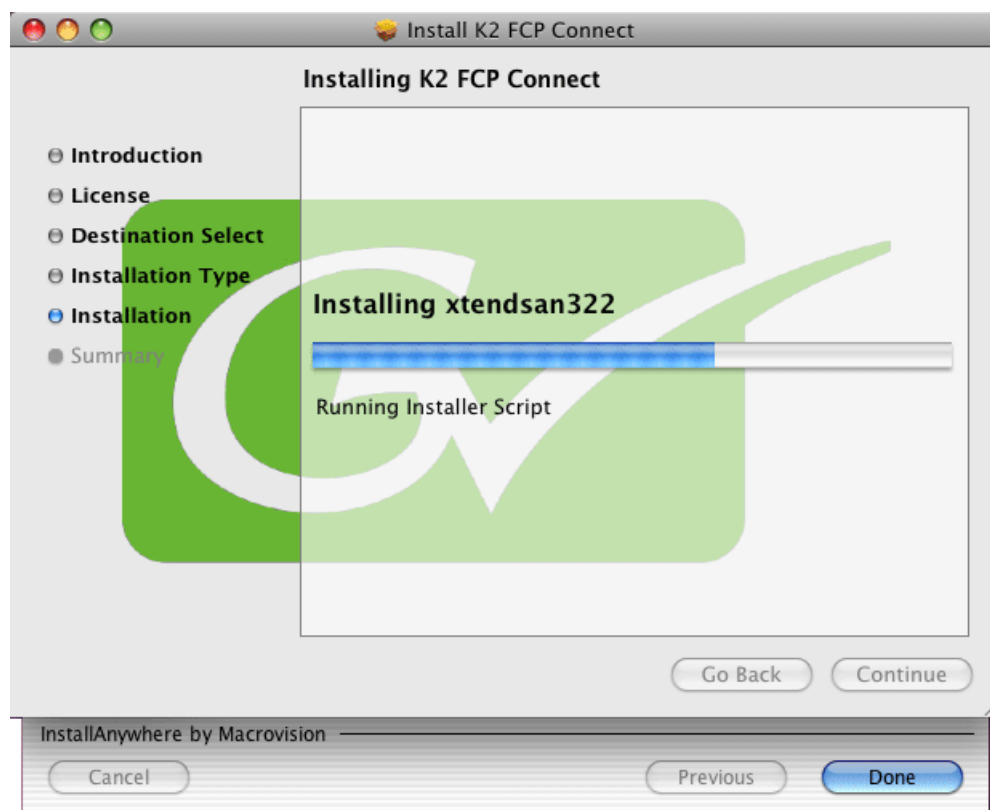
Before doing this task, procure the K2 FCP Connect installation files via download or CD distribution, as appropriate for your Grass Valley product.

1. From the Macintosh system, access the K2 FCP Connect installation files.
2. Double-click *K2FCPConnect.pkg*.

The Installer opens.

3. Click **Continue**, agree to software license terms as appropriate, and accept default packages.
4. Click **Install** and when prompted enter the Macintosh system's administrator username and password.

Software installs.



5. On the Xtend SAN install screen, make sure you click **Done**. If you do not do so, the K2 FCP Connect installation stalls.

**NOTE:** *The Xtend SAN install screen can be partially obscured behind the K2 FCP Connect install screen.*

6. Click **Close** when the installation completes successfully.

#### **Cable Macintosh systems**

Connect each Macintosh system as follows. If you have multiple Macintosh systems and a redundant K2 SAN, balance Macintosh systems between A and B switches.

1. Connect GigE port 1 to a control port on the K2 SAN Ethernet switch.
2. Connect GigE port 2 to a media port on the K2 SAN Ethernet switch.  
This connection is for the media (iSCSI) network.

#### **Configure Macintosh systems for control network**

Configure each Macintosh system as follows:

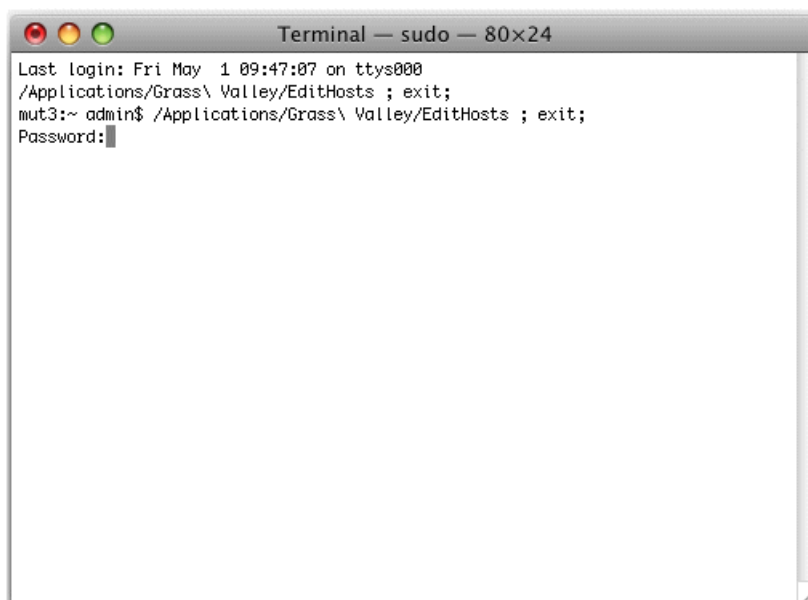
1. Open System Preferences, Network settings.
2. Set Ethernet 1 to configure manually (static IP).
3. Configure IP address, subnet mask, and other settings as required for the K2 SAN control network.

#### **Configure Macintosh hosts files**

On each Macintosh Final Cut Pro system, enter K2 SAN host table information as follows:

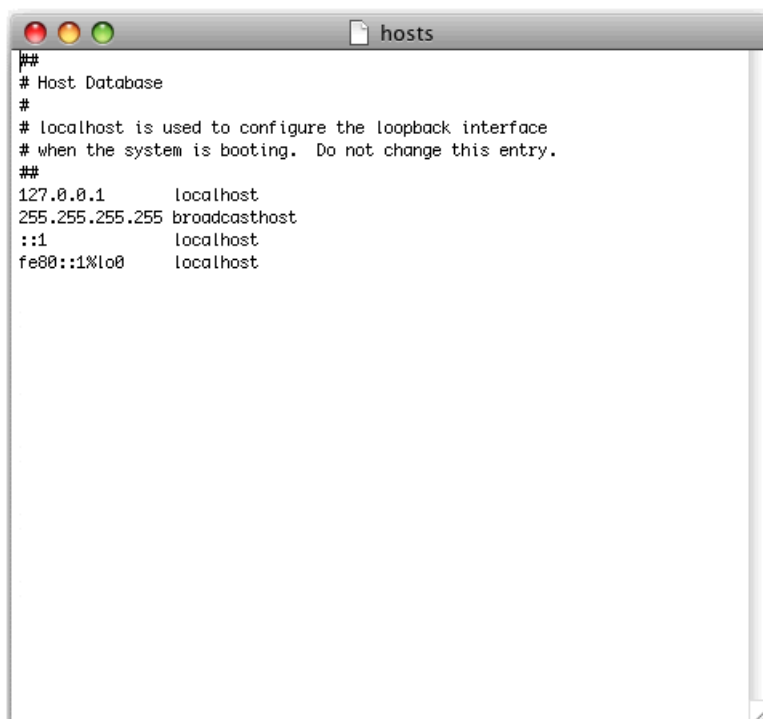
1. Open `Applications\Grass Valley>EditHosts`  
Terminal opens.





```
Terminal — sudo — 80x24
Last login: Fri May 1 09:47:07 on ttys000
/Applications/Grass\ Valley/EditHosts ; exit;
mut3:~ admin$ /Applications/Grass\ Valley/EditHosts ; exit;
Password:
```

2. Enter the Macintosh system's administrator password.  
The hosts file opens in a text editor.



```
hosts
##
# Host Database
#
# localhost is used to configure the loopback interface
# when the system is booting. Do not change this entry.
##
127.0.0.1    localhost
255.255.255.255 broadcasthost
::1        localhost
fe80::1%lo0 localhost
```

The following lines must remain in the Macintosh hosts file:  
127.0.0.1 localhost

255.255.255 broadcasthost

::1 localhost

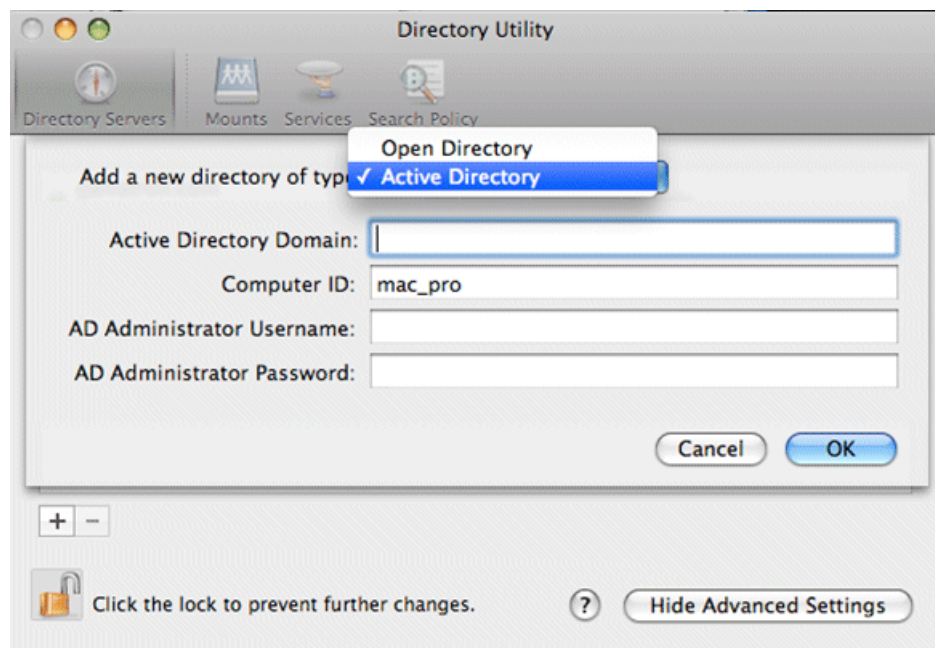
fe80::1%lo0 localhost

3. From the K2 SAN's hosts file, copy the host table information for all the K2 SAN devices and paste it into the Macintosh hosts file.
4. Save and close the hosts file.
5. Close the Terminal window.
6. Copy the new hosts file contents into hosts files on all the other Macintosh Final Cut Pro systems.

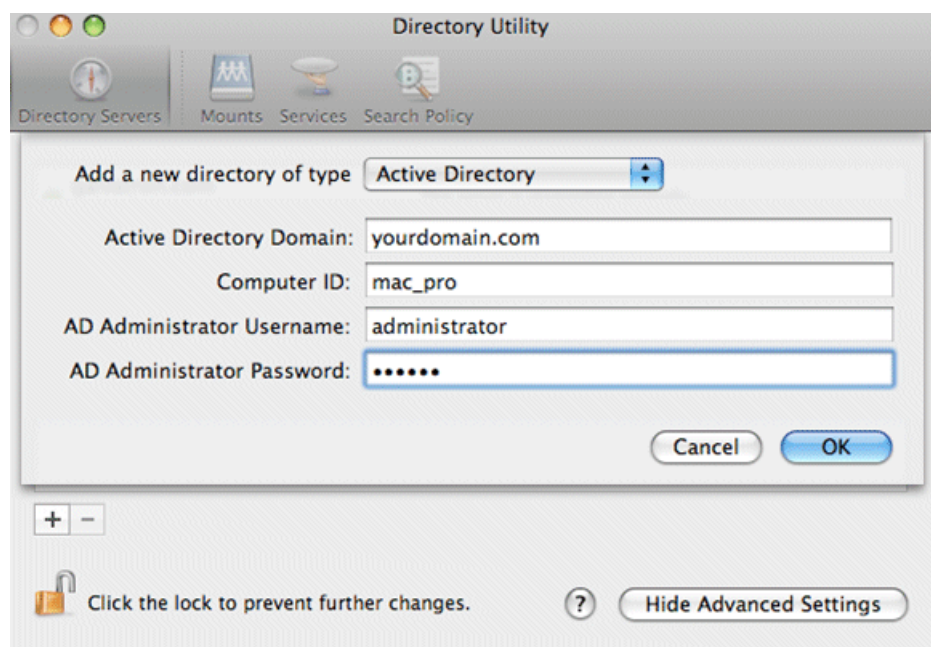
### Configure Macintosh systems for Active Directory Domain

If desired, MAC OS X can be configured to use Active Directory (AD) resources such as users and groups. Once a computer is bound to an AD domain, users belonging to that domain may login to the Macintosh system at the main login prompt. If you do this task, you must also enable Access Control Lists on the K2 Media Server (FSM).

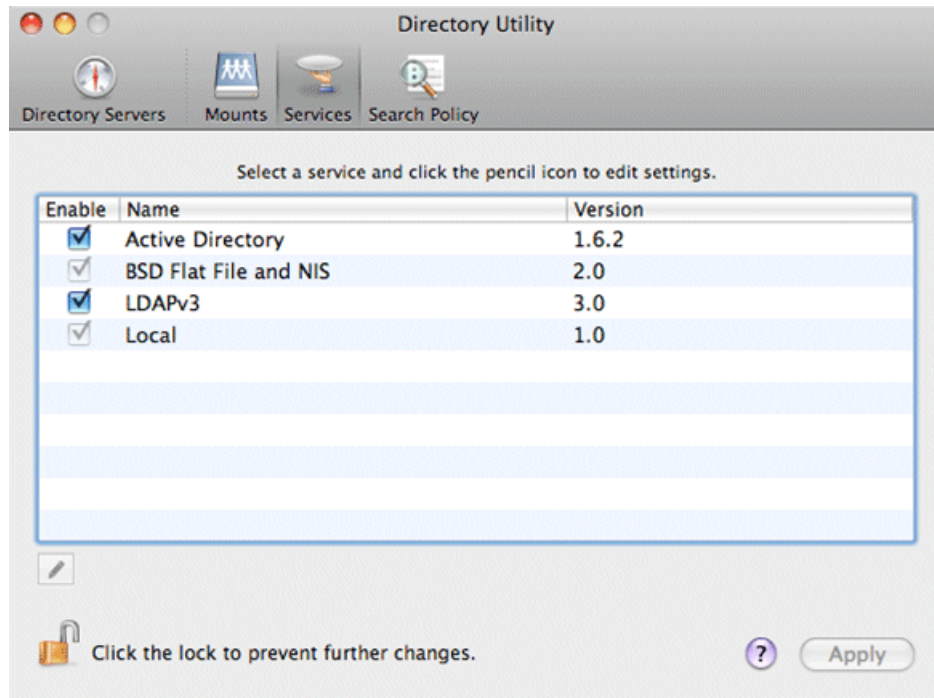
1. In the *Applications/Utilities* folder, open the **Directory Utility**.



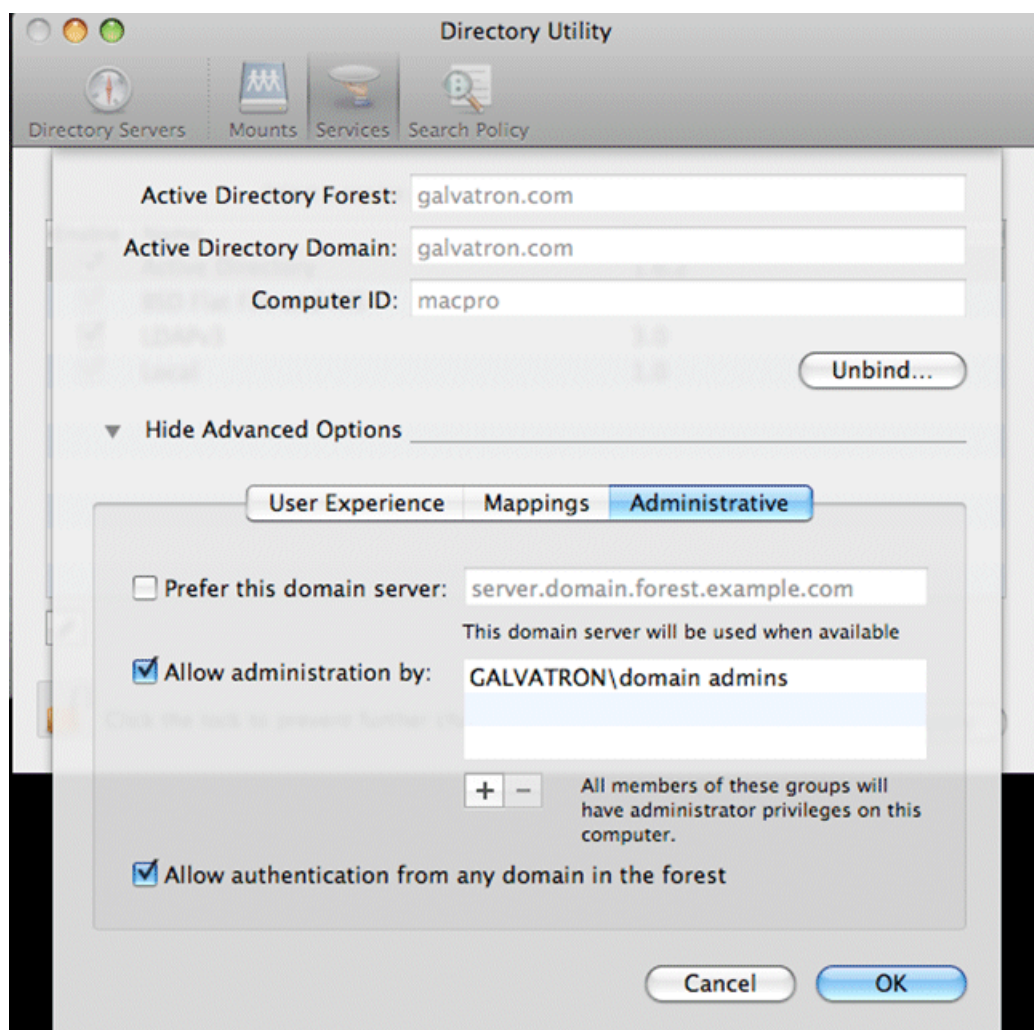
2. Click the **Directory Servers** tab.
3. Click the **+** icon in the lower left, above the padlock icon, to add a new domain binding.
4. In the **Add a new directory of type** drop-down list, select **Active Directory**.



5. Fill in the Active Directory information for the domain administrator account. The administrator account is only needed at the time of binding. Once the computer is bound to a domain, all users of the domain can be used to log in to the Macintosh system.
6. Click **OK**.  
The Macintosh computer goes through the binding process. If successful, the domain name is listed with the status message, "This server is responding normally".
7. Click **Services**.



8. Verify that the Active Directory option is checked.  
If you need to change options, first double-click the padlock icon on the lower left hand corner and authenticate as administrator.
9. If desired, add AD accounts or groups as administrators of the Macintosh computer as follows:
  - a) In the **Services** tab, double-click on the **Active Directory** name.
  - b) Open the advanced options and click on the **Administrative** tab.



- c) Verify that **Allow administration by:** checkbox is checked.
- d) Add any AD user or group of the domain to the list.  
You must type the user or group name, then a backslash, before the domain name.

### Licensing K2 FCP Connect on the K2 SAN

The following sections contain instructions for managing the K2 FCP Connect license.

### About K2 FCP Connect software licensing

K2 FCP Connect requires a license from Grass Valley. For iSCSI access, the license is installed on the K2 SAN's K2 Media Server that takes the role of file system server. If a redundant K2 SAN, the license is installed on primary and backup K2 Media Servers. The license is made available via a Grass Valley SabreTooth licensing service,

so when the Macintosh system attempts to connect to the K2 SAN as an iSCSI client, the connection is verified with the service and either allowed or disallowed.

No Grass Valley license is required to be installed on the Macintosh system or on the control point PC.

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

For iSCSI access, The License Wizard and the SabreTooth License Manager are installed on the K2 SAN's K2 Media Server that takes the role of file system server. If a redundant K2 SAN, they are installed on primary and backup K2 Media Servers.

License information is stored in text files that you can manage just like any other file on your system. Licenses are unique to the system for which they are requested and cannot be used on any other machine. You should back up the license text files to a separate drive or as part of a recovery image.

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

### **Requesting a license**

Software licenses are unique to the system for which they are purchased. They cannot be used on any other system. This requires that you provide a generated unique ID for the desired system to Grass Valley, which is then used to create your unique license.

1. Log on to the device that you want to license.

You must log in as a Windows administrator with a local account, not a domain account.

2. Open the License Request Wizard.

Find the License Request Wizard shortcut on the Windows desktop.

The License Request Wizard displays.

3. Read the on-screen instructions, then click **Next**.

The Customer dialog box displays.

4. Enter the information requested on this page then click **Next**.

You must provide a valid email address to receive your license file.

The Sales Number dialog box displays.

5. Enter the Sales Order Number in the field then click **Next**.

Typically the Sales Order Number is found on the Software License sheet that you received with your Grass Valley product.

The Summary dialog box displays.

6. Review the License Request information and click **Finish**.

A License Request text file, *License\_Request\_<SalesNumber>.txt*, is generated and saved to the Windows Desktop.

**NOTE:** *If you are requesting licenses for more than one application, be sure to modify the name of the first License Request text file before saving it to your desktop. (In Notepad, use the Save As command.) Otherwise, the second License Request text file will overwrite it.*

7. If a K2 Summit Production Client or K2 Solo Media Server and if the write filter is currently enabled, be aware that files on the desktop are lost on restart. Therefore do one of the following:
  - Save the License Request text file(s) to a different location.
  - Keep the K2 system running (do not restart) until after you have requested the license(s).
8. Do one of the following:
  - Attach the License Request text file to an email.
  - Paste the text directly into an email message.

You might want to keep a copy of the message for your records.

9. Send the email as instructed by the License Request Wizard.

An email will be sent from Grass Valley to the return email address you specified; your SabreTooth software license will be provided as a text file.

10. Save this email in case you ever need to re-image this machine.

Next add the license to the SabreTooth License Manager.

### **Adding a license**

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

1. Click on the License Manager icon on the Windows Desktop. The SabreTooth License Manager opens.

The SabreTooth License Manager opens.

2. Do one of the following:
  - Choose **File | Import License** and navigate to the file location to open the text file.

- Drag and drop the text file onto the License Manager.

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

You should save the permanent license to a backup system.

#### **Add Macintosh systems to SAN hosts file**

1. On the K2 SAN's control point PC, open the hosts file in a text editor.
2. Following the convention in the hosts file, enter text in one line for each Final Cut Pro Macintosh system as follows:
  - a) On a text line, type a Macintosh system's control network IP address.
  - b) Use the TAB key or Space bar to insert a few spaces.
  - c) On that same text line after the space, type the machine name, such as MacClient01.  
The machine name cannot have any spaces in it.

This sets up the host file for resolving the machine name on the control network.

3. Save the hosts file.
4. Similarly configure the hosts file on the other devices of the K2 SAN.
5. Copy the hosts file or otherwise make the hosts file accessible to each Final Cut Pro Macintosh system.

#### **Enable Access Control Lists on the K2 Media Server (FSM)**

Prerequisites for the K2 Media Server are as follows:

- Current compatible versions of the Windows operating system and SNFS software.
- Standard C:, D:, E: and V: disk volumes.
- SNFS has been configured with Grass Valley's Storage Utility.
- The SNFS configuration file is located at *D:\SNFS\config\default.cfg*.

If desired, you can enable Access Control Lists (ACLs). If you do this task, you must also configure Active Directory Domain on the Macintosh systems.

1. If a redundant K2 SAN, take FSM K2 Media Servers out of service and manage redundancy as directed in documented procedures.
2. Navigate to *D:\SNFS\config\* and open *default.cfg* in a text editor.
3. Enter/modify text lines as necessary to configure as follows:

```
WindowsSecurity Yes
EnforceACLs Yes
UnixIdFabricationOnWindows Yes
UnixDirectoryCreationModeOnWindows 0700
UnixFileCreationModeOnWindows 0600
```



```
UnixNobodyGidOnWindows 60001  
UnixNobodyUidOnWindows 60001
```

Avoid duplicate settings.

**NOTE: Once ACLs are enabled on the K2 Media Server (WindowsSecurity set to Yes), they cannot be disabled.**

4. Save the `default.cfg` file.
5. Restart the K2 Media Server.
6. If a redundant K2 SAN, repeat these steps on the redundant FSM K2 Media Server.
7. After restart of K2 Media Server(s) is complete, restart all clients of the K2 SAN.

### Add Mac Client to K2 SAN

Prerequisites for this task are as follows:

- You must be logged in to the K2 System Configuration application with permissions equivalent to K2 administrator or higher.
  - The devices of the K2 SAN do not need to be offline, and there is no restart of devices required.
1. In the K2 System Configuration application tree view, select the name of the K2 SAN, which is the top node of the storage system tree.
  2. Click **Add Device**  
The Add Device dialog box opens.
  3. Select **Mac Client**.
  4. Click **OK**.

The new client appears in the tree view.

Next, configure the new client on the K2 SAN.

### Configure Mac Client on K2 SAN

Use this procedure to configure each of your Macintosh Final Cut Pro systems on the K2 SAN as a SAN client device.

Prerequisites for this task are as follows:

- The K2 SAN's K2 Media Server(s) with role of file system server (FSMs) have the K2 FCP Connect license installed.
- You are logged in to the K2 System Configuration (K2Config) application with permissions equivalent to K2 administrator or higher.
- The client device is added to the K2 SAN and appears in the K2 System Configuration application tree view.
- The K2 SAN has adequate bandwidth available to meet the bandwidth needs of the client device you are adding.
- The client device is connected to appropriate networks and is powered up.

- The client device's IP address and other network properties are configured for the control network.
- Host table information for K2 SAN devices, the control point PC, and the client device is in the hosts file on the client device.
- The devices of the K2 SAN do not need to be offline, and there is no restart of devices required.

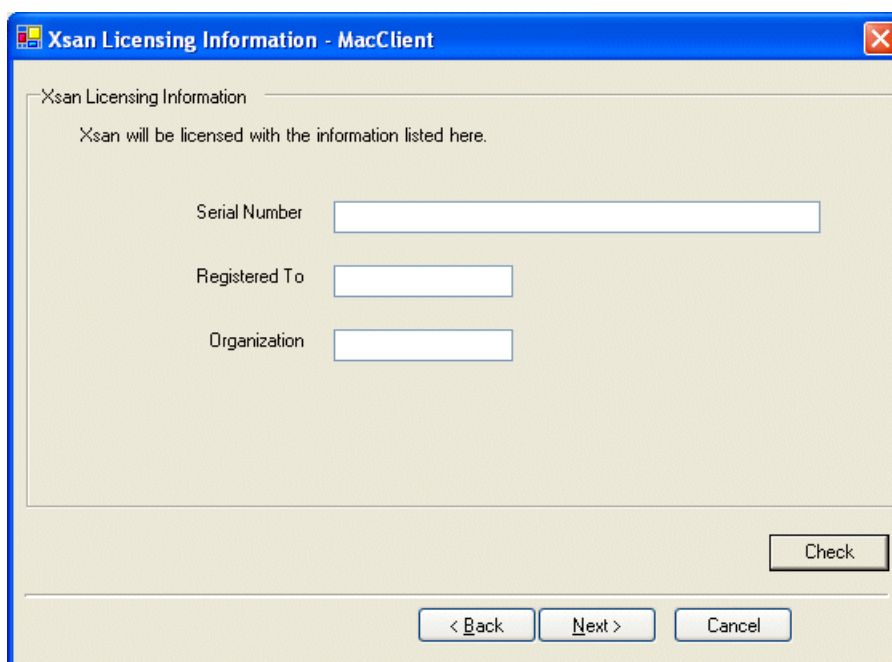
1. In the K2Config tree view, select the client device.
2. Click the **Configure** button.

The Client Configuration wizard opens.

**NOTE:** *If your system has a large number of iSCSI clients, you are prompted to restart the K2 Media Server when you configure clients and cross the following thresholds: 64 clients; 80 clients; 96 clients.*

3. Enter the network name for the client device, as currently configured on the device. If you have multiple client devices to configure, you should configure your highest bandwidth devices first, as this ensures load balancing is correct.
4. For Storage Access, leave **iSCSI** selected.
5. Click **Next**.

The Xsan Licensing Information page opens.



Xsan Licensing Information - MacClient

Xsan Licensing Information

Xsan will be licensed with the information listed here.

Serial Number

Registered To

Organization

Check

< Back   Next >   Cancel

6. Enter information exactly as received from Apple with your Xsan license. If you did not receive information for a field on this page, leave the field blank. For example, if a one-seat license, enter only the Serial number and leave the Registered To and Organization fields blank.

7. Click **Next**.

The Software Configuration page opens.

This page checks the client device for required software.

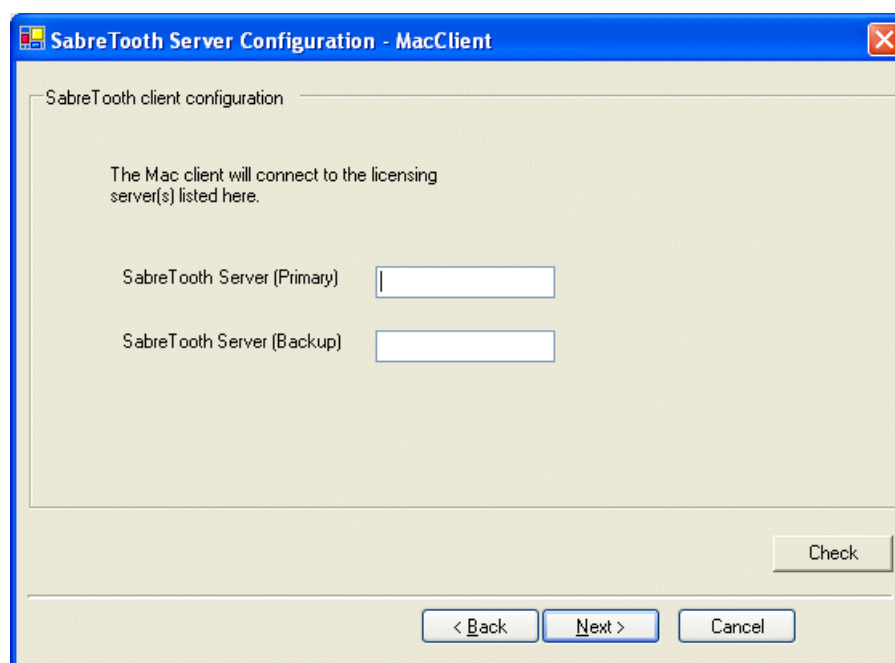
## 8. Identify software installed on the client device and proceed as follows:

- If any software with Yes in the Required column reports as Not Installed, you must install it on the client device. After installing the software, click Check Software.
- If all software with Yes in the Required column reports as Installed, click Check Software.

When all required software reports as Installed, continue with the next step in this procedure.

9. Click **Next**.

The SabreTooth Server Configuration page opens.



## 10. Enter the K2 Media Server (FSM) as follows:

- If a basic (non-redundant) K2 SAN, enter the media file system K2 Media Server as primary.
- If a redundant K2 SAN, enter primary and backup media file system K2 Media Servers.

11. Click **Next**.

The Network Configuration page opens.

This page configures both control and media (iSCSI) network connections. The top port is the port over which the K2 System Configuration application is communicating with the client device. If correctly configured, it is already assigned the control network IP address, which is displayed in the window.

12. Select the media (iSCSI) port and click **Modify**.  
A network configuration dialog box opens.
13. Enter the media network IP address and subnet mask and then click **OK**.
14. Click **Check**.  
The iSCSI Initiator Configuration page opens.  
This page load balances the client device's iSCSI connection to the K2 SAN. The iSCSI adapters on your K2 Media Server or servers are listed here as iSCSI targets.  
On redundant systems, if you have multiple client devices, they should be balanced between A and B.  
For pre-defined K2 SAN levels, K2Config determines the iSCSI target to which each client device subscribes, based on the bandwidth values that you enter. This enforces policies by which each client device has sufficient bandwidth for its intended use and no individual iSCSI target is oversubscribed.  
For custom K2 SANs (Level 4 or 40), qualified system designers can view subnets to help assign iSCSI targets.
15. Click **Modify**.  
The Bandwidth Input dialog box opens.
16. Enter the bandwidth of the Mac Client. This is calculated according to your system design, and provided to you by your Grass Valley representative.
17. Click **Assign TOE**.  
K2Config automatically chooses an iSCSI target to assign to the client device. A message appears that specifies the chosen iSCSI target, but allows you to choose a different iSCSI target.
18. Respond to the message as follows:
  - In most cases you should accept the iSCSI target chosen by K2Config. Click **Yes**, then **OK** to continue.
  - If your system design specifies a different iSCSI target, click **No**, then select the iSCSI target on the iSCSI Initiator Configuration page.
19. When the wizard reports that the configuration check is successful, click **Next**.  
The File System Client Configuration page opens.  
This page connects the client device as a media file system client to the K2 Media Server taking the role of media file system server. If there are redundant K2 Media Servers, both are listed on this page as file system servers.
20. Verify that the client device is connecting to the correct K2 Media Server or Servers, as follows:

- For non-redundant K2 Storage Systems, the client connects to the only server.
- For iSCSI redundant K2 Storage Systems, the client connects to server A as file system server 1 and server B as file system server 2, so that if there is a problem with one server, the other server is available.

21. Click **Next**.

The Completing the Configuration Wizard page opens.

22. Click **Finish**.

When prompted, restart the client device.

### Test K2 SAN file access

From a Macintosh system, perform create, read, write, and delete operations on a file on the V: drive. This verifies the media file system.

1. On the Macintosh desktop, verify that the hard drive icon labeled "default" is present.

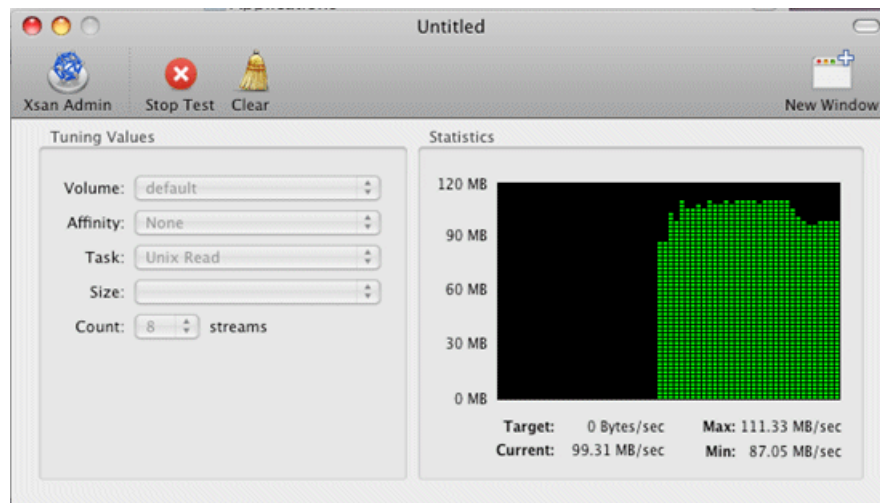


This is the K2 SAN storage, also known as the V: drive.

2. From the Macintosh system, open a text editor, create a text file, enter text, and save it on the V: drive.
3. Close the text editor.
4. In Finder, browse to the V: drive and open the text file.
5. Make a change to the text in the text file and then save and close the text file.
6. Delete the text file.

### Verify bandwidth of SAN connection

1. Install Xsan Tuner (distributed by Grass Valley) on the Macintosh by copying to `/Applications/Server`.
2. Open Xsan Tuner under `/Applications/Server/Xsan Tuner`.



3. Configure the Task field to **Unix Read** and the Count field to **8** streams.
4. Click **Start Test**.  
It might take several minutes to create the test files.
5. After test files are created click **Start Read Test**.
6. Let the Read test run for 1 minute. Report the min, max and current bandwidth.
7. Configure the Task field to **Unix Write** and Count field to **8** streams.
8. Click **Start Test**.  
It might take several minutes to create the test files.
9. After test files are created click **Start Write Test**.
10. Let the Write test run for 1 minute. Report the min, max and current bandwidth.

### Verify Access Control Lists

Prerequisites:

- Two domain users
- A correctly configured K2 SAN
- At least one Macintosh SAN client attached

If you are using Access Control Lists on Macintosh OS X and the Windows operating system, use this task to verify.

1. On the FSM K2 Media Server, do the following:
  - a) Create a new text file on the V: drive.
  - b) Right-click on the text file and select **Properties**.
  - c) Click the **Permissions** tab.
  - d) Select **Everyone** and then for the **Write** permission select the **Deny** check box.
  - e) Create a folder on the V: drive.

- f) Give full permissions to the first user (designated in this procedure as userA) on the domain.
  - g) Give read only permissions to the second user (designated in this procedure as userB) on the domain.
2. On the Macintosh system, do the following:
- a) Login as userA.
  - b) Right-click on the text file and select **Properties**.
  - c) Open up **Terminal** and change directory to the default volume, as follows:
 

```
cd /Volumes/default
```
  - d) Type the following command:
 

```
ls -le
```

```

mut6:default admin$ ls -le
total 2144672
-rwx-----  1 admin  wheel  114467448 Jul 31 10:38 K2FCPCConnect.pkg
-rwx-----  1 admin  wheel  983585471 Dec 29 2008 Shuttle_dv100 3.mov
-r--r--r--  1 admin  wheel    1006 Apr 23 11:52 automount.plist
drwxrwxrwx  13 admin  wheel    2048 Aug 25 17:33 clipDv100.gxf.cmf
drwxrwxrwx   5 root   wheel    2048 Aug 25 17:13 media
-rw----r-x+  1 60001  60001      0 Aug 26 16:36 test.txt
0: group:everyone deny write,append,writeattr,writeextattr
1: FFFFFFFE-EEEE-DDDD-CCCC-BBBB-AAAA7FFFFFF06 allow read,execute,readattr,readextattr,readsecurity
2: group:everyone inherited allow read,write,execute,delete,append,readattr,wri
teattr,readextattr,writeextattr,readsecurity,writesecurity,chmod
mut6:default admin$

```

- e) Verify that there is a "+" next the text file, plus a list of permissions below. If this is true then cross-platform ACLs are enabled.
- f) Open the Finder, go to the default volume and try to edit the text file. This should fail as the file should not be writeable.
- g) In the Finder, go to the folder you created earlier in this procedure and create a text file in the folder. This operation should be successful.
- h) Log out and then log back in as userB.
- i) In the Finder, go to the folder you created earlier in this procedure and try to create a text file in the folder. This operation should fail.

### Configure HotBin

Configure a HotBin on the K2 SAN to receive the finished media from Final Cut Pro.

1. Set up SNFS as follows:  
Add "GlobalSuperUser = Yes" to *default.cfg* file.
2. In K2 AppCenter, create a bin with an appropriate name, such as "dstBin".
3. Configure *dstBin* as a HotBin.  
Refer to the *K2 System Guide* for instructions.
4. When you configure a HotBin, in the Capture Services Utility you can adjust QuickTime Import Delay. The recommended setting is 15 seconds. Refer to the next topic for more information.

### About QuickTime import delay

When you copy a file into a K2 HotBin, the HotBin watches for the file to close and the copy operation to stop, which should indicate the file is complete, before it begins to import the file into K2 storage. However, Final Cut Pro repeatedly opens and closes any QuickTime file as it exports the file, so it is possible that the K2 HotBin can detect a file closed event and begin to import the file before Final Cut Pro is done. If this occurs, the K2 HotBin import for that file fails.

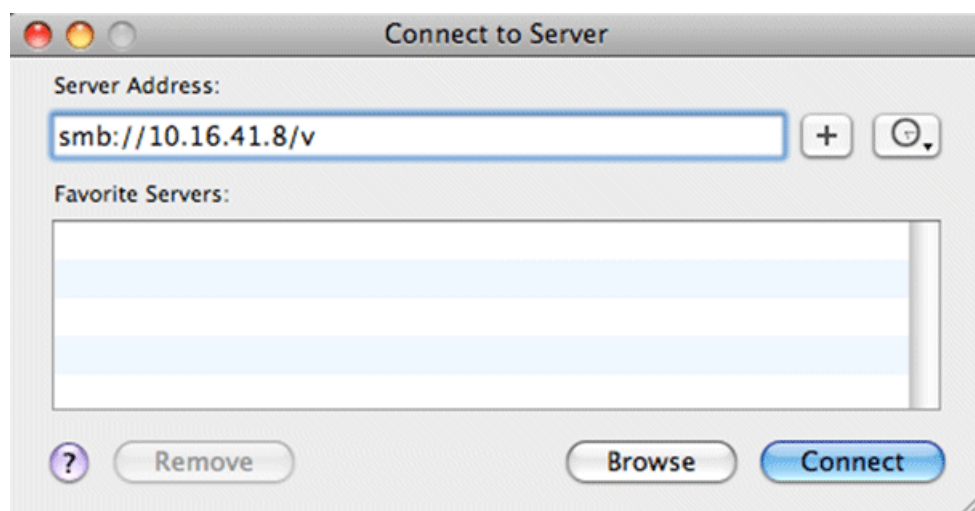
To avoid this problem, the QuickTime import delay allows you to adjust how long a QuickTime file must be idle (no data being written to the file) before the HotBin begins to import the file into K2 storage. The recommended default value is 15 seconds. If you have problems with failed imports and you suspect that Final Cut Pro is holding on to the file with pauses longer than 15 seconds, you should increase the QuickTime import delay time and re-try the import. The HotBin process constrains the QuickTime import delay range to between 10 and 60 seconds.

### Connecting via SAMBA/CIFS

This is an alternative to connecting to the SNFS volume via iSCSI. Once the Macintosh computer has been bound to a domain it can then connect to any domain controlled, shared volume via SAMBA. If connecting via SAMBA, XSan and K2 FCP Connect software do not need to be installed or configured.

1. On the Macintosh computer open the Finder program and at the top menu click **Go | Connect to Server**.  
The Connect to Server dialog box opens.





2. In the Server Address field, type `smb://`, then type the IP or DNS name of the server to which you are connecting, then type `/v` (this is the volume name).
3. Click **Connect**.  
If the volume is shared and behind a domain, you are prompted to authenticate.



The volume should be mounted in the `/Volumes` directory and viewable in the Finder program. Rights to files and folders are enforced based on the security profile of the user you authenticated with when connecting with SAMBA, not the user you are logged in as on the Macintosh computer.

## Using Final Cut Pro on a K2 SAN

Read the following topics to use access and edit K2 media with Final Cut Pro.

### Operation guidelines

Take the following into consideration as you use Final Cut Pro on the K2 SAN.

- Do not use the K2 AppCenter "Erase Unused Media" operation on clips that you are accessing on the K2 SAN.

### Media access

Access media on a K2 system as follows:

1. To open a QuickTime reference file, from the Macintosh system on which you are running Final Cut Pro, access K2 storage.  
For iSCSI access, this is the hard drive icon on the desktop labeled "default". This is also known as the V: drive.
2. Browse to the location of the media in your bin structure. The QuickTime reference file is named according to the following convention:  
`V:\Assets\<bin name>\<clip name>\<clip name>.mov`
3. When you have finished material that you have created in Final Cut Pro, export it to the K2 system.

### Export to K2 SAN

When exporting media to a K2 SAN, Final Cut Pro export options must be constrained so that the resulting media is playable on a K2. The exported media must match the frame rate of movies supported on the K2 system. This is especially important in XDCAM where there are 25, 29.97/30, 50 and 59.94/60 rates.

1. Create the Final Cut Pro clip with a single track of video.
2. Save the Final Cut Pro clip with a `.mov` extension.
3. Use the Final Cut Pro "Using QuickTime Conversion" method to export the Final Cut Pro clip as a stream movie to the K2 HotBin.

Make sure the frame rate is supported on the K2 system.

For material originally recorded on a K2 system, supported frame rates are as follows:

- If you are exporting 1080i material the frame rate must be "Current" or 29.97.
- If you are exporting 720p material for 720p conversions the frame rate must be "Current" or 59.94.
- If you are exporting 720p material for 1080i conversions the frame rate must be 29.97 or 59.94.

The HotBin imports the clip into the K2 system and then the K2 system creates a QuickTime reference file of the clip.

## Maintaining K2 FCP Connect

Read the following topics to evaluate and maintain K2 FCP Connect operations.

### About the GV Helper Tool

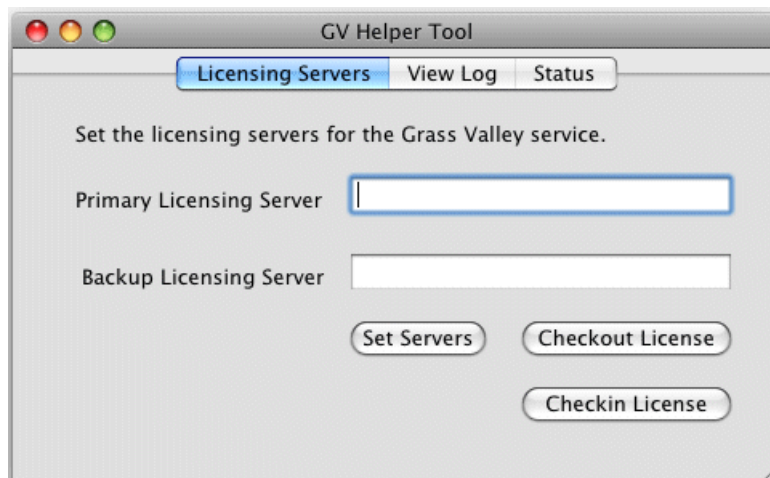
When you install K2 FCP Connect on your Macintosh system, the GV Helper Tool is also installed. You can open the GV Helper Tool from the *Applications\Grass Valley* directory. This utility provides features for maintaining K2 FCP Connect operations on the Macintosh system, as follows:

- Check license in/out to manage licensing on multiple Final Cut Pro Macintosh systems.
- Controls for stopping and starting the K2Config for Mac Daemon
- Access to logs

### Managing K2 FCP Connect licenses

You can drop the K2 FCP Connect license for a Final Cut Pro Macintosh system, and then later pick that license up again.

1. Open the GV Helper Tool.
2. Click the **Licensing Servers** tab.



3. For CIFS mount access, to drop the license currently used by the local Macintosh system to allow the iSCSI client connection to the K2 SAN, click **Checkin License**

4. For CIFS mount access, to assign an unused license to the local Macintosh system to allow it to make an iSCSI client connection to the K2 SAN, click **Checkout License**
5. You can also change the licensing server, which is the machine to which the Macintosh system looks to get its license, however take the following into consideration:
  - You can change the licensing server in K2Config as well as here in the GV Helper Tool.

Therefore it is recommended that you use K2Config, rather than the GV Helper Tool, to change the licensing server.

### **Stopping and starting the K2Config for Mac Daemon service**

To start and stop the K2Config for Mac Daemon service, run scripts in the */Applications/Grass Valley* directory.

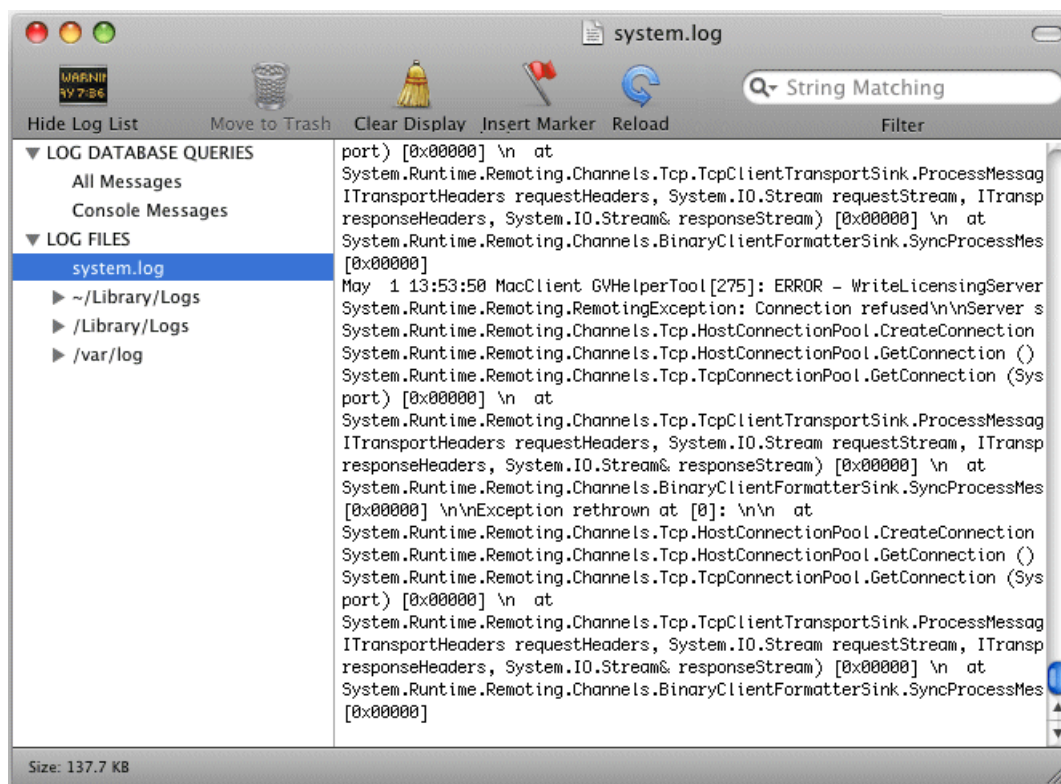
When you stop the K2Config for Mac Daemon, the service is stopped permanently, even after the Macintosh system is restarted. Once you have stopped the service, you must re-start it using the scripts.

### **Accessing logs**

1. Open the GV Helper Tool.
2. Click the **View Log** tab.



3. Click **View Log**.  
A Console window opens and displays logs.



4. Select **system.log**.

The system log displays. This is the log that contains entries relevant to the iSCSI connection to the K2 SAN.

5. To send log information to Grass Valley for analysis, copy text from the Console window, paste it into a text file and send the text file.

## ***Operation considerations***

- Do not neglect to make a “first birthday” image of each K2 product shortly after installation and configuration is complete.
- Changing system video standards (NTSC/PAL) requires a restart as part of the channel changes as soon as the new standard is selected. Configuration Manager causes an immediate restart of the K2 client if the system reference standard is changed and AppCenter is being used.
- Refer to the “Remote control protocols” appendix in the K2 System Guide for operation considerations related to AMP, VDCP, BVW, Harris, RS-422, etc.
- Tri-level sync is not supported on K2 systems.
- Before configuring audio tracks on a channel, eject all clips. This is required to put changes into effect.
- The K2 client and K2 Media Server can operate continuously for a long period of time, but the recommended operational practice is to restart at least once every three to six months.

# Known Problems

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

## AppCenter

---

CR102538	Description:	When attempting to create a sub-bin eleven levels deep, an error is displayed.
	Workaround:	Constrain nested sub-bins to ten levels deep or less.
CR102785	Description:	Consolidate media operation fails when the media file system is nearly full on the K2 Summit Production Client.
	Workaround:	Maintain free space on the media file system equivalent to the longest clip consolidated.
CR105208	Description:	Closed captioning and/or ancillary data not present in the last few seconds of a growing clip's playout. This occurs when playing out a clip that is being recorded, and the recording stops.
	Workaround:	Stop playout of growing clip before stopping recording. In any case the closed captioning and/or ancillary data is full-length in the recorded clip and present in subsequent playout.
CR106979	Description:	Timecode is incorrect if Time of Day source is set to LTC but LTC is disconnected or not present.
	Workaround:	Provide LTC or else set Time of Day source to System Clock.

---

## Storage Utility

---

CR94255	Description:	Bandwidth expansion of a K2 SAN can fail if the media file system is overly fragmented.
	Workaround:	Before attempting bandwidth expansion, contact Grass Valley Support for an audit of your file system.
CR101794	Description:	Storage Utility does not open for a nearline SAN. This occurs when in K2 Config you select the name of the K2 SAN, which is the top node of the storage system tree, when attempting to open Storage Utility.
	Workaround:	In K2Config tree view, under the nearline SAN's K2 Media Server, select the <b>File System Server</b> node to open its property page. On the property page click <b>Launch Storage Utility</b> .

---

**System**

---

CR88881	Description:	During failover testing a Failover Monitor error occurs, indicated by a "COM1 initialization failed" log message on redundant K2 Media Servers.
	Workaround:	Uninstall a serial port mouse driver. The driver is evidenced only when the error state occurs. On both K2 Media Servers, in Device Manager, look under Mouse Input devices. Identify the Serial Mouse, disable it, and then uninstall it. In addition check the boot.ini to make sure that the /fastdetect flag is enabled.
CR90857	Description:	The K2 Media Server displays an error because the Dell OpenManage server log fills up.
	Workaround:	Manually clear the log and then configure OpenManage to overwrite the log when full.
CR101017	Description:	VGA multi-view video monitor is disabled when logging on with remote AppCenter or when using Ctrl + Alt + Delete on keyboard on K2 Summit Production Client.
	Workaround:	Exit AppCenter, suspend channels, restart AppCenter, and then reset to use VGA multi-view video monitor.

---

**Installation**

---

CR102800	Description:	If uninstalling or installing K2 client software while applications or connections to AppService are open, the installation program becomes unresponsive.
	Workaround:	Use Task Manager to stop AppService. To prevent the problem from occurring, shutdown all application and connections before uninstalling or installing.

---