K2 Summit 9.3
Topic Library

This version of the K2 Summit Topic Library is provided for download. Once downloaded, this version is uncontrolled and is not tracked for updates. For the most current and up-to-date information refer to the online Topic Library at http://wwwapps.grassvalley.com/manuals/k2_summit_v9.3

Contacting Grass Valley

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

Grass Valley Web Site

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

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

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

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

END-OF-LIFE PRODUCT RECYCLING NOTICE

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

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

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

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

001187401

Contents

K2 Quick Start Guides

K2 Summit 3G Quick Start Guide

This Quick Start Guide is provided with a rotated orientation to optimize printing.

K2 Summit 3G Production Client Quick Start Guide

Before you begin, unpack the following items.

K2 Summit 3G Production Client

Recovery Flash Drive contains:
- K2 Summit Topic Library
- Software and disk images

NOTE: Do not lose the Recovery Flash Drive. It contains the recovery disk image for this specific K2 Summit system.

Rack slides

Licenses and Warranties

Power cords

LTC cables

Locate the documentation you need on the Recovery Flash Drive or access online at *http://www.apps.grassvalley.com/manuals/k2_summit/*

1. Make cable connections

Standard bi-directional channels

Each channel (C1, C2, etc.) can be an input (record channel) or an output (play channel). Connect video/audio IN and OUT to each channel, as appropriate for your intended use.

❶ Make SDI connections on each channel

Connections per channel (C1, C2, etc.)

SDI video in and out. Supports embedded audio.

AES audio

LTC I/O

RS-422

SDI connections

	Standard or 3G*	IN1	IN2	IN3
	Multi-Cam*	Active	Video1	Video2 Video3
	3D/Video + Key record*	Video (L eye)	Key (R eye)	
	3x/6x Super Slo-Mo*	Phase 1	Phase 2	Phase 3
		1topBot L	1topBot R	
	4K*			
	Standard or 3G*	Active	Active	Duplicates OUT1
	3D/Video + Key play*	Video (L eye)	Key (R eye)	
	Super Out*	Active	Super Out	Info
	4K*	1topBot L	1topBot R	

❷ Connect network cables to Ethernet ports

GigE Ports 1 2 3 4

❸ Connect power cord

❹ Connect VGA monitor

❺ Connect keyboard and mouse

❻ Optional PCIe board, such as a Fibre Channel board or a DynoZoom board

❼ Connect power cord

Ethernet cabling

Internal or direct-connect storage:
-Port 1 - Control network
-Port 2 - FTP/Streaming
-Ports 3 & 4 - Not used

Shared iSCSI storage basic:
-Port 1 - Control network
-Port 2 - Media (iSCSI) network

Shared iSCSI storage redundant:
-Port 1 & 4 - Control network
-Port 2 - Media (iSCSI) network A
-Port 3 - Media (iSCSI) network B

Shared FC storage basic:
-Port 1 - Control network

Shared FC storage redundant:
-Port 1 & 4 - Control network

SDI Connections:

*Some formats and conections require special license and configuration

Refer to the *K2 Topic Library* for complete configuration instructions.

2. Start up

❶ Before power on, take note of the chassis serial number, located behind the bezel/fan.

❷ Identify the Recovery Flash Drive, which is labeled with this unit's serial number. Make sure it remains stored with this specific unit.

❸ Replace the bezel/fan and identify the following:

Service LED, Service switch, Standby switch, Power LED

❹ Press the standby switch to power on.

❺ Log on with the default Windows admin account:
-Username: Administrator
-Password: adminGVI!

❻ On the Windows desktop, check the system tray. When the network indicates connectivity, the *K2 Summit* system is operational.

Normal startup sequence

Power LED goes on and stays on. Service LED stays off.

3. Configure network and, if necessary, storage

❶ Use SiteConfig as appropriate for your K2 system and on-site networking.

- **Stand-alone internal or direct-connect storage** – Install SiteConfig on a control point PC, discover the K2 Summit Production Client, and configure network interfaces.
  - Configure Control Team for the control network.
  - If desired, configure Media Connection #1 for the FTP/Streaming network.

  Refer to *K2 Topic Library* for instructions.

Default network settings

DHCP is enabled and the chassis serial number is the hostname.

- **Shared storage** – Configure network interfaces as instructed in the *K2 Topic Library*.

Ethernet connection names

This rear panel GigE port...	Is named this in Windows Network Connections...
1	Control Team (Control Connection #1)
2	Media Connection #1
3	Media Connection #2
4	Control Team (Control Connection #2)

❷ Configure network name resolution via host files or otherwise, as required by on-site networking. FTP/Streaming network hostnames must include "_he0" suffix.

❸ Configure storage as follows:

- **Internal storage** – No storage configuration is necessary. Storage is pre-configured.
- **Direct-connect storage** – Use Storage Utility to Bind RAID disks and make file system. Refer to the *K2 Topic Library*.
- **Shared storage** – Use the K2Config application to add the K2 Summit Production Client to the K2 SAN and configure it on the SAN. Refer to the *K2 Topic Library*.

4. Configure channels

❶ Open AppCenter and logon with the administrator account (User Name=Administrator/Password=adminGVI). If a licensing message appears, refer to *K2 Topic Library*.

❷ Click **System | Configuration**.

❸ Click tabs, buttons, and scroll bar to locate settings.

❹ Select from drop-down lists to make settings.

❺ Click **OK** and **Yes** to save settings.

K2 Solo 3G Quick Start Guide

This Quick Start Guide is provided with a rotated orientation to optimize printing.

K2 Solo 3G Media Server Quick Start Guide

Before you begin, unpack the following items.

- K2 Solo Media Server
- Recovery Flash Drive contains:
  - K2 Summit Topic Library
  - Software and images

  NOTE: Do not use the Recovery Flash Drive, it contains the image for this specific K2 Solo Media Server.
- Keyboard
- Mouse
- LTC cables
- Power cord
- Licenses and Warranties
- Accessories instructions

Locate the documentation you need on the Recovery Flash Drive or access online at *http://www.apps.grassvalley.com/manuals/k2_summit/*

1. Make cable connections

SDI connections

	IN1	IN2	IN3
Standard or 3G*	Active		
Multi-Cam*	Video1	Video2	
3DVideo + Key record*	Video (L eye)	Key (R eye)	
Super Slo-Mo*	Phase 1	Phase 2	Phase 3

	OUT1	OUT2
Standard or 3G*	Active	Active Duplicates OUT1
3DVideo + Key play*	Video (L eye)	Key (R eye)
Super Out*	Active	Super Out Info

Standard bidirectional channels

Each channel (C1, C2) can be an input (record channel) or an output (play channel). Connect video/audio IN and OUT to each channel, as appropriate for your intended use.

1. Make SDI connections on each channel
2. Connect network cables to Ethernet ports
3. If desired, connect reference
4. Connect VGA monitor
5. Connect keyboard and mouse
6. Connect power cord

Connections per channel (C1, C2, etc.)

- SDI video in and out. Supports embedded audio.
- AES audio
- LTC I/O
- RS-422

Make other connections as needed. Refer to the *K2 Topic Library* for complete instructions.

Ethernet cabling

- Port 1 - Control network
- Port 2 - FTP/Streaming
- Ports 3 & 4 - Not used

SDI Connections:

*Some formats and conections require special license and configuration. Refer to *K2 Topic Library* for configuration instructions.

2. Start up

1. Identify the following:
   - Standby switch
   - Power LED
   - Service LED
2. Press the standby switch to power on.
3. Log on with the default Windows admin account:
   - Username: Administrator
   - Password: adminGV!
4. On the Windows desktop, check the system tray. When the network icon indicates connectivity, the K2 Solo Media Server is operational.

Normal startup sequence

Power LED goes on and stays on. Service LED stays off.

3. Configure channels

1. Open AppCenter and logon with the administrator account (User Name=Administrator/Password=adminGV!). If a licensing message appears, refer to *K2 Topic Library*.
2. Click **System | Configuration**.
3. Click tabs, buttons, and scroll bar to locate settings.
4. Select from drop-down lists to make settings.
5. Click **OK** and **Yes** to save settings.

4. Record and play

Bi-directional channels

A channel becomes an input channel when you begin recording. The same channel becomes an output channel when you load a clip for playout.

1. Select a channel
2. Begin record
3. Stop record
4. Drag a clip into the channel
5. Adjust audio level as needed
6. Play the clip

Timecode for Record

On the AppCenter menu, click **Control | Options**. On the Options dialog box click **Timecode** and select the timecode for recording and display.

Continue with Quick Start procedures on the reverse side.

5. Create a playlist

6. Monitor

7. Configure network, if desired

Refer to *K2 Topic Library* for more information about SiteConfig and network configuration.

1. Take note of the chassis serial number, located on the rear of the unit.

Default network settings
DHCP is enabled and the chassis serial number is the hostname.

2. Choose your method for network configuration.
   - **SiteConfig** – Install SiteConfig on a control point PC, discover the K2 Solo Media Server, and configure network interfaces.
   - **Manual configuration** – At the local K2 Solo Media Server, use standard Windows operating system procedures.
3. Configure Control Team for the control network.
4. If desired, configure Media Connection #1 for the FTP/Streaming network.
5. Configure network name resolution via host files or otherwise, as required by on-site networking. FTP/Streaming network hostnames must include "-he0" suffix.

Ethernet connection names

This rear panel GigE port...	Is named this in Windows Network Connections...
1	Control Team (Control Connection #1)
2	Media Connection #1
(UNUSED) 3	Media Connection #2
(UNUSED) 4	Control Team (Control Connection #2)

8. For more information...

In AppCenter, click **Help | AppCenter Help Topics** and read the complete documentation for operating and configuring K2 Summit Production Client channels.

Find the complete K2 Topic Library from: *http://www.apps.grassvalley.com/manuals/k2_summit/*

Go to *http://www.grassvalley.com/support* and find solutions to problems.

Use the following information to contact product support by phone during business hours. Afterhours phone support is available for warranty and contract customers.

North America +800 547 8949
+1 530 478 4148

International—For local phone and email support go to: http://www.grassvalley.com/support/contact

grass valley
A BELDEN BRAND

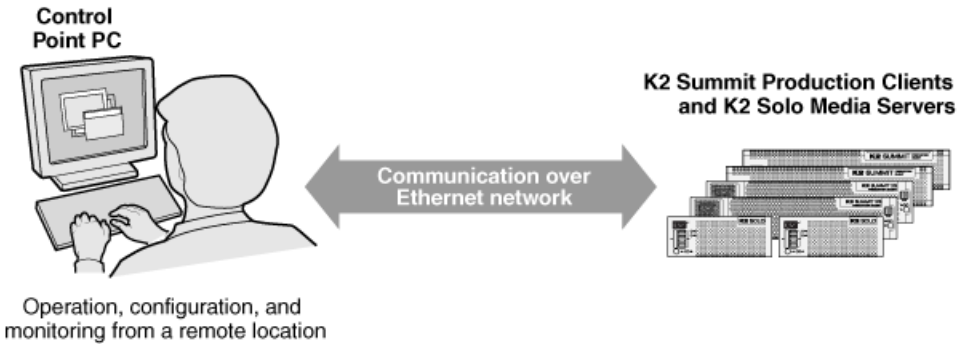
Using K2 AppCenter

Product Description

Topics in this section describe Grass Valley products.

About K2 systems

The K2 Solo 3G system is a cost-effective Broadcast Enterprise Server that incorporates IT server platform and storage technologies to deliver a networked solution to facilities for ingest, playout, news integration, sports, and media asset management. Each K2 system model is a comprehensive platform that provides a suite of user applications, system tools, and the largest range of third-party interactivity in the industry.



The K2 Solo 3G system is designed for “headless” operation from a remote control point using Grass Valley Control Point software. You can also use the Microsoft Windows Remote Desktop Connection application on your PC to connect to the K2 system for configuration or administration.

The K2 Solo 3G system is further described in the following topics. Also refer to topics on Transmission models for information unique to those products.

K2 Summit 3G system features

The following features apply to the K2 Summit 3G Production Client:

- Windows 7 64-bit embedded operating system.
- Embedded Security for protection against viruses and other unauthorized programs.
- Bidirectional channels (channel can be either an input channel or it can be an output channel).
- Two or four channels per chassis.
- SDI video inputs and outputs.
- AES/EBU or embedded audio inputs and outputs.
- Standard Definition (SD) video formats and High Definition (HD) video formats.
- Support for DV, MPEG-2, AVCHD/H.264, AVC-Intra, AVC - LongG, and Avid DNxHD. For details regarding licenses, hardware support, and video codec specifications, refer to related topics in the "Using K2 AppCenter" section of the K2 Topic Library.

- 3G codec module hosts codec option cards that are programmable for multiple formats and functions.
- Mixed format playback of SD or HD clips on the same timeline.
- Up/down/cross HD/SD conversion (e.g. SD and HD clips ingested, then played back as SD or HD clips) or as a different SD or HD format (e.g. 720p to 1080i).
- 4K, Super Slo-Mo, Multi-cam, and 3D/Video + Key features are available as part of the ChannelFlex Suite.
- 4K/UHD workflow and 4K/UHD Pan & Zoom using the GV DynoZoom software.
- High endurance SSD internal storage for 6-in/2-out configuration, 6x Super Slow Motion (SSM), and 4K/UHD workflow.
- VGA monitoring capability.
- Redundant power supply, cooling fans for reliability.
- 2.5 inch media storage drives.
- mSATA SSD system drive.
- Type IV CPU carrier module with 8 GB RAM.
- USB 3.0 interface for file exchange. (In K2 Summit 3G system only).
- Ability to create nested bins, i.e. sub-bins within bins.
- Freeze mode can be frame or field.
- Various video mix effects (e.g. dissolves between two video and audio tracks on the same channel, or fade thru matte color).
- Remote operation and configuration via AppCenter.
- Gigabit Ethernet.
- AMP, VDCP, and BVW remote control protocols supported.
- Remote control over RS-422 or Ethernet.
- Low-resolution proxy files created during record and live streaming from SDI In/out are available as part of the AppCenter Pro and Elite licenses.
- RAID media storage.
- Stand-alone internal storage, stand-alone external direct-connect storage, and external shared (SAN) storage.

K2 Summit system features

The following features apply to the first-generation K2 Summit Production Client:

- Bidirectional channels (channel can be either an input channel or it can be an output channel).
- Two or four channels per chassis.
- SDI video inputs and outputs.
- AES/EBU or embedded audio inputs and outputs.
- Standard Definition (SD) video formats and High Definition (HD) video formats.
- Mixed format playback of SD or HD clips on the same timeline.
- Up/down/cross HD/SD conversion (e.g. SD and HD clips ingested, then played back as SD or HD clips) or as a different SD or HD format (e.g. 720p to 1080i).
- VGA monitoring capability.
- Redundant power supply, cooling fans for reliability.
- 3.5 inch media storage drives.

- CompactFlash system drive.
- Ability to create nested bins, i.e. sub-bins within bins.
- Freeze mode can be frame or field.
- Various video mix effects (e.g. dissolves between two video and audio tracks on the same channel, or fade thru matte color).
- Remote operation and configuration via AppCenter.
- Gigabit Ethernet.
- AMP, VDCP, and BVW remote control protocols supported.
- Remote control over RS-422 or Ethernet.
- Super Slo-Mo, Multi-cam, and 3D/Video + Key features are available as part of the ChannelFlex Suite.
- Low-resolution proxy files created during record and live streaming from SDI In/out are available as part of the AppCenter Pro and Elite licenses. This requires the Type II carrier module.
- RAID media storage.
- Stand-alone internal storage, stand-alone external direct-connect storage, and external shared (SAN) storage.

K2 Solo 3G system features

The following features apply to the K2 Solo 3G Media Server:

- Windows 7 64-bit embedded operating system.
- Embedded Security for protection against viruses and other unauthorized programs.
- Bidirectional channels (channel can be either an input channel or it can be an output channel).
- Two channels per chassis.
- SDI video inputs and outputs.
- AES/EBU or embedded audio inputs and outputs.
- Standard Definition (SD) video formats and High Definition (HD) video formats.
- Support for DV, MPEG-2, AVCHD/H.264, AVC-Intra, AVC - LongG, and Avid DNxHD. For details regarding licenses, hardware support, and video codec specifications, refer to related topics in the "Using K2 AppCenter" section of the K2 Topic Library.
- 3G codec module. Codec option card not supported on K2 Solo 3G system.
- Mixed format playback of SD or HD clips on the same timeline.
- Up/down/cross HD/SD conversion (e.g. SD and HD clips ingested, then played back as SD or HD clips) or as a different SD or HD format (e.g. 720p to 1080i). Aspect ratios are adjusted.
- VGA monitoring capability.
- Compact Flash System drive.
- Type IV CPU carrier module with 8 GB RAM.
- USB 3.0 interface for file exchange.
- Ability to create nested bins, i.e. sub-bins within bins.
- Freeze mode can be frame or field.
- Various video mix effects (e.g. dissolves between two video and audio tracks on the same channel, or fade thru matte color).
- Remote operation and configuration via AppCenter.
- Gigabit Ethernet.

- AMP, VDCP, and BVW remote control protocols supported.
- Remote control over RS-422 or Ethernet.
- ExpressCard.
- Super Slo-Mo, Multi-cam, and 3D/Video + Key features are available as part of the ChannelFlex Suite.
- Low-resolution proxy files created during record and live streaming from SDI In/out are available as part of the AppCenter Pro and Elite licenses.
- Internal media storage.
- Support for Dyno S.

K2 Solo system features

The following features apply to the first-generation K2 Solo Media Server:

- Bidirectional channels (channel can be either an input channel or it can be an output channel).
- Two channels per chassis.
- SDI video inputs and outputs.
- AES/EBU or embedded audio inputs and outputs.
- Standard Definition (SD) video formats and High Definition (HD) video formats.
- Mixed format playback of SD or HD clips on the same timeline.
- Up/down/cross HD/SD conversion (e.g. SD and HD clips ingested, then played back as SD or HD clips) or as a different SD or HD format (e.g. 720p to 1080i). Aspect ratios are adjusted.
- VGA monitoring capability.
- CompactFlash system drive.
- Ability to create nested bins, i.e. sub-bins within bins.
- Freeze mode can be frame or field.
- Various video mix effects (e.g. dissolves between two video and audio tracks on the same channel, or fade thru matte color).
- Remote operation and configuration via AppCenter.
- Gigabit Ethernet.
- AMP, VDCP, and BVW remote control protocols supported.
- Remote control over RS-422 or Ethernet.
- ExpressCard.
- Super Slo-Mo, Multi-cam, and 3D/Video + Key features are available as part of the ChannelFlex Suite.
- Low-resolution proxy files created during record and live streaming from SDI In/out are available as part of the AppCenter Pro and Elite licenses. This requires the Type II carrier module.
- RAID 0 internal media storage.

K2 Summit/Solo formats, models, licenses, and hardware support

Formats are supported as in the following tables.

Table 1: First-generation K2 Summit/Solo system

Formats	Compression	1x	Multi-Cam, 3D/Video + Key	3x Super Slo-Mo	4K
SD	DV	Encode/decode	Encode/decode	Not supported.	Not supported.
	MPEG-2	Decode is standard. Encode requires codec option card.	Decode is standard. Encode requires codec option card.	Not supported.	Not supported.
	AVCHD	Not supported.	Not supported.	Not supported.	Not supported.
1080i/720p	DV	Encode/decode. Requires HD license.	Encode/decode. Requires HD license.	Encode/decode. Requires HD license.	Not supported.
	MPEG-2	Decode is standard. Encode requires codec option card. Requires HD license.	Decode is standard. Encode requires codec option card. Requires HD license.	Not supported.	Not supported.
	AVC-Intra	Encode/decode. Requires codec option card. Requires HD license.	Encode/decode. Requires codec option card. Requires HD license.	Not supported.	Not supported.
	AVCHD	Not supported	Not supported	Not supported	Not supported.
	AVC - LongG	Not supported	Not supported	Not supported	Not supported.
	Avid DNxHD	Not supported	Not supported	Not supported	Not supported.
1080p	AVC-Intra Class 100	Not supported	Not supported	Not supported	Not supported.

To add support for additional formats, contact your Grass Valley representative for upgrade information.

Table 2: K2 Summit 3G system

Formats	Compression	1x	3x Super Slo-Mo, Multi-Cam, 3D/Video + Key	6x Super Slo-Mo	4K
SD	DV	Encode/decode	Encode/decode	Not supported.	Not supported.
	MPEG-2	Encode/decode	Encode/decode. Requires codec option card.	Not supported.	Not supported.

Formats	Compression	1x	3x Super Slo-Mo, Multi-Cam, 3D/Video + Key	6x Super Slo-Mo	4K
	AVCHD/H.264	Decode only. Requires AVC license.	Not supported	Not supported	Not supported.
1080i/720p	DV	Encode/decode. HD license is required.	Encode/decode. HD license is required.	Encode/decode. Requires codec option card, plus HD and 6xSSM licenses. Requires K2 Summit 3G chassis with 2.5” hard drives for one channel or high endurance solid state drives for full features with two channels.	Not supported.
	MPEG-2	Encode/decode. HD license is required.	Encode/decode. Requires codec option card. HD license is required.	Not supported.	Not supported.
	AVC-Intra	Encode/decode. Requires HD and AVC licenses.	Encode/decode. Requires HD and AVC licenses.	Encode/decode. Requires codec option card, plus HD, 6xSSM and AVC licenses. Requires K2 Summit 3G chassis with 2.5” hard drives for one channel or high endurance solid state drives for full features with two channels.	Not supported.

Formats	Compression	1x	3x Super Slo-Mo, Multi-Cam, 3D/Video + Key	6x Super Slo-Mo	4K
	AVCHD/H.264	Decode only. Requires HD and AVC licenses.	Not supported	Not supported	Not supported.
	AVC - LongG	Decode only. Requires HD and AVC licenses.	Not supported	Not supported	Not supported.
	Avid DNxHD	Encode/decode. Requires HD and DNxHD licenses.	Encode/decode. Requires HD and DNxHD licenses.	Not supported	Not supported.
1080p	AVC-Intra Class 100	Encode/decode. Requires HD, 3G and AVC licenses.	Encode/decode. Requires codec option card, plus HD, 3G and AVC licenses.	Not supported	Encode/decode. Requires codec option cards and high endurance solid state drives. Requires HD, 3G, 4K and AVC licenses.

Table 3: K2 Solo 3G system

Formats	Compression	1x	Multi-Cam, 3D/Video + Key	3x Super Slo-Mo	4K
SD	DV	Encode/decode	Encode/decode	Not supported.	Not supported.
	MPEG-2	Encode/decode	Not supported	Not supported	Not supported.
	AVCHD/H.264	Decode only. Requires AVC license.	Not supported	Not supported	Not supported.
1080i/720p	DV	Encode/decode. HD license is required.	Encode/decode. HD license is required.	Encode/decode. HD license is required.	Not supported.
	MPEG-2	Encode/decode. HD license is required.	Not supported	Not supported	Not supported.
	AVC-Intra	Encode/decode. Requires HD and AVC licenses.	Encode/decode. Requires HD and AVC licenses.	Encode/decode. Requires HD and AVC licenses.	Not supported.

Formats	Compression	1x	Multi-Cam, 3D/Video + Key	3x Super Slo-Mo	4K
	AVCHD/H.264	Decode only. Requires HD and AVC licenses.	Not supported	Not supported	Not supported.
	AVC - LongG	Decode only. Requires HD and AVC licenses.	Not supported	Not supported	Not supported.
	Avid DNxHD	Encode/decode. Requires HD and DNxHD licenses.	Encode/decode. Requires HD and DNxHD licenses.	Encode/decode. Requires HD and DNxHD licenses.	Not supported.
1080p	AVC-Intra Class 100	Encode/decode. Requires HD and 3G licenses.	Not supported	Not supported	Not supported.

Features of internal storage models

K2 Summit/Solo systems have media drives as follows:

- First generation K2 Summit system — Up to eight media drives
- K2 Summit 3G system — Up to twelve media drives
- K2 Solo Media Server — Two media drives
- K2 Solo 3G Media Server — Two media drives

This makes the internal storage K2 system a self-contained, stand-alone unit, with no external devices for storage connections required. You can transfer media in and out of the internal storage K2 system via Gigabit Ethernet. You can also export media to a mapped drive or USB-attached storage. With the K2 Solo Media Server, you can also export media via an ExpressCard.

Features of external storage models

The external storage K2 Summit system contains only the system drive. There are no media drives in an external storage K2 Summit system. There are two types of external storage for media, as follows:

- Shared storage — Multiple external storage K2 Summit systems connect to the K2 SAN via Gigabit Ethernet or Fibre Channel to share a common pool of storage.
- Direct-connect storage — A single K2 Summit system with the optional Fibre Channel board installed connects directly to its own external (non-shared) RAID storage device. This makes the direct-connect K2 Summit system a self-contained, stand-alone unit, with no additional devices for storage connections required. You can transfer media in and out of the direct-connect K2 Summit system via Gigabit Ethernet.

About remote operation and monitoring

The K2 Summit/Solo system is designed as a “headless” unit. This means that there is no need to connect a keyboard, monitor, and mouse directly to the K2 system, as ongoing operation, configuration, and monitoring can be accomplished from a PC on the network. You can lock the K2 system locally, as you would normally lock a Windows computer, but still access it from a Control Point PC. From this Control Point PC, you can use channels from different sources in one channel suite. The K2 AppCenter application is included with the K2 system and supports this headless functionality.

Automation protocols and other optional applications can also be used to control K2 systems remotely. For more information, refer to the "Configuring the K2 System" section of this Topic Library.

The K2 AppCenter status bar can be used to monitor the K2 system as it ingests, outputs, or transfers media.

Windows Remote Desktop Connection

You can use the Microsoft Windows Remote Desktop Connection application to make a remote connection to a Grass Valley system that runs the Windows operating system.

Take the following into consideration when connecting to K2 systems:

- Before you can use the Remote Desktop Connection, you need network access and permissions to connect to the K2 system.
- You can use either the name or the IP address to access the K2 system.
- Do not use the Remote Desktop Connection to access the PC running the Control Point software or to access the AppCenter application; results may be unreliable.
- Take care when accessing an online K2 system on which media access is underway. The additional load on network and system resources could cause unpredictable results.
- Lack of robust video/graphic support can cause video display problems. Remote desktop connections can interrupt proxy and live streaming. AppCenter video monitoring is not supported through Remote Desktop Connection.

About K2 Summit system storage options

The K2 Summit system can have internal storage for stand-alone use, or it can have storage that directly connects to the K2 Summit system. Multiple K2 Summit systems can share storage on a K2 SAN.

The K2 SAN is Grass Valley’s shared storage solution that gives multiple clients access to a common pool of media. Clients access the shared media storage via a Gigabit Ethernet network and a Fibre Channel connection. Data is communicated using the Small Computer System Interface (SCSI) data transfer interface and the Internet SCSI (iSCSI) protocol. For more information on the K2 SAN, refer to this document.

Licensing

Grass Valley continues to develop the K2 product family to better meet a wide range of customer requirements. As these developments become available, you can add the specific functionality you need with Grass Valley software licenses. Detailed procedures for installing licenses come with option kits or are included in release notes for K2 products. Contact your Grass Valley representative to learn more about the licensing structure and for purchasing information.

Software version licenses

At major software releases, significant new features are added. If you are licensed for the software release, you can upgrade your software and received the benefits of the new features.

Licensable options

Optional applications, bundles of advanced features, and enhanced functionality are available as licensable options for K2 products.

AppCenter licenses are as follows:

	AppCenter Standard	AppCenter Pro	AppCenter Elite
Record	X	X	X
Continuous Record	X	X	X
Play	X	X	X
Sub-Clipping	X	X	X
Playlists	X	X	X
"Live" Mode (Chase Play)	X	X	X
Video Monitor in Control View	X	X	X
VM Multi-view	X	X	X
Playlist Import		X	X
Channel Ganging		X	X
Audio Track insert		X	X
CC Track insert		X	X
Audio Track assignments		X	X
Scheduled Record per channel (not playlist)		X	X
Scheduled Playback per channel (not playlist)		X	X
Super out on SDI 2 output		X	X
Playlist with M/E Transitions		X	X

	AppCenter Standard	AppCenter Pro	AppCenter Elite
Flying M/E Transitions		X	X
Proxy encoding - 4 Channels		X	X
Key+ Fill import (QT32)		X	X
Channel Flex Suite			X
- Multi-CAM			X
- 4K			X
- Video + Key			X
- 3D - Left + Right Eye			X
- Super Slo-Mo x2			X
- Super Slo-Mo x3			X
- Super Slo-Mo x6			X
Proxy encoding - 8 Channels			X

Other options and applications include the following:

- HD option
- AVC option (Summit/Solo 3G)
- Avid DNxHD option (Summit/Solo 3G)
- 3G option (Summit/Solo 3G)
- 3G 1080p option (Summit 3G)
- 4K option (Summit 3G)
- 3-input Multi-Cam channel (Summit/Solo 3G)
- K2 TimeDelay
- K2 XML Import capture service
- HotBin Export capture service
- P2 Import capture service
- K2 Extended File Services
- K2 InSync
- K2 FCP Connect

As development continues, new options become available. Contact your Grass Valley representative to learn more about current options.

Getting Started

Passwords and security on Grass Valley systems

To provide a basic level of security, Grass Valley systems recognize three different security levels based on Windows users and groups, and the systems ship from the factory with accounts

pre-configured accordingly. To access the system you must log on with the user name and password for one of the pre-configured accounts.

The following table shows the different types of users and their privileges. Passwords are case sensitive.

	Windows administrator	Grass Valley product administrator	K2 product administrator	Grass Valley product user
User name	Administrator	GVAdmin	K2Admin	GVUser
Password	adminGV!	adminGV!	adminK2	userGV!
AppCenter Configuration Manager	Full access	Full access	Full access	Can view
AppCenter	Full access	Full access	Full access	Full access; requires an account on the K2 Summit/Solo system
Storage Utility	Full access	Full access	Full access	Can't access
K2Config	Full access	Full access	Full access	Can't access
Server Control Panel	Full access	Full access	Can view	Can view
Windows Operating System	Full access	Full access	Limited access (based on Windows user account privileges).	Limited access (based on Windows user account privileges)

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

Starting AppCenter

You can start AppCenter by clicking on the AppCenter shortcut on the Windows desktop.

If you are using AppCenter on a local K2 Solo 3G system, you can begin using it immediately after you log on. The first time you run AppCenter remotely through a network-connected Control Point PC, you need to set up a channel suite before you can use AppCenter.

NOTE: If the* K2 Solo 3G system *was shut down using Windows XP Standby mode, AppCenter will not start up, even though the* K2 Solo 3G system *machine itself boots up normally.

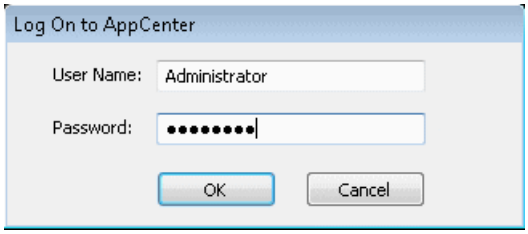
Starting AppCenter for the first time with a Control Point PC

Before you can run AppCenter from a network-connected PC running Control Point software, you must do the following:

1. Log on to AppCenter.
2. Configure a channel suite.

Logging on to AppCenter

The first time you start AppCenter, a Log On dialog box displays. Enter your user name and password.



NOTE: Your domain configuration might require that you use the syntax of machine name\user name. For example, if you have difficulty logging on to a* K2 Solo 3G system*, try logging on as <K2 system>\GVUser.

Once you have logged in, the Suite Properties dialog box displays.

Configuring a channel suite

You need to configure the channel suite before you can use it. To configure a channel suite, specify the K2 source that you want to use and add its channels to a channel suite. You can add channels from several sources to one channel suite, with a maximum of 16 channels in one channel suite.

1. At the blank Suite Properties dialog box, click the **Add** button. An Add Channel dialog box displays.
2. Enter the K2 Solo 3G system host name or IP address.
3. Click **OK**. A second Add Channel dialog box displays, listing the channels on the specified K2 Solo 3G system.
4. Select the channels you want in your channel suite and click **OK**.
5. Review the changes you have made to the Suite Properties dialog box and click **OK**.

Once you have saved the changes to the channel suite, you can modify the channel suite's name and location or rename or reorganize the channels. Descriptive channel names are especially helpful when using a channel suite with channels from multiple sources.

Starting AppCenter after creating a channel suite

For subsequent AppCenter startups using a Control Point PC, AppCenter will attempt to start by opening the last-used channel suite. If you have deleted or moved the last-used channel suite, you need to create a new channel suite or cancel the Channel Suite Properties dialog box and open the channel suite you want to use.

If you are running AppCenter with a Control Point PC, AppCenter opens with the last-used channel suite. To change the channel suite, select **System | Open Suite** or **System | New Suite**. To open one of the four last-used channel suites, select **System | Recent Suites**. Channel suites are saved by default in the C:\Profile\ChannelSuites directory in XML format.

If one of the channels is not available, the title bar for that channel will display its state, for example: "In Use", "Disconnected", and so on.

Locking AppCenter

You can lock both local AppCenter running on a K2 Solo 3G system and remote AppCenter running on a Control Point PC.

You can lock the AppCenter interface so that keyboard and mouse input is disabled.

- To lock AppCenter, do the following:
  - Click **System | Lock AppCenter**.

  The Lock AppCenter dialog box appears. All keyboard and mouse input to AppCenter is now disabled. The Lock AppCenter dialog box remains on the screen as an indicator that AppCenter is locked.
- To unlock AppCenter, do the following:
  - On the Lock AppCenter dialog box, click **Unlock** and when prompted "…unlock AppCenter?" click **Yes**.

  The Lock AppCenter dialog box closes. Keyboard and mouse input to AppCenter is now enabled.

Shutting down AppCenter

To shut down AppCenter, do one of the following:

- Click the standard Windows **X** button in the title bar.
- Select **System | Shutdown**. The Shutdown dialog box opens.

AppCenter shut down options

When you shut down AppCenter, you have the following options:

Shutdown Mode	Description
Exit to Windows	Exit AppCenter and display the Windows desktop. If shutting down AppCenter from a Control Point PC, close the channel suite and display the Windows desktop. If you select this option, a second dialog box displays asking you to confirm that you want to exit, since any applications that are running (including remote protocols) will be stopped. Use the desktop shortcut to restart AppCenter.
Suspend channel suite	Exit AppCenter and display the Windows desktop. Applications and remote protocols in suspended channel suites keep running. Channels may be commandeered by another user using another Control Point PC. If all channels in a suspended channel suite are taken over in this manner, the channel suite is shut down. If you want to shut down the current channel suite but keep AppCenter running, you can open or create a channel suite in the System menu. Use the desktop shortcut to restart AppCenter.
Restart	Exit AppCenter and restart the Windows operating system.
Shut Down	Shut down the Windows operating system and power-off the K2 Solo 3G system.

NOTE: If you shut AppCenter down locally, you must re-start it locally.

NOTE: If you shut down AppCenter from a network-connected Control Point PC, the* K2 Solo 3G system *is still running and can be accessed locally or from another network-connected Control Point PC.

About system messages

The following messages are displayed to indicate system status:

- Normal BIOS messages — These messages can be observed on a locally connected VGA monitor during normal startup processes.
- BIOS POST error messages — If there is a problem these messages are displayed on a locally connected VGA monitor. During the Power On Self Test (POST), the BIOS checks for problems and displays these messages.
- AppCenter startup messages — As AppCenter opens the system determines if health is adequate by checking critical subsystems. A dialog box is displayed that indicates progress and displays messages.
- Status bar and StatusPane messages — During normal operation AppCenter displays system status messages on the status bar. From the status bar you can open the StatusPane to see both current and previous messages. You can observe these messages in AppCenter on a locally connected VGA monitor or on a network connected control point PC.
- Storage Utility messages — While you are using Storage Utility, pop-up message boxes inform you of the current status of the storage system.

Critical system startup messages

The following messages appear in the AppCenter system startup message box as critical subsystems are checked during startup processes. If a critical failure is detected, the K2 Solo 3G system is rendered inoperable and the failure message appears.

Critical subsystem check messages	Failure messages
System Startup	Startup error
	Missing or bad hardware
	A real time processor is not functioning correctly
Checking hardware…	Hardware fault
Checking media disks…	One or more media disks failed to initialize
	Missing or bad hardware
	Missing or bad database
Checking file system…	No file system is running
Checking database…	Database fault
Checking real-time system status…	A real-time system failed to initialize
Updating configuration…	Failed to synchronize configurations
Starting services…	Unable to communicate with <service name>

AppCenter startup errors

If you start AppCenter and the K2 Solo 3G system is not running, or your login information is not correct, you will see a Startup Error message.

The following table describes the two most common startup error messages.

Startup Error	Description
Log on failed	Your user name or password is not valid for this K2 Solo 3G system. Remember that the password is case sensitive. • Click **Ignore** to view the AppCenter channels. If working remotely, you will see the channels from the last-used channel suite. Or, • Click **Retry** to enter the login information again. Or, • Click Abort. If you are accessing AppCenter through a network-connected Control Point PC, **Abort** lets you try to create a new channel suite. If you are accessing AppCenter locally, it lets you exit to Windows. For assistance with your user name or password, consult your Windows administrator.

Startup Error	Description
<K2 system>:<error>	The K2 Solo 3G system might be offline or have had difficulty with the start up checks. There are various reasons why AppCenter is having difficulty connecting to the K2 Solo 3G system; for example, the error might say there is no file system or that the K2 Solo 3G system has been taken offline for maintenance. • Verify that the host name or IP address is correct and see if you can correct the problem. • If working locally, reboot the K2 Solo 3G system. If working from a network-connected Control Point PC, select **System | Reconnect** from the AppCenter **System** menu.

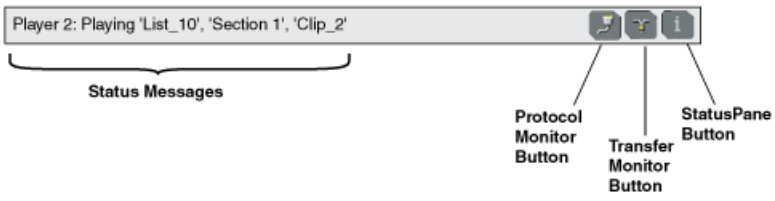
Viewing AppCenter system status messages

System status messages are displayed in the AppCenter status bar. There are two types of system status messages, as follows:

- Channel status messages — In normal operation, this type of message displays the current operating status of the selected channel.
- System error messages — If a problem develops with the system software or a hardware subsystem, this type of message is displayed for approximately 5 seconds. Afterward, the display returns to the channel status message and the error message is written to the status log file. When a message is written to the status log, a *Status Icon* indicates the severity of the message.

Status bar

System status messages appear in the AppCenter status bar, which is located across the bottom of the AppCenter window, and consists of a message area, several tool buttons, and a status icon. The button icons appear only when the related function is active. In the position of the StatusPane button, status icons appear.



The status bar displays information about the state of the delegated channel as well as low-level error messages. (High priority error messages are displayed in pop-up windows.)

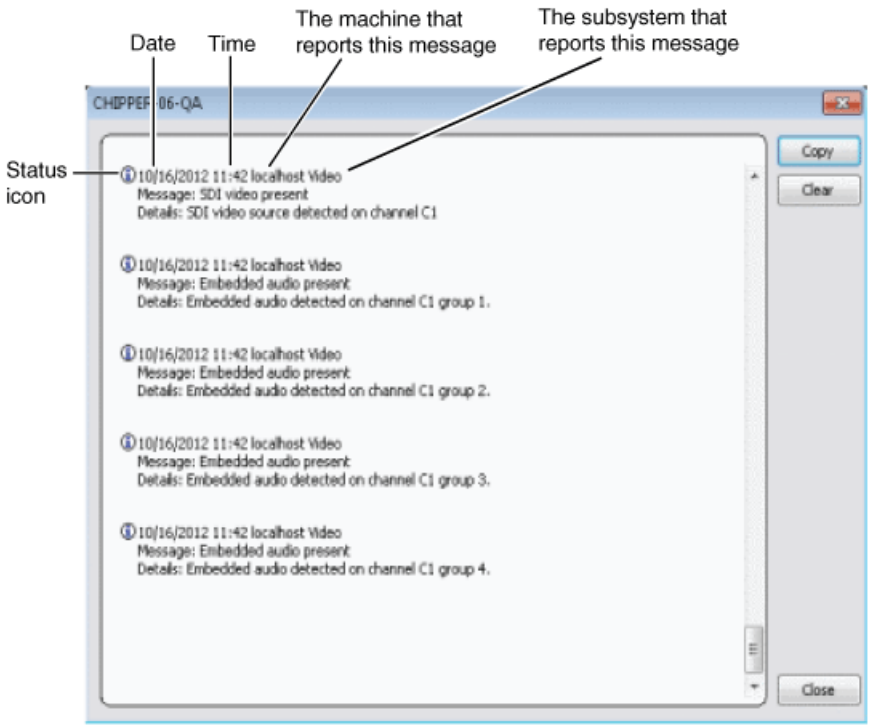
If you select a channel, a status message appears on the left-hand side of the status bar. If a potential error arises while an application is running in a channel, a status message flashes briefly on the left-hand side of the status bar, and an icon displays on the right-hand side. Double click on the icon to open the status pane to view a more detailed message about the channel's status.

The status icon changes depending on the status of the current status message.

Icon	Name	Description
	Information	A recent information message is present.
	Warning	There is at least one warning message, and no alert messages.
	Alert	There is at least one uncleared alert message.

Status pane

Current and previous system status messages can be viewed in the StatusPane. The system status pane also displays general information such as the video and audio settings on the channels. To open the StatusPane, click **Help | System Status**.



The StatusPane is used to view detailed system messages including status, warning, and error messages. System status messages provide status icons and a description of the status event reported by the message. If there is a problem, a corrective action is indicated. Use these messages along with troubleshooting problems to determine if a service procedure is necessary.

If you have a remote AppCenter Channel Suite with channels from multiple K2 systems, the messages from the different machines are combined in the StatusPane that you view from the Channel Suite. To help you determine which machine is generating a message, each message lists the machine name.

NOTE: If the Clear button is grayed out, you do not have the necessary privileges to perform this action, based on the type of user account with which you are currently logged on.

Copying StatusPane messages to the clip board

1. Select the message or messages in the StatusPane.
2. Click **Copy**.

After copying the message, it can be pasted using standard Windows techniques.

Clearing messages

Clearing messages from the StatusPane removes them from the logging database and the StatusPane. This also clears the state of the subsystem indicators so they no longer display the alert and warning symbols.

1. Open the StatusPane, then click **Clear**.
2. When a message prompts you to confirm, click **Yes**.

All messages are removed from the StatusPane and logging database.

Exporting log files

This topic describes how to export log files from the K2 Solo 3G system. The log files include the following:

- All application and media database messages
- Version information
- Configuration file, from Configuration Manger

The exported files are combined in a ZIP file. The ZIP file can be sent to Grass Valley product support where they can analyze the logs to determine the operational status of your system.

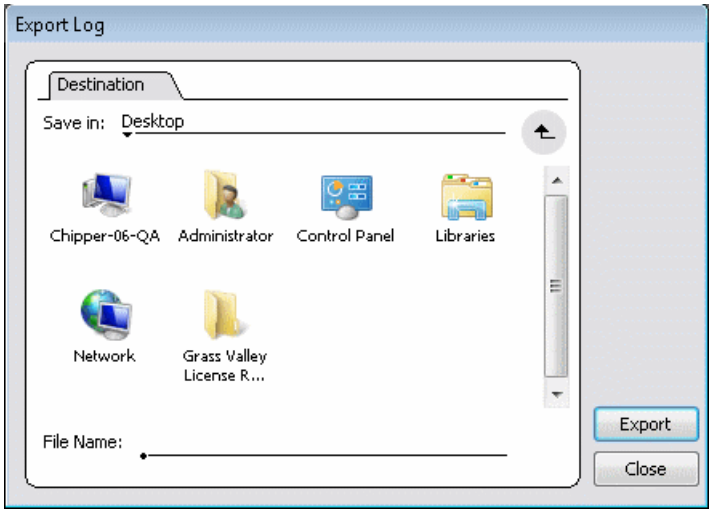
NOTE: ExportLog does not export StatusPane messages. To capture StatusPane messages, you can copy StatusPane messages to the clip board.

1. Log in as Administrator.

2. Do one of the following to open the Export Log dialog box.

   - In AppCenter click **System | Export Log**.
   - From the Windows desktop, click **Start | All Programs | Grass Valley| Export logs**.
   - From the Windows desktop, click **Start | Run**, type `c:\profile\exportlog` in the Run dialog box, then click **OK**.

   The Export Log dialog box opens.



3. Browse to *C:\Logs* to save the log file.
4. Name the log file.
5. Click **Export**. A progress bar appears.
6. When the export process is complete, and message confirms success. Click **OK** and close the Export Log dialog box to continue.
7. Find the log file at the specified location.

Configuration Manager

The Configuration Manager is the primary configuration tool for a K2 Solo 3G system. It makes settings that apply to the overall internal storage K2 Solo 3G system as well as settings that apply to individual channels.

Configuration Manager settings are stored in a database. When the K2 Solo 3G system starts up it reads the current settings from the database and configures itself accordingly. When you modify a setting in Configuration Manager you must save the setting in order to update the database and reconfigure the K2 Solo 3G system.

You can also save settings out of Configuration Manager into a configuration file, which is a stand-alone XML file. Likewise, you can load settings into Configuration Manager from a configuration file. However, you must use Configuration Manager as the means to save the settings to the database before the settings actually take effect. Configuration files are not linked directly to the database.

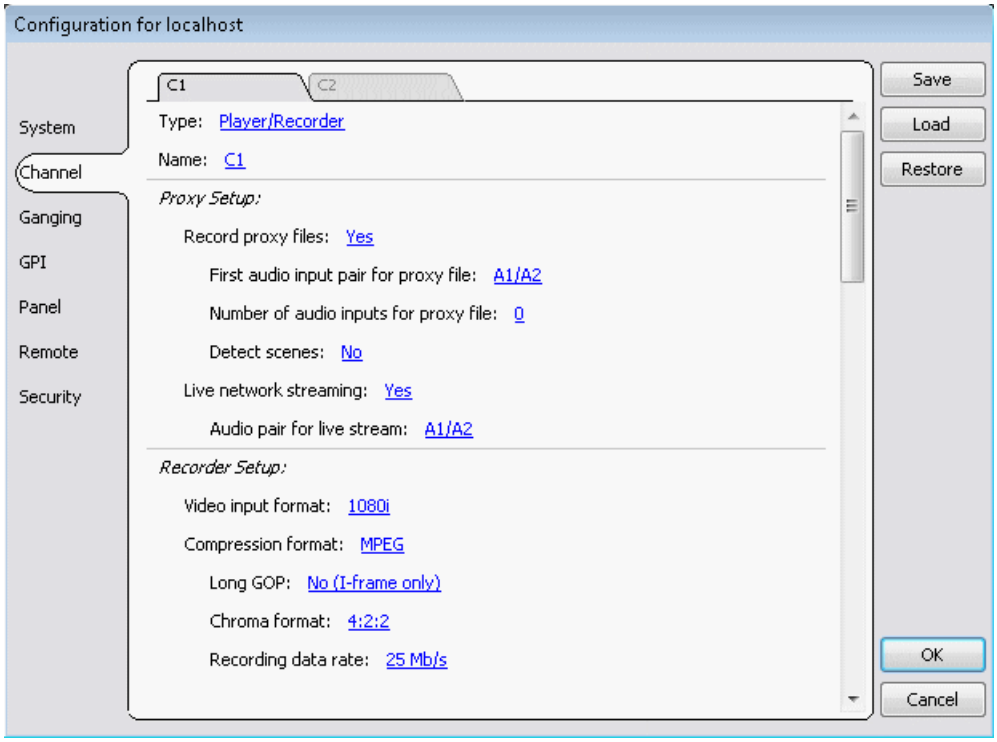
You can use configuration files as a means to back up your settings. You can also use configuration files to save several different groups of customized settings, each with a unique name, so that you can quickly load settings for specialized applications.

If you save a configuration file and then upgrade your K2 system software, there can be compatiblity issues. If the upgraded software version has new features, the saved configuration file might not be compatible.

Accessing Configuration Manager

You access Configuration Manager through the K2 AppCenter application from the local K2 Solo 3G system or from the Control Point PC.

To access the configuration settings, open AppCenter and select **System | Configuration**.



Saving and restoring Configuration Manager settings

Settings can be saved as a configuration file. You can save any number of uniquely named custom configuration files. You can load a configuration file to restore system settings.

To save custom settings:

1. In the Configuration Manager, click the **Save** button.
   The Save As dialog opens.
2. Use the up arrow or select folders to navigate to the folder in which you want to save the configuration file.

3. Enter a name for the configuration file.

   Do not name the file *Default*Config.xml, as this name is reserved for the factory default configuration file. Otherwise, standard Windows 2000 and up file naming restrictions apply.

4. Click **Save** and **Close**.

To restore custom settings:

1. If you want to save current settings, you should save them as a configuration file before continuing.
2. In the Configuration Manager, click the **Load** button.

   The Open dialog opens.

3. Use the up arrow or select folders to navigate to the custom configuration file.
4. Select the custom configuration file.
5. Click **Open**.

   The custom settings are loaded into Configuration Manager, but they have not been saved and put into effect.

6. Click **OK** to save and apply settings, and to close the Configuration Manager.

Restoring default Configuration Manager settings

You can restore factory default settings as follows:

- Restore some individual settings or groups of settings by selecting the **Default** button which appears below the settings in the configuration screen.
- Restore all the settings in Configuration Manager at once to their default values as explained in the following procedure.

1. If you want to save current settings you should do so before proceeding.
2. In the Configuration Manager dialog, click **Restore**.

   The default settings are loaded into Configuration Manager, but they have not yet been saved and put into effect.

3. Click **OK** to save settings and close Configuration Manager.

Storage Utility for standalone K2 Solo 3G system

There are two versions of Storage Utility:

- Storage Utility for the K2 SAN
- Storage Utility for stand-alone K2 systems

This manual explains Storage Utility for stand-alone K2 Solo 3G system. Refer to the *K2 SAN Installation and Service Manual* to learn about Storage Utility for the K2 SAN.

NOTE: For shared storage, run Storage Utility only via the* K2Config *application.

The Storage Utility is your primary access to the media file system, the media database, and the media disks of the K2 Solo 3G system for configuration, maintenance, and repair. It is launched from the K2 AppCenter application.

⚠ ***CAUTION: Use the Storage Utility only as directed by a documented procedure or by Grass Valley Support. If used improperly, the Storage Utility can render your K2 system inoperable or result in the loss of all your media.***

NOTE: Do not use the MegaRAID utility on a K2 system. This utility is for use by qualified Grass Valley Service personnel only. When this utility is opened it scans the SCSI bus and interferes with record and play operations.

Accessing Storage Utility

Grass Valley strongly recommends that you access Storage Utility by selecting **System | Storage Utility** in AppCenter. However, if you are unable to access AppCenter, then open Storage Utility by clicking on the Storage Utility desktop icon. 

For Storage Utility procedures for internal storage, refer to *K2 System Guide*. Refer to the *K2 SAN Installation and Service Manual* to learn about Storage Utility for the K2 storage system.

NOTE: Use the Storage Utility only as directed by a documented procedure or by Grass Valley Support. If used improperly, the Storage Utility can render your K2 system inoperable or result in the loss of all your media.

K2Config

The K2 System Configuration application (K2Config) is the primary tool for configuring systems in the category of a K2 SAN, which include online or production K2 SANs, K2 Nearline systems, and GV STRATUS Proxy Storage systems. Once the devices of the storage system are cabled and are communicating on the control network, you can do all the configuration required to create a working K2 SAN using the K2Config application. When you use SiteConfig for network configuration, you can import the SiteConfig system description file into the K2Config application to get you started with your SAN configuration.

After your K2 SAN is initially installed and configured, if you need to reconfigure the system you should do so using SiteConfig and the K2Config application. This enforces consistent policy and sequencing for configuration tasks, which makes the system easier to maintain and aids in troubleshooting should a problem arise.

The K2Config application runs on a control point PC and accesses the devices of the K2 SAN via the control network. You can configure the devices of the K2 SAN as follows:

- SAN-attached K2/Summit systems and K2 Media Server — These devices are configured directly by the K2Config application.
- K2 RAID storage devices — The K2Config application launches a remote instance of Storage Utility, which configures RAID storage devices. Storage Utility components run on the K2 Media Server and the configuration actually takes place via the Fibre Channel connection between the K2 Media Server and the RAID storage device.
- Ethernet switches — The K2Config application can launch a switch's web-based configuration application.

You can expand and select nodes in the tree view to view K2 SANs, individual devices, and configuration settings. The configuration file is saved on the V: drive, along with the media files in the shared storage system. The configuration file is updated and saved whenever you change a configuration using the K2Config application. That is why you must always use the K2Config

application to change settings on the storage system, so the most recently changed configurations will always be stored in the configuration file and displayed.

About SiteConfig

SiteConfig is Grass Valley's tool for network configuration and software deployment. SiteConfig is a ProductFrame application. ProductFrame is an integrated platform of tools and product distribution processes for system installation and configuration.

You can use SiteConfig as a stand-alone tool for planning and system design, even before you have any devices installed or cabled. You can define networks, IP addresses, hostnames, interfaces, and other network parameters. You can add devices, group devices, and modify device roles in the system.

As you install and commission systems, SiteConfig runs on a designated PC. It discovers devices, configures their network settings, and manages host files. SiteConfig also manages software installations and upgrades and provides a unified software package with compatible versions for deployment across multi-product systems.

You should use SiteConfig for network configuration and software deployment at installation and throughout the life of the system in your facility. This enforces consistent policy and allows SiteConfig to keep a record of changes, which makes the system easier to maintain and aids in troubleshooting should a problem arise.

SiteConfig displays information from a system description file, which is an XML file.

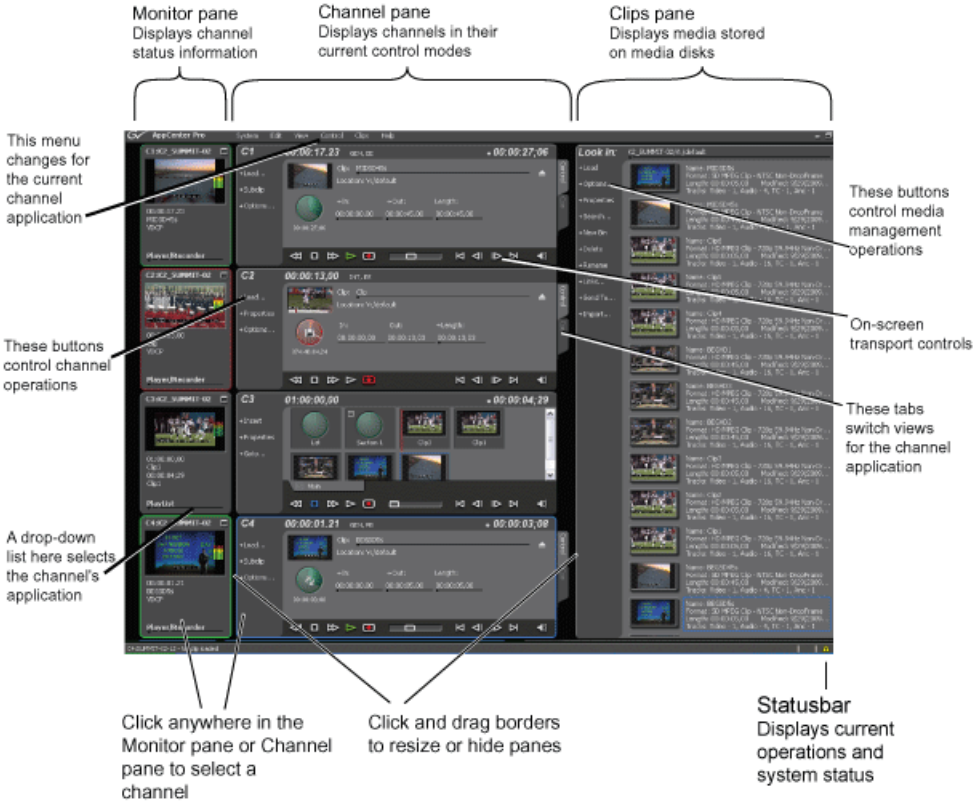
Using AppCenter

About AppCenter

AppCenter is the built-in video disk recorder and player application that provides a single interface for tasks such as channel control, configuration, clip management, media transfers, channel monitoring, and system monitoring.

You can access AppCenter using a network-connected PC with Control Point software or you can access it by connecting a VGA monitor, mouse, and keyboard to the K2 Solo 3G system. To support live video, the VGA resolution must be 1024 x 768 x 32 or greater to support live (moving) video monitoring. If the monitor resolution is not adequate, AppCenter might limit the number of visible channels to three or less.

NOTE: If you are using the optional K2 TimeDelay application, see the K2 TimeDelay online help for information on using TimeDelay with AppCenter.



Main components in the AppCenter user interface

The following table describes the main components in the AppCenter window:

AppCenter Component	Description
Monitor pane	Displays the current information for the channel. Displays a thumbnail of the clip currently loaded in the channel and indicates the current control application for the channel. Shows EE or playback video. Contains a drop down menu for changing the channel's application. For the currently selected channel, the monitor pane has a white background.
Channel pane	Displays each channel in its current application. Only one channel can be selected at a time. The currently selected channel is displayed with a white background.
Clips pane	Displays media stored on the K2 Solo 3G system and provides controls for media management.
Status Bar	Displays status and error messages, and includes tool buttons for opening Transfer Monitor, Status Pane, or the Protocol Monitor dialog box.

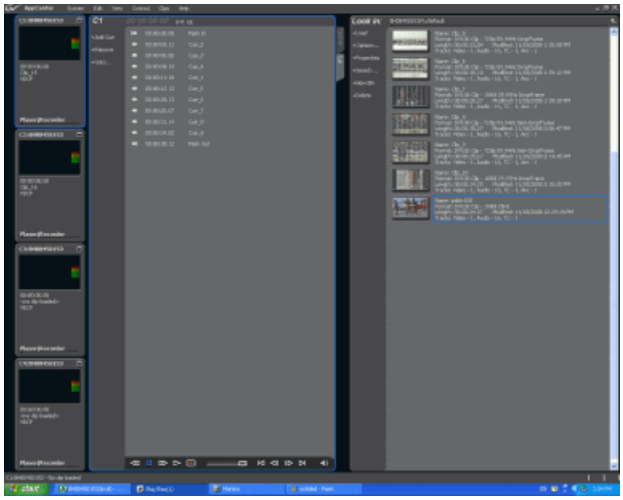
Playing channels in multi-view screen

- Select **View | Video Monitor** to fill the entire screen with a view of all four channels' monitor panes. This is useful when you want to monitor video from several different channels simultaneously.

The VGA resolution must be at least 1024 x 768 x 32 to support live video. The multi-view video monitor option is only available on a local K2 Solo 3G system; it is not accessible from a PC running Control Point software. It requires the Grass Valley AppCenter Pro application, which is separately licensed from the AppCenter application. For more information, consult your Grass Valley representative.

Playing the channel pane in full screen

- Select **View | Full screen** to fill the entire channel pane with only the selected channel. This is useful when you need more room to display information, such as a long series of clips in the text view of the player application.



- To return to split screen, select **View | Split screen**. If all channels cannot be displayed, a scrollbar appears on the left side of the pane. Scrolling in the channel monitor pane also applies to the control applications when viewed in Split Screen mode.

Tools in AppCenter

AppCenter includes the following tools for managing the K2 Solo 3G system and its assets.

Tools	Essentials Tasks
Configuration Manager	Configuring system settings
Transfer Monitor	Monitoring media transfers, including network transfers and file import/export
Online Help	Complete documentation of operational tasks

Conventions used in the AppCenter interface

The following table describes the graphical conventions used for the user controls in the AppCenter interface. These graphical elements are used throughout the interface to indicate such items as drop-down lists and text entry controls.

	Convention	Graphical Description and User Action
❶	Drop-down list	A horizontal line and arrowhead. Select and choose from a list of items in the drop-down list.
❷	Context Menu	This menu changes depending on the application of the selected channel: player/recorder or playlist.
❸	Text Entry Control	A horizontal line and small dot. Select to open the text entry dialog box.
❹	Eject Button	Select to eject the current clip
❺	View Tabs	Select one tab or the other to toggle between different views in Player application or in Playlist application.
❻	Timecode Entry Control	A horizontal line and small dot. Select to open the timecode entry dialog box.
❼	Meter bar Button	Select to toggle between the Meter bar and the application interface. The Meter bar contains audio meters, and the audio level controls.
❽	Assignable Button Groups	Some button groups are assignable. Holding down a button opens a pop-up menu that lists the alternative button choices. This allows you to customize the user interface to suit your workflow.

Terms and concepts used in AppCenter

Assignable buttons – Some buttons are assignable, meaning you can change the order that buttons appear in some button groups to better suit your workflow. Holding down the left mouse button on an assignable button causes a pop-menu to appear that lists the alternative button choices for that button.

Bin – A bin is a container used to organize assets like clips and lists in the same way as directories or folders are used on a typical computer system. Bins can be nested inside other bins. A bin is associated with a single disk volume.

Channel application – Channels in AppCenter are always in one application or another. Each application has its own set of buttons, lists, controls, and other characteristics, relative to the operations performed in that application. The name of the application for the channel is displayed in the channel's monitor pane, which is also where you can change the application for the channel.

Clip thumbnail – Used for visual identification of a clip. By default, the thumbnail is generated from the 16th frame of video. You can select a new thumbnail using Player. If no thumbnail is available, an icon is displayed showing there is no thumbnail.

Current Bin – The current bin functions as the target bin when recording clips or creating playlists. It is also the source bin used to load clips and lists.

Selected channel – There is always one channel that is selected. When a channel is selected, the channel is displayed with a blue outline around the channel pane. The monitor pane has a red outline if recording and a green outline if playing a clip or playlist; if selected while the channel is inactive, the monitor pane is also outlined in blue. The keyboard is delegated to controlling the selected channel. To select the channel either select a channel in the monitor pane or press a keyboard shortcut. Changing the channel selection does not disrupt other channels, they continue to operate in the background.

Storage – The term "Storage" is used to refer to external, shared storage. Storage that is used with a stand-alone K2 Solo 3G system will be specifically designated as "internal storage" or as "direct connect" storage, which is storage directly attached to the stand-alone.

Timecode – Timecode is displayed in hours:minutes:seconds:frames. However, the timecode syntax differs based on whether the video is drop frame or non-drop frame.

	First Field	Second Field
Non-drop frame	. (period)	: (colon)
Drop frame	, (comma)	; (semicolon)

For example, in drop frame timecode, a clip could start on 01:15:00,04 and end on 01:15:00;09.

Volume – The set of media drives that functions as a single physical disk.

Channels overview

A channel is a set of resources that together have the capability to record or play media. AppCenter channels have applications for performing tasks such as recording or playing. When AppCenter starts, each channel comes up in an application. There is always one channel selected in AppCenter. The title bar displays the selected channel's name and the control application running on it.

When a channel is selected, the control application that is using that channel is the active control application. To select a channel, click on the channel monitor pane or click the control application in the control applications pane. The selected channel can receive input from the keyboard. Selecting a channel does not affect processing on any of the other channels, which operate in the background.

In a channel suite, you can name a channel or change the order in which the channels appear in the AppCenter window.

Administrators can set user permissions for each channel. Depending on your security settings, you could be denied permission to operate a channel. For more information, see the *K2 System Guide*.

Channel suites

A channel suite is a collection of channels. If you are using AppCenter through a network-connected PC with Control Point software, the channels are accessed through a channel suite. Channel suites allow you to customize the channels to run particular applications or save the clips to specific locations. You can add channels from different sources to one channel suite. Each channel suite can have up to 16 channels.

NOTE: If you are running a* K2 Solo 3G system *locally, you cannot use channel suites. You can only use the channels on that K2 system.

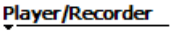
Channels in AppCenter

In AppCenter, the channels are labeled C1, C2, C3, C4 (for K2 Summit systems) or C1 and C2 (for K2 Solo systems). Each channel is bidirectional, that is, you can designate the channel to any application available on the system. Once you designate a channel to run a specific application, the channel remains designated to the application until you change it. You can change the channel's application in the Channel monitor. ChannelFlex Suite functionality is configured in Configuration Manager.

Channel applications overview

AppCenter channels have applications for performing essential tasks. When AppCenter starts, each channel comes up in its last used application. You can change the channel application.

Selecting a channel application

1. In the monitor pane, select the channel application drop-down list 

for the channel.
2. Choose an application.

The selected application replaces the current application and appears in the channel's space in the channel pane. The channel becomes the selected channel.

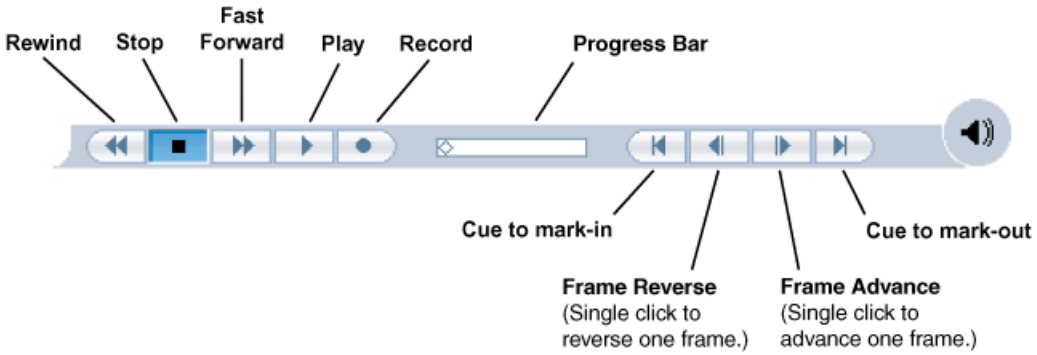
Available channel applications

AppCenter provides standard Playlist and Player/Recorder applications to run on a channel without any special licensing. TimeDelay, Event Monitor, ChannelFlex Suite and other licenses make additional channel applications available.

Remote protocol applications are configured on each channel under **Control | Options**. Standard remote protocol applications are AMP, BVW, VDCP. The Event Scheduler license enables the Event Monitor application.

Using on-screen transport controls

When a channel is selected, the on-screen transport controls appear. All standard channel applications have on-screen transport controls.



Using remote protocols

You can control AppCenter using remote control devices and applications software developed for the K2 Solo 3G system that use industry-standard serial or Ethernet control protocols. You can enable remote control mode from AppCenter.

About Event Scheduler support

When licensed for Event Scheduler, the Event Monitor application is available. This application is a monitor-only application that displays the list of events scheduled in Event Server for a channel. The events must be scheduled by another application.

Indicators and controls in Event Monitor are as follows:

black text	For an event whose time has passed (above the time cursor), this event has completed successfully. For an event in the future (below the time cursor), this event is not yet scheduled or pending.
red text	An error occurred when processing this event.
dashed red line	This is displayed over the event that is in progress.
blue text	This event is pending, on the timeline and ready to begin at the specified time.
expand/contract icon	This icon is displayed beside absolute events in the list. Use it to hide or show the events after it.

Configuring a channel for remote control

You can configure a channel for remote control either locally or through a network-connected Control Point PC. Operating remote control from AppCenter provides extended features that allow local and remote control at the same time.

You can select a remote protocol to use with individual channels.

To modify the remote protocol setting for a channel:

1. Click on the channel whose protocol you want to specify.
2. Select **Control | Options**. The Options dialog box displays.
3. If it is not already displayed, select the **Control** tab.
4. Select the desired protocol and remote settings, and click **OK**. If using VDCP protocol to control transfers, you must set up the video network and the *Controller ID*.

   NOTE: The protocol control port is pre-set and cannot be modified.
5. Test the system and recheck settings, if required.

Protocol Mode	Description
Local only	Allows you to monitor the record or play channel operations and view clip information locally only. There is no control from any external device.
Remote only	Allows you to monitor the record or play channel operations and view clip information only using remote protocol. All control comes from the external device. The buttons, menu items, and other interface controls are disabled. You can select this mode by choosing the Remote only option in the Options dialog box
Local and Remote	Allows you to control the record or play channel locally as well as remotely. You can select this mode by choosing Remote and Local in the Options dialog box.

Recording Clips

About recording clips

The Player/Recorder application records clips in AppCenter. You can play the clip while it is still recording, or you can finish the recording, and then play the clip or add it to a playlist. In addition to recording clips, you can add cue points to clips and create new sub clips.

The Player/Recorder application requires a player/recorder channel. The application has two views — Control view and Cue view. The Control view allows you to record clips. The Cue view is used to add, remove, or rename cue points within a clip and create new subclips.

Select record channel signal inputs – Before you start recording, you might need to select video, audio, and timecode inputs.

Missing or intermittent timecode:

- If VITC, LTC or ANC is the selected timecode source and the signal is missing, the current timecode display shows XX:XX:XX:XX while the clip is being recorded. After the recording has finished, the clip is automatically re-striped starting from 0. Also, clips recorded without timecode will show no mark-in/mark-out timecode after recording.
- When VITC or LTC is detected, but the signal is intermittent, the display shows XX:XX:XX:XX any time the signal disappears. Clips with missing or intermittent timecode will show this behavior during playback in a play channel.
- If VITC or LTC is intermittent, try one of the following solutions:
  - Use the internal timecode generator as the timecode source for recording.
  - Stripe the timecode after the clip is recorded using the Recorder/Player application.

Re-recording and appending clips is not supported through the AppCenter – You cannot record over a previously recorded clip. To replace the unwanted clip, delete it and record a new one. Also, appending to previously recorded clips is not supported; once the recording is stopped, you cannot start the recording again using the same clip. If a clip is currently loaded when record is selected, the clip is ejected, and a new clip is created before recording begins.

NOTE: Appending to previously recorded clips is supported through AMP Serial Control Protocol. Contact Grass Valley for more information on control devices available.

No pre-roll time — Recording begins as soon as record is selected.

About continuous record mode

Continuous record allows you to specify a fixed-length recording that records continuously. When the fixed length you specify is reached, AppCenter begins to erase the oldest media in 3 minute segments to make room for new media. In this way, new media is continuously recorded while the recording is kept to a fixed length. (For very long continuous records, the segment size groups up to 15 minutes.)

The continuous recording is stored as a program. The program thumbnail is displayed in the Clips pane immediately after the recording starts. While recording, you can load the continuous record program in another Recorder/Player application for playout or to create subclips. The media referenced by the subclips that you create is saved outside the continuous record program and does not subtract from the continuous record length. The subclips can be inserted in a Playlist application as play events.

NOTE: A program, such as a playlist, cannot be saved in AVI format.

Continuous mode operational considerations

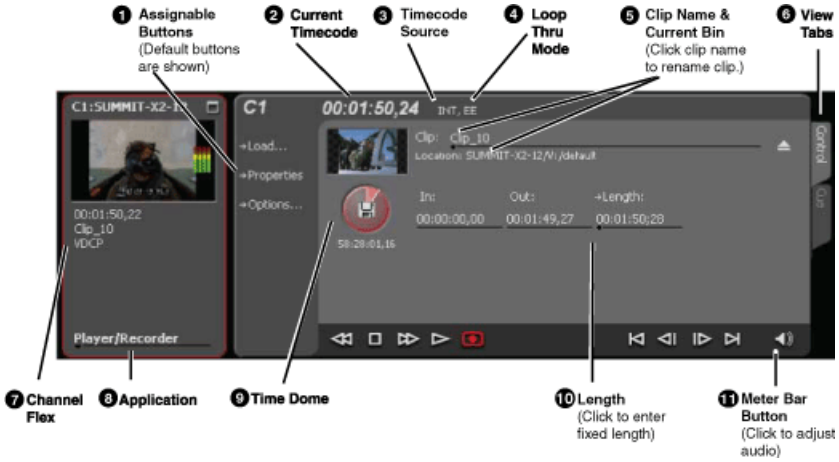
Consider the following when planning for Continuous Record operation:

- Maximum continuous record length– Maximum record length is limited by the amount of storage space and the compression settings used. If the fixed length you enter exceeds the available disk space, the fixed length is automatically adjusted to equal the available space.
- Modifying the continuous record name or length– You can modify the continuous record name or length during record. If you reduce record length, the oldest media outside the new record length is erased.

- Stopping continuous record– If the recording is stopped before the fixed length is reached, the resulting program duration is the time elapsed since the recording started. Like normal record mode, you cannot stop then start a continuous recording. Once record is stopped, you must eject the program and create a new continuous record.
- Transferring the continuous record program– The continuous record program cannot be transferred to a file or networked device until record is stopped.
- Continuous record storage space is not reserved– Continuous record is allowed to start as long as the record length you enter is less than the available storage; however, the storage space is not reserved. For example, you could have enough storage space to start the continuous record, but you are still allowed to transfer media or otherwise fill disk space. Warning messages are displayed in the AppCenter StatusBar when available storage reaches 10% total disk space. All recording is halted when media storage reaches its full threshold.
- Pausing the continuous record program in Recorder/Player application– You cannot pause the continuous record program in Recorder/Player application indefinitely. Eventually, the record length is reached and the video at the current position is erased. As this happens, the current position is advanced in 3 minute increments as the oldest unused media is erased.
- Changing thumbnail image– Thumbnail images displayed in the Clips pane are generated using the 16th frame of video. The thumbnail image for a continuous record program appears as normal until the fixed length is reached. Then, the thumbnail will update every 3 minutes as media is erased beginning with the oldest unused media. As the media used to generate thumbnails is erased, new thumbnails are generated.
- Erasing oldest media is suspended when creating a subclip– When creating subclips in Player application, erasing oldest media is suspended when the first mark is entered (mark-in or mark-out). This means that the continuous record program length could grow larger than the length specified. Erasing media is resumed and the oldest media outside the fixed length is purged when the second mark is entered and you select the Accept button. You could inadvertently fill storage space if you enter the subclip marks, but fail to click the Accept button. NOTE: Erasing oldest media is also resumed when you exit subclip mode by ejecting the subclip, or by clicking the Source Clip button.
- Use genlocked inputs for time delay– For error-free time delay operation, ensure that the video input is genlocked to the video reference signal. This will eliminate periodic picture shift.

Guide to using the Recorder/Player application: Control view

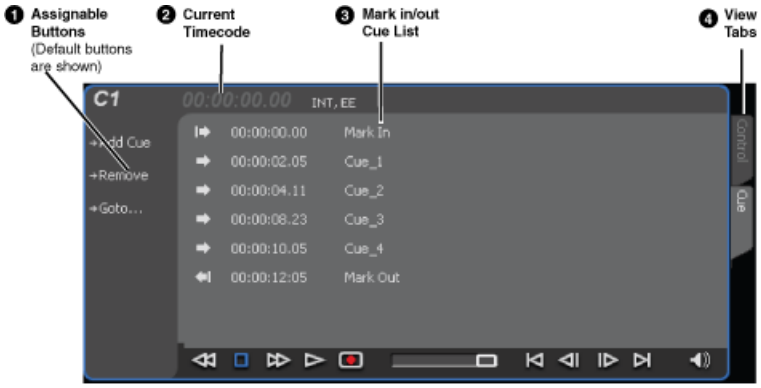
The following shows the basic controls in the Recorder/Player application found in AppCenter, which uses the Player/Recorder application to record a clip. The Player/Recorder channel is referred to as C1, C2, C3 or C4.



	Control	Description and User Operation
❶	Assignable buttons	Assignable buttons allow you to modify the button assignments to best suit your workflow. Hold down a button to open a pop-up menu that lists the alternative button choices.
❷	Current timecode	Indicates the current timecode of the timecode source selected for the channel. Text color is white during record, and dimmed at other times. The timecode value of XX:XX:XX:XX is displayed when the timecode source is not present or is invalid.
❸	Timecode source	The text displayed to the right of current timecode indicates the timecode source.
❹	Loop thru mode	This text indicates if “E-to-E (LoopThru) mode” is selected. See Record Menu below.
❺	Clip Name Edit Control	Displays the clip’s name and location in the media storage system. To rename the clip, click and enter text. You can change the current bin. You can use the Clips pane to manage and organize clips.
❻	View tabs	These tabs toggle between Control and Cue Points view.
❼	ChannelFlex	If the channel is configured to be a ChannelFlex type, it is displayed in this area. ChannelFlex requires an AppCenter Elite license.
❽	Application	A drop-down list allows you to select between None, Playlist, Player/Recorder, or (if licensed for AppCenter Elite) addition selections. If the Player/Recorder application is selected, you can play or record using the pane controls.

	Control	Description and User Operation
❾	Time Dome	This multi-function indicator displays either record progress only, or available storage and record progress. The Time Dome also indicates when the record channel is in Continuous Record mode. Available storage is estimated using the amount of free disk space and the video compression settings for the channel. The record progress indicator makes one revolution every 10 seconds in normal record, or one revolution during a fixed length recording. You can change the Time Dome function by right-clicking on the Time Dome and choosing an application from the pop-up menu.
❿	Length	Select the Length control to enter the clip length, then choose record. Recording continues until you choose stop or the specified fixed length is reached.
⓫	Meter bar button	Displays the Meter bar, which contains the audio record level controls and signal meters. Changes to the audio level are saved for the channel.
	Recorder **Control** menu	**Load Clip** – Opens the Load Clip dialog box. (Only available on the SD-00 K2 Summit Production Client) **New Clip** – Used to create and name clip prior to starting the recording. If a clip is already loaded, selecting New Clip ejects the current clip and creates a new one. **Schedule Start Time** – Opens the Trigger At entry box so a start time can be entered. **Locate** – Locates the currently loaded clip in the Clips pane. **Properties** – Opens the Properties dialog for the currently loaded clip. **Auto Subclips**– The auto subclip check box changes the way that the subclip mode behaves. When it is NOT checked, clips have to be accepted manually. When it is checked, a subclip will be created as soon as you set a mark out. **Widescreen** – Sets the channel for recording widescreen format. (720p and 1080i clips are always recorded in widescreen, whether this is selected or not.) **E-to-E (LoopThru) mode** – When selected, the following occurs: “EE” is displayed on the channel pane, next to the Timecode Source indicator; when no clip is loaded, the signal that is currently present at the channel input is passed through; when a record operation stops the clip remains in the Recorder. The signal that is currently present at the channel input passes through (video, audio, and timecode).

Guide to using the Recorder/Player application: Cue view



	Control	Description and User Operation
❶	Assignable Buttons	Assignable buttons allow you to modify the button assignments to best suit your workflow. Hold down the left mouse button to open a pop-up menu that lists the alternative button choices.
❷	Current Timecode	Indicates the current timecode of the timecode source selected for the channel. Text color is white during record, and dimmed at other times. The timecode value of *XX:XX:XX:XX* is displayed when the timecode source is not present or is invalid.
❸	Timecode Source	Indicates the mark in, mark out, and cue points of the recording session.
❹	View tabs	These tabs toggle between Control view and Cue Points view.
	Recorder Cue View **Control** Menu	In addition to commands described in the Assignable Buttons section, the Control menu of the Cue view contains the following option: **E-to-E mode** – When selected, the following occurs: "EE" is displayed on the channel pane, next to the Timecode Source indicator; when no clip is loaded, the signal that is currently present at the channel input plays out; when a record operation stops the clip remains in the Recorder. The signal that is currently present at the channel input plays out.

Before you record: Recorder settings checklist

Before recording, check the following recorder channel settings.

Record Channel Setting	Procedure
Verify video and audio input selection	In the monitor pane, check the thumbnail and its audio level indicators to verify the correct record channel inputs are selected. If there is a problem, correct the settings.
Verify video compression data rate. You can manage storage capacity and video quality by adjusting the record channel compression data rate. Generally set as high as possible to obtain the storage capacity needed.	Under the **System** menu, click **Configuration**.
Verify digital audio compression setting	Under the **System** menu, click **Configuration**.
Verify the timecode source. Make sure to select a valid timecode source. You can use the internal timecode generator, VITC, or LTC.	Refer to the procedure to change the timecode source.
Verify widescreen mode setting. This setting only applies to SD clips. If the SD video source is in widescreen format, select widescreen mode for the recorder. This attribute is saved with the clip. (720p and 1080i clips are always recorded in widescreen, whether this is selected or not.)	In AppCenter main menu, select the desired Player/Recorder channel, set the Control view tab, and select **Control | Options | Widescreen 16:9** to toggle widescreen mode. ***NOTE: The clip aspect ratio cannot be changed once the clip is recorded. If you want to change the clip's aspect ratio attribute you must re-record the clip.***
Adjust audio level (if needed). You can use the audio leveling feature to adjust the analog or digital audio input levels, excluding dolby encoded digital audio.	In the Recorder pane, select the **Meter bar** button. Adjust audio level using the graphical faders. Select the Meter bar button again to return to Recorder view.
Verify audio monitor settings. You can select which audio channels to monitor.	Select **Control | Options** and click the **Audio** tab.
Verify working bin. The clip is recorded to the currently configured working bin, regardless of the bin currently displayed in the Clips pane.	Select **Control | Options** and click the **Bin & AFD** tab.

Record Channel Setting	Procedure
Verify video compression settings. Choosing a video compression setting is a trade-off between image quality and storage capacity. Higher video quality produces larger files which take up more storage space and take longer to transfer to external devices.	Select **System | Configuration** to modify the video compression settings.

To record a clip

Topics in this section provide instructions for recording a clip.

Using New Clip record mode

To create and name a clip before recording starts:

1. Verify video, audio, widescreen, and other settings for your recording.
2. Select **New Clip** to create and load a clip.
3. To rename the clip, select the default clip name  , then enter a new clip name.
   If a Multi-Cam channel, you can name both clips.
4. Select the record button on the onscreen transport controls.

   The recording progresses until you select **Stop**.

Using Crash record mode

Crash record occurs when you start a recording without specifying a clip name. The clip is given a default name, then the recording continues until you select stop.

To crash record:

1. Verify video, audio, and other settings for your recording.
2. Select the record button on the onscreen transport controls.

   The recording progresses until you select **Stop**.

Scheduling a recording

This feature is part of the licensable AppCenter Pro option.

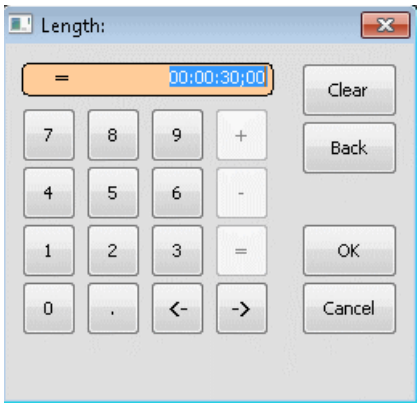
You can schedule a recording to start at a specified time. Scheduled Start Time uses Time of Day timecode source, which can be driven by either the system clock or LTC. VITC or Anc VITC/LTC cannot be used to drive the Time of Day.

1. Select **Control | Schedule Start Time**.
   Trigger at entry box appears.
2. Enter the time when you want the recording to start and click **OK**.
   The time of day, trigger time, and a countdown are displayed.

Using Fixed Length record mode

You can specify the clip length before recording, or during recording. As long as there is sufficient storage space, a fixed length recording continues until the clip length is reached or until you select stop.

1. Verify video, audio, and other settings for your recording.
2. Select **Length** in the Recorder pane.



   The Length dialog box appears.

3. Enter the clip length by typing only numbers, colons are added automatically.
4. Choose **OK** in the dialog box, or press **Enter**.
5. Select the record button on the onscreen transport controls.

Recording continues until **Stop** is selected or the desired length is reached. While recording, the mark in and mark out update with the current status of the clip. The Time Dome gives a visual indication of the percent complete as well as a countdown from the specified length down to **00:00:00:00**.

Specifying clip length after recording has begun

While a clip is recording you can enter the clip length as follows:

1. Select **Length** in the Recorder pane.

   The timecode dialog box appears.

2. Enter the desired length, then select **OK** or **Enter**.

   If the entered length is valid, and longer than the amount of material already recorded, the clip continues to record until it reaches the specified length or until you select **Stop**.

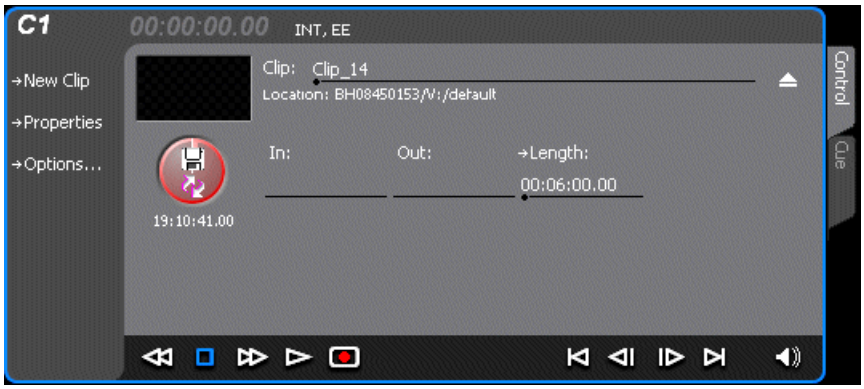
Using continuous record

You can configure Recorder for Continuous Record mode. Continuous record is useful for applications that normally use Continuous Record, for example a manual time delay.

1. Click the **Time Dome** button.

   The Time Dome pop-up menu appears.

2. Choose **Continuous Record** in the pop-up menu.



   The Time Dome changes to display continuous record.

3. Click **Length**.

   The Length dialog box appears.

4. Enter the clip length by typing only numbers, colons are added automatically.
5. Click **OK** in the dialog box, or press **Enter**.
6. Select the record button on the onscreen transport controls.

   Recording continues until **Stop** is selected. While recording, the mark in and mark out update with the current status of the clip. The Time Dome gives a visual indication record progress.

7. Load and play the clip in Player/Recorder application:

   - Drag and drop from the recording monitor pane to the playing monitor pane.

   The play channel becomes the selected channel, and the clip is cued and ready for play.

Previewing a clip that is recording

Preview loads the currently recording clip into a play channel. The play channel becomes the selected channel, and the clip is cued and ready for play.

To preview a clip:

1. Start the record process.

2. Preview the clip:
   a) In the Monitor pane, use the drop-down list to select the Player application.
   b) Drag the clip thumbnail from the channel running the Recorder application to the channel running the Player application.

   The play channel becomes the selected channel, and the clip is cued and ready for play. If a play channel is already playing a clip, no warning message is displayed in the status bar.
3. To play the clip, select the onscreen transport controls.

Using cue points while recording

Cue points enable you to move quickly from one frame to another in a clip. You can use cue points to manage clip play out or create subclips. You can add, remove, or rename cue points while a clip is being recording.

To add a cue to a clip while the clip is recording, you need to begin the recording while in Control mode. Once the recording has begun, you can switch to Cue mode and modify the clip with cue points.

Adding a cue point while recording

NOTE: While the clip is record mode, do not use the transport controls.

1. Select Player/Recorder from the application drop-down list.
2. Begin recording.
3. In the Record pane, click on the Cue tab. The Cue view displays.
4. Do one of the following:
   - Click the **Add Cue** button.
   - Select **Control | Add Cue**.

   A cue point is added to the cue list using a unique name, e.g. Cue_1.

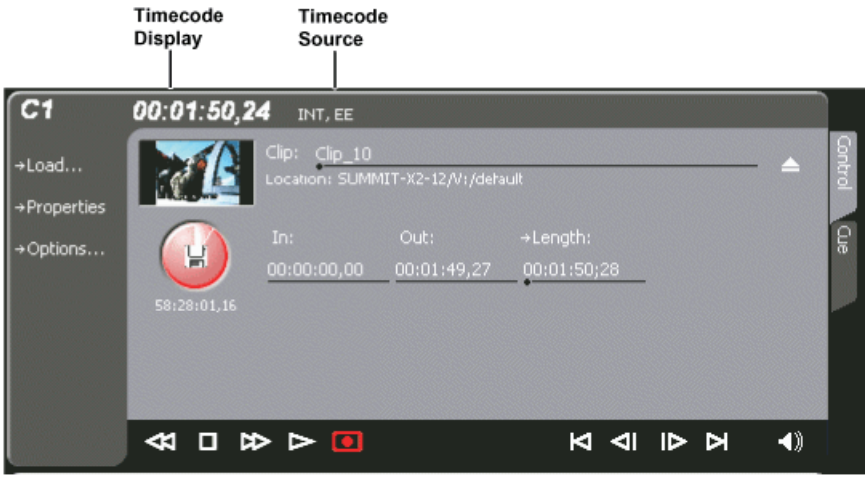
Removing a cue point

1. While recording, click on the Cue tab.
2. Select a cue point in the list.
3. Do one of the following:
   - Click the **Remove** button.
   - Select **Control | Remove**.

Renaming a cue point

1. While recording, click on the Cue tab.
2. In Cue view, select a cue point in the list.
3. Select **Control | Rename.**
4. Use the text entry dialog to enter a new cue name, then click **OK** or press **Enter**.

Changing the timecode source



To change the timecode source:

1. Click on the channel whose timecode you want to specify.
2. Select **Control | Options**. The Options dialog box displays.
3. **Timecode** tab.
4. Choose a timecode source, then click **OK**.

Timecode Source	Description
AncVITC	Available on HD channels only. Timecode is read from ancillary VITC.
VITC	Available on SD channels only. Timecode is read from the VITC input for the channel.
LTC	Available on HD/SD channels.Timecode is read from the LTC input for the channel.
AncLTC	Available on HD channels only. Timecode is read from ancillary LTC.
Time of Day	Available on HD or SD recordings. Time of Day is an internal generator. You can select either LTC feeds or Windows system clock as the clock source to drive the generator. LTC feeds can be from Channels 1, 2, 3, or 4.
Start Time	Available in HD or SD. When Start Time is selected, you can specify the timecode to use when the recording starts. The drop frame option is enabled when the system timing is set to the 525 line standard (NTSC). Drop frame timecode allows the generator to operate as an accurate clock.

Configuring the free run timecode setting

When you select this setting along with a timecode source setting, the K2 Solo 3G system system ignores any dropouts or discontinuities in the incoming timecode after a recording starts. You must make this setting on each channel. It is not a global, system-wide setting.

1. Click on the channel whose timecode you want to specify.
2. Select **Control | Options**. The Options dialog box displays.
3. Select the **Timecode** tab.
4. Select the **Free run while recording** checkbox and then click **OK**.

Selecting widescreen mode

When recording SD video that is 16:9 aspect ratio, select the widescreen attribute. To change the Widescreen attribute, select **Control | Widescreen**.

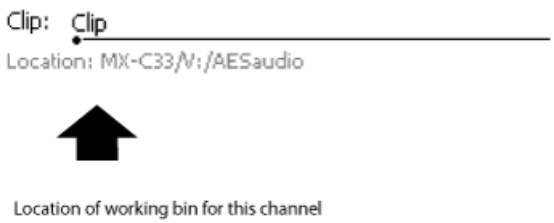
The attribute is saved as part of the video media file. On up-conversion playout, the attribute is used by the Player/Recorder channel to handle aspect ratio on playout when the clip is played on K2 Solo 3G system.

NOTE: AppCenter always records 720p and 1080i video in the 16:9 ratio, whether the widescreen attribute is selected or not.

Changing the current bin

On the K2 system, a fixed amount of disk space is reserved for storing media files— the V:\ partition. Within the V:\ disk partition, your clips and playlists are stored in *bins*, which function like directories in a file system. You can organize your media by creating and removing bins in AppCenter. You can have channels from multiple sources in one channel suite; the clips displayed are those on the source that has the currently selected channel.

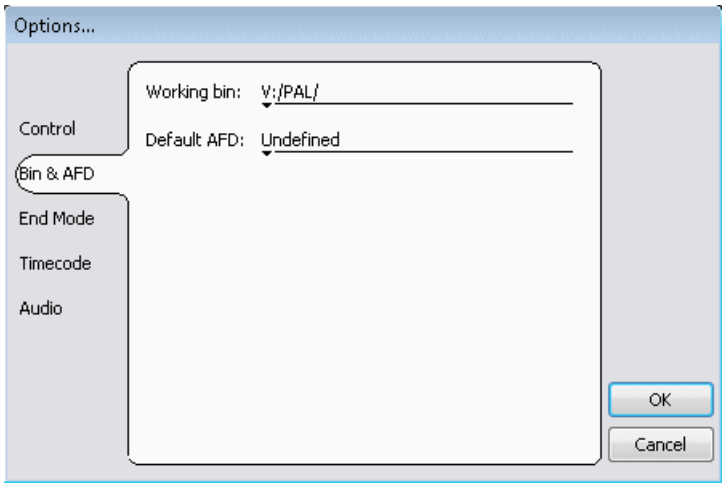
When recording starts, the new clip is stored in the *current bin,* which is also referred to as a working bin. Each channel has its own working bin. You can change the current bin to determine where you want the clip stored. The current bin name is displayed under the clip name in the display.



NOTE: If you rename the working bin, the bin automatically becomes the default bin.

- Change the current bin by doing the following:
  a) Make sure the record channel is selected.
  b) Click the drop-down list showing the clip's location, choose a bin.

- You can also change the current bin by doing the following:
  a) From the main menu, select **Control | Options.**
  b) Click the Bin & AFD tab, then choose a bin from the list.



You can also change the working bin by loading a clip into a channel (for example, by using drag-and-drop) from a bin that is not the current working bin for that channel. The bin from which you loaded the clip then becomes that channel's working bin.

Renaming a clip

You can rename a clip during or after recording.

To rename a clip:

1. Select the clip name control 

in the Recorder application.
2. Enter the new clip name using the on-screen keyboard.
3. Click **OK**, or press **Enter**.

   If a clip with the new name already exists in the current bin, an error message is displayed.

Viewing clip properties

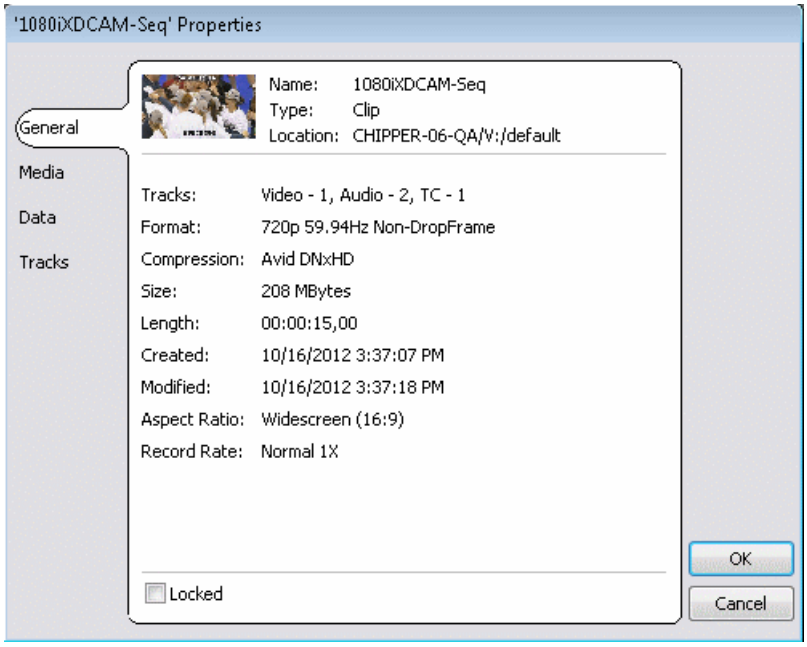
You can view the properties of a clip loaded in the Recorder application.

In the Record application, do one of the following:

- Click the **Properties** button.

- Select **Control | Properties.**

  The Properties dialog box opens.



Locating a clip

You can locate the currently loaded clip by displaying the contents of the current bin in the Clips pane, as follows:

1. After or during recording, select **Control | Locate**.
2. The Clips pane displays the contents of the bin where the clip is located.

Displaying available storage space

In the Recorder pane, you can display available storage using the Time Dome. The available storage displayed is the storage on the K2 system accessed by the currently selected channel.

1. Select the **Time Dome** button. 

   The Time Dome pop-up menu appears.

2. Choose **Available Storage** in the pop-up menu.

   The Time Dome changes to display available storage. 

   Available storage displayed is based on the channel recording compression setting in the Configuration dialog box; an HD channel has less available storage than an SD channel. (To access the Configuration dialog box, select **System | Configuration**.) A filled Time Dome represents no storage remaining. Available storage is also displayed numerically under the Time Dome. The white line functions as a "sweep second hand" to show record progress. It sweeps through a complete revolution every 10 seconds when crash recording or makes a single revolution on a fixed length record.

Playing and editing clips

About playing clips

The information in this chapter describes how to play and edit clips recorded on K2 Solo 3G system. You can play clips in a variety of ways including off-speed play and triggered by GPI. In addition to editing existing clips, you can create new clips using the subclip feature and add cue points to clips.

The Player/Recorder application allows you to play media stored on the K2 system, including clips and programs. The application requires a play channel and has two views— Control view and Cue view. The Control view allows you to play clips, trim clips, and create new subclips. The Cue view is used to add cue points within a clip. After adding cue points, you can use the cue list to start playback from any cue point in the list.

About Live Play (Chase Play)

With AppCenter Pro, you can record an event in one channel, drag the thumbnail into a play channel, and play the clip out while it is being recorded. This feature can also be controlled by the K2 Dyno™ Replay Controller. You can control the Live Play (Chase Play) as follows:

Control + L — The play channel plays **live**, playing the clip as it is recorded.

Spacebar — The play channel stops playing in Live Play mode.

Working with clips that are still recording

The following restrictions apply when working with a clip in the Player application that is currently recording:

- You cannot rename the clip. (However, you can rename the clip in the recording channel or from the Media pane.)
- The clip mark-in/mark-out points cannot be modified.
- Subclips created from a clip currently being recorded can only have a Mark Out equal to the last frame that has been recorded when the subclip is created. You cannot create a clip longer than has been recorded under the assumption that the unrecorded frames will "fill it in."
- The length of the record-to-play delay depends on if the clip is in local storage or shared storage. Refer to the "Operational Specifications" section for media file system performance specifications.

Otherwise, clips that are currently being recorded behave normally. As a reminder, “Read-Only” is displayed in the Player application when the clip loaded or playing is still being recorded.

Playing a playlist saved as a program

Playlists can be loaded and played in the Player or Playlist applications. You can also save a playlist as a program and then play it in the Player application. A program includes all the media in the playlist but does not include any event that breaks the flow of playout, such as a pause or a transition. When a program is loaded in the Player application, it is handled in the same way as a simple clip.

Selecting the Player application in AppCenter

The Player application requires a single play channel. If the play channel is currently being used in another application, such as a Playlist application, you can use the following steps to select the Player application. Selecting the Player application causes the play channel operation to stop, then the Player application is started.

To start the Player application on a play channel:

In the monitor pane, select the control mode drop-down list for the play channel, then choose **Player**.

The channel switches to the Player application and becomes the selected channel.

Guide to using Player: Control view

The Control view allows you to play a clip, modify its name, adjust mark in and mark out points, create sub-clips, and stripe timecode. Selecting the **Control** view tab shows the Control view. The following describes the essential controls in the Control view.

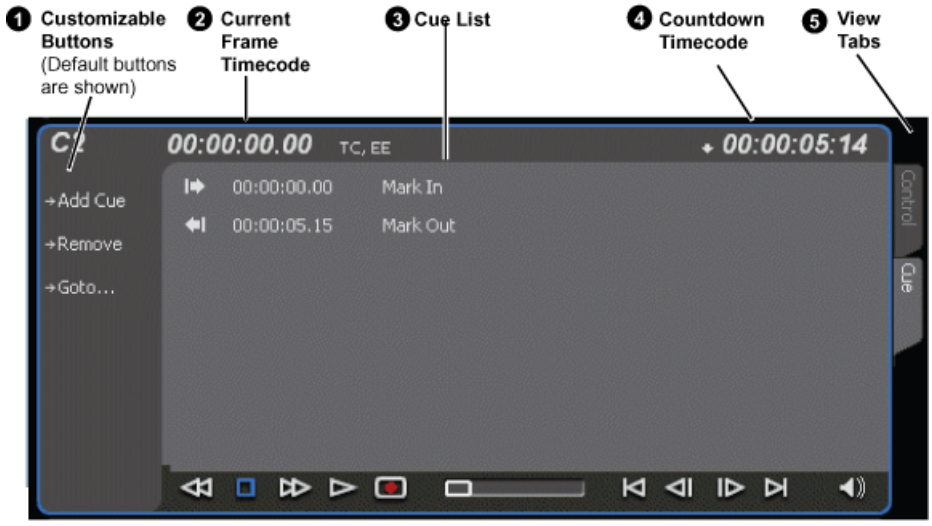
	Control	Description and User Operation
❶	Assignable Buttons	Assignable buttons allow you to modify the button assignments to best suit your workflow. Hold down a button to open a pop-up menu that lists the alternative button choices. The Subclip button toggles between the Source Clip and Subclip settings.
❷	Clip Timecode	Indicates the recorded timecode of the current frame being played. The timecode value of *XX:XX:XX:XX* is displayed when there is no recorded timecode.Stop mode is indicated by TC (recorded timecode) or Gen (zero-based, internal generated timecode).
❸	Clip Name & Current Bin	Displays the clip's name and location in the video storage file system. To rename the clip, click the Clip Name, then enter a new name.
❹	Countdown Timecode	Displays the time remaining in the clip .
❺	View tabs	These tabs toggle between Control and Cue views. Control is used for playing and editing of clips. During playback, you can use the Cue view to add cue points so that you can quickly cue a clip to a frame.
❻	ChannelFlex	If the channel is configured to be a ChannelFlex type, it is displayed in this area. ChannelFlex requires AppCenter Elite license.
❼	Application	A drop-down list allows you to select between none, Playlist, Player/Recorder, or additional selections if licensed for AppCenter Elite. If the Player/Recorder application is selected, you can play or record using the pane controls.
❽	Thumbnail	Used to visually identify the clip. By default, the thumbnail is generated using the 16th frame of video. To change the thumbnail, position the clip to the desired frame, then click the thumbnail.
❾	Time Dome Play Progress Media marks Loop playback	This multi-function control displays play progress, or play progress with media marks which shows the relative position of mark-in/mark-out points in the clip. The timecode underneath indicates play time remaining. The Time Dome is also used to enable loop play. Select the Time Dome, then use the pop-up menu to choose the display mode or to control loop play mode.

	Control	Description and User Operation
⑩	Set Mark-in and Set Mark-out	These buttons are used to set new mark-in or mark-out points. Position the clip to the desired frame, then click the In or Out buttons. Unused media is not deleted. To clear a mark, click the button, then choose yes in the pop-up dialog box. Marks are reset to the beginning or end of available media.
⑪	Meter bar Button	Displays the Meter bar, which contains the audio play level controls and signal meters. Click Save to save changes made to the clip audio level. Click Unity to return the audio levels to the last saved level. Click Mute to mute/unmute the audio.

Control	Description and User Operation
Player Menu - Control view	**Load** – Select to open the Load Clip dialog box, which displays the contents of the current bin. Select a clip, then choose OK to load. **New Clip** – Used to create and name a clip prior to starting the recording. If a clip is already loaded, selecting New Clip ejects the current clip and creates a new one. **Subclip** – Opens the Subclip mode, which allows you to create subclips from the currently loaded clip. A subclip is an entirely new clip that references media in another clip. **Goto** – Used to jump to a specific timecode. Select Goto, to open the Goto dialog box, then enter an absolute or relative timecode value, or use the scrub bar to go to the desired position. **Schedule Start Time** – Opens the Trigger At entry box so a start time can be entered. **Stripe Timecode** – Opens the Stripe Timecode dialog box, which allows you to replace the existing timecode track for the loaded clip. You can replace with time of day, or a specific start timecode. **Locate** – Finds the location of the selected clip. **Properties** – Opens the Properties dialog box for the currently loaded clip. **Auto Subclips** – The auto subclip check box changes the way that the subclip mode behaves. When it is NOT checked, clips have to be accepted manually. When it is checked, a subclip is created as soon as the user sets a mark out. **E-to-E (LoopThru) mode** – When selected, the following occurs: "EE" is displayed on the channel pane, next to the Timecode Source indicator; when no clip is loaded, the signal that is currently present at the channel input plays out; when a record operation stops the clip remains in the Recorder. The signal that is currently present at the channel input plays out. **Widescreen** – Sets the channel for recording widescreen format. **Options** – Opens the Options dialog for the currently loaded clip.

Guide to using Player: Cue view

The Player application Cue view is used to add cue points to the clip. The Cue view allows you to set, modify, and jump to cue points on the loaded clip. Clicking the **Cue** tab displays the Cue view. The following describes the basic controls in the Cue view.



	Control	Description and User Operation
❶	Assignable Buttons	Assignable buttons allow you to modify the button assignments to best suit your workflow. Hold down a button to open a pop-up menu that lists the alternative button choices.
❷	Current Frame Timecode	Indicates the recorded timecode of the current frame being played. The timecode value of *XX:XX:XX:XX* is displayed when there is no recorded timecode.
❸	Cue List	Displays a list of cue points that are set for the loaded clip. Cue points are listed in chronological order beginning with the mark-in point and ending with the mark-out point.
❹	Countdown Timecode	Displays the time remaining in the clip. To select the countdown mode you want to monitor, open the Options dialog box by selecting Options in the context menu.
❺	View tabs	These tabs toggle between Control view and Cue Points view.

Control	Description and User Operation
Player Menu	**Add Cue** – Used to add a cue to a clip: In the Control view, start the clip playing. Select the Cue tab. At the desired timecode, select Control | Add Cue. **Remove** – Used to remove a cue. **Rename** – Used to rename a cue. **Create Clip** – Creates a sub clip from highlighted cue points. **Create All** – Creates sub clips from all cue points. **Cue Selection** – Cues the first selected cue point for playback showing a still frame of video for the cue point. **E-to-E (LoopThru) mode** – When selected, the following occurs: "EE" is displayed on the channel pane, next to the Timecode Source indicator; when no clip is loaded, the signal that is currently present at the channel input plays out; when a record operation stops the clip remains in the Recorder. The signal that is currently present at the channel input plays out.

Loading media for playout

You can load clips or programs in the play display for playout.

NOTE: Loading a clip from a bin into a play channel changes the working bin for that channel.

Loading clips from the clips pane

1. Select a play channel by clicking in the channel's monitor pane.
2. Locate the clip in the clips pane. If necessary, change bins by clicking the current bin control and selecting from the drop-down list.
3. Load the clip in one of the following ways:
   - Drag the clip from the clips pane into the play channel.
   - Choose the **Load** button in the clips pane, then select the clip.
   - Double-click on the clip.
   - Select the clip, then press **Enter** on the keyboard.

Loading a clip from the Player application

1. Select a play channel by clicking in the channel's monitor pane.
2. Open the Load Clip dialog using one of the following:
   - Click the **Load** button in Player.
   - Select **Control | Load**.
3. If needed, use the **Look in** drop-down list to browse to the desired bin.

4. Select a clip in the Load Clip dialog, then click **OK**.

   The clip is loaded in the player.

Playing a clip

Once a clip is loaded in the Player application, you can play the clip or search for a specific frame of video using the transport controls.

Scheduling a clip to play

This feature is part of the licensable AppCenter Pro option.

You can schedule a clip to start playing at a specified time. Scheduled Start Time uses Time of Day driven by the system clock or LTC.

1. Select **Control | Schedule Start Time**.

   Trigger At entry box appears.

2. Enter the time when you want the recording to start and click **OK**.

   The time of day, trigger time, and a countdown are displayed.

Selecting loop play

Loop play allows the clip to play in a continuous loop until **Stop** is pressed. The Time Dome is used to enable/disable loop play.

- Click the **Time Dome** button  , then choose **Loop Mode** in the pop-up menu.

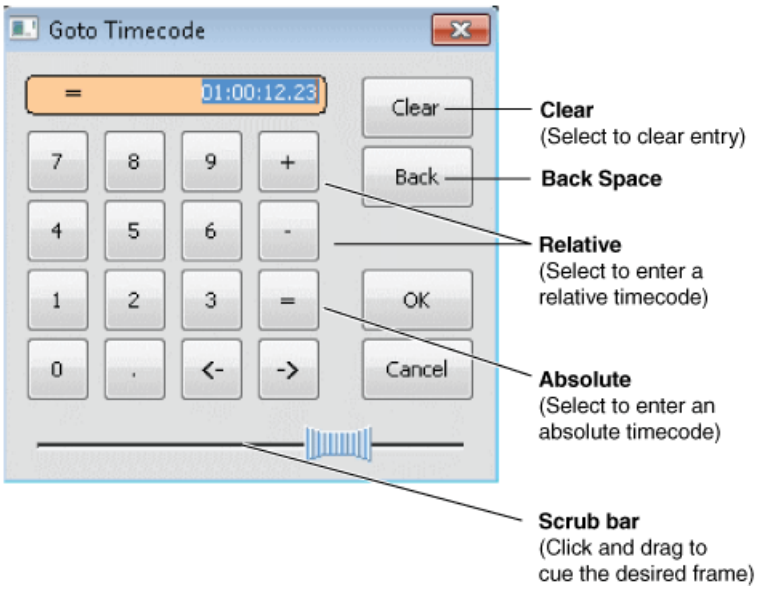
Jumping to a specific timecode

The Goto dialog box allows the player application to jump to the specific clip timecode that you enter. You can enter an absolute timecode value based on recorded timecode, or a relative timecode value, that is, cue the video to a point +/- some value relative the current frame. If you don't know the timecode value of the frame you want, you can click and drag the scrub bar to shuttle to the desired frame.

To jump to a specific timecode:

1. With a clip loaded in the Player application, do one of the following:
   - Click the **Goto** button.
   - Select **Control | Goto**.

   The Goto Timecode dialog box appears.



2. Perform one of the following:
   - Enter a **relative** timecode value, select the '+' or '-' key, enter timecode, then click **OK**.
   - Enter an **absolute** timecode value, select the '=' key, enter timecode, then click **OK**.
   - Click and drag the scrub bar to cue the desired frame.

Using cue points for playback

Cue view allows you to add cue points to a clip. You can use cue points to manage clip play out or create subclips. The following sections describe how to work with cue points.

About using cue points

When you select Cue view, a chronological list of cue points is displayed. The list begins with the mark-in point and ends with the mark-out point. You can add additional cue points to mark other frames within the clip. You can add cue points while the clip is playing or in stop mode. When you add a cue point, it is listed by a default name (such as "cue_1") and timecode value.

Cue points cannot be moved; however, you can remove a cue point and use the transport controls, or Goto Timecode dialog box to enter a new cue point at the current position.

Cue points can be used to:

- **Manage clip playout** – Jumps to the selected cue or next cue.

- **Create subclips** – You can create a subclip from the selected cue point. The selected cue point becomes the mark-in point, while the mark-out point is the same as the source clip. If more than one cue point is selected, a subclip is created using the first and last cue points.

When working with cue points, keep these considerations in mind:

- **Cue points are retained when a clip is copied or transferred (GXF or Streams)** – With using GXF or streams, cue points are stored with the clip. All the cue points of the original clip are retained when the clip is copied or transferred to another server. Cue points are not retained for other file transfers.
- **Cue points and trimming** – After you trim a clip by moving the mark-in or mark-out points, the cue points outside the new mark-in and mark-out points are cleared and must be reinserted.
- **Cue points and subclips** – Subclips created from a clip with cue points retain all cue points that fall between the marks of the new subclip. The subclip has its own mark in and mark out points.
- **Cue points and programs** – Cue points cannot be added to a program.

Viewing the cue list

1. Select a play channel by clicking in the channel's monitor pane.
2. Select the Cue tab.

   The Cue view appears showing the cue list for the clip loaded in the Player application. Initially, only the mark-in and mark-out cue points are listed.

Adding a cue point

While the clip is playing or in the stop mode, use the transport controls to find the desired frame in the clip, then do one of the following:

- Click the **Add Cue** button.
- Select **Control | Add Cue**.

A cue point is added to the cue list using a unique name, e.g. Cue_1. Using the preview feature, you can play and add cue points to a clip while it is still being recorded.

Removing a cue point

1. In Cue view, select a cue point in the list.
2. Do one of the following:
   - Click the **Remove** button.
   - Select **Control | Remove**.

Jump to the selected cue point

Use the following steps to jump to the selected cue point.

1. In Cue view, select a cue point in the list.
   a) Click the **Goto** button, then select **Selection**.

2. Press the **Play** button on the onscreen transport controls.

   Playout starts from the cued frame.

Jump to the next cue point

Use the following steps to jump to the next cue point. Depending on the current play position, the clip will cue to the next cue point in the clip.

1. In Cue view, click the **Goto** button, then select **Next Cue**.
2. Press the **Play** button on the onscreen transport controls.

   Playout starts from the cued frame.

Renaming a cue point

1. In Cue view, select a cue point in the list.
2. Select **Control | Rename.**
3. Use the text entry dialog to enter a new cue name, then click **OK** or press **Enter**.

Editing a clip

Topics in this section describe the process of editing a clip.

Moving clip mark-in/mark-out points

Every clip has a mark-in point and a mark-out point that refer to the first and last frames displayed when the clip is played. When first recorded, clip marks are set to the beginning and end of available media. You can edit the clip marks in order to reference only the desired media. When clip marks are moved, the unused media is not *deleted.* Clearing the marks resets them to the first and last frames of the recorded clip.

NOTE: If the source media has been erased, the subclip retains 1 second of media on each side of the mark-in and mark-out points.

The following restrictions apply when editing clip marks:

- Mark-in must precede the mark-out
- Marks cannot be set outside the recorded media
- Marks cannot be changed on a clip that is still being recorded.

NOTE: If more media exists after the current mark, a <<< or >>> symbol is displayed beneath the In/Out timecode. To permanently remove media outside the marks, refer to "Erasing a clip's unused media" under Managing Clip Media.

To move clip marks, load the clip in player, then use one of the following methods.

- Moving clip marks: Using the In/Out buttons
- Moving clip marks: Using the timecode entry controls
- Moving clip marks: Using the clip length control

Moving clip marks: Using the In/Out buttons

1. Use the transport controls to locate the desired frame.
2. In Control view, click the **In** button  to set mark-in point, or click the **Out** button  to set mark-out point.
3. In the Confirm Mark Change window, click **Yes**.

Moving clip marks: Using the timecode entry controls

1. In Control view, select the mark-in or mark-out timecode control  to open the timecode entry dialog box.
2. Enter a timecode value, then click **OK** or press **Enter**.

   Alternatively: Use the current position scrub bar  in the timecode entry dialog box to locate the desired frame, then select **OK**.

Moving clip marks: Using the clip length control

Entering a new clip length moves the mark-out point.

1. Click the **Length** timecode entry control.
2. Enter a new clip length and click **OK**.

   The clip length changes by moving the mark-out point.

Clearing mark-in/mark-out points

Clearing a mark point resets the mark to its default position — mark-in is set to the beginning of available media; mark-out is set to the last frame of available media.

To clear a mark point, do one of the following:

- In Play view, click and hold the **In** or **Out** button, then choose **Clear Mark** in the pop-up menu.
- In Play view, select the mark-in or the mark-out timecode control and click **Clear**, then **OK** to clear the mark.

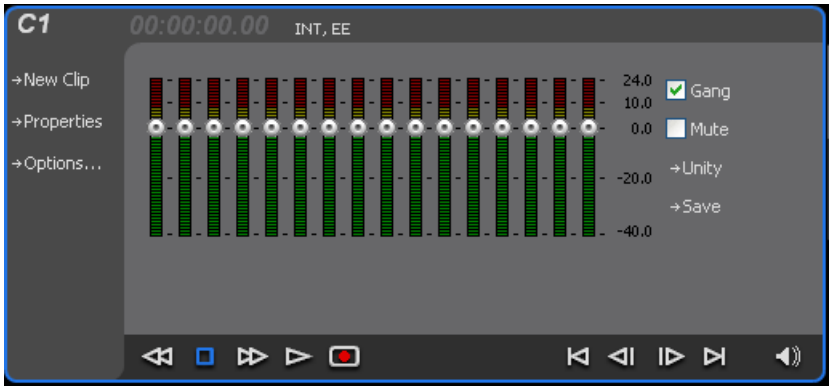
Adjusting clip audio level

The audio meter display provides audio level adjustment for clips loaded in the player display. Saved audio levels are used every time the clip is loaded and played. Unsaved changes are lost when the clip is ejected.

To adjust audio level:

1. In the Player application, click the Meter bar button. 

2. Adjust the audio level in one of the following ways:
   - Adjust the graphical faders individually or "ganged," which ensures all channels use the same gain.
   - Click **Unity** to set audio back to the last saved level.



3. Click **Save** to save changes to the clip audio level.
4. Click **Mute** to mute or unmute the clip audio level.
5. Click the Meter bar button again to return to the Player application.

Changing the clip thumbnail image

The clip thumbnail is displayed in AppCenter for visual identification of the clip. By default, the 16th frame is used to generate the thumbnail image.

To change the clip thumbnail:

1. While monitoring the play channel output, use the onscreen transport controls to position the clip to the desired video frame.
2. In Player, click on the thumbnail, then select **Yes** in the Change Thumbnail dialog box.

   NOTE: If clip marks are edited so that the video frame used to generate the thumbnail is outside the new clip marks, the thumbnail is reset to a position near the mark-in of the modified clip.

To reset the thumbnail:

- Select the thumbnail image, then choose **Reset** in the pop-up menu.

  This resets the clip thumbnail to the 16th frame in the clip.

Striping timecode (replacing the timecode track)

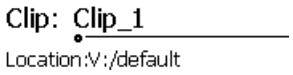
The stripe timecode dialog allows you to overwrite the existing timecode track for the loaded clip. You can replace the recorded timecode with time of day, or a specific start timecode value.

1. Load the clip in the play channel.
2. In Control view, select **Control | Stripe Timecode**. The Stripe Timecode dialog box opens.

3. Specify the replacement timecode:

   - **Time of Day** – The new timecode track will start with the current time of day and will contain continuous values ranging from the current time of day plus the length of the clip.
   - **Fixed Time** – After choosing this option, select the timecode entry control, and enter a start timecode value. The new timecode track will contain continuous values ranging from the specified starting value to the starting value plus the length of the clip.
   - **Drop frame** – The drop frame option is available when system timing is set to 525 line standard (drop frame is a timecode adjustment that applies to NTSC video only). Drop frame allows the timecode track to indicate the actual running time of the clip. Drop-frame time code yields precise running times, but frames are not all numbered sequentially. A frame number must be dropped periodically to keep the clock right.

Renaming a clip in the Player application



1. In the Control view, select the clip name control.
2. Enter the new clip name.
3. Click **OK**, or press **Enter**.

Creating Subclips

A subclip is a clip created by referencing a portion of media from another clip. For example, if you recorded a two hour clip, you could create several short subclips to use as previews or advertisements. Each subclip refers to a small portion of the original clip and is listed along with all other clips in the clips pane. When working with subclips, the original clip is sometimes called the *source clip*. After creating subclips, you can delete the source clip.

Subclips created from a clip that is still recording can only have a mark-out equal to the last frame that has been recorded when the subclip is created. You cannot create a subclip longer than what has been recorded with the assumption the media will “fill in”. You can create subclips from a clip being recorded in loop record mode. In loop record mode, media referenced by the subclips is retained while unreferenced media is discarded.

You can load subclips in the Control view and edit the mark-in/mark-out points the same as a clip, provided the unreferenced source media has not been erased.

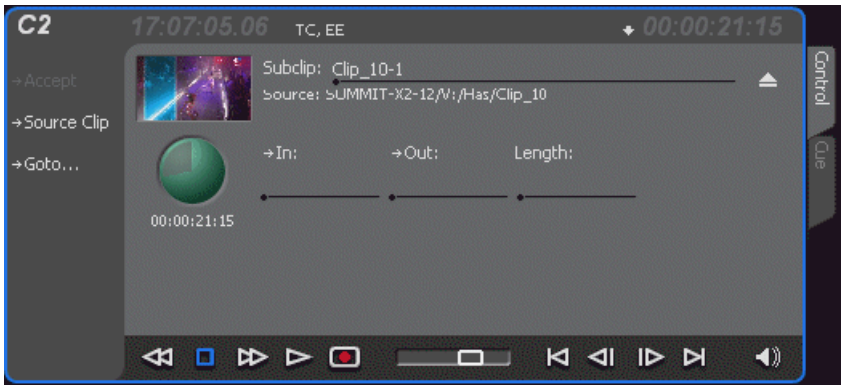
NOTE:

If the source media has been erased, the subclip retains 1 second of media on each side of the mark-in and mark-out points.

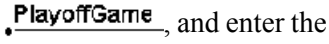
To create subclips

1. Load a clip in the player.

2. In the Player Control view, click the **Subclip** button.



The Subclip display appears with a new subclip loaded. The **In** and **Out** buttons are flashing indicating no mark-in or mark-out points are defined. The default subclip name follows the form <*source clip name*>-<*number*>, for example, if the source clip name is *PlayoffGame*, the subclip name is *PlayoffGame-1*.

3. To rename the subclip, click the subclip name control 

, and enter the new name in the Clip Name dialog, then click **OK**, or press **Enter**.

   Renaming the subclip creates a new seed name. For example, if you rename the subclip *PlayoffGame-1* to *Highlight*, subsequent subclips created are named *Highlight-1*, *Highlight-2*, and so on.

4. Enter the subclip marks as follows:
   a) Using the transport controls, position the clip to the desired frame for mark-in, then click the **In** button.
   b) Using the transport controls, position the clip to the desired frame for mark-out, then click the **Out** button.

   Alternatively: Select the mark-in or mark-out timecode entry controls and enter a specific timecode value.

   Alternatively: Select the **Length** timecode entry control and enter a clip length, then create either a mark-in or a mark-out point. If the source media has been erased, the subclip retains 1 second of media on each side of the mark-in and mark-out points.

   NOTE: Until you enter the subclip marks, the Accept button is grayed out.

5. In Subclip view, click **Accept**.

   The subclip is saved and ejected, then Player returns to Subclip view with a new subclip name loaded.

   NOTE: Clicking the Source Clip button or the Eject button prior to pressing the Accept button closes Subclip mode without creating a new clip. Both of these buttons are used to exit Subclip mode.

About Auto Subclip mode

In Auto-Subclip mode, you simply set mark-in, then set mark-out. On setting mark-out, the subclip is **automatically generated and ejected**, and a new subclip name is loaded in the Subclip display.

Auto Subclip mode is useful when you want to create subclips while a source clip is playing. You simply load a clip, press play, then create subclips by selecting In, Out, In, Out, etc.

To enable Auto Subclip mode:

- In the Player application Control view, click **Control | Auto Subclips**.

Creating subclips in Cue view

In Cue view, you can automatically create a subclip from a selected cue point. The selected cue point becomes the mark-in point, while the mark-out point is the same as the source clip. If more than one cue point is selected, a subclip is created using the first and last cue points. This feature allows you to manage the media of interest as a separate clip rather than media between cue points in a clip. For example, once you've made a subclip, it can be added to a playlist.

By default, subclips generated from the cue list are given names of the format <*clip name*>-<*first cue name*>. For example, a subclip generated from a cue point named "cue_1" in a clip named "MyClip" is named "MyClip-cue_1". If a clip already exists with this name, you are prompted to enter a unique name.

To create a subclip from media between two selected cue points:

1. Select two cue points in the cue point list.
2. Click **Control | Create Clip**.

To create a subclip using a selected cue point as mark-in:

1. Select the cue point to use as the mark-in for the new clip.
2. Click **Control | Create Clip**.

   The subclip is terminated by the source clip mark-out point.

To create a subclip for all cue points:

1. Click **Control | Create All**.

In some cases, a progress dialog is displayed as the clips are generated.

Each subclip is terminated using the mark-out of the source clip.

Viewing clip properties

To view the properties of a clip loaded in Player, do one of the following:

- Click the **Properties** button.
- Select **Control | Properties.**

Viewing clip options

Clip options allow you to choose which audio channels to monitor.

To view the options of a clip loaded in Player:

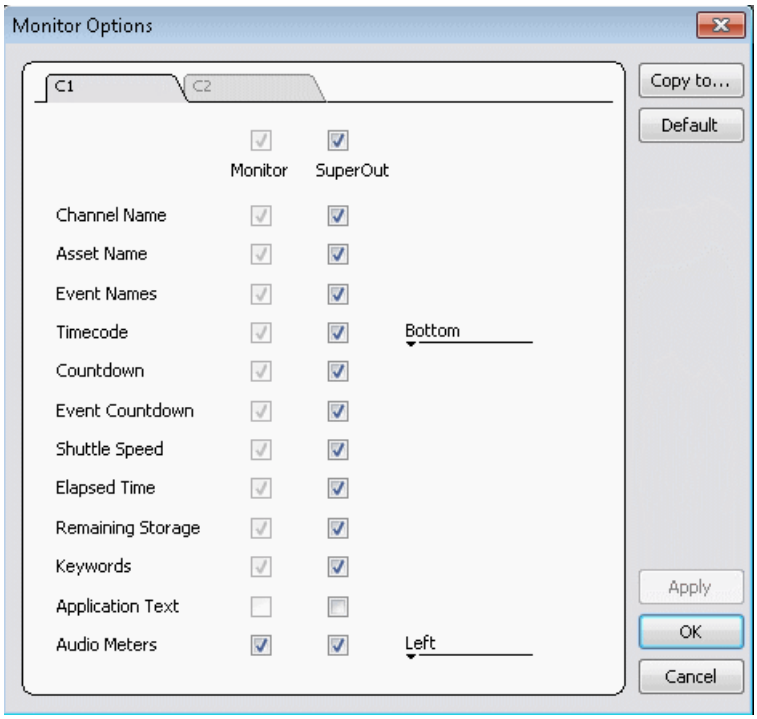
- Select **Control | Options.**

Displaying Super Out information on output/monitor

If licensed for AppCenter Pro or Elite, you can display information on a channel's SDI OUT2 signal and on the VGA video monitor.

1. Click **System | Monitor Options**.

   The Monitor Options dialog box opens.



2. Select the tab for the channel that plays the video with the information you are displaying.
3. Do one or both of the following:
   - To display information on the VGA video monitor for the channel, select the checkbox above **Monitor**.
   - To display information on the channel's SDI OUT2, select the checkbox above **SuperOut**.
4. Select the checkbox for each type of information you are displaying.
5. From the drop-down list, select the location to display the information.
6. Configure other channels as follows:
   - To configure other channels with the same settings as the current channel, click **Copy to**.
   - To configure other channels with their own settings, repeat previous steps as appropriate.
7. When fully configured, click **OK** to apply settings and close.

Working with playlists

Introducing the Playlist application

In addition to playing a single clip, AppCenter play channels can also play lists that contain clips and programs stored on the K2 system.

The following table summarizes the basic features supported in playlist application.

Basic Feature	Description
Editing playlists	Events in a playlist can be rearranged or removed, and new events added between existing ones.
Editing events in the list	Events can be renamed and trimmed. Trimming an event moves the mark-in and mark-out points. This only affects the event, not the source clip.
Event transitions	Transitions between all events in a list are made by a cut, i.e. the last frame of an event is followed by the first frame of the next event.
Loop on a section	Sections are provided within the list to provide flexibility during playout. A section can be set up to loop indefinitely. The section can be taken out of the loop by manual intervention.
Loop on a list	Lists can be set up to loop indefinitely. The list can be taken out of the loop by manual intervention.
Pause at the end of events	Events can pause playout at their end. At event pauses, you can choose to show black, freeze on last frame, or freeze on next event.
Pause at the end of sections	Sections can pause playout at their end. At section pauses, you can choose to show black, freeze on last frame, or freeze on next event.
Saving a playlist as a program	Playlists can be saved as a program. This saves the media and transitions, but nothing that breaks the flow of playout, such as pauses. You can insert a program into a playlist, or play a program in the standard Player application.
GPI output triggers	AppCenter provides 12 GPI output signals through a rear panel connector for controlling external equipment. You can configure events in a playlist to trigger GPI outputs. A GPI trigger does not disrupt playout of the play events. GPI triggers can be set to occur at the beginning or end of an event or section, or at these points with some offset.
GPI Input triggers	You can assign any of the 12 GPI inputs to control one or more play channels and the action you want the AppCenter channel(s) to take—play, VAR play, cue next event, or cue next section, etc. AppCenter includes more extensive GPI output trigger features.

Before using Playlist application

Read the following sections before using Playlist application.

Terms used in Playlist application

The following terms are used in the Playlist application.

Term	Definition
Playlist	A list is a sequence of events.
Event	Events are the components that make up a list. Events are created by adding a clip or program to sections in a list.
Section	Playlists created in AppCenter contain at least one section. All events in a playlist are contained in sections. Sections have properties that include repeat and pause. A playlist can have up to 100 sections. Each section can contain up to 1000 events.
Source Clip	The clip inserted in a list to create a play event.
Program	Playlists can be saved as a program in the K2 system. Programs created from a playlist include all the media and transitions in the playlist, but nothing that breaks the flow of playout, such as a pause at the end of an event. Programs are also created from the continuous record mode.

Symbols used in Playlist application

The following table describes the symbols used to describe the properties of items in the list— play events, sections, and the list itself.

Symbol	Description
	Locked: The item is locked and cannot be edited.
	Pause: At the end of playout, this item will cause playout to pause.
	Loop: At the end of playout, the item will repeat.
	GPI Output Trigger: This event or section triggers one or more GPI outputs.

Working with programs

A program is a clip generated from a playlist using the **Save As Program** feature in the Playlist application. A program includes all the media in the playlist, but does not include any event that breaks the flow of playout such as a pauses between events. You can insert programs into other playlists as an event, or load and play them using the standard Player application. You can also send a program to a file or a video network stream.

Using mixed aspect ratios in a playlist

AppCenter can play clips with different aspect ratios in a single playlist.

The AppCenter supports playout of mixed format clips displayed with default or selectable modes such as bars, crop, or stretch on both SD and HD outputs.

Refer to specifications about how the system displays mixed aspect ratios.

Using mixed video resolutions in a single playlist

Playlists can contain events with different video resolutions. When the list is played, the media is converted as needed to match the play channel video output type selected.

Inserting a clip that is still recording

Clips that are currently recording behave as other clips do in a list except for the following restriction: the event-out timecode is set to the last recorded frame at the time the clip is inserted. You can move the event-out timecode as needed while the clip is still recording or after record is stopped.

Improving performance while modifying a playlist

If you are making multiple changes to a playlist, especially a long playlist, you can improve response time by playing the list while editing it. This allows you to add/remove/modify events without waiting for database updates, since changes to the playlist are not saved until playout stops.

Inserting a playlist in a playlist (workarounds)

While AppCenter does not support a true “nested” playlist, you can retain some of the functionality of inserting a playlist in a playlist in the following ways.

- Save the list as a program, then insert it into another playlist as an event.
- Use multi-item select and copy/paste.
- Copy/paste events or sections within the same list or from other lists.
- Copy the list in the Clips pane, then load and edit the list.

Selecting Playlist application

The Playlist application requires a single play channel. If a play channel is currently being used by another application, you can select the Playlist application. Selecting the Playlist application causes the current application to exit when Playlist application is started.

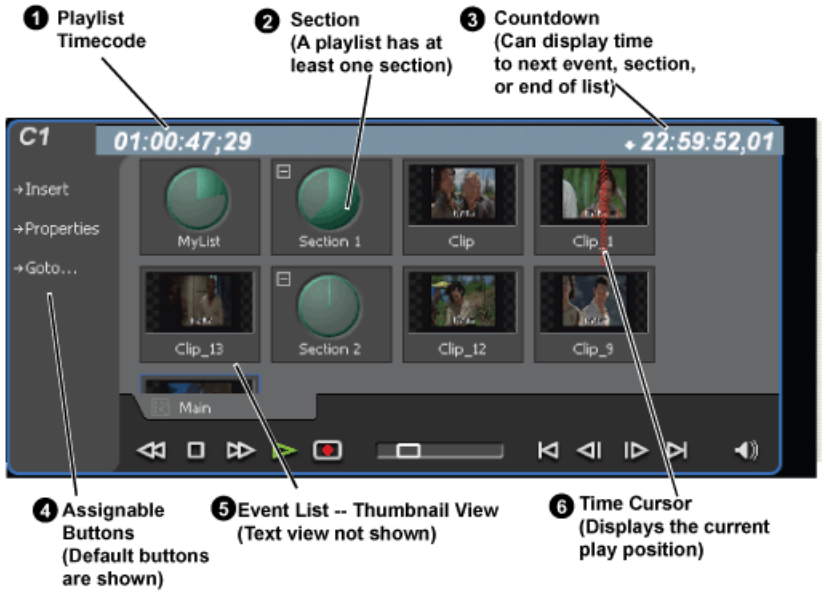
To start Playlist application on a play channel, in the channel's monitor pane, select the application drop-down list and choose **Playlist**. The channel switches to Playlist application and becomes the selected channel.

Changing the channel application in AppCenter to Playlist switches the working bin to the bin displayed in the Clips pane rather than the bin specified for that channel. This behavior is also observed if you have the working bin set to one bin but load a clip from another bin onto the channel.

Guide to using Playlist application

Playlist allows you to manage a list— insert, move, or modify events, and to control playout of the list. You can also select the type of display for the asset list– text view, or thumbnail view. The following describes the basic controls.

List in thumbnail mode



	Control	Description and User Operation
1	Playlist Timecode	Though each play event contains the timecode information from its source clip, the timecode for the list is generated internally. This timecode can be an offset from a specific timecode (the default is 01:00:00;00).
2	Section (Text View) Section (Thumbnail View)	A list has at least one section, but can have up to 100. All events belong to a section, and each section can have up to 1000 events. In Thumbnail View, the section is displayed as a Time Dome which shows the amount of the section that has played. An empty Time Dome indicates the section has not started to play. Sections can be expanded or collapsed to reveal or hide the events that belong to the section. Expanded sections are indicated by a '-' symbol.

	Control	Description and User Operation
❸	Countdown Timecode	Displays the time to the next event, section or end of the list.
❹	Assignable Buttons	Assignable buttons allow you to modify the buttons located in the Playlist toolbar to best suit your workflow. Holding down a button opens the button pop-up menu that lists the alternative button choices.
❺	Event List	The Event List contains play events. Play events are created from clips or programs that can be added to the list in two ways: drag and drop from the Clips pane or using the Insert button in the Clips pane. By default, play events added to a list inherit the source clip's name, but you can rename events. Play events and sections can be configured to trigger GPI outputs. GPI triggers can be set to occur when the event or section starts, ends, or at these points plus or minus some offset. A GPI trigger does not disrupt playout of the play events that follow it. You can view the Event List in either the text view or thumbnail view. Thumbnail view displays clip thumbnails along with Time Domes for the list play progress, and section play progress. To change the view, select Options in the Playlist menu.
❻	Time Cursor	The time cursor indicates the current play position. The time cursor is displayed over the event currently being played.

Control	Description and User Operation
Playlist Menu	**Insert Event** — Opens the Insert Event dialog box, which allows you to insert all event types. **Add Section** — Adds a section to the end of the list. Once you add the section, you can move it. **New List** — Opens the New List dialog box where you can choose the current bin and specify the new list name before creating it. When a new list is created, the current list is ejected and the new list is created containing one section and no events. **Open List** — Closes the current list and allows you to open an existing list. **Eject List** — Ejects the current list. **Import List** — Imports a text file and saves it in a playlist format. **Rename List** — Rename the list currently loaded in Playlist application. **Save As Program** – Saves the current list as a program. The new program is listed in the Clips pane with other assets. Programs can be played using the Player application, or inserted in a list in Playlist application. **Set Event In** – Used to change the in point of the event. Event In/Out changes do not affect the source clip's mark in and out values, but only the event's marks used by the Playlist. **Set Event Out** – Used to change the out point of the event. Event In/Out changes do not affect the source clip's mark in and out values, but only the event's marks used by the Playlist. **Split event** — Used to break one event into two events of the same name. **Combine events** — Used to combine two events into one in a playlist. **Locate** – Locates the list or source clip for an event, depending on the selection, in the Clips pane. **Properties** – Opens the properties dialog box for the selected item— list, section, or play event. Properties dialog box includes pages for setting up list timecode, adding metadata, and setting list attributes that will occur when playback reaches the end of the list. Options include repeat, or pause. Section properties and event properties dialog boxes include options for setting the end behavior— repeat or pause, and GPI output properties. **Move Up** – Moves the selected event up in the list. **Move Down** – Moves the selected event down in the list. **Goto** – Opens the Goto pop-up menu which allows you to jump to selection, next event, next section, or a timecode that you specify. **Options** – Opens the Options dialog box which allows you to choose the list monitoring information displayed in the Playlist application and the monitor pane.

Selecting Text or Thumbnail view

The event list has two viewing modes: Thumbnail view and Text view. Thumbnail view displays events as thumbnails along with the section and the list time domes. The text view lists events descriptions in text format. You can select which event attributes are displayed in text view.

Use the following steps to select the view mode best for you:

1. Select **Playlist | Options**.

   The Options dialog box appears with the View settings tab selected.

2. Select a view mode:

   - **Text View -** displays events in text form including an event icon, name and an additional attribute selectable using the **Show** drop-down list. Show attributes are: **Duration**, **Name only**, **Start time**, or **Start time and duration**.
   - **Thumbnail View -** displays events in thumbnail form along with the event name.

3. Click **OK** to save settings and close the Options dialog box.

Selecting monitor information

You can select the monitoring information displayed for the list. The selections you make determine the list attributes that are displayed in the following locations:

- **List information displayed in the monitor pane -** List information is displayed under the thumbnail in the monitor pane. You can select the list attributes displayed in the monitor pane.
- **Countdown timecode displayed in the Playlist toolbar -** The countdown timer can count down to the next section, the next event, or the end of list.

To select the monitor mode:

1. Select **Playlist | Options**.

   The Options dialog box appears.

2. Click the **Monitor** tab.

   The Monitor settings page appears.

3. Select one of the monitor information options.
4. Click **OK** to save settings and close the Options dialog box.

Creating a simple playlist

When Playlist application is started, an empty channel pane displays “No List”. You must create a new list. The first list is by default labeled “List”; new lists are named “List_n”, where n is the first

number that results in a unique file name. You cannot eject a list. Instead, create a new list or open an existing playlist.

1. Do one of the following:
   - To create a new list, select **Playlist | New List**.

     The New List dialog box is displayed.
   - For an existing playlist, click the Insert button and select an event.
2. Select the bin where you want to store the list, edit the default name for the new list, then click **OK**.

   NOTE: Make sure you do not violate asset naming limitations.

The current list closes and the new list is created containing one section and no events.

Inserting media in a playlist

A new list contains one section and no events. Events are played in the order they are inserted. You can move events in the list up or down, or insert new events between existing ones by selecting the insertion point.

Selecting the insertion point in a playlist

- When using the **Insert** button or menu item, the insertion point is after the currently selected event.
- When using the drag and drop method, you see a drop cursor as you drag the event over the list. The drop cursor indicates where the new event will be inserted.

NOTE: The time cursor only indicates the current play position, and cannot be selected and moved. Selecting and dragging may inadvertently select and move the event.

Inserting events

To insert a play event, do one of the following:

- Drag and drop assets from the Clips pane using the drop cursor to locate the insertion point.
- Drag and drop from the monitor pane of a play channel. Select the thumbnail or video image, then drag to the playlist channel. Use the drop cursor to locate the insertion point.
- Double-click an asset in the Clips pane. The asset is inserted in the list after the insertion point.
- Select an event in the list as the insert point, then select one or more assets in the Clips pane. Click **Insert** in the Clips pane to insert the event after the insert point.
- Select an event in the list as the insert point, then click **Insert** in the Playlist channel, and select one or more assets in the Insert Event dialog box. Click **OK** to insert the events.
- In the Insert Event dialog box you can click on the **Event Name** text entry control and type the name of a clip. This selects the clip for insertion into the playlist. With this method it is no longer necessary to browse to the clip in order to select it.
- Press CTRL + N to open a text entry dialog in which you can type the name of a clip. This selects the clip for insertion into the playlist.

Using copy and paste to insert play events

Any asset that can be selected can be placed on the clipboard and pasted into another application that accepts that type of asset. For example, you can copy a play event from the Playlist application on one play channel and paste it into the Playlist application on another play channel. You can also copy a clip from the Clips pane and paste it into the Playlist application.

The Cut, Copy, and Paste operations are performed by using the AppCenter's Edit menu, by using the standard keyboard shortcuts (CTRL+C, CTRL+X, CTRL+V), or by using the right-click menus of cut, copy and paste.

- To insert an asset from the Clips pane using the clipboard:
  a) In the Clips pane, select one or more assets.
  b) Copy the assets to the clip board.
  c) Select an insertion point in the list.
  d) Paste the asset from the clipboard into the list.
- To use the clipboard to move or copy events already in a play list:
  a) Select the event(s) you wish to move or duplicate.
  b) Copy or Cut the selection to the clipboard.
  c) Select the new insertion point in the list.
  d) Paste the event(s) from the clipboard into the list.

Combining events in a playlist

To combine two or more events in a playlist into one event, follow these steps:

1. Highlight all events. A blue line is visible around all the highlighted events.
2. From the file menu, select **Playlist | Combine events**. The events are now combined under the name of the first event in the selection.

   NOTE: The individual assets are not combined, merely the events in the playlist.

Splitting an event in a playlist

To split an event into two events, follow these steps:

1. Highlight the event. A blue line is visible around the highlighted event.
2. Play the event to the point where you want to split it.
3. From the file menu, select **Playlist | Split events**. The event is now split into two events of the same name. You can rename or delete one event without affecting the other.

   NOTE: The asset is not split and renamed, merely the event.

Playing a list

Once the list is complete, you can open it, play it, and eject it as described in the following sections.

Opening a playlist

If you want to open the same playlist simultaneously on multiple channels, the channels must be running on the same K2 Solo 3G system, otherwise, a “Failed to open…” message is displayed.

To open a list, do the following:

1. Select **Playlist | Open List**.

   The Open List dialog box appears.

2. Locate and select the list you want to open, then click **Open**.

   Before the list is opened, the currently loaded list is closed. In Playlist application there is no eject button, so you can open an existing list or create a new list without manually closing the currently loaded list.

   NOTE: If a playlist has been locked, you cannot open it.

Playing a playlist

You can perform the following operations to play a playlist using the AppCenter user interface. You can also use the keyboard shortcuts for all transport controls.

To...	Do this...
Begin playing at the top of the list	Open the list, then press the **Play** button on the onscreen transport controls.
Continue playout after a pause in the list	Press the **Play** button on the onscreen transport controls.
Play the specified timecode	Select **Goto**, and then choose **Timecode** in the Goto pop-up menu. Specify a timecode in the dialog box and click **OK**.
Play the next event	Select **Goto**, and then choose **Next Event** in the Goto pop-up menu.
Play the next section	Select **Goto**, and then choose **Next Section** in the Goto pop-up menu.
Play an event or section	First, select the event or section, then click **Goto**, and choose **Selection** in the Goto pop-up menu. Then press the **Play** button on the onscreen transport controls.
Avoid delays when jumping to a new event or section	First select the new event or section, then wait until the diamond or standby icon is filled in before jumping to the new event or section.

Playlists always play the default audio tracks, even when named mapping is in place.

Ejecting a playlist

To eject a list, do the following:

Select **Playlist | Eject List**.

The list is ejected from the Playlist channel.

Editing and rearranging events in a playlist

The following topics explain how to edit and rearrange events in a playlist.

Editing event marks

You cannot edit events while the list is playing. Every event has a event-in point and an event-out point that refer to the first and last frames displayed when the event plays. When first created, event marks are set to the mark-in and mark-out of the source clip. You can edit the event marks in order to reference only the desired media.

The following restrictions apply when editing event marks:

- Event-in must precede the Event-out.
- Event marks cannot be set outside the recorded media of the source clip.

NOTE: If more media exists outside the current mark, a <<< or >>> symbol is displayed beneath the current event mark timecode.

Setting the Event In/Out marks

To move clip marks:

1. Use the transport controls to locate the desired frame.
2. Select **Playlist | Set Event In** to set mark-in point or **Playlist | Set Event Out** to set mark-out point. The Confirm Marks dialog box opens.
3. Click **Yes** to accept the edited mark.

Modifying the Event In/Out marks

To modify event marks:

1. Select the event you are modifying.
2. Open the properties dialog box by doing one of the following:
   - Select **Playlist | Properties**.
   - Click the **Properties** button.
3. Click the **General** tab.
4. Select the Event In, Event Out, or Length edit control and do one of the following:
   - To modify marks, enter the timecode value to specify mark locations.
   - To clear marks, click the **Clear** button or delete the timecode value.

5. Click **OK**.

Moving events

To the change the order of events in a list, perform one of the following:

- Drag and drop the event into another location in the list.
- Select an event, then choose **Move Up** or **Move Down** buttons on the **Playlist** menu. The event moves up or down one position in the list.
    - Use the **Edit** menu to **Copy**, **Cut**, or **Paste** the event. When you paste the event, it is inserted after the currently selected event.

      NOTE: You can paste events that you copied from a list running on another playlist channel.

Removing events

To remove an event, perform one of the following:

- Select the event, then press the Delete key on your keyboard.
- Select the event, right-click, then select **Remove**.
- Use the **Edit** menu to **Cut** the event. (When you paste the event elsewhere, it is removed from this playlist.)
- Right-click on the event and select **Cut**. (When you paste the event elsewhere, it is removed from this playlist.)

Copying events

To copy an event, perform one of the following:

- Use the **Edit** menu to **Copy** the event.
- Right-click on the event and select **Copy**.

Renaming events

To rename an event, perform the following:

1. Select the event, then select **Playlist | Properties**.
2. Click on the name of the event in the Properties dialog box and use the on-screen keyboard to change the name.
3. Click **OK**.

   NOTE: Make sure you do not violate asset naming limitations.

Locating the event source clip

The Locate menu item is used to locate and select the source clip in the Clips pane that generates an event.

To locate the source clip:

- Select the event, then select **Playlist | Locate**.

  The source clip is selected in the Clips pane.

Viewing event properties

1. Select the event.
2. Open the properties dialog box by doing one of the following:
   - Select **Playlist | Properties**.
   - Click the **Properties** button.
   - Right-click the event and select **Properties**.

Managing sections in a list

A list has at least one section; all events belong to a section. Sections management tasks include the following:

- Adding and removing sections
- Moving and copying sections
- Renaming sections

Adding and removing sections

A playlist has at least one section but can have up to 100 sections. All events belong to a section, and each section can have up to 1000 events.

To add a section:

1. Select **Playlist | Add Section.** The new section is inserted at the end of the list.
2. Use the **Edit** menu to **Cut**, **Copy**, or **Paste** a section. When you paste the section, it is inserted after the currently selected section.

   NOTE: You can paste a section that you copied from a list running on another play channel.
3. Right-click on the section and select **Cut**, **Copy**, or **Paste**.

To remove a section, perform one of the following:

- Select the section in the list, right-click and select **Remove**.
- Use the **Edit** menu to **Cut** a section.
- Select the section, then click the **Remove** button.

This button only appears in full screen viewing mode (unless you have customized your user interface to include it as one of the assignable buttons).

Moving and copying sections

To change the order of sections in a list, perform one of the following:

- Drag and drop the section into another location in the list.

- Select a section, then select **Playlist | Move Up** or **Move Down**.

  The section moves up or down one position in the list.
- Use the **Edit** menu in the AppCenter toolbar or standard keyboard shortcuts to **Cut**, **Copy**, or **Paste** the section.

  When you paste the section, it is inserted after the currently selected section.
- Right-click on the section and select **Cut**, **Copy**, or **Paste**.

NOTE: You can paste sections that you copied from a list running on another play channel.

Renaming sections

To rename a section:

1. Select the section.
2. Open the properties dialog box by doing one of the following:
   - Select **Playlist | Properties**.
   - Click the **Properties** button.
   - Right-click on the section and select **Properties**.
3. Select the section name, then enter a new name.

   NOTE: Make sure you do not violate asset naming limitations.
4. Click **OK**.

Adding play effects

These settings determine what happens at the end of the list, section, or event when the list is played.

To repeat at the end of a playlist

You can loop on a list until you manually stop playing.

1. Open the list properties dialog box by doing one of the following:
   - Select the list icon in the event list, then click the **Properties** button.
   - Right-click on a list and select **Properties**.
2. Click **End**, then choose the **Repeat** option.
3. Click **OK** to close.

NOTE: If you leave a player channel in Loop mode, a remote protocol-controlled playlist might either miss all of the events and stop or simply cue the clip and not play.

To pause at the end of a section

To pause at the end of a section:

1. Select the section.

2. Open the properties dialog box by doing one of the following:
   - Select the section icon in the event list, then click the **Properties** button.
   - Right-click on a section and select **Properties**.
3. Click **End**.
4. Select the **Pause** drop-down list. Use the drop-down list to choose whether to **Freeze on last frame, Freeze on next event, none, Show black** or **Show E-to-E**.
5. Click **OK**.

Based on your selection, the section repeats when it comes to the end or each event's properties are modified to include the specified pause type. During playback, each event will remain paused at its end until you intervene. The pause symbol appears in the corner of the event thumbnail.

To pause at the end of an event

1. Select the event.
2. Open the properties dialog box by doing one of the following:
   - Select the list icon in the event list, then click the **Properties** button.
   - Right-click on a list and select **Properties**.
3. Click **End**.
4. Use the **Pause** drop-down list to choose whether to **Freeze on last frame, Freeze on next event, Show black** or **Show E-to-E**.
5. Click **OK**.

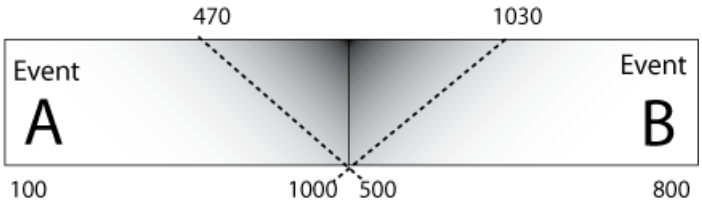
The pause symbol appears in the corner of the event thumbnail.

About transition effects

This feature is part of the licensable AppCenter Pro option on supported formats.

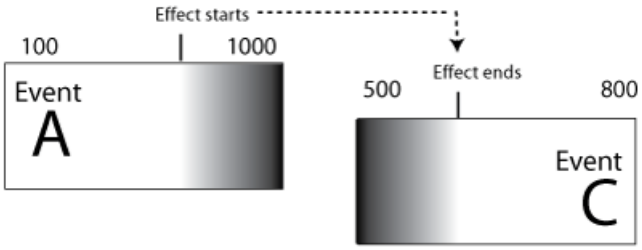
In Summit, AppCenter Pro lets you make transitions to all events in a section or list. There are two types of transitions: you can apply transitions to all the events in a section or playlist, or you can apply transitions that only apply when you skip from one event to another.

Transition effects applied to playlist, section, or event properties



When you use the Properties| All Events feature to apply a transition such as the "Dissolve" effect to adjacent events, there is some overlap. In this example, Event B starts at 500, but AppCenter Pro starts the fade effect at 470. If there is no extra material at 470, a still frame will be displayed until 500 is reached.
This effect can apply to an event, a section, or a whole playlist depending on whether you have selected playlist, section, or clip properties.

Transition effects applied while skipping from one event to another



When you apply a transition effect such as "Dissolve" and skip from one event to another using Options | Go To , AppCenter Pro starts the effect at the indicated point on event A and ends the effect at the indicated point on event C. (There is no overlap.)

To add pauses or transitions to all events in a playlist, section, or event

Properties for each event currently in this section of the playlist are modified to include the specified pause or transition type. If you later add an event to this section and you want it to have the same effect, you must manually modify its properties. Properties of events added later are not automatically modified unless you select Apply to new events.

If you have selected Pause, during playback each event will remain paused at its end until you intervene. The pause symbol ● appears in the corner of the event thumbnail.

NOTE: Apart from Freeze, all transition effects require AppCenter Pro licensing.

To add a pause or transition at the end of an event or all events in a playlist or section:

1. Select the event, section, or list.
2. Open the properties dialog box by doing one of the following:
   - Click the **Properties** button.
   - Right-click on a section and select **Properties**.
3. Click **All Events**.
4. To add a pause, select the **Pause** drop-down list, select **freeze on last frame**, **freeze on next event**, **none**, **show black**, or **show E to E**.
5. To add a transition, select the **Transition** dropdown list, select **none**, **dissolve**, **Fade thru black, Fade thru white, Audio cross-fade**, or **Audio fade thru silence.** If desired, click **include audio**.
6. If you are adding a transition, you can also enter a time for the length of the transition: **.25**, **.50**, **.75**, **1.00**, **1.50**, or **2.00** seconds.
7. To have the effect apply to events added from this point on, Apply to New Events button.
8. When finished, click the **Apply All** button. (If you click **OK**, the dialog box closes without saving any changes.)

To add transitions to all events in a playlist

The AppCenter Pro handles transitions made on the fly.

NOTE: All transition effects require AppCenter Pro licensing.

To add an on-the-fly pause or transition to a playlist:

1. With the playlist open, select **Playlist | Options** and select the **Go To** tab.
2. Select the desired transition, and click **OK**.

   NOTE: Check specifications for limitations on the transition length.

When you use the **Go To** feature to skip from one event, the transition takes effect.

To remove pause from all events in a section

To remove pauses at the end of all section events:

1. Select the section.
2. Open the properties dialog box by doing one of the following:
   - Click the **Properties** button.
   - Right-click on a section and select **Properties**.
3. Click **All Events**.
4. Select the **Change event pauses** check box, then choose the **Remove all pauses** option.
5. Click **OK**.

Pauses are removed from all events in the section. The section now plays without pausing between any events.

Adding GPI output triggers to playlists

You can assign GPI output triggers to events and sections in a playlist. The GPI outputs can be used to trigger external equipment when the list plays. Before you can use GPI output triggers in a list, you must use Configuration Manager to assign GPI outputs to a channel that is running the Playlist application. If you want to play a list that was created on another channel, you must ensure that GPI triggers assigned to all applicable channels use the same names, otherwise the GPI triggers will not occur. Using identical GPI naming also allows copying and pasting sections and events between lists to be played on different channels.

To trigger GPI outputs:

1. Use Configuration Manager to assign GPI outputs to the current Playlist channel by selecting **System | Configuration**.
2. Make the changes to the GPI settings.
3. Select an event or section in the playlist, then open the properties dialog box by doing one of the following:
   - Click the **Properties** button.
   - Right-click on an event or section and select **Properties**.
4. Select Trigger GPI, then use the drop-down list to select a GPI output. If no GPI outputs are listed, use Configuration Manager to assign GPI outputs to the current channel, then return to this step.
5. Select the trigger action for the GPI output:

Action	Trigger point
Start of event or section	First frame of event or section
End of event or section	Last frame of event or section
Start plus	Start of event or section plus the time you enter. Offset should not exceed the event or section total length.If the offset time entered exceeds the event or section length, a warning message is displayed.
End minus	End of event or section minus the time you enter. Offset should not exceed the event or section total length. If the offset time entered exceeds the event or section length, a warning message is displayed.

6. Click **OK** to save settings.

Managing playlists

You can manage playlists by doing the following tasks.

Saving a copy of a playlist

When you are creating a new playlist, you might find it easier to use an existing, similar playlist as your starting point, rather than creating a list from scratch. To do this you must first save a copy of the playlist with a new name. Then you can alter it without changing the original playlist.

To save a copy of a playlist:

1. In the Clips pane, select the playlist.
2. Copy the playlist onto the clipboard, using the **Edit** menu or standard keyboard shortcuts.
3. Paste the playlist into the Clips pane. If you paste the list into the same bin that you copied it from, a dialog box appears giving you the choice to Abort, Ignore, or Retry (saving as a different name).
4. Load the copied playlist into the Playlist application, and alter it to create your new playlist.

Renaming a playlist

You can rename a playlist using the Playlist menu.

1. Select the playlist in the Clips pane.
2. In the Playlist file menu, select **Playlist | Rename List**.
3. Use the on-screen keyboard to enter and new name and click **OK**.

   NOTE: Make sure you do not violate asset naming limitations.

   The renamed list appears in the Clips pane.

Locking a playlist

You can lock a list to prevent changes from being made.

1. Make sure that the list to be locked is selected in the list pane.
2. Open the list properties dialog box, doing one of the following:
   - Select the list icon in the event list, then click the **Properties** button.
   - Right-click on the list and select **Properties**.
3. Click **General**, then choose the **Locked** option.
4. Click **OK** to close. The lock symbol appears.

Setting the playlist timecode

The playlist timecode is displayed in the toolbar. This selection is also used to generate LTC timecode for the play channel. You cannot stripe the playlist timecode; however, you can stripe the timecode of the loaded clip.

To select the playlist timecode:

1. Open playlist properties dialog by performing one of the following:
   - Click the **Properties** button.
   - Right-click on a list and select **Properties**.

   The List Properties dialog box is displayed.
2. Click **Timecode** in the properties dialog box.
3. Select **Drop Frame**.

   The drop frame option is available when system timing is set to 525 line standard. Drop frame allows the playlist timecode to indicate the actual running time of the list.
4. Specify a start time, then click **OK**.

   The start timecode is displayed in the toolbar.

Locating a playlist in the Clips pane

- Select **Playlist | Locate**.

  The bin containing the list is shown in the Clips pane.

Viewing playlist properties

Select the playlist, then open the properties dialog box by doing one of the following:

- Select **Playlist | Properties**.
- Click the **Properties** button.
- Right-click on a playlist and select **Properties**.

Saving a list as a program

Playlists can be saved as a program so that they can be managed as a single clip. This saves the events in the list, but nothing that breaks the flow of playout such as pauses or effects between events or sections. Saving a list does not consume media storage space since the program merely references the source clip media that is already stored in the media file system. If the source clips are deleted, the media referenced by the program is preserved.

You can insert programs into other playlists, or load and play them using the standard Player application. In Player application, you can edit the program mark-in and mark-out points providing the source clips referenced by the program have not been deleted. If that is the case, 1 second of media is preserved before and after the program mark-in and mark-out allowing some trimming.

1. Load the playlist in the Playlist application.
2. Select **Playlist | Save As Program**.
3. Use the **Save In** control to change the current bin if required.
4. Select the **Program Name** text entry control to change the program name, then click **OK**.

   NOTE: Make sure you do not violate asset naming limitations.

The list is saved as a program in the current bin.

Importing a text file as a playlist

This feature is part of the licensable AppCenter Pro option.

Import text file as playlist — If you are licensed for AppCenter Pro, you receive the import text file as playlist feature. With this feature you can specify a playlist as a text file and then import it into AppCenter. You can choose to import the playlist as a new list or append to an existing list. When appending to an existing list, the imported playlist is added as a section at the end of the existing list.

The information in the text file must be arranged as follows:

- The text file must have at least three columns, separated by spaces or tabs.
- For each row, one column must specify the clip name, one column must specify the mark in point, and one column must specify the duration.
- The clip name can include a path, or it can be a simple clip name with no path. Spaces in the path/name are not allowed.
- The format for specifying a path with the clip name is volume:/binname/clipname. For example, *V:/default/Clip_1*.
- If the clip name has no path, the clip must be in the current bin.
- Timecode can be formatted with separators or without separators. If without separators, it must be in format HHMMSSFF. If with separators, it can be in single-digit format H:M:S:F, it can be in double-digit format HH:MM:SS:FF, or it can have the single-digit and double-digit formats combined. Colon, semicolon, period, and comma are all legal timecode separators.
- A “wild character” 99:99:99:99 can be used, in either the mark in or duration columns, to indicate that the clip should be inserted in its entirety.
- A section can be specified in the following 3 ways:
  - <section>

    Results in a section with a default name and no pause
  - <section> MyCommercialPod

    Results in a section named "MyCommercialPod" with no pause
  - <section> MyCommercialPod StopBlack

    Results in a section named "MyCommercialPod" with a pause at the end that displays black. Pause type can be any of the following: StopBlack, StopFreeze, StopNext, or StopEE.
- Timecode values are allowed to be out of range, as AppCenter normalizes timecode values when the playlist is played out. For example, if in the text file, the seconds value is greater than 60, as in 00:25:75:00, AppCenter rounds up the minutes value and converts the timecode to 00:26:15:00.
- You can specify sections in the imported playlist by adding a row at the beginning of a section that contains just the <*section*> specifier.

The following example shows the contents of a text file that specifies a playlist with two sections.

```
Clip01 00:00:00:00 00:00:30:00
Clip03 00:25:00:00 00:01:00:00
Clip10 00:00:20:00 00:00:05:00
```

```
Clip11 00:00:04:00 00:00:02:00
Clip12 00:00:25:00 00:00:02:00
Clip13 00:00:00:00 00:00:05:00
<section>
V:/abin/Clip15 00:41:46:00 00:00:04:00
V:/abin/Clip16 00:10:00:00 00:00:05:00
V:/abin/Clip17 00:20:00:00 00:00:05:00
V:/abin/Clip18 00:30:00:00 00:00:05:00
V:/abin/Clip19 00:10:00:00 00:00:05:00
V:/abin/Clip04 00:00:00:00 00:10:00:00
```

Importing a text file as a playlist into AppCenter

To import a text file as a playlist into AppCenter, do the following:

1. Select a channel with its application set to playlist.
2. If the text file contains simple clip names with no path, in the Clips pane select the bin that contains those clips.
3. Click **Playlist | Import List**.

   The Import dialog box opens.
4. Browse to and select the text file that specifies the playlist, then click **Import**.

   The Import File Layout dialog box opens.
5. Specify which column in the text file contains names, which column contains mark in points, and which column contains durations, then click **OK**.

   The playlist appears in AppCenter.

All playlist sections added during an import have a pause added automatically at the end.

Managing clip media

Managing clip media

The AppCenter Clips pane is used to manage the assets stored in K2 media storage. Almost all the media management tasks you'll perform fall in the following topics.

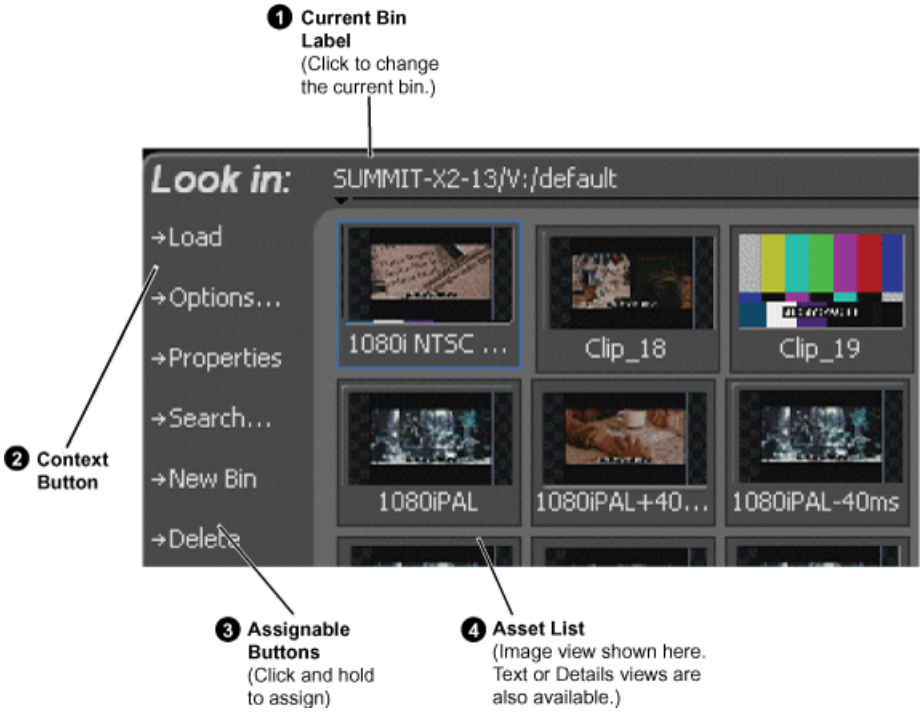
Guide to using the Clips pane

The Clips pane in the AppCenter user interface provides tools for managing assets stored on the media drives. Assets include clips, and playlists, and programs. In addition to the typical file management tasks such as browse, copy, move, delete, and managing the directory structure, you'll also use the Clips pane to transfer files to other devices, and to import or export assets using standard file formats.

When using a AppCenter remotely from a Control Point PC, you can have channel suites with channels from K2 Solo 3G system that access internal storage or shared K2 storage systems. The storage displayed is the storage accessed by the active channel, that is, the channel currently selected.

Viewing the Clips pane

The Clips pane is always displayed in AppCenter. The size of the Clips pane changes when you resize the monitor pane or the channel pane. At its minimum size the Clips pane displays a single column of clip thumbnails.



	Control	Description and User Operation
❶	Current Bin Label	Displays the name and location of the current bin, or the summary of the search or link operation. At first time start-up, the current bin is `V:/default`. The bin named 'default' is on the internal disk volume. Click the current bin label to change the current bin and organize bins.
❷	Context Button	The operation and label of the context button changes with the application of the selected channel. • Load – Displayed when the selected channel is in Player application or Recorder mode. Loads the asset selected in the asset list. • New Event– Displayed when the selected channel is in Playlist application Event View. Creates an unattached event in the playlist that can be previewed and then inserted. • Insert – Displayed when the selected channel is in Playlist application List View. Inserts selected assets into the playlist. ***NOTE: Double-clicking the asset in the asset list performs the same function as clicking the context button.***

	Control	Description and User Operation
❸	Assignable Buttons	Assignable buttons allow you to modify the button assignments to best suit your workflow. Hold down a button to open the button pop-up menu that lists the alternative button choices. • Properties– Opens the Properties dialog for the selected asset. • Search– Opens the search dialog box. • New Bin– Creates a new bin. To create a new bin in the current disk volume, click New Bin, then enter the new bin name using onscreen or external keyboard. • Options– Opens the options dialog box which allows you to modify how assets are displayed in the asset list. • Delete– Deletes the selected item(s). • Rename– Opens the Rename dialog box. • Send to– Opens the Send to dialog box used to send the asset to a file, or streaming transfer to another networked device.
❹	Asset List: Select from three view options— Text, Image, or Details	Displays the list of assets located in the current bin. You can scroll through the list using the up/down arrow keys on an external keyboard. Right-click to open the Asset Context menu. You can change how assets are shown by selecting the view option. View options include Image (thumbnail), Text, or Details (includes thumbnail and detailed text). Assets recorded using a different video standard or compression type than the current system setting cannot be loaded and played on the K2 Summit Production Client. For example, if you record a PAL clip, you cannot play it on a channel that is configured for NTSC. These assets appear “grayed” in the Clips pane asset list.

Terms used in the Clips pane

The following table describes the terms used in the Clips pane.

Asset	Description
Bin	A container used to organize assets, similar to a directory or folder on a computer. A bin is contained within a disk volume. The K2 system supports nested bins, that is, a bin contains another bin.
Current Bin	The current bin functions as the target bin when recording clips, or as the source bin when loading clips. The current bin contents are listed in the Clips pane. The *V:/default* bin is created automatically. The name *default* cannot be edited and the bin cannot be deleted.
Disk Volume	The K2 Solo 3G system media storage disk volume is formatted using the K2 system media file system. The disk volume uses the drive letter ‘V:’. The disk volume can be internal or it can be part of the K2 external storage system.

Asset	Description
Playlist	A sequence of events that can be loaded and played using the Playlist mode. Playlists are created in the Playlist application by adding clips or programs to a list.
Media	Media is the video, audio, and timecode source material recorded on the disk drives. Each media type is stored in its own file, which is referenced by one or more clips for playback.
Clip	A clip references the media files stored on the media drives to allow playback of the video and associated audio and timecode recorded from a single source. Deleting a clip deletes the media referenced by the clip only if it is not referenced by another clip. You can use the Find Links feature to find related assets.
Program	Programs are generated from continuous record mode or from a playlist using the Playlist mode. Programs generated in Playlist application include all the media and transitions in the playlist, but nothing that breaks the flow of playout, such as a pause at the end of an event.

About the Current Bin drop-down list

To access the Current Bin drop-down list, click the Current Bin label.

Current bin menu items

Menu Item	Description and User Operation
Organize Bins	Opens the Organize Bins dialog box used to manage bins— create, delete, rename, change current bin..
Bin List	List of all the bins in the current disk volume. A volume must always have at least one bin. The default bin is created automatically.
Recycle Bin	Displays the contents of the Recycle Bin. All assets deleted from the asset list are stored in the Recycle Bin until it is emptied.

About the Clips menu

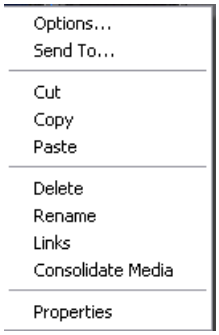
Click **Clips** in the AppCenter main menu to display the Clips pane context menu. The following table describes the context menu items.

Menu Item	Description
New Bin	Creates a new bin in the current disk volume. Use the onscreen or external keyboard to enter the bin name.
Organize Bins	Allows you to manage the bins.
Empty Recycle Bin	Permanently removes all items from the Recycle Bin. By default, deleted assets are moved to the Recycle Bin and remain there until it is emptied.
Delete	Deletes the selected asset.

Menu Item	Description
Rename	Opens the Rename dialog box for the selected asset.
Select All	Selects all items in the asset list. Operations available for Select All include: delete, send to, and copy.
Search	Opens the Search dialog box, which is used to perform basic or advanced searches.
Links	Opens the Links dialog box allowing you to locate other assets that are linked to the selected asset. For example, a subclip is linked to the source clip.
Send To	Opens the Send To dialog box, which is used to send assets to a different location– another bin, disk volume, or another K2 Solo 3G system. Send To is also used to export clips or programs to local windows drives or networked devices.
Import	Opens the Import dialog box, which is used to import assets from the following sources: • Media streams from another K2 Summit Production Client. • Other media file formats from a local drive or over the network.
Properties	Opens the Properties dialog box for the selected asset.
Options	Opens the Options dialog box, which allows you to change the way assets are displayed in the asset list.

About the asset context menu

To open the asset context menu, right-click the asset.



Menu Item	Description
Options	Opens the Options dialog box which allows you to change the way assets are displayed in the asset list.
Send To	Opens the Send To dialog box which is used to send assets to a different location– another bin, disk volume, or another K2 Summit Production Client. Send To is also used to export clips or programs to local windows drives or networked devices.

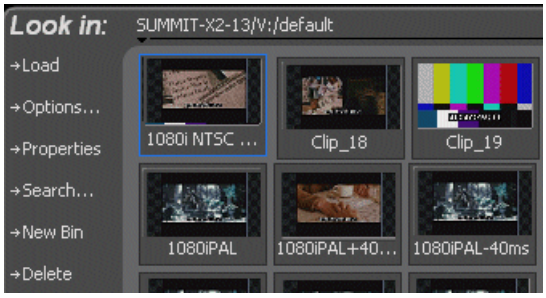
Menu Item	Description
Cut, Copy, Paste	Used to move assets, or make a additional copies. Copying a clip does not consume media disk space. Only a new reference to existing media is created.
Delete	Deletes the selected asset.
Rename	Opens the Rename dialog box for the selected asset.
Links	Opens the Links dialog box allowing you to locate other assets that are linked to the selected asset.
Consolidate media	Erase unused media.
Properties	Opens the Properties dialog box for the selected asset.

Modifying the asset list view

The asset list in the Clips pane displays the contents of the current bin and the results from searches or from requests for linked assets. You can choose one of three views to best suit your workflow.

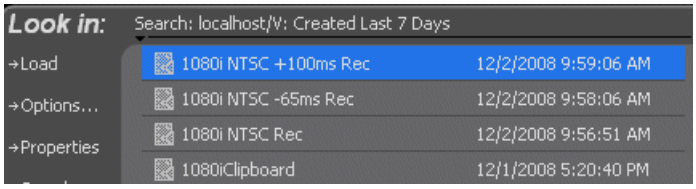
1. Select **Clips | Options**.

2. In the View tab, select one of the following view options:
   a) Image view



   Displays the asset name and thumbnail image for each asset in the bin. Playlists are displayed as a stack of thumbnails. You can change the video frame used to generate the thumbnail.

   b) Text view



   The text view displays an icon and name for each asset and one attribute of your choice. To select an asset attribute, select the **Show** drop-down list in the View Options dialog box, then select one of the following attributes.

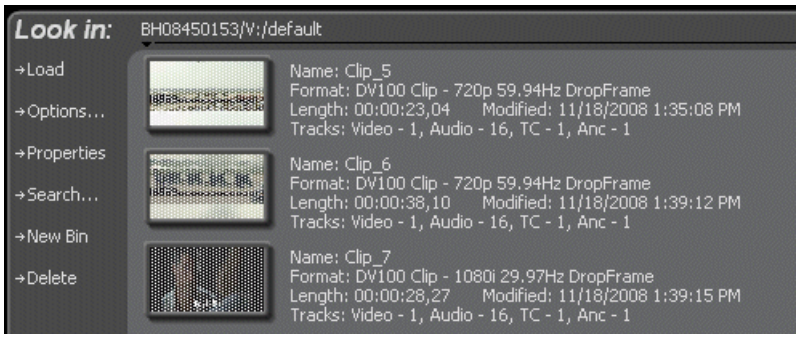
   Attribute display options:

   - Create Date
   - Modified Date
   - Length
   - Type
   - Location (full path)

   The following table describes symbols shown in Text view

Asset Symbols used in the Text View	Asset Type
	Clips with audio and video
	Video only clip
	Playlist

   c) Details view



Details view displays assets with both a thumbnail and a detailed text description.

3. If you want to sort the assets, click the Sort tab, then choose how you want assets sorted.
4. Click **OK**.

The clips pane displays with the new view and sort order.

Working with bins

Topic in this section provide information about K2 system bins.

Using security with bins

By default, permission is set to Full Control for "Everyone" on K2 bins. In case of conflicts arising from a user belonging to multiple groups, the Deny permission always overrides the Allow permission. K2 administrators may create users and groups and set permissions for them. For information on how to implement security permissions, see the *K2 System Guide*.

Changing current (working) bin.

- In the Clips pane, click the Current Bin label, then choose a bin from the list.
- You can also change the working bin by loading a clip into a channel (for example, by using drag-and-drop) from a bin that is not the current working bin for that channel. The bin from which you loaded the clip then becomes that channel's working bin.

Exploring bins

Exploring a bin in the Organize Bins dialog box causes it to display in the Media Monitor pane. Exploring a bin does not make that bin the default setting for recording clips. A clip that is being recorded is stored in the working bin that has been specified for its channel. Each channel has its own working bin. To change the current bin where a clip will be recorded, click the Options button on the channel pane. Loading a clip from a bin into a play channel changes the working bin for that channel.

1. In the Clips pane, select the Current Bin drop-down list, then select **Organize Bins**.
2. In the Organize Bins dialog box, select a bin, then click **Explore**.

   NOTE: If the Explore button is grayed out, you do not have Explore permission. Without permission to explore a bin, you cannot rename or delete a bin either. For information on security and permissions, see the K2 System Guide.

3. Close the Organize Bins dialog box.

Creating a new bin

1. Open the Organize Bin dialog box using one of the following methods:
   - Select **Clips | New Bin**.
   - Click the **New Bin** button in the clips pane.
   - In the Clips pane:
     - Select the Current Bin drop-down list, then select **Organize Bins**.
     - In the Organize Bins dialog box, select where you want the bin to be created (e.g. at the top level or as a sub bin of an existing bin), then click **New Bin**.

   NOTE: Make sure you do not violate bin naming and nesting limitations.
2. Enter the new bin name, then click **OK**.

   The new bin appears in the Organize Bins dialog box.

   NOTE: There are additional buttons displayed, which permit you to rename or delete the bin.
3. Close the Organize Bins dialog box.

Deleting a bin

NOTE: Even with the appropriate permissions, you cannot delete a bin containing assets that are locked or in use. However, the unlocked assets in the bin can be deleted.

1. In the Clips pane, select the Current Bin label, then select **Organize Bins**.
2. In the Organize Bins dialog box, choose the bin you want to delete.
3. Click the **Delete** button.

   Deleted bins and assets are moved to the Recycle Bin unless the "*Remove items immediately when deleted.*" option is set for the Recycle Bin.

   Holding down the SHIFT key during delete also bypasses the Recycle Bin.
4. Click **Yes** in the Confirm Delete dialog box.
5. Close the Organize Bins dialog box.

Renaming a bin

1. In the Clips pane, select the Current Bin label, then select **Organize Bins**.
2. In the Organize Bins dialog box, select the bin you want to rename.

   NOTE: If the Rename button is grayed out, you do not have permission to rename the bin.
3. Click **Rename**.
4. Edit the bin name.

   NOTE: Make sure you do not violate bin naming limitations.

5. Click **OK**.

   NOTE: If you rename the working bin, it changes to the default bin. If the renamed bin contains assets that are locked or in use, two bins will appear after renaming— one with the new name and one with the old name containing the problem asset.

6. Close the Organize Bins dialog box.

Working with assets

Assets displayed in the Asset List include clips, subclips, playlists, and programs. Refer to the following sections to work with assets.

Renaming an asset

1. Select the asset in the Asset List.
2. Select **Rename** using one of the following:

   - Select **Clips | Rename**.
   - Select **Rename** in the asset context menu.
   - Click the **Rename** button in the Clips pane.

   The Rename dialog box appears.

   If the Rename button is not displayed in the Clips pane, refer to assignable buttons in the Guide to using the Clips pane section.

3. Edit the asset name, then click **OK**.

   NOTE: Make sure you do not violate asset naming limitations.

   NOTE: Assets that are locked or in use cannot be renamed.

Selecting multiple assets

You can select multiple assets in the Clips pane as follows:

- Select **Clips | Select All**.
- Using mouse and keyboard, hold the SHIFT or CTRL key on the keyboard while selecting multiple assets with the mouse or arrow keys.

Moving an asset to another bin

There are two ways to move an asset to another bin: Using Cut/Paste or the Send To dialog box.

Using the cut and paste commands

1. Select the asset(s) in the asset list.
2. Cut the asset to the clipboard using one of the following:

   - Select **Cut** in the asset context menu.
   - Select **Edit** in the AppCenter main menu, then choose **Cut**.
   - Use keyboard shortcut **Ctrl + X**.

3. Change the current bin to the target bin.
4. Paste the asset(s) from the clipboard to the current bin.

   The Paste operation is accessed in the same way as Cut.

   NOTE: If an asset is locked or currently being recorded, it remains in the existing bin while the remaining assets are moved to a new bin with the specified name.

Using Send To

1. Select the asset(s) in the Asset List.
2. To open the Send To dialog box using do one of following:

   - Select **Clips | Send To**.
   - Select **Send To** in the asset context menu.
   - Click the **Send To** button in the Clips pane.

   If the Send To button is not displayed in the Clips pane, refer to assignable buttons in the Guide to using the Clips pane section.

   The Send dialog box appears.
3. Click the Bin tab.
4. Select **Move to** in the right-hand drop-down list.
5. Select the target bin name.
6. Click the **Send** button to close the Send dialog box, and move the file.

Copying an asset

The copy command creates a new asset that references the same media files belonging to the original asset. Copying an asset does not duplicate the media files. Copying does not impact the media storage space available.

The naming convention for copied assets in the same bin adds an underscore ("_") and a number after the original name. For example, the copied clip for "Clip1" will be "Clip1_1", "Clip1_2" and so on.

You can copy or move assets in two ways, as follows:

Using the copy and paste commands

1. Select the asset(s) in the asset list.
2. Copy the asset to the clipboard using one of the following:

   - Select **Copy** in the asset context menu.
   - Select **Edit** in the AppCenter toolbar, then choose **Copy**.
   - Use the keyboard shortcut **Ctrl + C**.

3. If needed, change the current bin to the target bin.

4. Paste the asset(s) from the clipboard to the current bin.

   The Paste operation is accessed in the same way as Copy.

   NOTE: If an asset is locked or currently being recorded, it remains in the existing bin, while the remaining assets are moved to a new bin with the specified name.

Using Send To

1. Select the asset(s) in the Asset List.
2. To open the Send To dialog box do one of following:

   - Select **Clips | Send To**.
   - Select **Send To** in the asset context menu.
   - Click the **Send To** button in the Clips pane.

   If the Send To button is not displayed in the Clips pane, refer to assignable buttons in the Guide to using the Clips pane section.

   The Send dialog box appears.
3. In the Send dialog box, click **Bin**, then **Copy to** in the left-hand drop-down list.
4. Select the target bin name.
5. Click the **Send** button to close the Send dialog box, and copy the file.

Deleting an asset

You can delete assets to free storage space. You can safely delete a clip without harming the subclips, playlists, and programs created from it. The media referenced by subclips, playlists, and programs is preserved when the clip is deleted. Once the source clip is deleted, subclips and playlist events retain an extra 1 second of media before and after their mark points to allow some trimming.

If you want to delete an asset that has a sub-clip or that is part of a playlist or a program, you must first use the Consolidate Media feature.

Deleted assets are moved to the Recycle Bin unless the bypass Recycle Bin option is used. You must empty the Recycle Bin to free storage space.

To delete an asset:

1. If associated with playlist, program, or sub-clip, right-click on the asset and select **Consolidate Media**.
2. Select the asset or assets in the Asset List.

3. Select **Delete** using one of the following:

   - Select **Clips | Delete**.
   - Select **Delete** in the asset context menu.
   - Click the **Delete** button in the Clips pane.

   If the Delete button is not displayed in the Clips pane, refer to assignable buttons in the Guide to using the Clips pane section.

   A progress dialog box appears when deleting multiple assets. If the selected asset is contained in the Recycle Bin, it is permanently removed; otherwise, it is moved from its original bin into the Recycle Bin. If an item of the same name is already in the Recycle Bin, the new item is automatically renamed.

   NOTE: Assets that are locked or currently being recorded cannot be deleted.

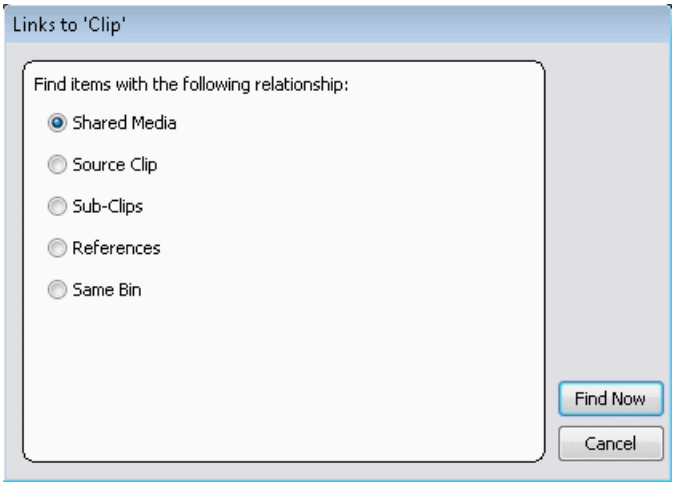
Erasing a clip's unused media

For K2 Summit/Solo systems, you can use the Consolidate Media feature to delete unwanted material from trimmed clips, subclips, programs or playlists. Although similar to the Erase Unused Media feature in K2 Media Client systems, there are some differences in how material is handled. The following table describes the similarities and differences.

When using...	K2 Media Client Erase Unused Media	Summit Consolidate Media
Trimmed clips (Media not referenced by any subclip, program, or playlist)	Any unused storage is released; the media outside the in/out marks is erased.	No effect; nothing is erased.
Subclips, programs, or playlists	With the Erase Unused Media feature, the source clip and the subclip both reference the same media. Unused media is not erased from a subclip unless the source clip has first been deleted manually.	With the Consolidate Media feature, the subclip media is copied from the source material. Once you have consolidated the media, you can manually delete the source media; the subclip is not affected. Consolidating the media also removes the links to the assets. ***NOTE: Before consolidating media, make sure you have enough storage for the newly copied material. Maintain free space equivalent to the longest clip consolidated.***

NOTE: One second of media is retained (for editing) before and after the trimmed clip, subclip, program or playlist.

When you consolidate media, the links between the assets are also removed.



Consolidating media

To consolidate media:

1. Select the clip in the asset list.
2. Right-click on the asset and select **Consolidate Media**.

   A Consolidating message box appears.

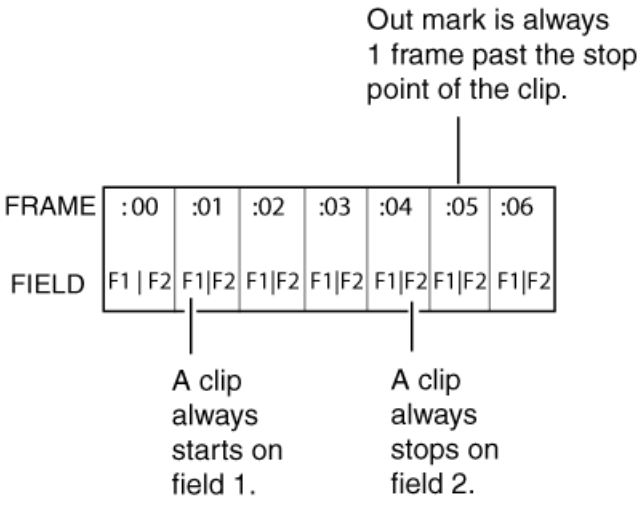
   NOTE: To verify that the media has been consolidated, you can check the file size in the V:\ drive.

After consolidating media, the following is true:

- Media outside the clip marks is erased except that portion referenced by a subclip, playlist event, or program.
- All subclips and events generated from the source clip retain 1 second of media before the mark-in and after the mark-out.
- Event-in becomes the first video frame of the file.
- Event-out becomes the last video frame of the file.
- Clip length becomes the total file length.

Understanding field dominance

In interlaced video, each frame is composed of two fields. In Grass Valley systems such as a K2 Solo 3G system, video is field-1 dominant; each frame consists of field 1 followed by field 2. For example, when you navigate through the clip to the beginning, the K2 Solo 3G system system goes to field 1. When you navigate through a clip to the end, the K2 Solo 3G system goes to field 2.



The in point of any trimmed clip always starts at field 1 of a frame. The out point of a trimmed clip is always one frame past the stop point of the clip. For example, if the last playable frame is 01:15:00,04 then the out-point mark is 01:15:00;05.

Locking an asset

Locked assets cannot be renamed, deleted, or modified in any way.

To lock an asset:

1. Select the asset in the Asset List.
2. To view the Properties dialog box for the selected asset, do one of the following:
   - Select **Clips | Properties**.
   - Select **Properties** in the asset context menu.
   - Click the **Properties** button in the Clips pane.

   If the Properties button is not displayed in the Clips pane, refer to assignable buttons in the Guide to using the Clips pane section.

   The Asset Properties dialog box appears.
3. Click the General tab, then select the **Locked** check box to lock the asset.
4. Click **OK** to close the Properties dialog box.

Working with the Recycled Bin

To work with the recycled bin, refer to the following topics.

Viewing the Recycled Bin contents

- In the Clips pane, select the Current Bin label, then select **Recycled Bin**.

  The Recycled Bin assets are displayed in the asset list as the current bin. You can work with assets in the Recycle Bin just like any other bin.

Emptying the Recycled Bin

1. In the Clips pane, select the Current Bin label, then select the **Organize Bins**.
2. In the Organize Bins dialog box, select **Recycled Bin** from the bin list.
3. Click **Empty**, then **Yes** to confirm.
4. Close the Organize Bins dialog box.

Bypassing the Recycled Bin when deleting

NOTE: Holding down the SHIFT key during delete also bypasses the Recycled Bin.

1. In the Clips pane, select the Current Bin label, then select the **Organize Bins**.
2. In the Organize Bins dialog box, choose **Recycled Bin**.
3. Select **Remove items immediately when deleted** or hold down the SHIFT key during delete.
4. Close the Organize Bins dialog box.

Locating assets

Three tools are provided for locating assets: Sorting, Search, and Links. You can set how assets are sorted by selecting the "sort by" attribute for the asset list. For example, you can sort by name, modified date, length, etc. The Search dialog box provides both basic search and advanced search modes for locating assets anywhere in the K2 system media storage. Advanced search mode allows you to define search criteria for assets based on user-defined metadata. The Links dialog box helps you determine assets that are related. For example, you can locate the source clip used to generate a subclip or you can determine if there are copies of a given clip.

Sorting assets in the Asset List

You can sort assets by file attributes such as date, name, length, and create date using the Options dialog box.

To change how assets are sorted:

1. Open the Options dialog box using one of the following methods:

   - Select **Clips | Options**.
   - Right-click an asset, then select **Options** in the asset context menu.
   - Click the **Options** button in the Clips pane.

   If the Options button is not displayed in the Clips pane, refer to assignable buttons in the Guide to using the Clips pane section.

2. Click the **Sort** tab in the Options dialog box.

3. Choose the desired sorting attribute and order, then click **OK**.

   The Asset List sorts in the order specified.

NOTE: When assets are added or renamed, assets may not remain listed according to the selected sort order. To re-sort the assets, repeat this procedure, or press F5 to refresh the Asset List.

Using Basic search

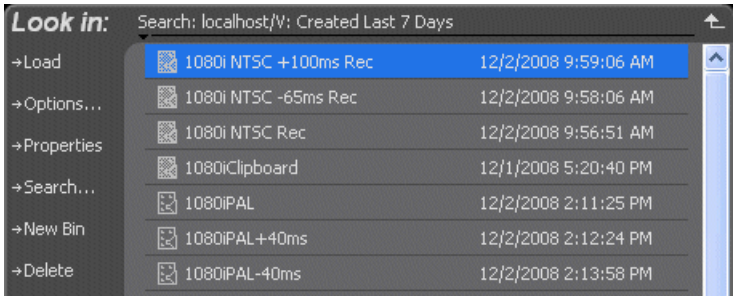
The Search dialog box provides the basic search mode for locating assets anywhere in the K2 system media storage.

1. Open the Search dialog box by doing one of the following:
   - Select **Clips | Search**.
   - Click the **Search** button in the Clips pane.

   If the **Search** button is not displayed in the Clips pane, refer to assignable buttons in the Guide to using the Clips pane section.
2. Choose **Basic** search, then specify search criteria on the **Text**, **Date** and **Type** tabs. The search is performed using the combination of search criteria on all three tabs.
   - **Search by text** – If you know all or part of an asset name, use the **Text** tab. Select the text entry control, then type all or part of the asset name in the "Enter Search Text" dialog box. The default text search mode is "any word" or "word portion". For example, if you enter the word *fire*, search will find all asset names that contain fire, for example, *fires* and *house fire*. For an "exact phrase" search, use a single quote or double quote to specify the phrase. For example, if you enter *"forest fire"*, search will locate all asset names that contain the phrase *forest fire*.

     If the **Search names only…** option is selected, the search is applied to asset names. If not selected, the search includes all asset metadata.
   - **Search by date** – If you are searching for assets created or modified within a specific date or time range, use the **Date** tab. By default, the **All Dates** box is selected. To specify date criteria, select the **Find items** option to enable the controls under it. Use the drop-down list to choose **Created** or **Modified**, then do one of the following:
     - Select the **between** option, and then specify a date range. Click the edit control to display a calendar for easy input.
     - Select the **in the last** option, and then use the drop-down lists to specify a time within a recent number of minutes, hours, days, or months.
   - **Search by Type** – In the **Type** tab, select the type of assets— clips, programs or lists to be searched. Search results will only include the selected types.
3. Once you have selected the search criteria, click **OK** to start the search.

The search results are displayed in the Clips pane. The text in the Current Bin control is replaced with a brief summary of the search. For example, *Search: movie* - indicates all the clips, programs and lists with names like movie1, movie2, or *Search: Created Last 7 Days* for assets created in the last week.



When you perform a search, the most recent four searches are displayed. The older ones get removed. At any one time, you see four searches at most in the bin list. There is no way to delete these.

Using Advanced Search

The Search dialog box provides the advanced search mode that provides an extended set of attributes for locating assets anywhere in the K2 system media storage.

1. Open the Search dialog box by doing one of the following:
   - Select **Clips | Search**.
   - Click the **Search** button in the Clips pane.

   If the **Search** button is not displayed in the Clips pane, refer to assignable buttons in the Guide to using the Clips pane section.
2. Choose **Advanced** search to create and view advanced search criteria.

   When Advanced search is used, Basic search criteria are ignored.
3. Click **Add** to add new search criteria, or click **Remove** to remove it, then click **OK** to start the search.

   You can select advanced search attributes along with their conditions and value choices. Advanced searches can include metadata attributes.
4. Once you have added all the search criteria, click **OK** to add the criteria.
5. Click **OK** to start the search.

The search results are displayed in the Clips pane. The text in the Current Bin control is replaced with a brief summary of the search.

Finding linked assets

The Links dialog box helps you locate assets that are related based on the links criteria that you can specify.

1. In the asset list, select the asset for which you want to find linked assets.

2. Open the Links dialog box by performing one of the following steps:

   - Select **Clips | Links**.
   - Right-click an asset, then select **Links**.
   - Click the **Links** button in the Clips pane.

   If the Links button is not displayed in the Clips pane, refer to assignable buttons in the Guide to using the Clips pane section.

3. Choose one of the link relationships to use.

Link Relationship	Description
Shared media	Find all assets that reference the same media files, that is, the same video, audio, timecode files in the media file system.
Source clip	Find the source clip from which a subclip was created.
Subclips	Find all subclips created from the selected clip.
References	When a playlist or program is selected, find all the assets that are referenced by the playlist or program.When a clip is selected, find all the playlists and events that reference that clip.
Same bin	Generate a list of assets that are located in the same bin

4. Click **Find Now**.

The results of the link operation are displayed in the Clips pane. The text in the Current Bin label is replaced by a brief summary of the links operation.

NOTE: Unlike the search results, link results are not cached. You must perform the Links operation each time to discover linked assets.

Working with asset metadata

The properties dialog box displays information about an asset. The properties dialog box also includes a user defined metadata feature that allows you to define and add your own information about an asset. You can specify the metadata name, data type, and value.

The metadata you add for one asset automatically appears on properties pages for all existing and future assets, except with no value entered. The values you specify for an asset are retained with the asset for the following operations: copy, move, and send to. The metadata you define for an asset can be used as search criteria in advanced search.

Metadata types and their possible values are described in the following table.

Data Type	Value	Example: Name/Value
String	User-defined string	Producer: John Doe
Integer	An integer value	Episode: 4
Float	A number expressed in floating point	Version: 1.2
Date	Date	Air Date: 10/31/03

Data Type	Value	Example: Name/Value
Boolean	True or False	QA: False

Adding and modifying asset metadata

Use the following steps to add or modify metadata in the properties dialog box. The metadata names you add will appear in the properties dialog box for all assets.

1. Select an asset in the Clips pane asset list.
2. Open the Properties dialog box using one of the following methods:

   - Select **Clips | Properties**.
   - Select **Properties** in the asset context menu.
   - Click the **Properties** button in the Clips pane.

   If the Properties button is not displayed in the Clips pane, refer to assignable buttons in the Guide to using the Clips pane section.

   The properties dialog box appears.
3. Click the **Data** tab, then click **Add Data** or **Modify** on the data page.
4. Define or modify metadata using the following steps:
   a) Select **Name**, then enter the metadata name in the Name dialog box. Names are not case sensitive. “Episode” and “episode” are treated the same. You cannot modify names of existing metadata.
   b) Select **Type**, then choose a data type from the drop-down list. Metadata types include: String, Integer, Float, Date, and Boolean.
   c) Select **Value**, then enter a metadata value in the Value dialog box.
   d) Click **OK** to close the Add or Modify dialog box and save changes.

Clearing metadata

Clearing metadata removes the value entered for the selected metadata but does not delete the metadata name from the properties data page.

1. Select the asset in the Clips pane asset list.
2. Open the Properties dialog box using one of the following:

   - Select **Clips | Properties**.
   - Select **Properties** in the asset context menu.
   - Click the **Properties** button in the Clips pane.

   If the Properties button is not displayed in the Clips pane, refer to assignable buttons in the Guide to using the Clips pane section.

   The properties dialog box appears.
3. Click the **Data** tab, then scroll to locate and select the metadata entry you want to clear.
4. Click **Clear**.

   The metadata value is now blank.

5. Repeat step 3 and step 4 to clear other metadata values.
6. Click **OK**.

If the metadata name is used by any other asset, that is, a value has been entered on another properties page, the metadata name will remain on all properties pages.

Deleting asset metadata

You may need to delete a metadata name, that is, remove it from all properties pages when it becomes obsolete, or to repair a typographical error. There is no "delete metadata" feature; however, metadata names are checked every time you close a properties dialog box. If a metadata name is not being used, that is, no values are entered for the metadata name on any asset properties page, the metadata name is automatically deleted and removed from all metadata pages.

Deleting justly created metadata name

To delete a metadata name you just created:

1. In the asset Properties dialog box, click **Data**.
2. Select the metadata name you want to delete.
3. Click **Clear**.
4. Click **OK**.

The metadata name is removed from all asset properties pages since no metadata value exists for any asset.

Deleting a metadata name already in use

To delete a metadata name already in use:

- To completely purge a metadata name, you must clear the metadata value on all asset properties data pages. When the last asset is cleared, and the properties dialog is closed, the metadata name is purged and removed from all properties pages.

Viewing asset properties

The properties dialog box varies depending on the asset.

Viewing clip properties

1. Select the clip in the Clips pane asset list.
2. Open the Clip Properties dialog box using one of the following:
   - Select **Clips | Properties**.
   - Select **Properties** in the asset context menu.
   - Click the **Properties** button in the Clips pane.

   If the Properties button is not displayed in the Clips pane, refer to assignable buttons in the Guide to using the Clips pane section.

The Clip Properties dialog box appears. There are three pages in the clip dialog box. **General**, **Media**, and **Data**. The General and Media pages are self explanatory. The Data page is used to add metadata to the clip.

Viewing the General properties page

The General properties page displays basic information about the clip, including tracks, format, compression, size, etc. A radio button enables you to lock the clip.

Viewing Media Properties page

The Media page displays all the relevant clip timecodes, including clip marks, and the first and last frame of the clip. A Time Dome gives a graphical display of the relative position of the marks within the recorded media. The Aspect Ratio Conversion drop-down list allows you to specify how you want AppCenter to handle an aspect ratio conversion.

Viewing Data properties page

This page allows you to define your own metadata and specify values for that metadata.

Viewing playlist properties

- The playlist properties dialog box includes features that control list playback in the Playlist mode.

Viewing program properties

1. Select the program in the Clips pane asset list.
2. Open the Program Properties dialog box using one of the following methods:
   - Select **Clips | Properties.**
   - Select **Properties** in the asset context menu.
   - Click the **Properties** button in the Clips pane.

   If the Properties button is not displayed in the Clips pane, refer to assignable buttons in the Guide to using the Clips pane section.

The Program Properties dialog box is displayed with three pages; **General, Media,** and **Data**. The General page is self explanatory. The Media page has information about mark in- and mark-out times. The Data page is used to add metadata to the program.

Viewing bin properties

1. In the Clips pane, select the Current Bin label, then select **Organize Bins**.
2. In the Organize Bins dialog box, select a bin. The bin properties are displayed in the Organize Bins dialog box.

Viewing volume properties

1. In the Clips pane, select the Current Bin label, then select **Organize Bins**.

2. In the Organize Bins dialog box, select a disk volume. The volume properties are displayed in the Organize Bins dialog box.

Importing and exporting media

Importing and exporting files

This section describes the process of importing and exporting files using AppCenter. You can also transfer media with the following methods:

- FTP applications
- Import/export services that use watched folders
- Protocols such as AMP
- Programs and applications that request transfers using the K2 API

Related Topics

Using FTP for file transfer on page 291
Import/export services on page 305
Using AMP protocol to control K2 systems on page 195
About importing and exporting files on page 128

About importing and exporting files

You can import and export files using standard multimedia. Source files can be located on a mapped network drive. The source and destination devices must be in the same domain.

If importing or exporting files by accessing a K2 Solo 3G system with remote AppCenter on a network-connected Control Point PC, your view of the “local” Windows file system is a view of the Control Point PC. However, the “local” drives (such as C:) that AppCenter uses for source and destination are not the local drives of the Control Point PC. Therefore you must map a network drive on the Control Point PC to create a verified source or destination. To do this, go to the source machine, create a shared folder, then on the Control Point PC map that shared folder as a network drive. Then you can import or export using the shared network drive. Refer to procedures later in this section.

NOTE: Do not use the K2 Summit/Solo C: system drive for any kind of transfers.

If importing or exporting files on a K2 Summit SAN-attached system, while it appears as if your view of the “local” Windows file system is that of the K2 Summit SAN-attached system, in actuality the “local” drives (such as C:) that AppCenter uses for source or destination are the local drives of the K2 Media Server. Therefore you must similarly map a network drive on the K2 Summit SAN-attached system to create a verified source or destination. To do this, on the source machine create a shared folder, then on the K2 Summit SAN-attached system map that shared folder as a network drive. Then you can import or export using the shared network drive. Refer to procedures later in this section.

K2 media storage (the V: drive) is the only local drive in the K2 Solo 3G system that have adequate capacity for transfers. If files have to be imported or exported from "local" disks, the only disks a user can use is the V: drive. Otherwise, you must use a mapped network drive.

If importing from a 3rd party external drive, playing media while importing is not supported.

NOTE: If you import to a file or stream media that has the same name as an asset already existing in the destination location, an Abort/Rename/Retry dialog box appears.

Adding a remote host

Grass Valley recommends manually adding each remote host that you want to import or export files to. Do this for K2 systems.

To import/export between systems using AppCenter, follow these steps:

1. Open Configuration Manager and select the Remote tab.
2. Add each system that you want to have available as a source or a destination.
   a) Enter the name or the IP address of the K2 Solo 3G system where you want to import or export streaming media assets. (Grass Valley recommends that you use host names. For more information on host files, see the *K2 System Guide*.)
   b) When adding a remote host that uses AMP remote control protocol, select a Controller ID.

To map a source or destination drive

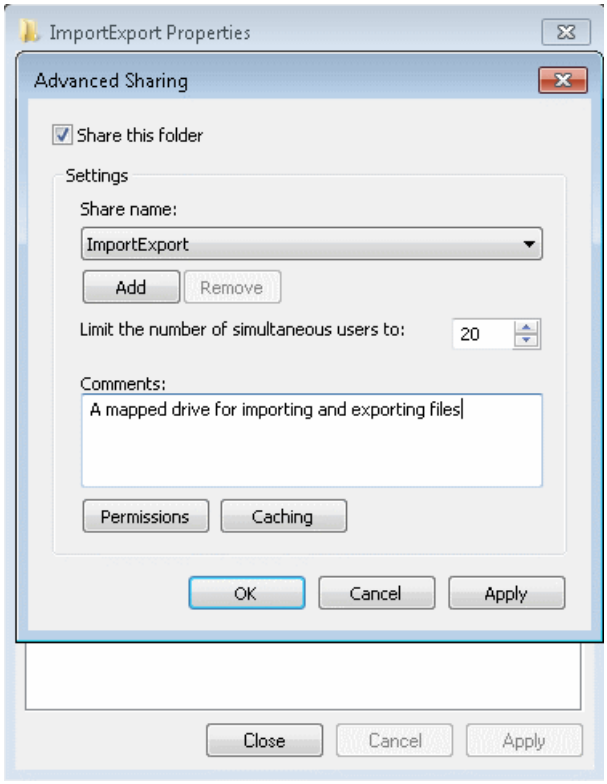
This procedure provides a mapped network drive for file import/export on the machine on which you are using AppCenter, such that you can use the drive as a verified source or destination via AppCenter's Import or Send To features. This is required in the following cases:

- When using AppCenter on a Control Point PC for any file import or export. You cannot use the local drive for file import or export on a Control Point PC.
- When using AppCenter on a K2 Summit SAN-attached system for any file import or export. You cannot use the local drive for file import or export on a K2 Summit SAN-attached system.
- When using AppCenter on an standalone K2 Solo 3G system and the source or destination is not on the local K2 Solo 3G system.

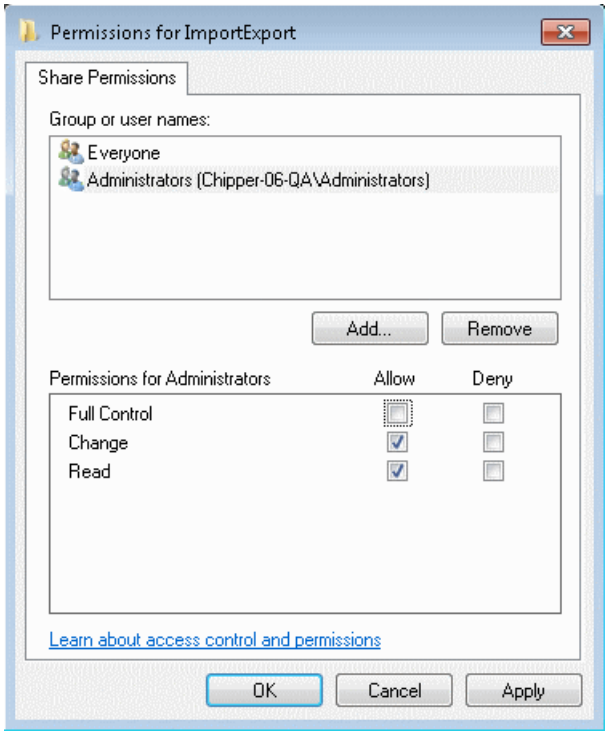
1. On the machine that is the source or destination, create a folder to be used for file import and export.

2. Share the folder using standard Windows procedures.

   You must map drive of source device only, not K2 Solo 3G system.

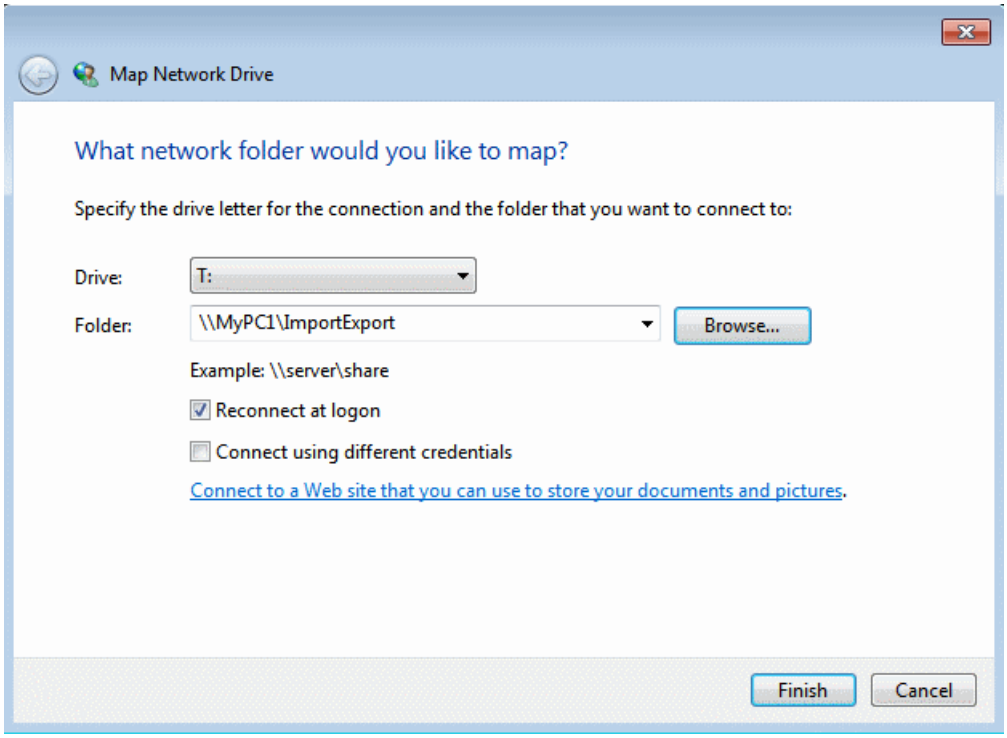


3. Make sure that permissions are set to allow read and write access to the appropriate user or group accounts, according to your site's security policies.



NOTE: A drive that you map for export must not require user credentials for access. If user credentials are required, the export transfer fails.

4. On the machine on which you are using AppCenter, map the shared folder as a network drive. For example, if the shared folder is on *MyPC1*, map the T: drive to *\\MyPC1\ImportExport*.



You can now use the mapped network drive as a source or destination for file transfer using the AppCenter Import or Send To features.

To import a file

Use the following procedures to import a video file.

When you import media from a file, the media is converted and stored using the K2 system native file format.

The file to be imported must be in a verified source location for file import. Examples of verified sources are as follows:

- When using AppCenter on a standalone K2 Solo 3G system and the source is a local drive, the local drive is a verified source. It is not necessary to share a folder or map a drive.
- When using AppCenter on a K2 Summit SAN-attached system and the source is a local drive on the K2 Summit SAN-attached system, create a verified source as follows:
  - On the K2 Summit SAN-attached system, share a folder.
  - On the K2 Summit SAN-attached system, map the shared folder as a network drive.
- When using AppCenter on a Control Point PC and the source is a local drive on the Control Point PC, create a verified source as follows:
  - On the Control Point PC, share a folder.
  - On the Control Point PC, map the shared folder as a network drive.

- When using AppCenter on a Control Point PC and the source is a local drive on a K2 Solo 3G system you are accessing with AppCenter, create a verified source as follows:
  - On the K2 Solo 3G system, share a folder.
  - On the Control Point PC, map the shared folder as a network drive.

NOTE: The appearance of the asset list and file open dialog boxes is determined by the Options setting.

To import a video file, do the following:

1. Verify the current bin. The current bin is the destination directory for the import operation.
2. Place the file to be imported in a verified source location.
3. In the AppCenter main menu, select **Clips | Import**.

   The Import dialog box opens.
4. Click **File**.
5. In the Source section, browse to locate and select the source file.

   The **Look in** label shows the current location. The list under the **Look in** label displays the contents of the current location. The Import dialog automatically filters the list of files to show only the type of files that can be imported (such as .gxf, .mxf, and so on). You can select items in the list (such as a *machine*, drive, or folder) to explore its contents.

   Clicking the up-arrow button moves up one directory level in the storage hierarchy.

   The Look in drop-down list allows you to choose from one of the most recent source locations visited (history).
6. Verify the destination directory indicated next to **Bin Name**. This is where the imported file is placed.
7. Modify the clip name, if needed, by selecting the **Clip Name** edit control.
8. Click **Import** and proceed as follows.

   If you are importing a video file, the import begins. You do not need to continue with the next step in this procedure.

   NOTE: Import is a background task and can be monitored using the Transfer Monitor.
9. Once you have specified how to import the file, click **OK.**

About exporting files

You can export K2 system clips using standard media file formats.

Files can be exported over an Ethernet connection to network drives or to common forms of removable media.

NOTE: If you export to a file or stream media that has the same name as an asset already existing in the destination location, an Abort/Rename/Retry dialog box appears.

About sending files to standalone external drives

Transferring to and from a USB drive is supported on a local standalone K2 Solo 3G system. (You can also transfer files in K2 Solo Media Server using a PCIE Express card.) USB drive transfers on K2 Summit SAN-attached system or Control Point PCs are not supported. Assets must be exported to a USB drive one at a time. Attempts to export more than one asset at the same time will result in the transfer aborting.

The following are operational considerations when sending files to external drives:

- **Estimating clip file sizes** - AppCenter does not prevent you from sending a file that is larger than the space available on the target disk. The transfer fails when the disk becomes full. To avoid this problem, check the clip size reported in the clip properties dialog box. You can use this to estimate the disk space required for the clip.
- **Best transfer performance** - File transfers are handled concurrently, up to four at a time. Additional transfer requests are queued.
- **Adding/Removing USB devices** - The USB connectors on the rear panel and front panel can be used to connect a mouse, keyboard, USB drive, or other USB device. Do not plug or unplug these devices while the K2 Solo 3G system is being used for critical play to air activity.
- **Maximum file sizes when exporting assets to USB drives** - Exporting assets with long durations may result in file sizes that exceed 4GB. Some USB drives are formatted using FAT/FAT32, which has the 4GB maximum file size limitation. Attempting to send a file to these disk volumes will cause the transfer operation to fail. Disk volumes formatted using NTFS allow larger maximum file sizes. Before exporting an asset, be sure to check that the file size is less than 4GB, otherwise, ensure that the file system on the target drive supports larger files sizes.

To export to a file

The destination must be a verified destination for file export. Examples of verified destinations are as follows:

- When using AppCenter on a standalone K2 Solo 3G system and the destination is a local drive, the local drive is a verified destination. It is not necessary to share a folder or map a drive. On the K2 Summit SAN-attached system, share a folder.
- When using AppCenter on an K2 Summit SAN-attached system and the destination is a local drive on the K2 Summit SAN-attached system, create a verified destination as follows: On the K2 Summit SAN-attached system, map the shared folder as a network drive.
- When using AppCenter on a Control Point PC and the destination is a local drive on the Control Point PC, create a verified destination as follows: On the Control Point PC, share a folder. On the Control Point PC, map the shared folder as a network drive.
- When using AppCenter on a Control Point PC and the destination is a local drive on a K2 Solo 3G system you are accessing with AppCenter, create a verified destination as follows: On the K2 Solo 3G system, share a folder. On the Control Point PC, map the shared folder as a network drive.

To export to a file, do the following:

1. Verify that the source and destination devices are in the same domain.
2. Select the clip or clips in the Clips Pane that you want to send to a file.

3. Open the Send to dialog box using one of the following steps:
   - Select **Clips | Send to**
   - Right-click the clip in the Clips Pane and select **Send to**

   The Send dialog box opens.
4. Click **File,** then locate and select the destination directory.

   The **Save in** label shows the current destination. The list under the **Save in** label displays the contents of the current destination. You can select items in the list (such as a *machine*, drive, or folder) to explore its contents.

   Clicking the up-arrow button moves up one directory level in the storage hierarchy.

   The Save in drop-down list allows you to choose from one of the most recent target locations used (history).
5. Use the **File Type** drop-down list to select the file format.
6. If desired, modify the destination file name using the **File Name** edit control. File Name: MyClip
7. Click **Send**.

NOTE: Export is a background task and can be monitored using the Transfer Monitor. If the operation fails for any reason, the asset is deleted from the target location.

If the file export does not behave as expected…

If you have trouble locating an exported file, you might not be using a verified destination. Check that the destination is really at the location you expect. For example, if you select what appears to be the local drive in the Send dialog box, you might discover that the file actually goes to a different machine, as explained in the following table.

If you are using AppCenter on a...	The local drive is located on...
Standalone K2 Solo 3G system	The standalone K2 Solo 3G system
K2 Summit SAN-attached system	The K2 Media Server that takes the role of FTP server for that K2 Summit system.
Control Point PC remotely accessing a standalone K2 Solo 3G system	The standalone K2 Solo 3G system
Control Point PC remotely accessing a K2 Summit SAN-attached system.	The K2 Media Server that takes the role of FTP server for the K2 Summit SAN-attached system.

Importing and exporting streaming media

This section describes the process of importing and exporting streaming media using AppCenter. You can also transfer media using an FTP application. For information on using FTP, refer to the "Configuring the K2 System" section of this Topic Library.

About importing and exporting streaming media

You can transfer media between a K2 Solo 3G system and other Grass Valley media devices using the **Import** and the **Send to** features. The K2 system supports streaming media transfers over the FTP/streaming network. Source or destination devices for a streaming transfer include K2 Solo 3G system. The format for such streaming is GXF. You must configure your network for streaming transfers prior to using these features.

NOTE: If importing to or exporting from other products, you must first add the remote host in Configuration Manager.

A transfer job is created for each "import" or "send to" operation. Once created, transfer jobs are added to the transfer job queue where they are dispatched in a first in, first out basis. Transfer jobs are handled in the order they appear in the queue. A standalone K2 Solo 3G system can handle up to four concurrent transfer jobs. Any additional, up to 100 requests at a time, wait in the queue. You can use the Transfer Monitor to check the status of your transfer requests.

NOTE: The bit rate while streaming clips between machines is not symmetrical. For example, when streaming to a remote machine the data rate can be twice as fast as the rate streaming from a remote machine. This is due to the way transfer statistics are measured.

Movie formats for GXF imports/exports:

Depending on system software versions of source and destination devices, it might be required that all video and audio segments in a GXF transferred file be of the same media type. Refer to release notes for the software version for more information.

Transfer timings and Interchange Standards

The timing of the transfer with record/play operations depends on the clip's storage location. For information about transfer timings or interchange standards, refer to the operational specifications.

Importing streaming media

K2 Solo 3G system allows playout of movies that are still transferring in. Make sure the bandwidth of the import task is greater than the media bit rate.

NOTE: The appearance of the asset list and file open dialog boxes is determined by the View Option setting. Use the Clips Pane context menu to choose Image or Text view.

1. In the Clips Pane, select the bin to which you want to stream media. The current bin will be the *destination* bin for the import operation.
2. Select **Clips | Import**.

   The Import dialog box opens.
3. Click **Stream**.

4. In the Source section, browse to locate and select the source clip. (For some cross-product transfers, depending on software versions, you might need to specify the volume, bin, and media asset name. Refer to release notes for specifications.)

   The **Look in** label shows the current location. The list under the **Look in** label displays the contents of the current location. You can select items in the list such as *machine*, disk volume or a *bin*, to explore its contents.

   Clicking the up-arrow button moves up one directory level in the storage hierarchy.

   The **Look in** drop-down list allows you to choose from one of the most recent source locations visited (history).

5. In the Destination section, **Bin Name** displays the name of the current bin which specifies the destination bin.
6. Specify a clip name, if desired, by clicking the **Clip Name** edit control.
7. Click **Import** to start the transfer.

NOTE: Import is a background task and can be monitored using the Transfer Monitor.

Exporting streaming media

1. In the Clips Pane, select the asset(s) you want to transfer.
2. Open the Send to dialog box using one of the following steps:
   - Select **Clips | Send to**
   - Right-click the clip and select **Send to**

   The Send to dialog box appears.
3. Click **Stream**, then locate and select the stream destination.

   The **Stream to** label shows the current destination. The list under the **Stream to** label displays the contents of the current location. You can select items in the list (a *machine*, disk volume, or a *bin*) to explore its contents.

   Clicking the up-arrow button moves up one directory level in the storage hierarchy.

   The **Stream to** drop-down list allows you to choose from one of the most recent target devices (history).
4. Click **Send** to transfer the asset(s).

NOTE: Send to is a background task and can be monitored using the K2 system Transfer Monitor tool.

Monitoring media file transfers

The Transfer Monitor is used to monitor all K2 system transfer jobs and their status. A transfer job is created for each “send to” or “import/export” operation. Once created, transfer jobs are added to the transfer job queue where they are dispatched in a first in, first out basis. Up to four transfer jobs can execute simultaneously. Any additional jobs wait in the queue.

NOTE:

If the System | Transfer Monitor menu option is grayed out, review your level of user access.

Starting the Transfer Monitor

To start Transfer Monitor, perform one of the following:

- Select **System | Transfer Monitor**
- In the AppCenter Statusbar, double-click the **Transfer Monitor** button. 

The Transfer Monitor button appears when a transfer job is present.

Transfer Monitor pages and buttons

In the Transfer Monitor, transfer jobs are categorized and displayed on one of three pages—Receiving, Sending, and Completed pages. On each page the transfer jobs are displayed using a thumbnail image along with a brief description of its source, destination and status. Jobs that have encountered errors are shown with a red circle next to a brief description of the error(s).

- **Source** – The source of the transfer job. If the source includes multiple files, the first file name is displayed plus a '…' sign beside it. You can find the full path of all the source files from the Properties page.
- **Destination** – The destination of the transfer job. You can find the full path of all the destination files from the Properties page.
- **Status** – For ongoing transfer jobs, the transfer rate is displayed in megabytes per second and percentage of job completed. All jobs waiting in the queue are shown as "Pending". Jobs that encountered an error or errors are displayed with a red circle next to a brief description of the error(s).
- **Properties Button** – Used to view more detailed information about a transfer job.
- **Remove Button** – Used to abort and remove jobs from the transfer queue.

Receiving Page

The Receiving page displays all import transfer jobs.

Sending Page

The Sending page displays all "Send to" transfer jobs and their status.

Completed Page

The Completed page displays all jobs that have completed successfully. Completed jobs are automatically cleared after approximately 36 hours. You can manually clear jobs from the completed list using **Remove** or **Remove All**.

Viewing transfer jobs in Transfer Monitor

Each transfer job is displayed in the Transfer Monitor with a thumbnail image along with a brief description of its source, destination and status. Jobs that have encountered errors are shown with a red circle by them.

NOTE: When viewing transfers to or from a* K2 Summit SAN-attached system*, be aware that the transfer will display in Transfer Monitor referencing the name of the K2 Summit system. However, in the Import or Export dialog box, you will need to specify the name of the shared storage itself. For example, the source would listed as K2-StorageSystem/V:/TransferTest/ in the import menu but in transfer monitor it would be displayed as K2-SummitProductionClient-B22/V:/TransferTest/.

You can find more detailed information about a transfer job from its Properties page. The Properties information can be accessed while the transfer is taking place or after it has finished, regardless of whether the media has been transferred successfully or not.

- Source: The source of the transfer job. If the source includes multiple files, the first file name is displayed plus a '…' sign beside it. You may find the full path of all the source files from the Properties page.
- Destination: The destination of the transfer job. You may find the full path of all the destination files from the Properties page.
- Status: For ongoing transfer jobs, the transfer rate is displayed in megabytes per second and percentage of job completed. All jobs waiting in the queue are shown as “Pending”. Jobs that encountered errors are displayed along with an error code. You may find a more detailed error message in the Properties page.

Viewing detailed transfer job properties

1. In the Transfer Monitor, select a transfer job.
2. Click **Properties.**
3. When the Transfer Job Properties dialog box appears, select the **Transfer** tab to examine transfer properties.

Removing transfer jobs from the completed list

You can remove transfer jobs from the Completed page.

1. In Transfer Monitor, click **Completed**.
2. Remove the transfer jobs using one of the following:
   - Select the job to remove, then click **Remove**.
   - Select the jobs to remove, then click **Remove All**.

Using Channel Suites

Using channel suites

Use channel suites for remote AppCenter operation of one or more K2 Summit//Solo systems. Channel suites are part of the Control Point software installed on a remote PC. You cannot use channel suites on a local K2 Solo 3G system.

You can manage your channel suites from the System menu. When you open AppCenter, the system automatically opens the last-used channel suite. If you have a channel suite already running when you open a channel suite or create a new one, a dialog box displays asking if AppCenter should shut down or suspend current channel suite and applications in it.

If you select **Close Channel Suite**, you exit AppCenter and close the channel suite. Any channels that are running are stopped.

If you select **Suspend**, you exit AppCenter but the K2 Solo 3G system keeps running any current application. (For example, if recording, the application keeps recording.) In this state, any channels

in the channel suite may be commandeered by another user. If all the channels in the channel suite are taken over in this manner, a suspended channel suite is shut down.

If there is an unplanned shut down on the K2 Solo 3G system, the channels in remote AppCenter display a “disconnected” status in the channel title bar. Select **System | Reconnect** to connect to the K2 Solo 3G system again. If the AppCenter application crashes on your network-connected Control Point PC, connections with the K2 Solo 3G system are put into a suspended state while waiting for the PC to reconnect. The K2 Solo 3G system continues to run any current applications or protocol.

A channel suite is saved as an XML file on the Control Point PC. The default location is *C:\Profile\ChannelSuites*. In this XML file, information for channel order, alias names, and the application that runs on a channel is stored. For example, if you run the Recorder application on a channel, the next you open the channel suite the Recorder application persists on that channel.

Managing channel suites

The following table describes the basic channel suites tasks and the actions necessary to complete them.

Task	Action
Add a channel to the currently active channel suite	In AppCenter, select **System	Suite Properties** and click **Add**. You can add up to 16 channels to a channel suite.
Configure the channel settings	In AppCenter, select **System	Configuration**.
Create a new channel suite	In AppCenter, select **System	New Suite**, name the channel suite, and add channels. Note: you can create a new channel suite while currently running a different channel suite. When you finish creating the suite, you are offered the choice of closing down or suspending the current channel suite. By default, the new channel suite is saved in the `C:\Profile\ChannelSuites` directory. You can overwrite an existing channel suite by selecting **System	New Suite**, highlighting the name of the channel suite you want to overwrite, and then proceeded as if it were an entirely new channel suite.
Delete a channel from the currently active channel suite	In AppCenter, select **System	Suite Properties** and click **Remove**. Deleting a channel removes it from the channel suite. It does not affect the channel itself.
Delete a channel suite	In the Windows Explorer application, locate the channel suite. Channel suites are saved by default in the `C:\Profile\ChannelSuites` directory in XML format. Highlight the file and hit the **Delete** key.
Open a channel suite	In AppCenter, select **System	Open Suite** Channel suites are saved by default in the `C:\Profile\ChannelSuites` directory in XML format. Note: to open one of the last four recently used channels, select **System	Recent Suites**.
Organize channels in a channel suite	In AppCenter, select **System	Suite Properties**. Highlight the channel you want to reorder and click either **Move Up** or **Move Down**.

Task	Action
Rename a channel in a channel suite	In AppCenter, select **System | Suite Properties** and click **Rename**. Channel names must be 16 characters or less. Note: to rename an open channel suite, AppCenter must shut down all the channels and then re-open the suite.
Rename a channel suite	In AppCenter, select **System | Suite Properties**. In the Suite Properties dialog box, enter the new suite name and click **Save**. Note: renaming a channel suite while it is running causes all the channels to stop and any clips to be ejected. AppCenter needs to reconnect to the K2 Solo 3G system that are affected by this change.

Using channel suites with multiple K2 systems or storage locations

Channel suites have the capability to operate channels from multiple sources through one Control Point PC. You can move from a channel on one source to a channel on another without disrupting playout.

You can use a channel suite with channels that access media stored on different K2 Solo 3G system or K2 SANs. The clip bin displayed is the bin where the channel currently active stores its clips.

Take care when loading clips into channels. When the clips for the currently active channel are displayed in the Clips pane, you might not be able to load those clips into a channel that is not currently active, if that channel is on a different source. For example, if you have channels in your channel suite from standalone K2 Solo 3G system “A” and from standalone K2 Solo 3G system “B”, you cannot drag and drop a clip from the “A” system to load it into a “B” system channel. To load a clip across storage locations in this manner requires a transfer of the clip from system “A” to system “B.” You must perform that transfer as a separate task, as attempting a cross-system load of a clip does not trigger a transfer.

Accessing a K2 Solo 3G system from multiple Control Point PCs

You can have the same channel suite saved on different Control Point PCs. This is useful in the event of a Control Point PC crash while running AppCenter. Within two minutes of an unplanned shut down, the K2 Solo 3G system suspends the channels in the affected channel suite. If you have the same channel suite on another Control Point PC (that is, a channel suite with the exact same name), you can open the channel suite on the other Control Point PC. When you do this you must use the same user credentials. Then you can continue your work.

Sharing channels with other users

Channels are used exclusively by one application and one user, but multiple users on different PCs can access different channels on the same server at the same time. You can share channels with users who are accessing the same source from networked-connected Control Point PCs. To release a channel, select <None> in the application drop-down list in the channel monitor pane. The title bar of the channel changes to “Available”.

If a channel is in use by another user, you can still have the channel as part of your channel suite. In this status, the channel says “in use” in the title bar of the clip and includes information on the current user, computer, and application.

Taking over a channel

While you are using a channel, another user can commandeer it. When this happens the channel says “in use” in the title bar of the clip and includes information on the current user, computer, and application.

- If you click on an application drop-down list in a channel that another user has assigned an application to, a pop-up message asks you to confirm that you want to take the channel over.
- For example, if user1 has designated Channel 1 to run a Player application on Control Point PC1, user2 can go into Channel 1 in his channel suite on Control Point PC2 and select Recorder from the application drop-down list. User2 will see this message:

  ‘Channel1:*K2 system*’ is currently used by ‘user1’ running ‘Player’ on ‘PC1’. Are you sure you want to eject this clip and launch a ‘Recorder’?
- Clicking Yes will allow the second user to begin the new application on this channel.

Channel suites and channel configuration considerations

While you can separate the channels on a single K2 Solo 3G system for operation by using one or more channel suites, the channels on a K2 Solo 3G system are always combined in one interface when you use Configuration Manager. This means that it is possible to open Configuration Manager from within a channel suite and configure a channel that is not present in that channel suite. Therefore, make sure you know the control and operating status of a channel before you modify its configuration.

Likewise, if your channel suite has channels from multiple sources, it is possible to open Configuration Manager on each of those sources from within the one channel suite. Therefore, make sure you select the channel you intend to configure before you open Configuration Manager.

When you modify channel configuration in Configuration Manager, the changes are saved in a configuration file on the K2 Solo 3G system, not on the network-connected Control Point PC.

Administrators can set user permissions for each channel. Depending on your security settings, you could be denied permission to operate a channel. For more information, see the *K2 System Guide*.

Take special care when modifying a channel configuration as follows:

- Changes that apply to all channels on a K2 Solo 3G system. This can affect media operations in other channel suites that contain channels from that K2 Solo 3G system.
- Changes that require rebooting the K2 Solo 3G system, such as switching the video reference from NTSC to PAL. This can stop the media operations in other channel suites that contain channels from that K2 Solo 3G system.

NOTE: Configuration changes require K2 admin access privileges.

Audio/Video Configuration

Using Configuration Manager

To modify settings in Configuration Manager, you must be currently logged in to AppCenter with administrator privileges.

NOTE: Using HD requires an XDP (HD) license. If you do not have an HD license, refer to the SD configuration specifications only.

Open Configuration Manager from the AppCenter menu bar at **System | Configuration**.

NOTE: If you are accessing a* K2 Solo 3G system *from a Control Point PC with a channel suite that has channels from multiple sources, make sure that you select a channel from the* K2 Solo 3G system *that you want to configure before opening Configuration Manager.

About video scaling settings

The AppCenter video scaling feature allows you to play clips with different aspect ratios and picture resolutions on the same play channel.

AppCenter handles video scaling as follows:

- When recording a SD clip, you should specify whether the clip is standard or widescreen video. This sets the clip aspect ratio attribute. This attribute is saved as part of the media file. If the SD clip is played out on a HD channel, the aspect ratio attribute is recognized.
- SD material that is transferred or recorded into the system, along with its audio and metadata, is upconverted with selected aspect ratio when played on an HD channel. HD material is downconverted along with its audio when played on SD channel. HD and SD clips can be played back-to-back.
- Agile playout of mixed format clips displays with default or selectable modes such as bars, crop, or stretch on both SD and HD outputs.
- During play channel setup, you must select the video output for each play channel– standard or high definition. This will determine if the clip picture resolution needs up-conversion or down-conversion.
- For each play channel you must specify the active format description (AFD) settings to use when the picture image needs to be resized. Selections include crop, bars, halfbars and stretch.
- There are two settings: **Aspect Ratio** and **Aspect Ratio Conversion**. The K2 Solo 3G system applies these settings as follows:
  - The K2 Solo 3G system uses the Aspect Ratio setting only when AFD is known and when down-conversion takes place.
  - The K2 Solo 3G system uses the Aspect Ratio Conversion setting only when AFD is not present or is undefined and either up-conversion or down-conversion takes.

  For example, if you change the Aspect Ratio Conversion setting and then play a clip with AFD present, the output does not change.
- For the highest video quality, select a video output format that eliminates the need for up or down conversion.
- AppCenter can play clips with different aspect ratio attributes in a single playlist.

***NOTE: Some video output connectors become inactive for some video type selections. For more information on video output connectors, see* the "Configuring the K2 System" section of this Topic Library.**

About aspect ratio conversion modes

The aspect ratio conversion mode setting for the play channel determines how the picture image is resized for playout.

Applying AFD settings

Active Format Description (AFD) can be used to automatically determine the proper aspect ratio to use for up- and down-conversions.

In AppCenter, you can specify the AFD settings:

- in the Clip Properties dialog box, for that clip only
- in the Channel Options dialog box, for newly recorded clips on that channel

You can also make settings in Configuration Manager to specify under what conditions the K2 Solo 3G system should process AFD (for output only, on a per-channel basis).

When recording, the following AFD settings are available:

SD	HD
Undefined	Undefined (Undefined means no AFD has been set; the clip remains as is.)
16:9 Full screen	4:3 Pillarbox
4:3 Full screen	16:9 Full screen
16:9 Letterbox	14:9 Pillarbox
14:9 Letterbox	16:9 Full screen with 4:3 center

Channels with HD licenses need to set the AFD values when aspect ratio conversion has been performed while playing out video. Channels that are SD-only do not perform aspect ratio conversion; AFD values do not need to be adjusted on those channels.

Clips with AFD recorded on a K2 Media Client will play on a K2 Solo 3G system, and vice versa. Clips will have either ARC or AFD properties, not both. AFD in ancillary data is preserved in the data track during recording.

NOTE: Other methods of expressing AFD, such as video index or bar data, are not supported.

Setting AFD in the Clip Properties

Any modification to the AFD settings made here applies to the selected clip only.

1. In the Clips pane, right-click on the clip.
2. Select **Properties**.

3. In the Clip Properties dialog box, click on the **Media** tab.
4. Click the AFD drop-down list. Select the AFD setting and click **OK**.

Setting AFD in the Channel Options

Any modification to the AFD settings made here applies to input on the selected recorder or player/recorder channel only.

1. In AppCenter, select the channel where you want to set the AFD value.
2. Click the **Options** button.
3. In the Options dialog box, click on the Bin & AFD tab.
4. Click the AFD drop-down list. Select the AFD setting and click **OK**.

Setting AFD in the Configuration Manager

AFD settings made in Configuration Manager apply only to output on the specified channel.

1. From the File menu, select **System | Configuration**.
2. In Configuration Manager, click the Channel tab and the specific channel tab that you want to modify.
3. Scroll down to AFD settings and select one of the options:

For this setting...	Configure as needed...

AFD Settings	Defines AFD in clips output from the K2 Solo 3G system. You can select the following:
	• **Record AFD as clip property**:
	  • Yes – When an AFD setting is present it is set as the default in clip properties. This is the default K2 system behavior.
	  • No – When an AFD setting is present it is not set in clip properties.
	• **Generate AFD on Output**:
	  • Always – As automatically determined by the K2 system.
	  • When Known – As set in clip properties.
	  • Never – Pass-through any AFD already present.
	• **SD 16:9 Full screen up-conversion AFD**: Select AFD code1010 or 1001, as required by your site's downstream processing. This does not affect the visual display at the K2 system output.

4. Click **OK** to apply the setting

Configuring video reference standard settings

The video reference standard setting is global to the K2 Solo 3G system and applies to all channels. For the reference standard currently selected, the only clips available for playout are those that use that reference standard. Clips that use a different reference standard are disabled (grayed out).

NOTE: When you change the video reference standard setting, a restart is required to put the change into effect.

1. In AppCenter, open the Configuration Manager.
2. Click **System**.
3. Configure settings as follows:

For this setting...	Configure as needed...
Reference Standard	Choose **NTSC** or **PAL**.
	Determine status of **Reference present**. • Green LED — source present • Black LED — source not present
	Determine status of **Reference locked**. • Green LED — system locked • Black LED — system not locked

Configuring reference file type on a standalone K2 Summit/Solo system

1. In AppCenter, click **File | System | Configuration**.
   Configuration Manager opens.
2. In Configuration Manager, click the **System** tab.
3. In Reference Files settings, for the **Reference file type** setting, select one of the following:
   - None — K2 software does not create reference files.
   - QuickTime — K2 software creates QuickTime reference files.
4. Click **OK** to apply the setting.
5. Restart the standalone K2 Solo 3G system to put the change into effect.

Configuring MXF Export Type on a standalone K2 Summit/Solo system

1. In AppCenter, click **File | System | Configuration**.
   Configuration Manager opens.
2. In Configuration Manager, click the **System** tab.

3. In MXF Export settings, for the **MXF Export Type** setting, select one of the following:
   - **377M**: SMPTE ST 377:2004 compliant. Ensures compatibility with older products.
   - **377-1**: SMPTE ST 377-1:2009 compliant.
4. Click **OK** to apply the setting.
5. Restart the standalone K2 Solo 3G system to put the change into effect.

Configuring MXF Export Type on a K2 SAN system

1. In the K2Config application, for the K2 Media Server with role of FTP server, access the FTP Server Configuration page as follows:
   - On a SAN that is already configured, in the tree view click **FTP Server**.
   - On a SAN that is not yet fully configured, work through the Configure K2 Server wizard until you reach the FTP Server Configuration page.
2. On the FTP Server Configuration page select one of the following:
   - **377M**: SMPTE ST 377:2004 compliant. Ensures compatibility with older products.
   - **377-1**: SMPTE ST 377-1:2009 compliant.
3. Manage the required K2 Media Server restart as follows:
   - On a SAN that is already configured, you must restart the K2 Media Server to put the change into effect. Follow the restart procedure appropriate for the basic or redundant K2 SAN.
   - On a SAN that is not yet fully configured, continue to work through the Configure K2 Server wizard. The restart at the end of the configuration process is sufficient.

About tri-level sync

The K2 Solo 3G system supports tri-level sync as a genlock reference source. The reference must be in an HD format and frame rate that is supported by the K2 Solo 3G system, as follows:

- Reference Standard: NTSC (59.97Hz)
  - 1080i 29.97
  - 720p 59.94
- Reference Standard: PAL (50Hz)
  - 1080i 25
  - 720p 50

The K2 Solo 3G system automatically detects, switches, and syncs to the reference. When you configure the reference standard for either NTSC (59.97Hz) or PAL (50Hz) in K2 AppCenter Configuration Manager, a restart is required to put the change into effect and the system starts with a SD reference format by default. It then attempts to detect a reference in a format and frame rate that is compatible with the current reference standard setting. When the K2 Solo 3G system detects a reference in a supported format, it automatically switches to that format. This allows the system to switch between SD and HD tri-level formats with frame rates that are compatible with the reference

standard setting. When the K2 Solo 3G system locks to a new reference format, it saves the format and frame rate information, and upon restart it returns to the saved format and frame rate.

Do not use a progressive reference with an interlace output. For example, do not use 720p tri-level sync for interlace output formats (such as SD and 1080i). Output timing can be off by a field with this type of incompatibility.

The K2 Solo 3G system treats the following conditions as a loss of reference:

- No reference is present
- A reference in an unsupported format is present
- A reference in a supported format is present but it has a frame rate that is not compatible with the current reference standard setting.

In these cases the K2 Solo 3G system internal genlock flywheel provides a stable reference for the last reference set. The system reports this status in K2 AppCenter Configuration Manager Reference Standard by a black "Reference present" indicator.

Configuring record channel video settings

Video record compression settings are not global; they can be set on a channel by channel basis.

⚠ ***CAUTION: When using a* K2 Summit SAN-attached system *with shared storage, bear in mind that any configuration changes that result in an increased bandwidth (such as increasing the bit rate, media formats, and ratio of record channels to play channels) affect load balancing. Therefore, if you change your intended use of a* K2 Summit SAN-attached system *and increase its bandwidth requirements, you risk losing media access. For a more detailed description of load balancing, see* this document.**

1. If you are using a channel suite with channels from multiple sources, select a channel from the K2 Solo 3G system that you want to configure.
2. In AppCenter, click **System | Configuration**.

   Configuration Manager opens.
3. Click **Channel**, and select a channel.

4. Configure settings as follows:

For this setting...	Configure as needed...
Type	If licensed for AppCenter Elite you can configure the channel to be a ChannelFlex Suite Channel. When you do so, settings change accordingly.
Name	If desired, enter a name for the channel.
Input format	Changing video input format does not require a restart of the K2 Solo 3G system. If changing between SD and HD, however, there is a wait time up to 24 seconds for each recorder channel after clicking the **OK** button in Configuration Manager.
Recorder Setup: Video input format	If 720p or 1080i or 1080p 3G Level A is selected: • Green LED — input present • Black LED — input not present
Recorder Setup: Compression format	Settings are available, based on codec option cards, HD licensing options, and input formats.
Video Input: Input type	K2 Solo 3G system are SDI only.
Ancillary data timecode inputs (LTC or VITC)	If 720p or 1080i or 1080p 3G Level A is selected: • Green LED — input present • Black LED — input not present
Automatic VITC detection	Turn on or off as desired. VITC settings vary based on selection.
Starting VITC line or VITC line 1	Available range varies, based on NTSC or PAL selection
Ending VITC line or VITC line 2	Available range varies, based on NTSC or PAL selection
AFD settings	Refer to AFD specifications.

Configuring record channel audio settings

On the K2 Solo 3G system, available settings change depending on the audio input selected, as in the following sections.

AES/EBU audio settings

1. In AppCenter, click **System | Configuration**.
   Configuration Manager opens.
2. Click **Channel**, and select a player/recorder channel.
3. For **Audio input type**, select **AES / EBU**.

4. Configure as follows:

For this setting...	Configure as needed...
Number of audio inputs	Select the number of inputs. Settings below change, based on your selection.
A1/A2 input format	Select the input format.
A3/A4 input format	Select the input format.
Timing offset	Between -200ms and +200ms. The default value is 0 ms.
Audio Input Tags	Add tags for languages or other purposes to this channel's audio tracks.
Display audio meters	Select **System | Monitor Options**, select the **Display the Following Channel Status** radio button, and check the **Audio Monitors** box.

Embedded audio settings

1. In AppCenter, click **System | Configuration**.
   Configuration Manager opens.
2. Click **Channel**, and select a player/recorder channel.
3. For **Audio input type**, select **Embedded**.
4. Configure as follows:

For this setting...	Configure as needed...
Number of audio inputs	Select the number of inputs. Settings below change, based on your selection.
Embedded input group(s)	Selections available are dependent on "Number of audio inputs" setting above
A1/A2... input format	Select the input format.
Timing offset	Between -200ms and +200ms. The default value is 0 ms.
Audio Input Tags	Add tags for languages or other purposes to this channel's audio tracks.
Display audio meters	Select **System | Monitor Options**, select the **Display the Following Channel Status** radio button, and check the **Audio Monitors** box.

Configuring play channel video settings

1. If you are using a channel suite with channels from multiple sources, select a channel from the K2 Solo 3G system that you want to configure.
2. In AppCenter, click **System | Configuration**.
   Configuration Manager opens.
3. Click **Channel**, and select a channel.

4. Scroll to locate and configure settings as follows:

For this setting...	Configure as needed...
Type	If licensed for AppCenter Elite you can configure the channel to be a ChannelFlex Suite Channel. When you do so, settings change accordingly.
Name	If desired, enter a name for the channel.
Video Output	NTSC or PAL available depending on video reference standard setting.
Aspect ratio	Select a HD or SD format.
Aspect ratio conversion	Select the conversion option. Refer to topics about aspect ratio conversions.
Still-play mode	Determines how to generate the still-play signal for the play channel when it is setup to freeze on last frame of video in stop mode. You can select the following: • **Field (interpolated)**: This is the default setting and uses the content of one field for both fields during still-play for a one field freeze. This mode eliminates the motion jitter that can be present in Interlaced mode. • **Frame (interlaced)**: This mode displays two fields in still play mode for a two field freeze. With this mode you might see some motion jitter in still-play.
Test Mode (Colorbars + Tone)	Temporarily displays 75% colorbar signal on the channel output. It also generates an audio tone on all audio outputs. This setting is for test purposes only, so it is not saved.
Video Output Timing	Delays the video output.
Ancillary data timecode output	If 720p or 1080i selected, inserts the recorded timecode track as ancillary timecode on playout. Overrides any ancillary timecode packets stored on data track. Refer to specifications about data track support.
VITC output generator	If SD is selected, you can select VITC lines.

For this setting...	Configure as needed...

AFD Settings	Defines AFD in clips output from the K2 Solo 3G system. You can select the following:
	• **Record AFD as clip property**:
	  • Yes – When an AFD setting is present it is set as the default in clip properties. This is the default K2 system behavior.
	  • No – When an AFD setting is present it is not set in clip properties.
	• **Generate AFD on Output**:
	  • Always – As automatically determined by the K2 system.
	  • When Known – As set in clip properties.
	  • Never – Pass-through any AFD already present.
	• **SD 16:9 Full screen up-conversion AFD**: Select AFD code1010 or 1001, as required by your site's downstream processing. This does not affect the visual display at the K2 system output.

Configuring play channel audio settings

1. In AppCenter, click **System | Configuration**.
   Configuration Manager opens.
2. Click **Channel**, and select a player/recorder channel.
3. Configure as follows:

For this setting...	Configure as needed...
Embedded output group(s)	Select **None** or **Groups 1, 2, 3, 4**.
Timing offset	Between -200 ms and +200 ms. The default is 0 ms.
Force PCM Status Bit	Select **Yes** to set the status of all playout audio tracks to PCM. This setting applies to both PCM audio tracks and non-PCM audio tracks. Do not use this setting unless required by your specific workflow.
Audio Output Tags	Add tags for languages or other purposes to this channel's audio tracks.
Display audio meters	Select **System	Monitor Options**, select the **Display the Following Channel Status** radio button, and check the **Audio Monitors** box.

Adjusting play speed options

1. In AppCenter, click **System | Configuration**.
   Configuration Manager opens.

2. Click **Channel**.
3. Click **Panel**.
4. Configure as follows:

For this setting...	Configure as needed...
Jog speed	Playback advances or retards one frame at a time according to the direction of the setting.
Shuttle speed	Sets the speed for shuttle play or playback.
VAR setting	Variable speed play. Specify the play speed; otherwise, the speed remains at the preset play speed or the last variable play speed used.
Always start at VAR preset	Initial play speed can be set to start at the preset speed.

Configuring data track settings

Do not configure these settings unless you are qualified and understand your system's data track requirements. Consult with Grass Valley for recommendations.

1. In AppCenter, click **System | Configuration**.
   Configuration Manager opens.
2. Click **Channel**, and select a player/recorder channel.
3. Select a video input format.
4. Scroll down and locate **Data Track** settings.
5. Configure as follows:

For this setting...	Configure as needed...
Record ancillary data	Select **Yes** to create a data track and store ancillary data packets.
CEA-608 to DTV CC transcoder	Select **Yes** to automatically convert CEA-608 closed caption data to 708 DTV CC packets.
Record uncompressed VBI and captioning to data track	Available if SD selected. Selecting No retains compatibility with Profile XP Media Platform.
Uncompressed VBI lines	Available if SD selected.
Teletext Output Lines	Click a link in this section to map one or more Teletext lines to play out on a different line.
Output OP-47 packet on line	Map the video line which OP-47 ancillary data packets are output for playout, or select **Source line** to leave the packets unmoved.

Configuring timecode settings

1. In AppCenter, click **System | Configuration**.
   Configuration Manager opens.
2. Click **System**.
3. Configure as follows:

For this setting...	Configure as needed...
Time of Day	Select one of the following: • **System Clock**: This settings uses the Windows operating system clock. If you select this source you should verify that the clock's time is correct. • **LTC Input**: Choose if using LTC timecode. Select which channel you want to use as the Time of Day source.

Configuring proxy and live streaming settings

On the K2 Solo 3G system, configure proxy and live streaming settings as in the following sections. For complete information about proxy and live streaming, refer to related topics in the "Configuring the K2 System" section of this Topic Library.

Enable proxy files

1. In AppCenter, click **File | System | Configuration**.
   Configuration Manager opens.
2. In Configuration Manager, click the **Channel** tab.
3. Select a channel.
4. In Proxy Setup settings, set **Record proxy files** to **Yes**.
5. Select the audio included in the proxy file as follows:
   - Select the first audio input pair to include in the proxy file.
   - Select the number of audio inputs to include in the proxy file.

   The K2 Summit system includes audio pairs beginning with the first pair selected and then each subsequent audio pair up to the selected number of audio inputs.
6. If you want to the K2 Summit system to automatically detect scene changes and include them in the proxy file, do the following:
   - Set **Detect scenes** to **Yes**.
   - Select a minimum scene length. This is the length of time the K2 Solo 3G system waits after detecting a scene change to begin attempting to detect the next scene change.
7. Select another channel and configure as desired.
8. Click **OK** to apply the settings.

Enable live streaming

1. In AppCenter, click **File | System | Configuration**.
   Configuration Manager opens.
2. In Configuration Manager, click the **Channel** tab.
3. Select a channel.
4. In Proxy Setup settings, set **Live network streaming** to **Yes**.
5. Select the audio input pair to include in the proxy stream.
6. Select another channel and configure as desired.
7. Click **OK** to apply the settings.

Configure live streaming multicast

This task describes using AppCenter to configure multicast settings.

1. In AppCenter, click **File | System | Configuration**.
   Configuration Manager opens.
2. In Configuration Manager, click the **System** tab.
   These setting apply to all channels on the K2 Summit system.
3. In Proxy Setup settings, select the multicast IP base.
   The K2 Summit system applies channel-specific IP addresses from this base.
   Your choices are constrained to those specified by IANA for multicast.
4. Select the multicast port base.
   This is the first UDP port address for elementary streams.
5. Click **OK** to apply the settings.

GPI and other configurations

Using GPI input and output triggers

The K2 Solo 3G system provides 12 GPI inputs and 12 GPI outputs on a single DB-25 pin rear panel connector. GPI input triggers can be used to control channels, including recording, playing, stopping, and skipping a playlist event. GPI output triggers can be defined for channels and inserted in playlists to control external equipment as the list is played.

If you want to trigger record via GPI input on four channels simultaneously, make sure all the channels have new clips waiting for the GPI input, in the cue record state.

For information about GPI connectors, see topics in the "Configuring the K2 System" section of this Topic Library.

Configuring GPI triggers

Use the configuration tool provided in the AppCenter file menu. Select **System | Configuration** to define the GPI input or output triggers for a channel.

The following features are part of the licensable AppCenter Pro option.

The Control drop-down list has three selections: Application, Position Trigger, and Channel State.

- Application — allows you to select the GPI trigger on the level of the Playlist application. Must be used in conjunction with a specified channel. For example, if after having selected a channel in the Configuration Manager, you then select Application, you can open up the Playlist Properties dialog box and assign a GPI output event to each clip or event in a Playlist.
- Position Trigger — indicates the position when the GPI output is triggered, e.g. at the beginning or the end of a clip.
- Channel State — indicates the status of the channel when the GPI output is triggered, for example when recording or when idle. Used in conjunction with a trigger state. For example, in a Playlist application, you can set the trigger so that the GPI output is triggered when clip is first loaded but not when it's playing or when it’s re-cued to beginning.

GPI triggers

To access GPI settings, select **System | Configuration** and click on the GPI tab. The settings are located under two tabs: GPI-Input and GPI-Output. GPI output triggers have user-assignable names. The following tables describe the GPI functions under each tab.

GPI Input

On the GPI tab, select GPI-Input…	Make settings as needed…		
GPI Input 1. . . GPI Input 12	Trigger channel(s)	C1, C2, C3, C4	Select the channel to trigger the GPI input.
GPI Input 1. . . GPI Input 12	Trigger action	Play	Play current loaded clip or playlist in assigned Player channel.
		Record	Start recording a clip in Recorder channel.
		Stop	Stop playback or record of assigned channel.
		Rewind	Rewind playback of assigned channel. Channel stays in rewind mode until the beginning of clip is reached or another transport action is taken.

On the GPI tab, select GPI-Input…	Make settings as needed…		
		Fast Forward	Fast forward playback of assigned channel. Channel stays in the fast forward mode until the end of clip is reached or another transport action is taken.
		Cue Start	Cue to start of clip loaded in Player or Playlist channel.
		Cue End	Cue to end of clip loaded in assigned channel.
		Eject	Ejects the current clip.
		Cue Next Event	Goes to next event in a Playlist and stops.
		Cue Prev Event	Goes to previous event in a Playlist and stops.
		Cue Next Section	Goes to next section in a Playlist and stops.
		Cue Prev Section	Goes to previous section in a Playlist and stops.
		Take Next Event	Used with Event Scheduler. Starts playback or record of the next event, regardless of start type.
		Take Next Scheduled Event	Used with Event Scheduler. Starts playback or record of the next event with a scheduled start time or approximate start time. (Note: follow events are skipped.)
		VAR Playback	Plays loaded clip in VAR mode with preset speed.
GPI Input 1. . . GPI Input 12	Active	High Low	Select the active signal (high or low) required. This is determined by the external equipment connected to the GPI input.

GPI Output

On the GPI tab, select GPI-Output…	Make settings as needed…		
GPI Output 1. . . GPI Output 12	Channel	C1, C2, C3, C4	Select the channel on which to trigger the GPI Output.

On the GPI tab, select GPI-Output…	Make settings as needed…		
GPI Output 1. . . GPI Output 12	Active	High Low	Select the active signal (high or low) required. This is determined by the external equipment connected to the GPI Output.
GPI Output 1. . . GPI Output 12	Control (This menu and the items on it are part of the licensable AppCenter Pro option)	Application Position trigger Channel state	Determines whether the GPI output is triggered by the application (e.g., by the Properties dialog box in Playlist), the position (e.g. at the beginning or end of a clip) or the state of the selected channel (e.g. playing, recording, idle, etc.)
GPI Output 1. . . GPI Output 12	Trigger name (Available when Application selected)	GPI-Out-X	Enter the name of the action triggered by the GPI output.
GPI Output 1. . . GPI Output 12	Trigger at (Available when Position trigger selected)	Start of material End of material Start of material plus End of material minus	When Start/End of material plus/minus offset appears
GPI Output 1. . . GPI Output 12	Activate when (Available when Channel state selected)	Playing Recording Cued for play Cued for record Idle	Once a channel has been selected, this setting triggers the GPI output when the channel is in the specified state.

NOTE: If you want to play a list that was created on another play channel, you must ensure that GPI triggers assigned to the play channels use the same names; otherwise the GPI triggers will not occur. Using identical GPI names also allows copying and pasting sections and events between lists.

Configuring FTP Overwrite setting

1. In AppCenter, click **File | System | Configuration**.
   Configuration Manager opens.
2. In Configuration Manager, click the **System** tab.

3. In FTP settings, for the **Allow FTP Overwrites** setting, select one of the following:
   - **Yes**: Clips with existing names get overwritten during an FTP put operation.
   - **No**: An FTP put operation specifying an existing clip name causes the FTP put operation to fail. (This is the default behavior)
4. Click **OK** to apply the setting.

   For more information, see topics in the "Configuring the K2 System" section of this Topic Library.

Related Topics

Using FTP for file transfer on page 291

Adding a remote host

Open Configuration Manager to access remote host settings.

On the Remote tab…	Make settings as needed…
Host name	Enter the name or the IP address of the K2 Solo 3G system where you want to import or export streaming media assets. (Grass Valley recommends that you use host names. For more information on host files, see topics in the "Configuring the K2 System" section of this Topic Library.
Controller Id	When adding a remote host that uses AMP remote control protocol, select a Controller id.

Setting security access permissions

Open Configuration Manager to access security settings. For more information, see topics in the "Configuring the K2 System" section of this Topic Library.

Channel Ganging and Track Mapping

Channel Ganging

This feature is a part of the licensable AppCenter Pro option.

Channel ganging allows you to link two or more channels in a ‘gang’ to synchronize control of the channels.

About Channel Ganging

This feature is part of the licensable AppCenter Pro option.

Channel ganging allows you to control the playing or recording of clips on all the channels in the gang. Ganging record channels together allows you to record up to 4 video or 32 audio tracks. When

you gang play channels together, you can play one clip on all channels or control the playing of different clips on all the channels in the gang.

If a clip is created with more than 16 audio tracks, but only one video track, when you play it back on a gang of play channels, only the first video channel plays the video track. (A ganged clip with 16 audio tracks or less plays the video track in all the play channels in the gang.)

NOTE: Do not gang play and record channels together. Do not gang playlists.

Configuring channel ganging

Channels must assigned to a gang using the **Ganging** tab in the Configuration Manager.

1. In AppCenter, select the Player/Recorder application in the channel pane.
2. Select **System** then **Configuration** and click on the **Ganging** tab.
3. Assign the channels to a gang, and check the appropriate boxes. For a description of the configuration choices, see “Components of the channel ganging configuration” on page174.
4. To save changes, do one of the following:
   - To apply changes to the current configuration file, click **OK**.
   - To save the changes in a new configuration file, click **Save**, to save the configuration file, then click **OK**.

   If the **Record/play same clip on all channels of Gang** box has been checked, the channel pane label switches to G1 or G2 in the first channel in the gang. The other channels in the gang display “In Use” in the channel pane and “Gang” in the application drop-down list.

NOTE: You cannot remove a channel from a gang by setting the channel application to <none>. To remove a channel from a gang, change the channel’s ganging assignment in Configuration Manager.

Components of the channel ganging configuration

The following table describes the main components in the Ganging Configuration window.

Feature	Description
Gang 1, Gang 2	Allows you to select which channels to gang together. You can have up to two gangs on any one K2 Solo 3G system.

Feature	Description
Record/Play same clip on all channels of gang	**If this box is checked:** Ganged channels can record multi-track audio and video. The controls on the first channel affect all the channels in the gang, including settings for loop playback, continuous record, and E-to-E. Starting a record causes the same clip to be recorded on all the record channels in the gang. The first channel displays the name of the clip and the number of the gang, G1 or G2. The other record channels in the gang display "The channel is currently used by" in the channel pane. If you configure a gang of play channels and load a multi-track clip onto one channel, the rtacks are automatically loaded on the other channels in the gang. For example, if you have four ganged play channels and load a clip with three tracks, the first three channels load the three tracks. **If this box is not checked:** The settings on the first channel for loop playback, continuous record, and E-to-E affect all the channels in the gang. Though the channels are labeled as a gang (G1 or G2), if recording each channel functions as a single record channel. To begin recording, eject any existing clip, select **New Clip** and press the **Record button** on each channel. If playing, the ganged channels can play different clips on each channel. The play and stop controls are synchronized, but each clip must be loaded or ejected on a each channel. Adding cue points to one clip does not affect the cue points on different clips in the other channels. This box is disabled if any of the channels in the gang are configured as ChannelFlex channels.

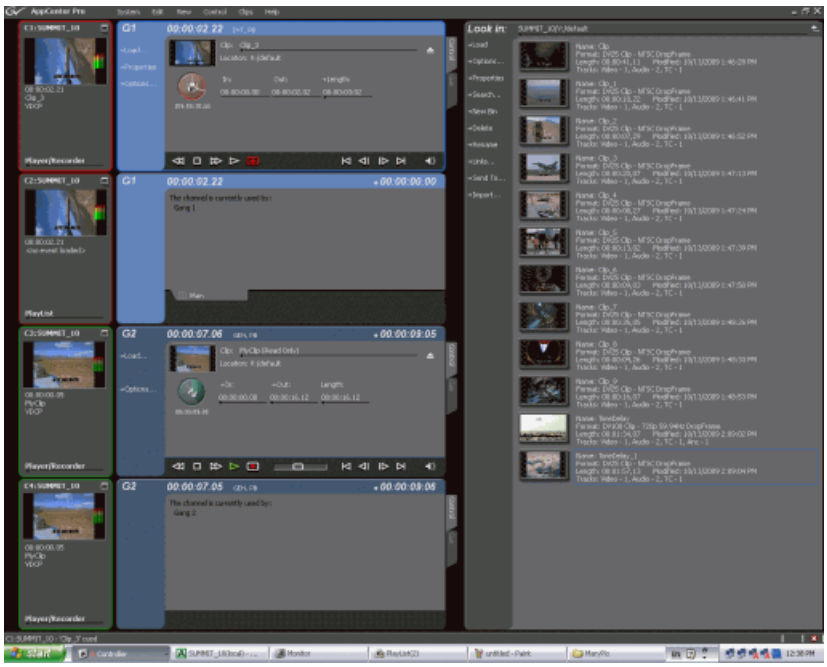
Feature	Description
Record audio from all channels to same clip	**If this box is checked:** The audio from more than one channel in the gang is recorded. Up to 32 audio tracks can be recorded on one clip: for example tracks 1-16 from the first channel and tracks 17-32 from the second channel, or four tracks from each channel in a gang of four channels, and so on. To direct the routing, you can assign label tags to the audio tracks before or after the clip is recorded. When you play the clip, unless you specify otherwise, the first 16 audio tracks play on the first channel and the second 16 audio tracks (tracks 17-32) play on the second channel. If there is only one video track and you play the clip on a gang of player channels, the video plays on the first channel only. The other video channels, if any, play black. **If this box is not checked:** The audio from the first channel in the gang is recorded, up to a total of 16 audio tracks. If there is only one video track and you play the clip on a gang of player channels, the video plays on all the channels in the gang. This box is disabled if any of the channels in the gang are configured as ChannelFlex channels
Record video from all channels to same clip	**If this box is checked:** Video from all channels in the gang is recorded. You can record up to four video tracks on one clip. The order of video tracks in the clip is determined by the order of channels in the group. **If this box is not checked:** Only video from the first channel in the gang is recorded. This box is disabled if any of the channels in the gang are configured as ChannelFlex channels.

Using channel ganging

Ganging record channels allows you to create multi-track clips with one record session. Ganging play channels allows you to play different audio or video simultaneously on two different channels. For example, you could have an English audio track on one play channel, while another channel played a Spanish audio track. Or you could play one video on two channels, with SD output on one channel and HD output on the other. (If using HD video, the SD channel would down-convert and the HD channel would pass the video through.) Once configured, a gang of channels can be controlled by clicking on the channel controls. You cannot gang play and record channels together, or playlists.

The following illustration shows two gangs: the first gang (G1) recording a clip and the second gang (G2) playing another clip. Both gangs have been configured to record audio and video on more than one channel. In G1, if you click the Record button on the first channel pane, both channels record the clip. Any of the controls in the first channel affect both channels in the gang, including settings for loop playback, continuous record, and E-to-E. In G2, the same clip is playing out on both channels.

The first channel displays the name of the clip and a thumbnail of the video. The monitor pane for each channel displays the channel number, machine name, and is outlined in red or green to indicate whether the gang is a play or a record.



NOTE: A* K2 Solo 3G system *treats all the channels in a gang as if they were set to the same application. If you create a four-channel gang but set two of the ganged channels to Player/Recorder and the other two to <none>, the resulting clip will have four video tracks. Playing a clip on a gang with extra channels can result in hearing audio on channels that aren't playing video. For example, if you play a clip with two video tracks on a three-channel gang, the last channel has no video, but audio is still embedded.

Unganging Channels

You can only ungang a channel from Configuration Manager; you cannot change the allocation of the channel by changing the selection on the application drop-down list. Unganging the channels again causes all of the channels to stop recording or playing.

Track Mapping

This feature is a part of the licensable AppCenter Pro option.

Track mapping lets you label video and audio tracks, and control audio input and routing.

About track mapping

This feature is part of the licensable AppCenter Pro option.

AppCenter lets you configure audio input and output routing, assign labels to audio tracks, or specify which video track you want to be the key. You can have multiple tracks with the same name in a clip. Track mapping is supported for individual clips. It is not supported for clips in a playlist.

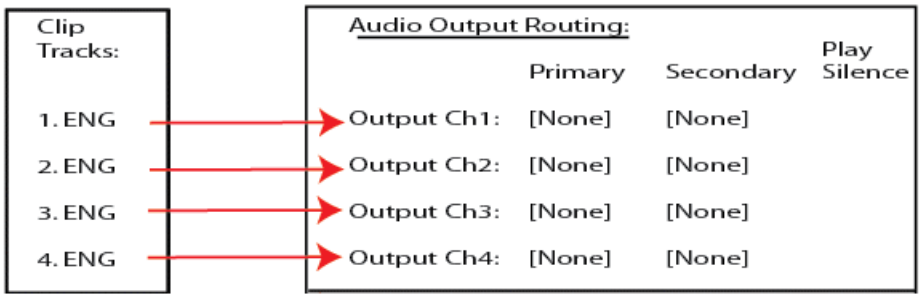
Labeling the audio tracks in a clip and the output channels in Configuration Manager allows you to map specific tracks to specific output channels. You can assign output labels to primary output channels alone or to both primary and secondary output channels. (If there is no label on the primary output channel, you cannot assign a label to the secondary output.)

AppCenter maps the audio tracks to the output channels based on specific criteria. The following sections give a detailed description of the track mapping that results based on each of these criteria:

- If no labels are assigned to any output channel
- If unique labels are assigned to audio tracks and output channels
- If unique labels are assigned to audio tracks and output channels
- If language groups are used
- If the primary output alone is labeled
- If both primary and secondary outputs are labeled
- If no output labels match the track labels
- If no labels are assigned to any output channel

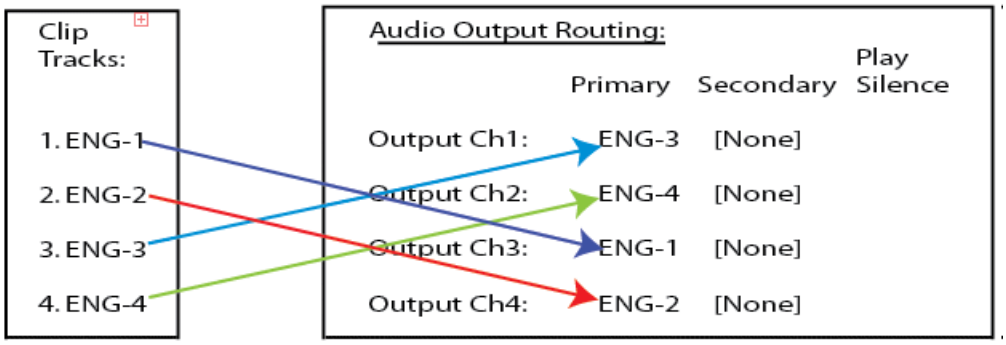
If no labels are assigned to any output channel

If no audio output routing is specified, AppCenter plays out the audio tracks according to their order in the clip, regardless of the labels of the individual tracks. In the following illustration, the first four audio tracks are routed to audio output channels 1 through 4.



If unique labels are assigned to audio tracks and output channels

If you assign unique labels to each of the tracks in a clip, and assign the same labels to a corresponding output channel, AppCenter routes each track exclusively to its matching output channel. The following illustration shows one example of how unique labels are evaluated.



If language groups are used

You can have multiple tracks and output channels with the same label. If multiple tracks have the same label, AppCenter evaluates where to map the tracks as follows:

- An output channel's primary and secondary output labels are considered together as a "language group" when assigning an audio track for playout. If two channels have the same primary label but have different secondary labels, then those channels have different language groups. For example, a channel with labels FRE+ GER is considered a different language group than a channel with labels FRE + ENG.
- Each output channel, in order from first to last, is evaluated to determine if the label or language group matches a labeled audio track in the clip. The first channel with a label or language group that matches the track label plays that audio track. If the clip has several audio tracks with the same label, the first matching output channel plays the first audio track, the second matching output channel plays the second audio track, and so on.
- The Play Silence box. If the AppCenter does not find a matching label or language group for the output channels, and the Play Silence box has been checked in Configuration Manager, the channel plays silence. Otherwise, if AppCenter finds no match, the output channel plays the correspondingly numbered audio track.

This evaluation process is further described in the following sections:

- If the primary output alone is labeled
- If both primary and secondary outputs are labeled
- If no output labels match the track labels
- If Play Silence if checked
- If Play Silence is not checked

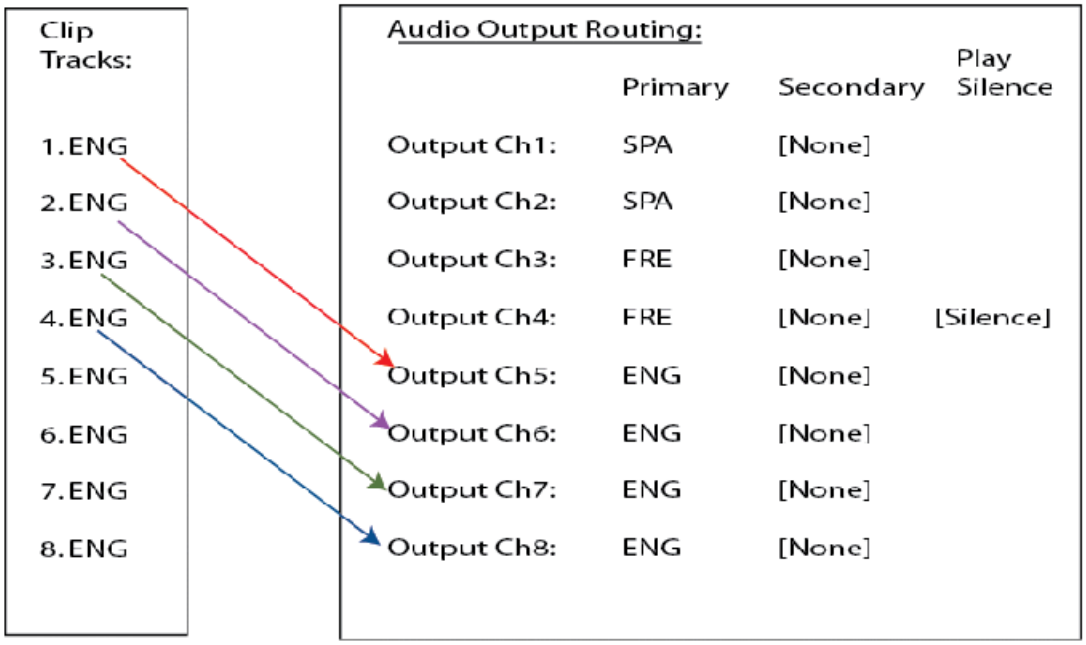
If the primary output alone is labeled

If the output routing channels are assigned primary labels, AppCenter evaluates the labels to see if they match with the track labels in the clip as follows:

- If there are no secondary labels assigned, then only the primary labels are evaluated.
- Labels are evaluated in numerical order, that is, from the first to last.
- After labels are evaluated in numerical order, the Play Silence check box is evaluated to determine if it is checked or un-checked.

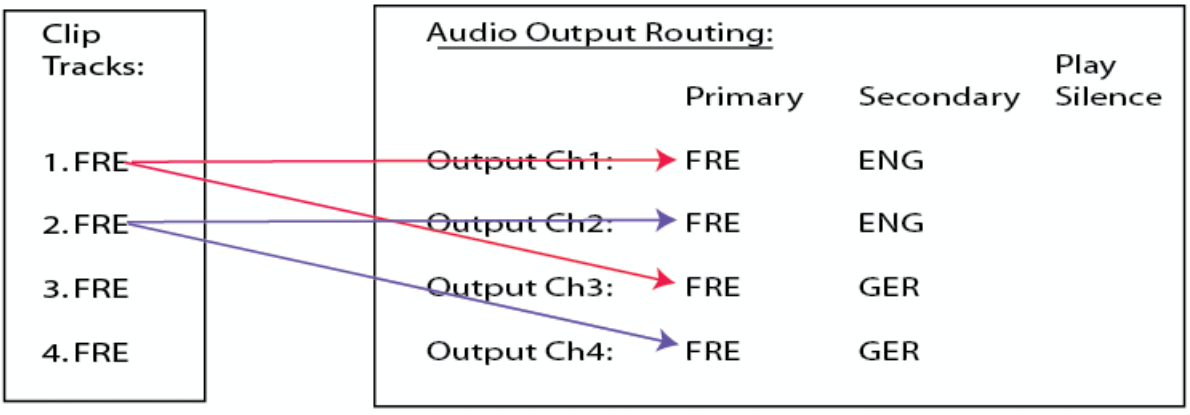
The following illustration shows an example of how AppCenter maps non-unique labeled audio tracks to non-unique labeled output channels. In this example, the first four output channels have primary output labels that do not match with any of the track labels, so they are bypassed.

Because AppCenter maps the first track label to the first matching output label, the first ENG track is routed to the first audio output labeled ENG (in this example, output channel 5), the second ENG track is routed to the next audio output labeled ENG (output channel 6), and so on.



If both primary and secondary outputs are labeled

The primary and secondary labels of an output channel are considered a “language group”. A clip’s audio track label is matched to a language group’s primary label. For example, consider the following illustration:



The language group for channel 1 and channel 2 (FRE + ENG) is different than the language group for channel 3 and channel 4 (FRE + GER). If a clip has audio tracks 1–4 labeled “FRE”, channels 1–2 play out clip tracks 1–2, and channels 3–4 also play out clip tracks 1–2.

If no output labels match the track labels

If no output labels match any track labels in the clip, AppCenter evaluates the output routing based on whether the Play Silence box is checked or not. (The Play Silence box is configured in Configuration Manager.

If Play Silence is checked

If AppCenter finds an output channel with a label that matches the label on an audio track in the clip, the Play Silence box is ignored.

However, if no matching label is found, and the Play Silence box has been checked in Configuration Manager, the channel plays silence.

If Play Silence is not checked

If there are no matching labels for output channels and the Play Silence box has not been checked in Configuration Manager, the output channel plays the matching numbered audio track. Basically, the output channel behaves as if it were unlabeled.

Configuring track mapping

To set up track mapping in AppCenter, you need to add audio tags in Configuration Manager and name the tracks in the clip itself.

You can do the following during configuration:

- Add audio tags
- Rename a video or audio track

Adding audio tags

This feature is part of the licensable AppCenter Pro option.

Before recording a clip, you can add audio tags to the audio input and output. Select a name from the drop-down list or enter a track name. Adding input and output tags before recording a clip can help streamline the routing of the tracks. A track name cannot be more than 16 characters long. You can also label audio tags after recording a clip.

1. In the Channel tab of the Configuration Manager, scroll down to the Audio Input or Audio Output section. The sections are grouped under each channel tab.
2. Click **<Add Tags...>**.
   - To assign a label to audio input tracks, click on the drop-down list next to the track you want to label, and select the label, or enter in a name.
   - If you are labeling audio output tracks, you can assign primary or secondary labels or check the Play Silence box.
3. Click **OK**. The tags are now displayed in the Configuration Manager.
4. To have the changes apply to this configuration file, click **OK**.

5. To save the changes in a new configuration file, click **Save** save the configuration file, and then click **OK**.

Renaming a video or audio track

If no input tags have been specified, any audio tracks that you have recorded appear in the Clip Properties dialog box as **A1**, **A2**, etc. The video tracks by default are labeled **Video**. Multiple video and audio tracks can be labeled with the same name.

1. Open the Clip Properties dialog box and select the Tracks tab.
2. Highlight the track and perform one of the following actions:
   - Click the **Rename** button.
   - Right-click with the mouse and select Rename.
   - Double-click on the track name.
3. A drop-down list displays, allowing you to select a new name for the track. You can also enter in a name. Track names can be up to 16 characters long.

Using track mapping

You can add, remove, or re-arrange audio or video tracks in a clip through the Tracks tab of the Clip Properties dialog box.

Importing audio tracks

This feature is part of the licensable AppCenter Pro option.

You can import an audio track from an audio file. The file must be in the .wav format with a sample rate of 48 kHz. The imported file is aligned to the start of the clip.

1. Highlight the clip that you want to import the track into.
2. Open the Clip Properties. (list ways) and select the Track tab.
3. Click the **Import** button.
4. The Windows Open dialog box displays the following:
5. Browse to the .wav file to import and click **OK**.

   When you import a file, the new track appears at the end of the working asset's track list. The file name is used as the initial audio track label. After the file has been imported, you can highlight the track and rename it with the **Rename** button.

   If the duration of the imported audio track(s) is lesser than the clip duration, silent audio will be played for imported tracks after the valid audio duration.

Adding a video or audio track

This feature is part of the licensable AppCenter Pro option.

You can view, edit, add or remove video and audio tracks in an clip. The tracks should be of the same format. (For example, if you have an NTSC clip, do not add a PAL track to it.) You can have up to four video tracks or 32 audio tracks in one clip. Added tracks are aligned to the start of the clip.

Clips may contain tracks of different lengths. The length of the overall clip is limited to the length of the original track. For example, if you have a clip that is thirty seconds long and you add a two-minute audio track, AppCenter adds only the first thirty seconds of audio from the added track.

NOTE: If an additional track is longer than the original track, any material beyond the length of the original track is not played as shown in the illustration below.

If an additional track is shorter than the original track, video plays black, ancillary data tracks are blank, and audio is silent as illustrated below.

To add a video or audio track, follow these steps:

1. In the Clips Properties dialog box, select the Tracks tab.
2. Click the **Add Track** button.

   The Select Asset dialog box displays.
3. Browse to the asset that has the tracks you want to add. Click **OK**. The Select Tracks dialog box displays.
4. You can select a track by checking the box next to the track or, within the audio or video sections, by highlighting the track you want to add, right-clicking with the mouse, and then checking the box. When you have selected the tracks, click OK. The Clip Properties dialog box shows yellow sunbursts next to the track icons of the newly added tracks.
5. To accept the changes, click **OK**.

Removing a video or audio track

To remove a video or audio track, follow these steps:

1. Open the Clip Properties dialog box and select the Tracks tab.
2. Highlight the track and perform one of the following actions:

   - Click the **Remove** button.
   - Right-click with the mouse and select Remove.
   - Press the Delete key on the keyboard.

Re-arranging the order of the tracks

You can change the order of the tracks, by using the mouse to drag and drop tracks within the video and audio sections. Grass Valley recommends grouping tracks with the same label together. Grouping

like tracks together can be helpful if you have several tracks with the same label and you need to configure the audio output routing in the Configuration Manager.

ChannelFlex Suite

ChannelFlex Suite and licensing

The features in this chapter are part of the ChannelFlex Suite, which requires the AppCenter Elite license.

K2 Summit/Solo formats, models, licenses, and hardware support

Formats are supported as in the following tables.

Table 4: First-generation K2 Summit/Solo system

Formats	Compression	1x	Multi-Cam, 3D/Video + Key	3x Super Slo-Mo	4K
SD	DV	Encode/decode	Encode/decode	Not supported.	Not supported.
	MPEG-2	Decode is standard. Encode requires codec option card.	Decode is standard. Encode requires codec option card.	Not supported.	Not supported.
	AVCHD	Not supported.	Not supported.	Not supported.	Not supported.
1080i/720p	DV	Encode/decode. Requires HD license.	Encode/decode. Requires HD license.	Encode/decode. Requires HD license.	Not supported.
	MPEG-2	Decode is standard. Encode requires codec option card. Requires HD license.	Decode is standard. Encode requires codec option card. Requires HD license.	Not supported.	Not supported.
	AVC-Intra	Encode/decode. Requires codec option card. Requires HD license.	Encode/decode. Requires codec option card. Requires HD license.	Not supported.	Not supported.
	AVCHD	Not supported	Not supported	Not supported	Not supported.
	AVC - LongG	Not supported	Not supported	Not supported	Not supported.
	Avid DNxHD	Not supported	Not supported	Not supported	Not supported.

Formats	Compression	1x	Multi-Cam, 3D/Video + Key	3x Super Slo-Mo	4K
1080p	AVC-Intra Class 100	Not supported	Not supported	Not supported	Not supported.

To add support for additional formats, contact your Grass Valley representative for upgrade information.

Table 5: K2 Summit 3G system

Formats	Compression	1x	3x Super Slo-Mo, Multi-Cam, 3D/Video + Key	6x Super Slo-Mo	4K
SD	DV	Encode/decode	Encode/decode	Not supported.	Not supported.
	MPEG-2	Encode/decode	Encode/decode. Requires codec option card.	Not supported.	Not supported.
	AVCHD/H.264	Decode only. Requires AVC license.	Not supported	Not supported	Not supported.
1080i/720p	DV	Encode/decode. HD license is required.	Encode/decode. HD license is required.	Encode/decode. Requires codec option card, plus HD and 6xSSM licenses. Requires K2 Summit 3G chassis with 2.5” hard drives for one channel or high endurance solid state drives for full features with two channels.	Not supported.
	MPEG-2	Encode/decode. HD license is required.	Encode/decode. Requires codec option card. HD license is required.	Not supported.	Not supported.

Formats	Compression	1x	3x Super Slo-Mo, Multi-Cam, 3D/Video + Key	6x Super Slo-Mo	4K
	AVC-Intra	Encode/decode. Requires HD and AVC licenses.	Encode/decode. Requires HD and AVC licenses.	Encode/decode. Requires codec option card, plus HD, 6xSSM and AVC licenses. Requires K2 Summit 3G chassis with 2.5” hard drives for one channel or high endurance solid state drives for full features with two channels.	Not supported.
	AVCHD/H.264	Decode only. Requires HD and AVC licenses.	Not supported	Not supported	Not supported.
	AVC - LongG	Decode only. Requires HD and AVC licenses.	Not supported	Not supported	Not supported.
	Avid DNxHD	Encode/decode. Requires HD and DNxHD licenses.	Encode/decode. Requires HD and DNxHD licenses.	Not supported	Not supported.
1080p	AVC-Intra Class 100	Encode/decode. Requires HD, 3G and AVC licenses.	Encode/decode. Requires codec option card, plus HD, 3G and AVC licenses.	Not supported	Encode/decode. Requires codec option cards and high endurance solid state drives. Requires HD, 3G, 4K and AVC licenses.

Table 6: K2 Solo 3G system

Formats	Compression	1x	Multi-Cam, 3D/Video + Key	3x Super Slo-Mo	4K
SD	DV	Encode/decode	Encode/decode	Not supported.	Not supported.

Formats	Compression	1x	Multi-Cam, 3D/Video + Key	3x Super Slo-Mo	4K
	MPEG-2	Encode/decode	Not supported	Not supported	Not supported.
	AVCHD/H.264	Decode only. Requires AVC license.	Not supported	Not supported	Not supported.
1080i/720p	DV	Encode/decode. HD license is required.	Encode/decode. HD license is required.	Encode/decode. HD license is required.	Not supported.
	MPEG-2	Encode/decode. HD license is required.	Not supported	Not supported	Not supported.
	AVC-Intra	Encode/decode. Requires HD and AVC licenses.	Encode/decode. Requires HD and AVC licenses.	Encode/decode. Requires HD and AVC licenses.	Not supported.
	AVCHD/H.264	Decode only. Requires HD and AVC licenses.	Not supported	Not supported	Not supported.
	AVC - LongG	Decode only. Requires HD and AVC licenses.	Not supported	Not supported	Not supported.
	Avid DNxHD	Encode/decode. Requires HD and DNxHD licenses.	Encode/decode. Requires HD and DNxHD licenses.	Encode/decode. Requires HD and DNxHD licenses.	Not supported.
1080p	AVC-Intra Class 100	Encode/decode. Requires HD and 3G licenses.	Not supported	Not supported	Not supported.

Super Slo-Mo

This feature is part of the ChannelFlex Suite, which requires the AppCenter Elite license. This feature also requires the HD license.

About Super Slo-Mo

This feature is part of the ChannelFlex Suite, which requires the AppCenter Elite license. This feature also requires HD, 3G, and AVC licenses.

You can connect a Super Slo-Mo camera to two or three SDI inputs on a K2 Summit/Solo channel. You must configure the channel to record Super Slo-Mo. When so configured, the channel is record-only, not bi-directional record/play. The K2 Solo 3G system records Super Slo-Mo at 2x frame rate, 3x frame rate, or 6x frame rate, as configured. This creates a Super Slo-Mo clip. A Super Slo-Mo clip contains no audio or ancillary data.

The K2 Solo 3G system accommodates LTC, ancLTC, or ancVITC timecode for a Super Slo-Mo clip as follows:

- A Super Slo-Mo clip contains embedded timecode extracted from Super Slo-Mo phase 1.
- For 2x frame rate, timecode repeats every two frames.
- For 3x frame rate, timecode repeats every three frames.
- For 6x frame rate, timecode repeats every six frames.

The result is that a Super Slo-Mo clip can function as if it has 1x clip length and timecode, even though it is actually 2x, 3x, or 6x times longer.

A Super Slo-Mo channel is in E-to-E (LoopThru) mode.

You can play the Super Slo-Mo clip on a standard bi-directional record/play channel. SDI OUT2 provides the Super Out feature on phase 1.

Import/Export and GXF transfer of a Super Slo-Mo clip are supported with other K2 Summit/Solo systems at version 7.1.x software or higher.

An indicator icon  that a clip is a Super Slo-Mo clip appears in the Clips pane and in clip properties.

Super Slo-Mo requirements and restrictions

This feature is part of the ChannelFlex Suite, which requires the AppCenter Elite license. This feature also requires the HD license.

- Phase 1, Phase 2, and Phase 3 inputs must be locked and phase aligned with each other.
- Phase 1, Phase 2, and Phase 3 must be connected to a channel's SDI IN1, SDI IN2, and SDI IN3 respectively.
- You cannot change the 2x/3x/6x configuration while recording is underway.
- Loss of any phase input results in black for that phase of video in the clip.
- Super Slo-Mo clips are HD and therefore the Super Slo-Mo feature requires the HD license.
- When recording a Super Slo-Mo clip, no audio and ancillary data tracks are created.
- Super Slo-Mo cameras in the following list are supported:
  - Grass Valley LDK8300 Camera; 3x and 2x
  - Grass Valley LDK8000 SportElite HD; 2x
  - Grass Valley LDX HiSpeed Camera; 3x
  - Grass Valley LDX XtremeSpeed Camera; 3x and 6x
  - Sony 3300 - 3x only; 2x is not supported
- When exporting a 2x, 3x, or 6x Super Slo-Mo clip, AVI, MXF, and MOV (QuickTime) file types do not retain the original Super Slo-Mo timecode information. Therefore upon import, the timecode numbers will no longer match the video material.

- Stream/Import/Export of a Super Slo-Mo clip is not supported with K2 systems at a 3.x version of software.
- The maximum continuous record length for a Super Slo-Mo clip is 24 hours.
- This feature is not compatible with TimeDelay.
- One or more Super Slo-Mo channels can be a part of an AppCenter channel gang, but the "Record/play same clip on all channels of Gang" feature is not available for that gang.
- 6x Super Slow Motion camera support is not available on K2 Solo.

Super Slo-Mo camera formats

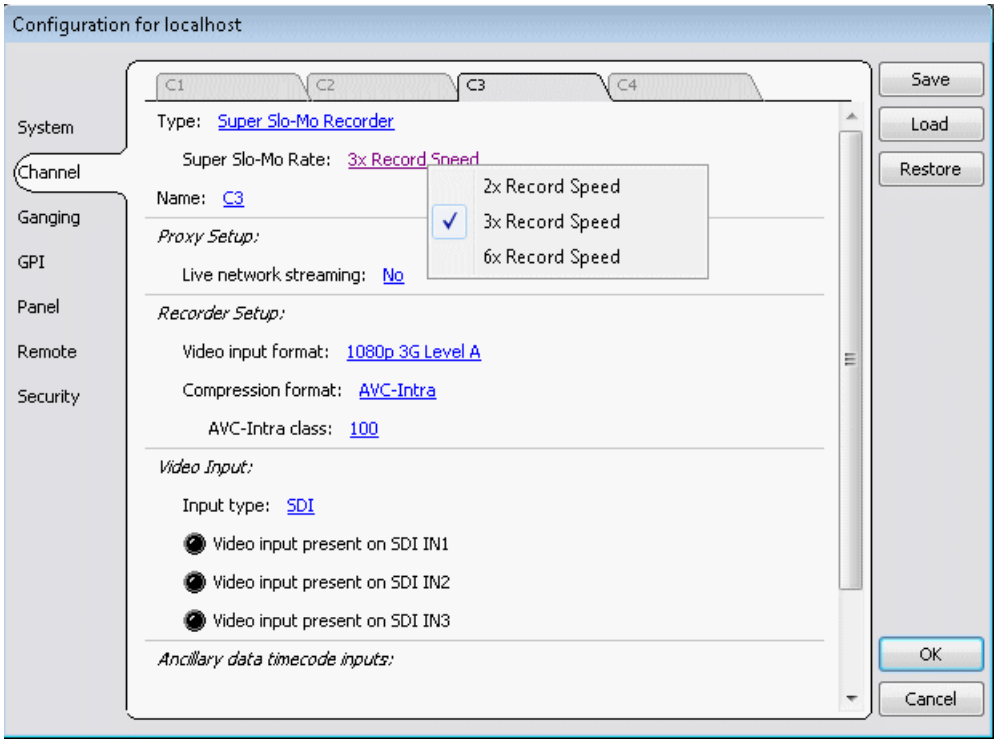
Formats specified for output by Super Slo-Mo cameras are supported as follows:

Camera	Format	Frame Rate (Hz)	Speed support
Grass Valley LDK8000 SportElite HD Camera	• 720p • 1080i	• 50/59.94/100/119.88 • 50/59.94/100/119.88	2x;
Grass Valley LDK8300 Camera	• 720p • 1080i	• 50/59.94/100/119.88/150/179.82 • 50/59.94/100/119.88/150/179.82	2x; 3x
Grass Valley LDX HiSpeed Camera	• 720p • 1080i	• 50/59.94/150/179.82 • 50/59.94/150/179.82	3x
Grass Valley LDX XtremeSpeed Camera	• 720p • 1080i • 1080p	• 50/59.94/150/179.82/300/359.64 • 50/59.94/150/ 179.82/300/359.64 • 50/59.94/150/179.82	• 3x in 720p; 1080i; 1080p • 6x in 720p; 1080i
Sony 3300	• 720p • 1080i	• 50/59.94/150/179.82 • 50/59.94/150/179.82	3x

Configuring Super Slo-Mo

This feature is part of the ChannelFlex Suite, which requires the AppCenter Elite license. This feature also requires the HD license.

1. Open Configuration Manager, click **Channel**, and select a channel tab.



2. For Type, select **Super Slo-Mo Recorder**.

   Only those settings supported by a Super Slo-Mo channel are displayed.

   NOTE: If you have the AppCenter Elite license yet the Super Slo-Mo option does not appear, it means you do not have the HD license, which is required for Super Slo-Mo. You must also have the appropriate compression license, such as DV or AVC licenses.

3. For Super Slo-Mo Rate, select one of the following:

   - **2x Record Speed**
   - **3x Record Speed**
   - **6x Record Speed**

4. If desired, assign a name to the channel.
5. Select Video input format.

Multi-Cam

This feature is part of the ChannelFlex Suite, which requires the AppCenter Elite license.

About Multi-Cam

This feature is part of the ChannelFlex Suite, which requires the AppCenter Elite license.

You can connect up to three video sources to SDI IN1, SDI IN2, and SDI IN3 in a channel. You must configure the channel as a Multi-Cam record channel. The K2 Solo 3G system records up to three clips, one from each video input, and automatically gives them default names.

If ancillary data and/or timecode is present on SDI IN1, each Multi-Cam clip contains that ancillary data and/or timecode. LTC timecode is also shared for all clips.

The K2 Solo 3G system can record the same audio for all clips, or it can record separate audio for each clip. You can configure these audio options as desired.

In E-to-E (LoopThru) mode, SDI OUT1 and SDI OUT2 show the signal coming in at SDI IN1, SDI IN2, and SDI IN3 respectively. When in this mode, the VGA Video Monitor displays up to three inputs, but at a smaller size, in the area for the single channel.

Each Multi-Cam clip plays as a standard clip on a standard bi-directional record/play channel.

Multi-Cam requirements and restrictions

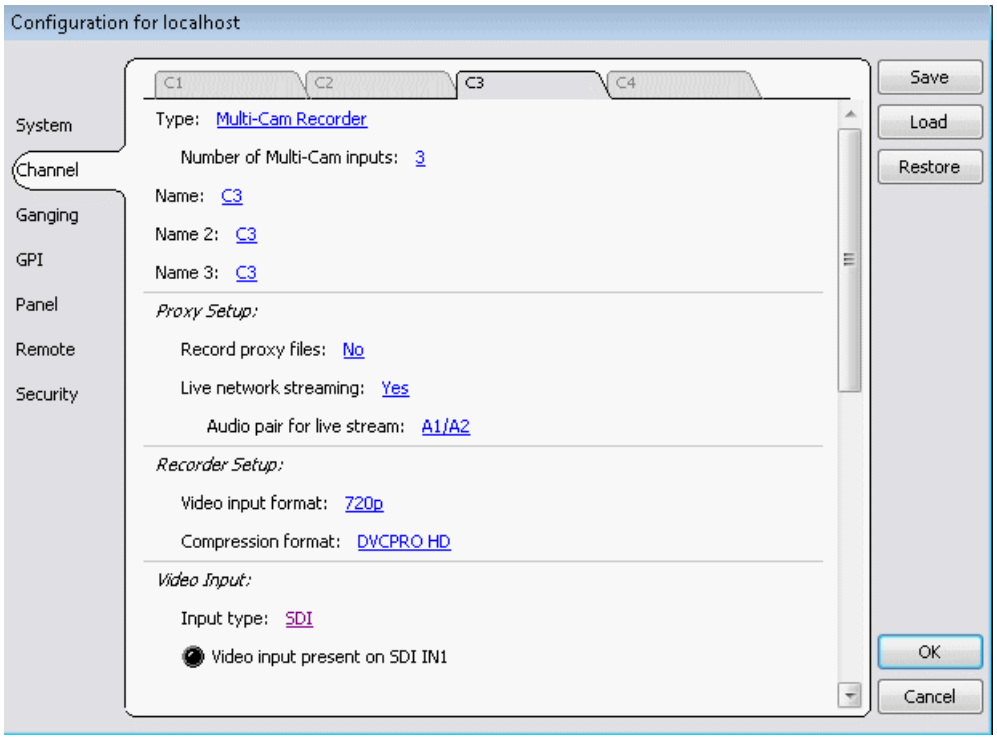
This feature is part of the ChannelFlex Suite, which requires the AppCenter Elite license.

- SDI IN1, SDI IN2, and SDI IN3 must be frequency locked with each other.
- Input 1, Input 2, and Input 3 must be connected to a channel's SDI IN1, SDI IN2, and SDI IN3 respectively.
- When recording the same audio for all clips, embedded audio is extracted only from the Input 1 and the number of recorded audio tracks is limited to sixteen.
- When recording audio separately for each clip, you can have up to sixteen tracks per Multi-Cam input.
- When in split audio mode, we can record only 4 audio per clip in 3-input Multi-Cam channel.
- This feature is not compatible with K2 TimeDelay.
- One or more Multi-Cam channels can be a part of an AppCenter channel gang, but the "Record/play same clip on all channels of Gang" feature is not available for that gang.
- Requires the K2 3-input Multi-Cam license that enables support for 3-input Multi-Cam on a single K2 channel. A single license will only enable a single channel. Multiple licenses required for multiple K2 channel support.
- Avid DNxHD is available but not qualified for use with K2 Summit version 9.3.

Configuring Multi-Cam

This feature is part of the ChannelFlex Suite, which requires the AppCenter Elite license.

1. Open Configuration Manager, click **Channel**, and select a channel tab.



2. For Type, select **Multi-Cam Recorder**.
3. For Number of Multi-Cam inputs, select **2** or **3**.
4. For Name, enter a name to identify input **SDI IN1**.
5. For Name 2, enter a name to identify input **SDI IN2**.
6. For Name 3, enter a name to identify input **SDI IN3**, if applicable.
7. Scroll down to the Audio Input section and do one of the following:
   - If you want all clips to have audio from Input 1, set **Split audio** to **No**.
   - If you want each clip to have audio from its own input, set **Split Audio** to **Yes**.

8. If you set Split audio to Yes, choose one of the following settings for **Number of split audio inputs**:

Setting	Embedded audio	AES audio
2+2	The first two audio tracks on Input 1 go to clip 1. The first two audio tracks on Input 2 go to clip 2.	AES audio tracks 1 and 2 go to clip 1. AES audio tracks 3 and 4 go to clip 2.
4+4	The first four audio tracks on Input 1 go to Clip 1. The first four audio tracks on Input 2 go to clip 2.	AES audio tracks 1- 4 go to clip 1. AES audio tracks 5-8 got to clip 2.
8+8	The first eight audio tracks on Input 1 go to Clip 1. The first eight audio tracks on Input 2 go to clip 2.	Not supported.
2+2+2	The first two audio tracks on Input 1 go to clip 1. The first two audio tracks on Input 2 go to clip 2. The first two audio tracks on Input 3 go to clip 3.	AES audio tracks 1 and 2 go to clip 1. AES audio tracks 3 and 4 go to clip 2. AES audio tracks 5 and 6 go to clip 3.
4+4+4	The first four audio tracks on Input 1 go to clip 1. The first four audio tracks on Input 2 go to clip 2. The first four audio tracks on Input 3 go to clip 3.	Not supported.

9. Configure remaining channel settings as appropriate.

3D/Video + Key

The features in this section are part of the ChannelFlex Suite, which requires the AppCenter Elite license.

About 3D/Video + Key

This feature is part of the ChannelFlex Suite, which requires the AppCenter Elite license.

You can connect SDI IN1 and SDI IN2 on a K2 Solo 3G system channel to use the 3D/Video + Key feature. SDI IN1 is Video or Left Eye. SDI IN2 is Key or Right Eye. To record, you must configure the channel as a 3D/Video + Key record channel. The K2 Solo 3G system records a single 3D/Video + Key clip with two video tracks.

In a 3D/Video + Key clip, video track 1 is Video (or right eye) and video track 2 is Key (or left eye). If ancillary data and/or timecode is present on SDI IN1, the 3D/Video + Key clip contains that ancillary data and/or timecode. The clip's audio is recorded from SDI IN1. You can also create a 3D/Video + Key clip using the Add Track feature.

In E-to-E (LoopThru) mode, SDI OUT1 and SDI OUT2 show the signals coming in at SDI IN1 and SDI IN2 respectively. When in this mode or when playing a 3D/Video + Key clip, the VGA Video Monitor displays the two video signals, but at a smaller size, in the area for the single channel.

When you play a 3D/Video + Key clip on a channel that is configured as a 3D/Video + Key play channel, SDI OUT1 plays the Video (or right eye) and SDI OUT2 plays the Key (or left eye). When

you play a standard clip on a channel that is configured as a 3D/Video + Key play channel, SDI OUT2 plays a full Key (white). AppCenter Playlist and Loop Play support 3D/Video + Key clips. A 3D/Video + Key play channel supports playlist mode.

You can stream a 3D/Video + Key clip as GXF to/from other K2 Summit/Solo systems.

3D/Video + Key requirements and restrictions

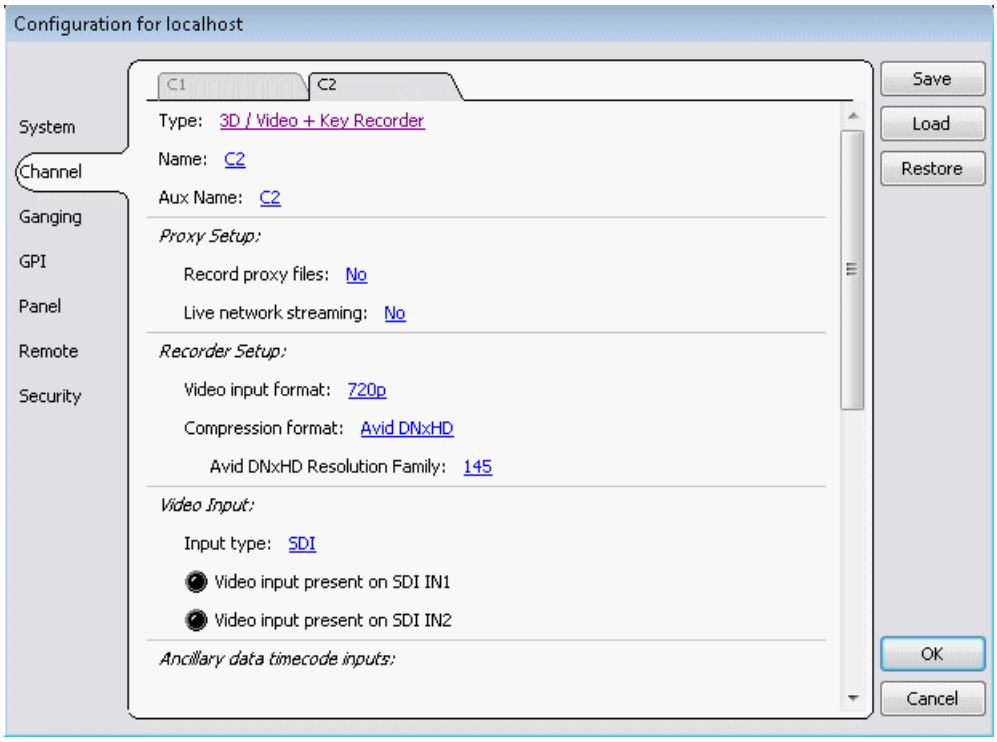
This feature is part of the ChannelFlex Suite, which requires the AppCenter Elite license.

- Video and Key tracks must be the same compression format.
- Video or Left Eye must be connected to the channel's SDI IN1 and Key or Right Eye must be connected to the channel's SDI IN2.
- SDI IN1 and SDI IN2 must be frequency locked with each other.
- Audio is limited to eight embedded tracks or eight AES tracks recorded per channel, recorded from SDI IN1.
- A 3D/Video+Key player channel does not support agile playback or transition (mix) effects.
- A 3D/Video+Key player channel does not support a two-head player model.
- A 3D/Video+Key player channel does not support offspeed play greater than 1 or less than -1. During these offspeed play operations the video is not synchronized between the two video tracks. However, both video outputs will resync when recued.
- Super Out is not supported on a channel configured for 3D/Video + Key.
- 3D/Video + Key is not compatible with TimeDelay.
- One or more 3D/Video + Key channels can be a part of an AppCenter channel gang, but the "Record/play same clip on all channels of Gang" feature is not available for that gang.
- AVC-Intra Class 100 not supported.

Configuring 3D/Video + Key

This feature is part of the ChannelFlex Suite, which requires the AppCenter Elite license.

1. Open Configuration Manager, click **Channel**, and select a channel tab.



2. For Type, select **3D / Video + Key Recorder** or **3D / Video + Key Player**.
3. If you selected **3D / Video + Key Recorder**, enter names as follows:
   a) For Name, enter a name to identify SDI IN1.
   b) For Aux Name, enter a name to identify SDI IN2.
4. If you selected **3D / Video + Key Player**, enter names as follows:
   a) For Name, enter a name to identify SDI OUT1.
   b) For Aux Name, enter a name to identify SDI OUT2.
5. Configure remaining channel settings as appropriate.

4K

This feature is part of the ChannelFlex Suite, which requires the AppCenter Elite license.

About 4K

This feature is part of the ChannelFlex Suite, which requires the AppCenter Elite license. The 4K feature is only available on the K2 Summit 3G system chassis. First generation K2 Summit system and K2 Solo 3G system chassis are not supported.

You can set a K2 Summit 3G system channel to 4K Recorder (Top) to record two of the four quadrants of a 4K image. The next channel is automatically set to 4K Recorder (Bottom) to record the other two quadrants. Both channels are ganged to act as one recorder, so two adjacent ganged channels are used to record all four quadrants of a 4K image.

NOTE: Only C1 or C3 have the option to be selected as 4K Recorder (Top) or 4K Player (Top). There are no selectable 4K options for C2 and C4. C1 will always gang with C2, and C3 will always gang with C4.

When you record a 4K clip, SDI IN1 of the first channel is 4K Recorder Top Left and SDI IN2 is 4K Recorder Top Right. On the next channel, SDI IN1 is 4K Recorder Bottom Left and SDI IN2 is 4K Recorder Bottom Right.

When you play a 4K clip, two adjacent ganged channels are used to play all four quadrants of a 4K clip. On the channel configured as a 4K Player (Top) channel, SDI OUT1 is 4K Player Top Left and SDI OUT2 is 4K Player Top Right. On the next channel, SDI OUT1 is 4K Player Bottom Left and SDI OUT2 is 4K Player Bottom Right.

You can record a single 4K clip with four 1080p video tracks and one timecode track. You can also have proxy live streaming of the 4K clip to/from other K2 Summit 3G systems.

4K requirements and restrictions

This feature is part of the ChannelFlex Suite, which requires the AppCenter Elite license.

- Requires 3G CODEC boards with mezzanines, 3G licenses, 4K licenses, K2 Summit 3G system chassis and SSD drives.
- SDI IN1 and SDI IN2 must be frequency locked with each other.
- Video input format must be 1080p 3G Level A.
- Compression format must be AVC-Intra Class 100.
- Audio and ancillary data tracks are not supported.
- ShareFlex is not supported.
- Proxy file generation and scene change detection are not supported.

Configuring 4K Channels on the K2 Summit system

This feature is part of the ChannelFlex Suite.

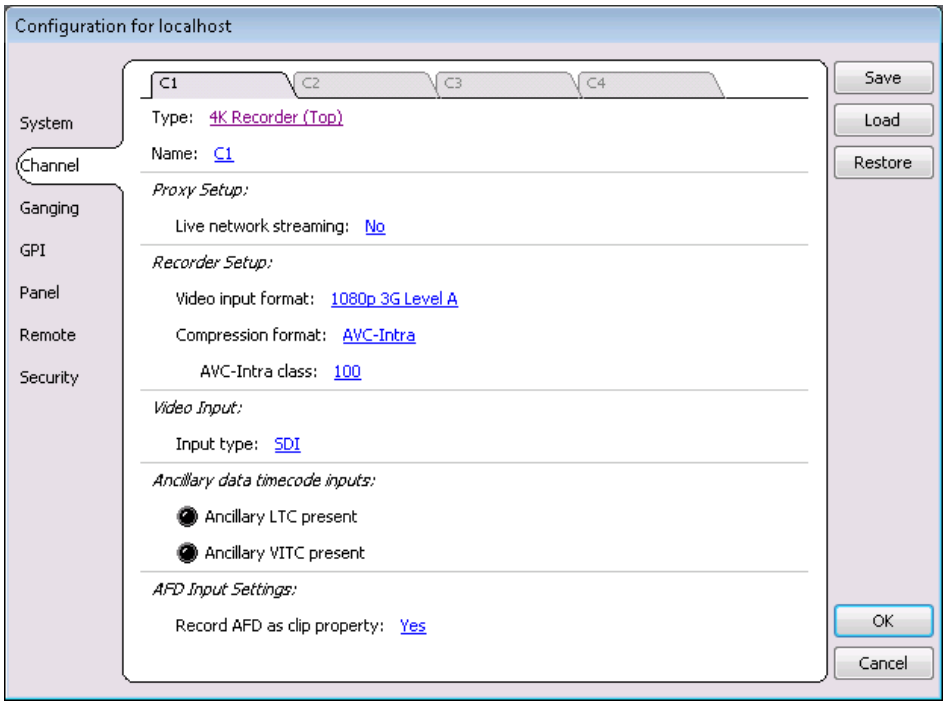
The following licenses must be installed:

- K2-APPCENTER-ELITE license
- K2-XDP-2HDL
- K2-XDP2-AVC-2CH
- K2-XDP2-3G-2CH 1080p licenses (two required to work with DynoZoom, if not only one is required)
- K2-XDP2-UHDTV1 4K licenses (two required to work with DynoZoom, if not only one is required)

NOTE: On a K2 Solo 3G system that supports DynoZoom, the DynoZoom board in the K2 Summit system and the DynoZoom Frame must be connected via PCIe and the DynoZoom Frame must be powered on before the K2 Summit system is powered on.

1. Open Configuration Manager and click **Channel**.

2. Select **C1**.



3. For Type, select **4K Recorder (Top)**.

   Only those settings supported by a 4K Recorder channel are displayed.

   NOTE: If you have the AppCenter Elite license yet the 4K Recorder option does not appear, it means you do not have the 1080p license and the 4K license, which are also required.

   When you set C1 to 4K Recorder (Top), C2 is automatically set to 4K Recorder (Bottom). No settings are available for configuration on C2, because they are automatically configured, dependent on C1 settings.

4. For **Live network streaming**, select **No**.
5. If desired, assign a name to the channel.
6. Select **C3**.
7. For Type, select **4K Player (Top)**.

   Only those settings supported by a 4K Player channel are displayed.

   When you set C3 to 4K Player (Top), C4 is automatically set to 4K Player (Bottom). No settings are available for configuration on C4, because they are automatically configured, dependent on C3 settings.

8. For **Live network streaming**, select **Yes**.
9. If desired, assign a name to the channel.
10. Save settings and close.

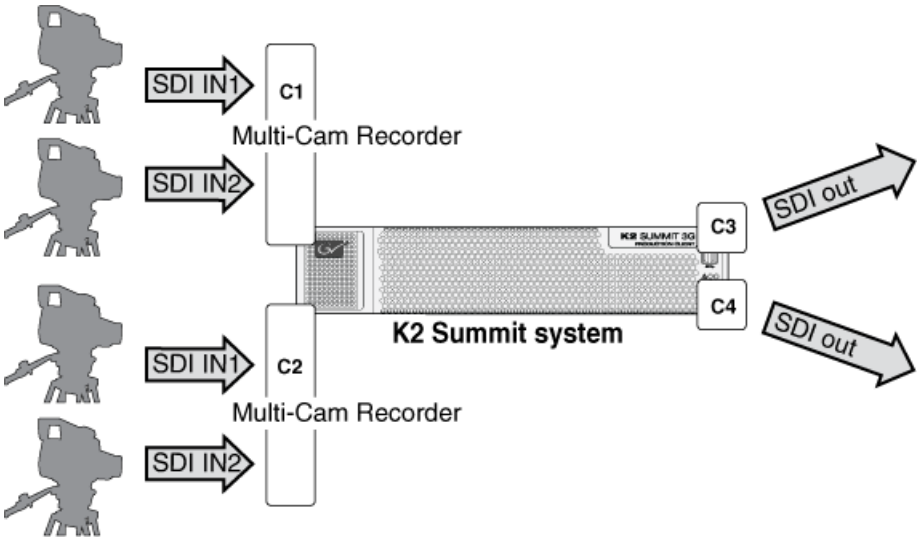
ChannelFlex Suite supported combinations

The overall load on system resources must be considered when using multiple inputs and outputs per channel on multiple channels, as each input/output stream consumes system resources. FTP

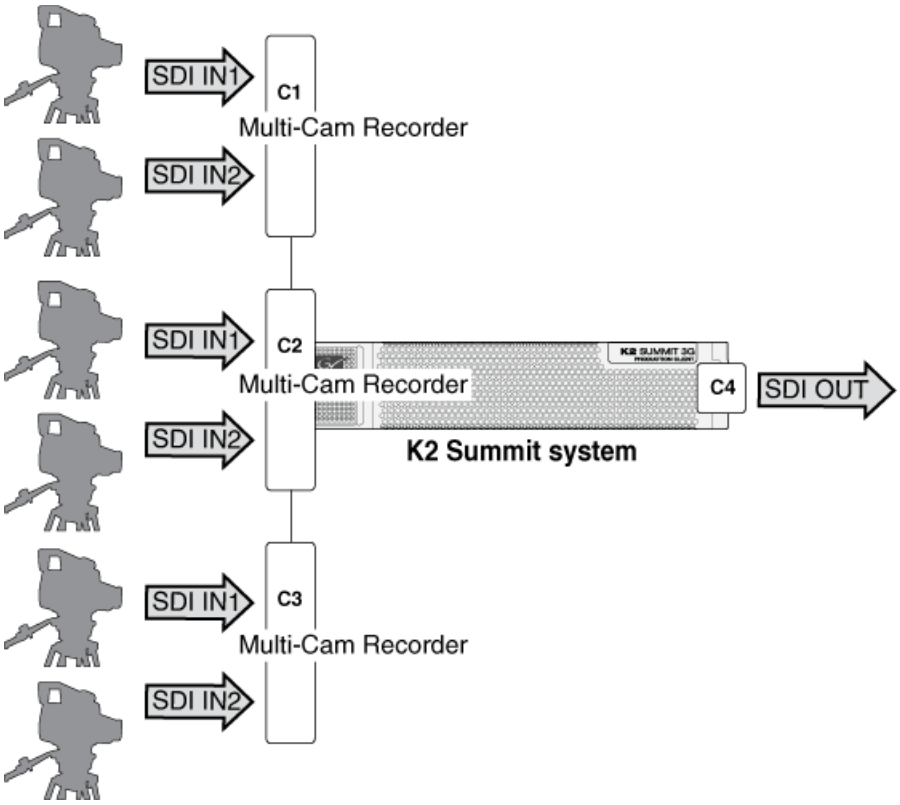
transfers, off-speed play, and media drive rebuilds also consume system resources, so they must be considered as well. The channel combinations illustrated below are typical applications that maximize ChannelFlex channels. These combinations have been qualified by Grass Valley, with the following considerations:

- These combinations assume an HD format with 100 Mbps data rate, which produces a high load on system resources.
- If you use off-speed play above 1x at the same time an FTP transfer is underway, the available FTP bandwidth can be reduced by as much as 50%.
- If a media drive rebuild is in progress it can result in a slight reduction in available FTP bandwidth.

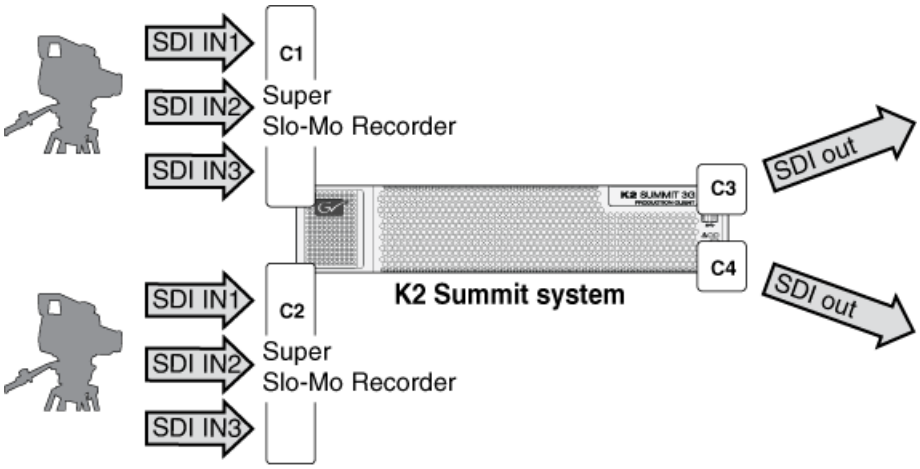
K2 Dyno Replay system, 4 IN, 2 OUT



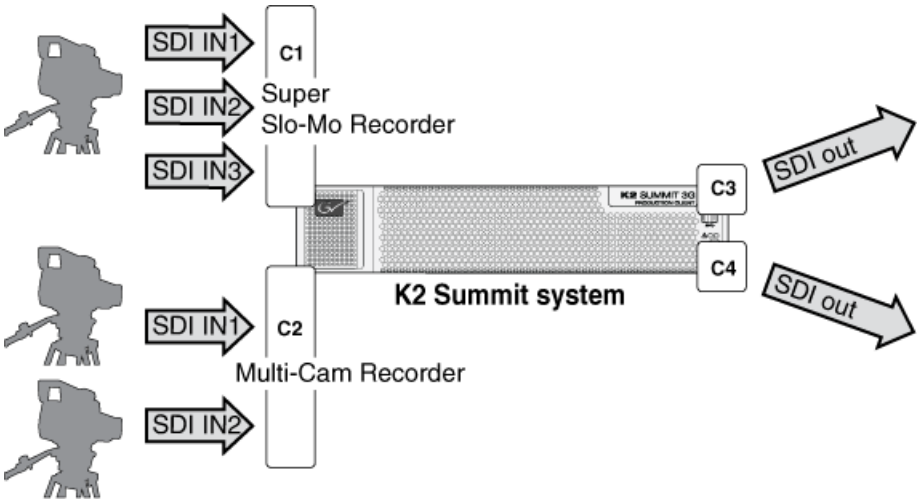
K2 Dyno Replay system, 6 IN, 1 OUT



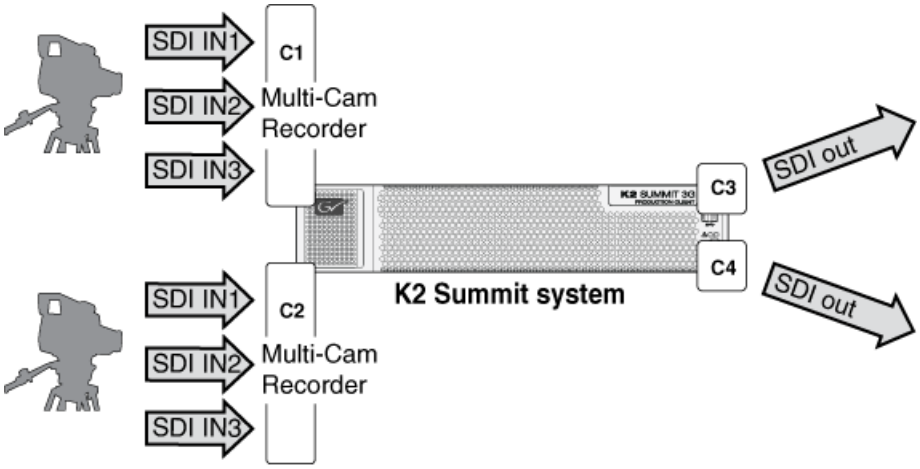
K2 Dyno Replay system, 2 (3x/6x) SSM IN, 2 OUT



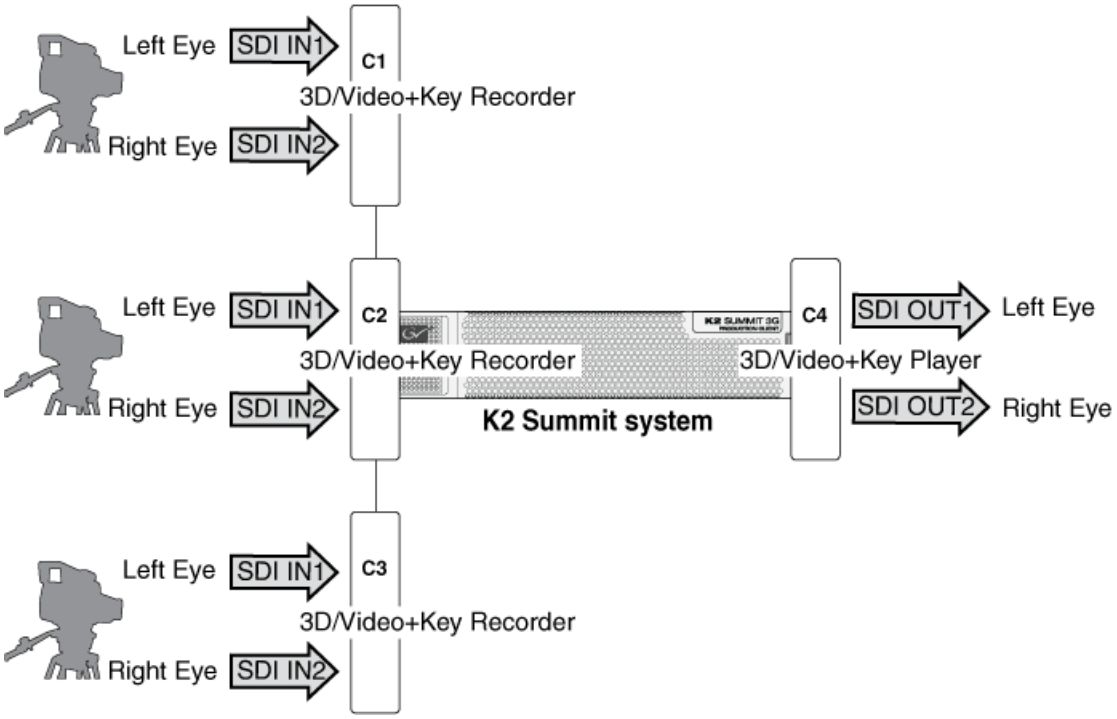
K2 Dyno Replay system, 1 (3x/6x) SSM IN, 1 Multi-Cam IN, 2 OUT



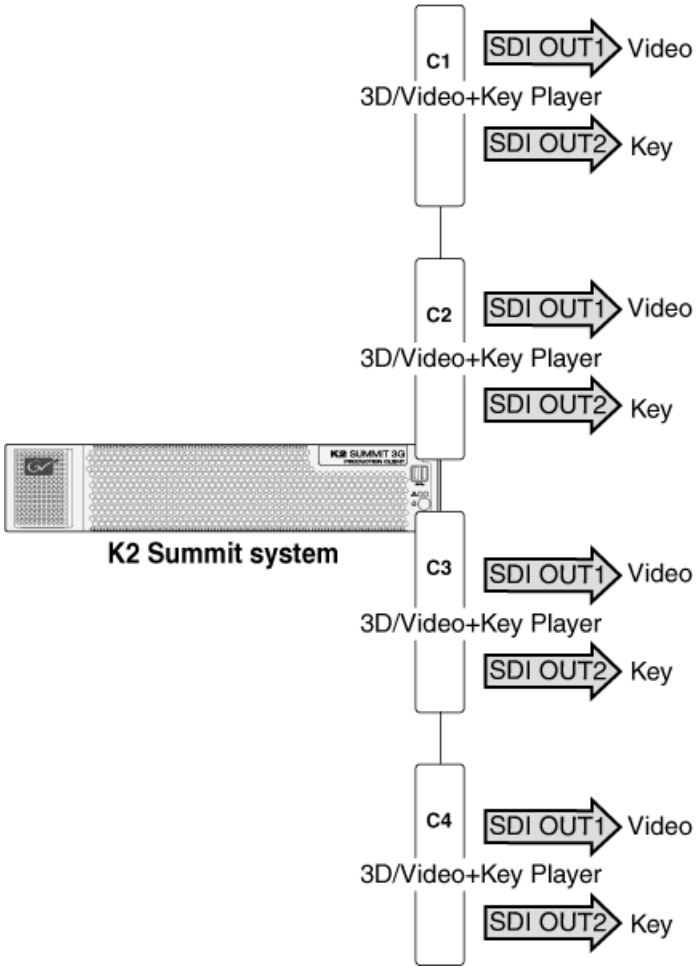
Multi-Cam, 6 IN, 2 OUT



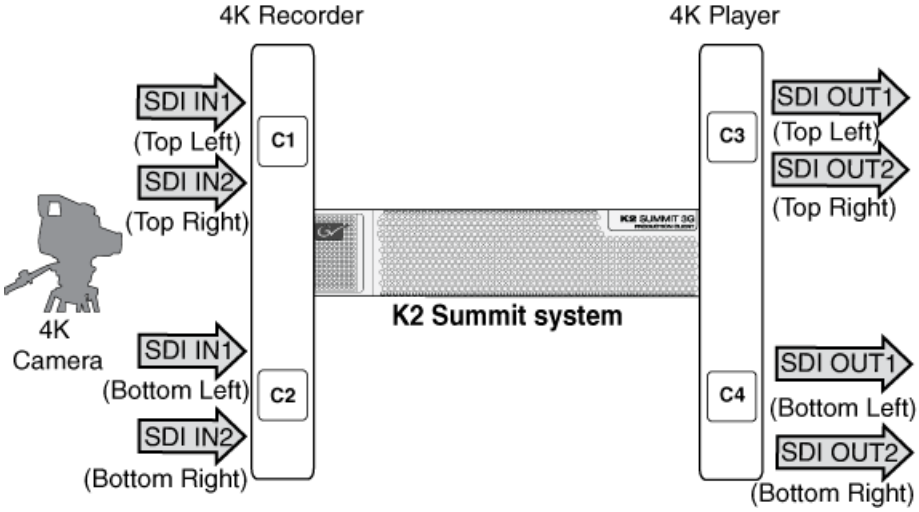
3D – 3 L/R Eye IN, 1 L/R Eye OUT



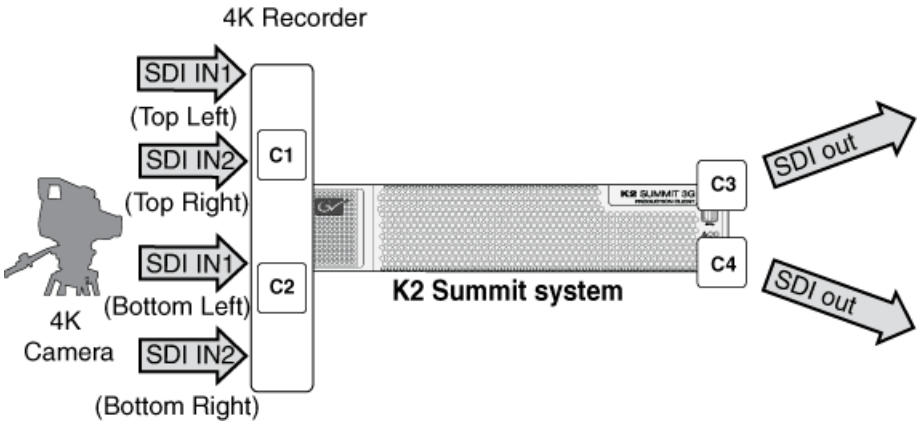
Key/Fill Playout



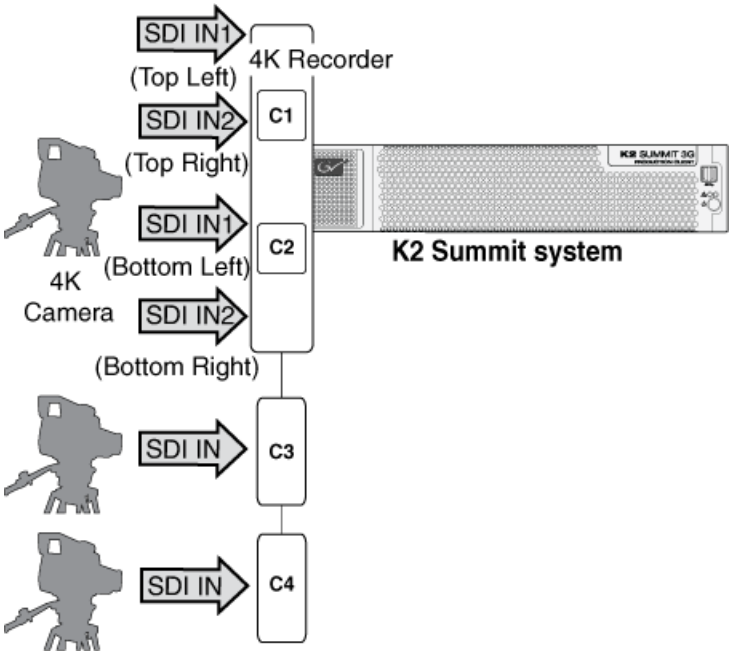
4K – 4 IN, 4 OUT



4K – 4 IN, 2 OUT



4K – 6 IN



About introducing ChannelFlex Suite on existing K2 systems

When you upgrade to a K2 system software version that supports ChannelFlex Suite and then begin to use ChannelFlex Suite features, you increase the number of inputs and outputs on the K2 Solo 3G system. To support this increased load on system resources, you must adjust your system, as follows:

- Standalone K2 Solo 3G system – This includes standalone K2 Summit systems, direct-connect storage K2 Summit systems, and K2 Solo Media Servers. These system require an updated RTIO setting. You must update this setting when you upgrade.

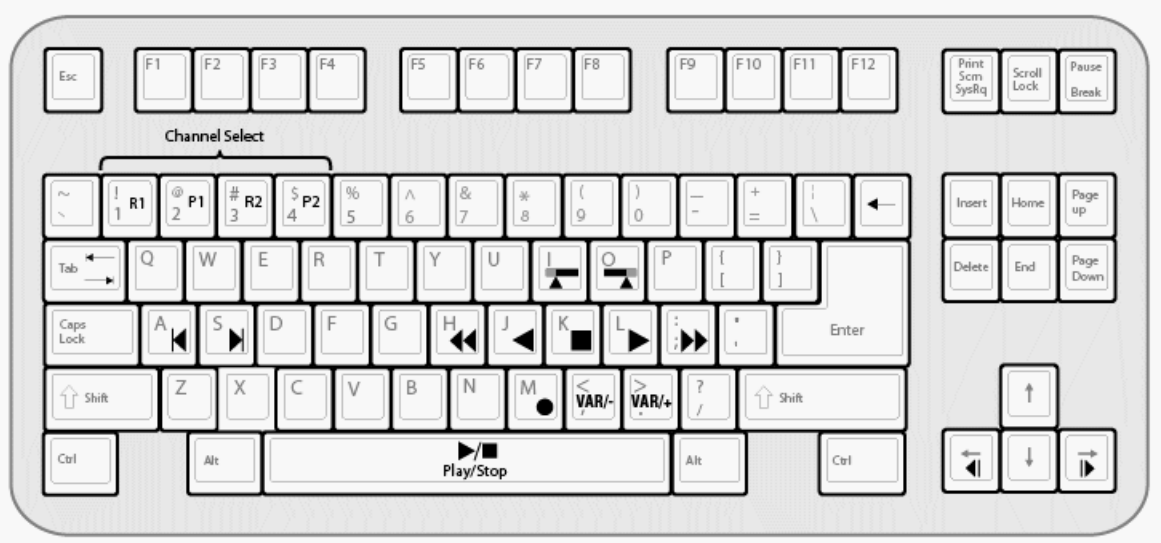
- K2 SANs – These system might require additional disks for bandwidth and additional K2 Media Servers to act as iSCSI bridges (TOEs), depending on the number and type of inputs and outputs you are adding by your use of ChannelFlex Suite features. Contact your Grass Valley representative to evaluate your system and its suitability for supporting your use of ChannelFlex Suite.

Keyboard Shortcuts

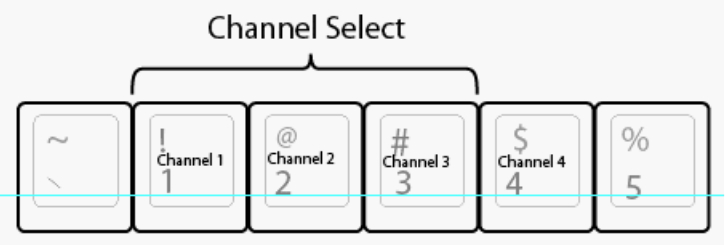
About keyboard operation

A keyboard can be used to control the K2 Solo 3G system. A full keyboard is shown below.

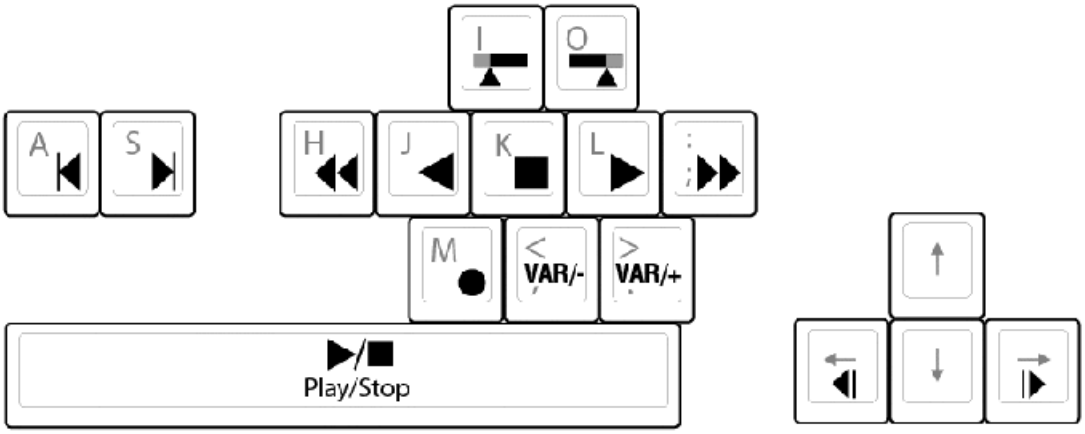
NOTE: Keyboard shortcuts are disabled when text entry dialog boxes are open.



Channel select controls



Basic transport controls



Off-speed play controls

For this action...	Press
Play faster	Shift + L (Repeat this key sequence to increment the play speed up to the maximum forward shuttle speed.)
Play slower	Shift + J (Repeat this key sequence to decrement the play speed up to the maximum reverse shuttle speed.)
VAR/speed increment	period (.) (Press for VAR play mode, then repeat to increment VAR speed.)
VAR/speed decrement	comma (,) (Press for VAR play mode, then repeat to decrement VAR speed.)

Shuttle speed controls

For this action...	Press	For this action...	Press
+ 0.2X speed	Shift + 1	- 0.2X speed	Ctrl + 1
+ 0.33 speed	Shift + 2	- 0.33 speed	Ctrl + 2
+ 0.5X speed	Shift + 3	- 0.5X speed	Ctrl + 3
+ 1X speed	Shift + 4	- 1X speed	Ctrl + 4
+ 1.5X speed	Shift + 5	- 1.5X speed	Ctrl + 5

For this action...	Press	For this action...	Press
+ 2X speed	Shift + 6	- 2X speed	Ctrl + 6
+ 4X speed	Shift + 7	- 4X speed	Ctrl + 7
+ 9X speed	Shift + 8	- 9X speed	Ctrl + 8
+ 16X speed	Shift + 9 (see Note A below)	- 16X speed	Ctrl + 9 (see Note A below)
+ 32X speed	Shift + 0 (see Note B below)	- 32X speed	Ctrl + 0 (see Note B below)

NOTE: A) If shuttle speed, as configured in Configuration Manager, Panel, is set to "+16X to -16X"

NOTE: B) If shuttle speed, as configured in Configuration Manager, Panel, is set to "+ 32X to - 32X"

Speed controls are not cumulative. Each keyboard shortcut sets speed relative to baseline normal (zero) speed, rather than adding/subtracting from current speed.

Stop-Mode transport controls

For this action...	Press
Cue to mark-in	A, Shift + I
Cue to mark-out	S, Shift + O
Next frame	Arrow-right
Previous frame	Arrow-left
Go forward 1 second	Shift + Arrow-right
Go back 1 second	Shift + Arrow-left

Mark-Point and Cue controls

For this action...	Press
Set mark-in	I
Set mark-out	O
Clear mark-in	Ctrl + I
Clear mark-out	Ctrl + O

Miscellaneous controls

Action	Press
Live Play (Chase Play)	Ctrl + L (To toggle back to the regular setting, press the Space bar
Copy	Ctrl + C
Cut	Ctrl + X
Paste	Ctrl + V
Open online help	

List controls

The following shortcuts are used to control lists such as text view in Clips pane, or Playlist's List view.

Action	Press
Select previous item in list	Up arrow
Select next item in list	Down arrow
Scroll to previous page	Page Up
Scroll to next page	Page Down
Scroll to top of list	Home
Scroll to bottom of list	End
Delete current selection	Delete, Backspace

Playlist controls

Action	Press
Next event	Shift + S, Ctrl + S, Ctrl + Arrow-right
Previous event	Shift + A, Ctrl + A, Ctrl + Arrow-left

Action	Press
Next section	Shift + Ctrl + S, Shift + Ctrl + Arrow-right
Previous section	Shift + Ctrl + A, Shift + Ctrl + Arrow-left
Goto an event	Hold down the Alt key while clicking the event

Remote control protocols

About remote control protocols

This section provides information for using remote control protocols to operate K2 Solo 3G systems. It is intended for use by installers, system integrators, and other persons responsible for setting up automation systems at a customer site.

For information about configuring AppCenter to enable protocol control of a K2 channel, refer to topics in the "Using K2 AppCenter" section of the K2 Topic Library.

Using AMP protocol to control K2 systems

Advanced Media Protocol (AMP) is an extension of the Odetics protocol.

AMP commands are available via Ethernet or RS-422 serial ports.

The automation setting for preroll should be at least 10 frames.

Preroll is 1 second for mixed compression format playout. Preroll is 10 frames for same compression format playout.

The AMP's socket interface uses IANA assigned port number 3811 for TCP.

In AppCenter, you must set a channel’s options to enable protocol control of the channel. Subsequently, when the K2 Solo 3G system starts up, the channel is immediately available for protocol control. Manual log on is not required.

For channels in gang mode, the protocol must connect to the lowest numbered channel in the gang. This is required to support jog/shuttle of ganged channels.

AMP Two-Head Player Model

The AMP protocol supports the use of a *two-head player model* in that two clips can be loaded for playout, as follows:

- Current clip — The AMP “preset id” is the active clip.
- Preview clip — The AMP “preview preset id” is the preview clip. The preview clip becomes the current clip and begins playing when the current clip completes. When controlling AMP in Auto mode, the “in preset” (and “out preset”) command should be sent before the Preview in commands.

Related specifications are as follows:

- A 3D/Video+Key player channel does not support a two-head player model.

Controlling transfers with AMP

Remote control automation applications can initiate transfers via AMP. The AMP command must be sent to the K2 Solo 3G system, not the K2 Media Server. This applies to both stand-alone and shared storage K2 systems.

If using AMP to initiate transfers between K2 systems and Profile XP systems, you must send the AMP command to the K2 system, not the Profile XP system. Transfers (both push and pull) are successful if the K2 system hosts the command. Transfers fail if the Profile XP system hosts the command.

Transfers initiated by AMP between K2 systems and M-Series iVDRs are not supported.

AMP channel designations

When using AMP protocol with Ethernet and the K2 Solo 3G system, the first port maps to the first channel, the second port maps to the second channel, and so on.

AMP internationalization

AMP supports UTF-8 2 and 3 byte characters. Unicode movie names pass through as opaque bits.

Using VDCP protocol to control K2 systems

Video Disk Control Protocol (VDCP) commands are available via RS-422 serial ports.

Preroll is 1 second for mixed compression format playout. Preroll is 10 frames for same compression format playout.

The K2 AppCenter Recorder application in protocol mode allows a default bin to be assigned to each record channel.

In AppCenter, you must set a channel's options to enable protocol control of the channel. Subsequently, when the K2 Solo 3G system starts up, the channel is immediately available for protocol control. Manual log on is not required.

For channels in gang mode, the protocol must connect to the lowest numbered channel in the gang. This is required to support jog/shuttle of ganged channels.

Loop-play mode on the K2 Solo 3G system is not supported under VDCP control.

The following categories of VDCP commands are not supported:

- Deferred (Timeline) Commands --these are the basic timeline commands but use the time specified by the PRESET STANDARD TIME
- Macro commands
- Archive Commands

- To control a given K2 channel, use only that channel's specific RS-422 rear panel connector. Send the VDCP "Open Port" and "Select Port" commands only to the RS-422 connector that is associated with the channel being controlled.

VDCP two-head player model

The VDCP protocol supports the use of a *two-head player model* in that two clips may be loaded for playout, as follows:

- Current clip — The VDCP "preset id" is the current clip.
- Preview clip — The VDCP "preview preset id" is considered the preview clip. When a play command is received, the preview clip becomes the active clip and begins playing after the preroll time has passed. If a play command has not been issued by the end of the clip, playout stops according to the VDCP end mode settings for that channel (last frame, black, first frame of preview clip).

Related specifications are as follows:

- A 3D/Video+Key player channel does not support a two-head player model.

Controlling transfers with VDCP

Remote control automation applications can initiate transfers via VDCP. The VDCP command must be sent to the K2 Solo 3G system, not the K2 Media Server. This applies to both stand-alone and shared storage K2 Solo 3G system.

If you are using VDCP to perform video network transfers, you must configure the K2 Solo 3G system so that there is a unique Controller ID for each host.

If using VDCP to initiate transfers between K2 systems and Profile XP systems, you must send the VDCP command to the K2 system, not the Profile XP system. Transfers (both push and pull) are successful if the K2 system hosts the command. Transfers fail if the Profile XP system hosts the command.

Transfers initiated by VDCP between K2 systems and M-Series iVDRs are not supported.

VDCP internationalization

VDCP does not support UTF-8 or Unicode, so use ASCII only for clip names and bin names.

PitchBlue workflow considerations

The K2 Solo 3G system supports the H.264 format used in the PitchBlue workflow. However, you must consider the intended PitchBlue workflow when using this H.264 media, as it is not supported for general purpose use outside of the PitchBlue workflow.

The K2 Solo 3G system ingests the PitchBlue material without any error correction. The material often has anomalies, such as incomplete last frame, that the K2 Solo 3G system accepts as-is. When PitchBlue plays out this material under VDCP automation control, it plays the known-good material only. The automation playout system tracks the portions of the imported PitchBlue content for playout by interacting with the traffic and other related playout automation components. Anomalies

can be identified so that they are not played out. In this way, the automation playout system avoids the errors that would otherwise occur if the material were used for general purpose playout without automation control.

Therefore, you must adhere to the complete PitchBlue workflow from ingest through playout for all PitchBlue material. Do not attempt to play out PitchBlue material except as part of the prescribed PitchBlue workflow.

NOTE: Playing out PitchBlue material in any other way can cause errors.

Using BVW protocol to control K2 systems

BVW commands are available via RS-422 serial ports.

A subset of BVW commands is supported through AppCenter in protocol mode.

Insert/Edit is not supported.

In AppCenter, you must set a channel's options to enable protocol control of the channel. Subsequently, when the K2 Solo 3G system starts up, the channel is immediately available for protocol control. Manual log on is not required.

For channels in gang mode, the protocol must connect to the lowest numbered channel in the gang. This is required to support jog/shuttle of ganged channels.

To set in and out points with BVW protocol, load clips only from the working bin.

Special considerations for automation vendors

The following information is provided for your convenience as you set up your chosen automation product to control K2 systems. Consult your automation vendor for complete information.

Harris settings

The Harris automation product uses VDCP protocol.

The following settings are required for the Harris automation product:

Setting	Mixed compression format playout	Same compression format playout	Comments
Disk Prerolls	1 second	10 frames	—
Frames to send Play early (Preroll Play)	1 second	10 frames	These two settings should be the same as the Disk Prerolls setting. However, if there is extra fixed latency in your RS-422 communication path, you might need to adjust the settings differently.
Frames to send Record early (Preroll Record)	1 second	10 frames	
Disk Port Comm Timeout	60 frames	60 frames	This is the minimum required by K2. Do not use the Harris default value, which is 10.

Setting	Mixed compression format playout	Same compression format playout	Comments
Back To Back Rec	Unchecked	Unchecked	K2 does not support this feature.

RS-422 protocol control connections

You can control the K2 Solo 3G system with remote control devices and software developed for the K2 system that use industry-standard serial protocols: AMP, BVW, and VDCP. (AMP protocols can also use Ethernet connections.) You can connect one RS-422 cable to each channel. Each RS-422 connection controls the channel to which it is connected only. Connect the RS-422 cabling as required, then refer to topics in the "Using K2 AppCenter" section of the K2 Topic Library to configure the K2 system for remote control.

Specifications for the RS-422 connection are as follows:

- Data Terminal Equipment (DTE)
- 38.4K Baud
- 1 Start bit
- 8 Data bits
- 1 Parity bit
- 1 Stop bit

Security and protocol control

The K2 security features can be configured to restrict protocol control of channels.

Specifications

K2 Summit Transmission models specifications

Refer to the section about K2 Summit Transmission models for specifications unique to that system. If a specification is not unique to a K2 Summit Transmission model, then the general K2 Solo 3G system specification found in this section applies.

AC power specification

Table 7: K2 Summit 3G AC power specification

Characteristic	Specification
Power supply	Dual, redundant
Mains Input Voltage	90 to 260V auto-range, 47-63Hz

Characteristic	Specification
Power consumption	450W typical (standalone) 390W typical (SAN client) Maximum AC current 8A @ 115VAC, 4A @ 230VAC

The specification is shown in the following table.

Table 8: First-generation K2 Summit AC power specification

Characteristic	Specification
Power supply	Dual, redundant
Mains Input Voltage	90 to 260V auto-range, 47-63Hz
Power consumption	350W typical (standalone) 300W typical (SAN-attached) Maximum AC current 7A @ 115VAC, 3.5A @ 230VAC

The specification is shown in the following table.

Table 9: First-generation K2 Solo and K2 Solo 3G Media Server AC power specification

Characteristic	Specification
Power supply	Single
Mains Input Voltage	100-240V, 50/60 Hz
Power consumption	180W typical Maximum AC current 4A @ 115VAC, 2A @ 230VAC

⚠ ***WARNING: Always use a grounded outlet to supply power to the system. Always use a power cable with a grounded plug, such as the one supplied with the system.***

Environmental specifications

The K2 Summit 3G system specification is shown in the following table:

Characteristic	Specification
Ambient Temperature Non-Operating	-40° to +60° C
Ambient Temperature Operating	10° to +40° C

Characteristic	Specification
Relative Humidity	Operating 20% to 80% from 10° to +40° C Non-Operating 10% to 85% from -30° to +55° C Do not operate with visible moisture on the circuit boards
Operating Altitude	To 10,000 feet IEC 950 compliant to 2000 meters
Storage Altitude	To 40,000 feet
Non-Operating Mechanical Shock	30G 11 ms trapezoid
Random Vibration Operational	0.27 GRMS (5-500Hz)
Random Vibration Non-Operational	2.38 GRMS overall .019 g2/Hz (5-100Hz) .009 g2/Hz (200-350Hz) .0065 g2/Hz (500 Hz)
Equipment Type	Information Technology
Equipment Class	Class 1
Installation Category	Category II Local level mains, appliances, portable equipment, etc.
Pollution Degree	Level 2 operating environment, indoor use only.

The first generation K2 Solo 3G system specification is shown in the following table:

Characteristic	Specification
Ambient Temperature Non-Operating	-40° to +60° C
Ambient Temperature Operating	10° to +40° C
Relative Humidity	Operating 20% to 80% from 10° to +40° C Non-Operating 10% to 80% from -30° to +60° C Do not operate with visible moisture on the circuit boards
Operating Altitude	To 10,000 feet IEC 950 compliant to 2000 meters
Storage Altitude	To 40,000 feet
Non-Operating Mechanical Shock	30G 11 ms trapezoid
Random Vibration Operational	0.27 GRMS (5-500Hz)

Characteristic	Specification
Random Vibration Non-Operational	2.38 GRMS overall .0175 g2/Hz (5-100Hz) .009375 g2/Hz (200-350Hz) .00657 g2/Hz (500 Hz)
Equipment Type	Information Technology
Equipment Class	Class 1
Installation Category	Category II Local level mains, appliances, portable equipment, etc.
Pollution Degree	Level 2 operating environment, indoor use only.

Specifications vary for transmission products.

Mechanical specifications

The K2 Summit 3G Production Client specification is shown in the following table

Dimension	Measurement
Height	3.5 in (89mm)
Width	17.6 in (447 mm)
Depth [1]	24.3 in (617 mm) total 23.0 in (585 mm) rack depth
Weight:	55.0 lbs (25.0 kg) maximum

The first generation K2 Summit Production Client specification is shown in the following table

Dimension	Measurement
Height	3.5 in (89mm)
Width	17.6 in (447 mm)
Depth [2]	24.3 in (617 mm) total 23.0 in (585 mm) rack depth
Weight:	53.0 lbs (24.0 kg) maximum

The K2 Solo Media Server specification is shown in the following table

Dimension	Measurement
Height	3.5 in (89mm)
Width	8.25 in (210 mm)
Depth	17.7 in (446 mm)
Weight:	16.5 lbs (7.5 kg)

[1] Adjustable rack-mounting ears accommodate different rack depth limitations.
[2] Adjustable rack-mounting ears accommodate different rack depth limitations.

Electrical specifications

The following sections describe the electrical specifications:

Serial Digital Video (SDI)

The K2 Summit/Solo system specification is shown in the following table

Parameter	Specification
Video Standard	SD: 525 Line or 625 Line component HD: 720p or 1080i
Number of Inputs	1 per channel standard. 2 or 3 per channel when licensed for ChannelFlex Suite.
Number of Outputs	2 per channel
Data format	Conforms to SMPTE 259M (SD) and 292M (HD)
Number of bits	10bits
Embedded Audio Input	SD data format conforms to SMPTE 259M (48kHz, 20bits) HD data format conforms to SMPTE 299 48 kHz (locked to video) and 16- or 24- bit PCM Compatible with AC-3 and Dolby-E
Embedded Audio Output	Output data format is 48 kHz 24-bit User can disable embedded audio on SDI output
Connector	BNC, 75 ohm, No loop-through
nominal Amplitude	800mV peak-to-peak terminated
DC Offset	0 +0.5V
Rise and Fall Times	SD: 400 - 1500ps; measured at the 20% and 80% amplitude points HD: less than 270ps
Jitter	less than 0.2UI peak-to-peak
Max Cable Length	SD 300 meters HD 125 meters
Return Loss	greater than or equal to 15db, 5Mhz to 1.485Ghz

Genlock Reference

The K2 Summit/Solo system specification is shown in the following table:

Characteristic	Description
Signal Type	NTSC/PAL Color Black Composite Analog
Connectors	2 BNC, 75 ohm passive loop through
Signal Amplitude Lock Range	Stays locked to +6 dB and -3 dB
Input Return Loss	Greater than or equal to 36 dB to 6MHz
Tri-level sync	Supported

System Timing

The K2 Summit/Solo system specification is shown in the following table. All delay values shown are relative to Black Reference.

Characteristic	Description
Encoder timing	Derived from the video input
Nominal Playback Output Delay	Adjustable (Default: Zero timed to reference genlock)
SD Output Delay Range (Independent for each play channel)	525 lines • Frames: 0 to +1 • Lines: 0 to +524 • Samples: 0 to +1715 clock samples
	625 lines • Frames: 0 to +3 • Lines: 0 to +624 • Samples: 0 to +1727 clock samples
HD Output Delay Range (Independent for each play channel)	1080i at 29.97 FPS (SMPTE ST 274:2008) • Frames: 0 to +1 • Lines: 0 to +1124 • Pixels: 0 to +2199
	1080p at 59.94 FPS (SMPTE ST 274:2008) • Frames: 0 to +1 • Lines: 0 to +1124 • Pixels: 0 to +2199
	720p at 59.94 FPS (SMPTE ST 296:2012) • Frames: 0 to +1 • Lines: 0 to +749 • Pixels: 0 to +1649

Characteristic	Description
	1080i at 25 FPS (SMPTE ST 274:2008) • Frames: 0 to +1 • Lines: 0 to +1124 • Pixels: 0 to +2639
	1080p at 50 FPS (SMPTE ST 274:2008) • Frames: 0 to +1 • Lines: 0 to +1124 • Pixels: 0 to +2639
	720p at 50 FPS (SMPTE ST 296:2012) • Frames: 0 to +1 • Lines: 0 to +749 • Pixels: 0 to +1979
Loop through/EE	The video, AES, and LTC inputs pass to the output connectors as loop through.

AES/EBU Digital Audio

The K2 Summit/Solo system specification is shown in the following table

Parameter	Specification
Standard	AES3
Audio Inputs	4 Channels per video input/output on DB-25. Supports 32 KHz to 96 KHz inputs, which are sample rate converted to 48 KHz, 16 bit, 20 bit, or 24 bit digital audio sources.
Audio Outputs	4 Channels per video output. Audio mapping is direct and fixed. AES outputs are active at all times. Audio is output using a 48kHz clock derived from the video reference. Supports 16- or 24-bit media. On playout, audio is synchronized with video as it was recorded. Compatible with AC-3 and Dolby-E
Input Impedance	110 ohms, balanced
Audio time shift	Configurable relative to video for both record and playout.

LTC Input/Output

The K2 Summit/Solo system specification is shown in the following table

Parameter	Specification
Standard	SMPTE 12M Longitudinal Time Code, AC coupled, differential input
Number of Inputs	1 per video input - Shared 6 pin conn. with output
Number of Outputs	1 per video output
Input Impedance	1K ohm
Output Impedance	110 ohm
Minimum Input Voltage	0.1 V peak-to-peak, differential
Maximum Input Voltage	2.5 V peak-to-peak, differential
Nominal Output Voltage	2.0 V peak-to-peak differential.
LTC Reader	LTC reader will accept LTC at rates between 1/30 and 80 times the nominal rate in either forward or reverse directions.
LTC Transmitter	LTC transmitter outputs LTC at the nominal frame rate for the selected standard at 1x speed, forward direction only.

VITC Input/Output

The K2 Summit/Solo system specification is shown in the following table.

Parameter	Specification
VITC waveform	lines 10-20 NTSC (525 Line); lines 10-22 PAL (625 Line) VITC is decoded on each SDI input and inserted on each SDI output. VITC Reader configurable for a search window (specified by two lines) or set to manual mode (based on two specified lines). VITC Writer inserts VITC data on two selectable lines per field in the vertical interval. The two lines have the same data. VITC is not decoded off of the video reference input.

RS-422 specification K2 Summit 3G system

The RS-422 interface conforms to ANSI/SMPTE 207M-1997 standard (SMPTE 422).

The K2 Summit/Solo system specification is shown in the following table.

Characteristic	Description
Number of Inputs/Outputs	1 per channel
Connector type	Female RJ45

RS-422 specification first generation K2 Summit/Solo system

The RS-422 interface conforms to ANSI/SMPTE 207M-1997 standard (SMPTE 422).

The K2 Summit/Solo system specification is shown in the following table.

Characteristic	Description
Number of Inputs/Outputs	1 per channel
Connector type	Female DB9 pin

GPI I/O specifications

The K2 Summit/Solo system specification is shown in the following table.

Characteristic	Description
Number of Inputs/Outputs	12 inputs and 12 outputs.
Connector type	Female DB 25pin
GPI Input	TTL 0-0.8 V Low; 2.4-5 V High; 1 mA external current sink
GPI Output	Max Sink Current: 100 mA; Max Voltage: 30 V Outputs are open drain drivers. Max. voltage when outputs are open = 45V Max. current when outputs are closed = 250mA Typical rise times approximately 625ns Typical fall times approximately 400ns

Operational specifications

This section contains specifications related to media operations.

Video codec description K2 Summit/Solo

First generation K2 Summit Production Client, K2 Summit 3G Production Client, and K2 Solo Media Server specifications are shown in the following tables. Licenses and/or hardware options are required to enable the full range of specifications.

DV formats

Format	Sampling	Frame Rate	Data Rate	Other
DVCAM 720x480i 720x576i	4:1:1/4:2:0	29.97, 25	28.8 Mbps	Conforms to IEC 61834

Format	Sampling	Frame Rate	Data Rate	Other
DVCPRO25 720x480i 720x576i	4:1:1	29.97, 25	28.8 Mbps	Conforms to SMPTE 314M
DVCPRO50 720x487.5i 720x585i	4:2:2	29.97, 25	57.6 Mbps	Conforms to SMPTE 314M
DVCPRO HD 1280x1080i 1440x1080i	4:2:2	29.97, 25	100 Mbps	Conforms to SMPTE 370M
DVCPRO HD 960x720p	4:2:2	59.94, 50	100 Mbps	Conforms to SMPTE 370M

MPEG-2 formats

Format	Sampling	Frame Rate	Data Rate (Mbps)	Other
720x480i	4:2:0	29.97	2-15	I-frame and long GoP
720x480i	4:2:2	29.97	4-50	I-frame and long GoP
720x512i	4:2:2	29.97	4-50	I-frame and long GoP
720x576i	4:2:0	25	2-15	I-frame and long GoP
720x576i	4:2:2	25	4-50	I-frame and long GoP
720x608i	4:2:2	25	4-50	I-frame and long GoP
D10/IMX 720x512i	4:2:2	29.97	30, 40, 50 CBR	I-frame only
1280x720p	4:2:0	59.94, 50	20-80	I-frame and long GoP
1280x720p	4:2:2	59.94, 50	20-100	I-frame and long GoP
D10/IMX 720x608i	4:2:2	25	30, 40, 50 CBR	I-frame only
1920x1080i	4:2:0	29.97, 25	20-80	I-frame and long GoP[3]
1920x1080i	4:2:2	29.97, 25	20-100	I-frame and long GoP
XDCAM-HD 1440x1080i	4:2:0	29.97, 25	18 VBR, 25 CBR, 35 VBR	Long GoP

[3] Decode of lower bit rate is possible

Format	Sampling	Frame Rate	Data Rate (Mbps)	Other
XDCAM-HD422 1920x1080i	4:2:2	29.97, 25	50 CBR	Long GoP
XDCAM-HD422 1280x720p	4:2:2	59.94, 50	50 CBR	Long GoP
XDCAM-EX 1920x1080i	4:2:0	29.97, 25	35 VBR	Long GoP
XDCAM-EX 1280x720p	4:2:0	59.94, 50	25 CBR, 35 VBR	Long GoP

K2 systems record closed GoP structure. If an open GoP clip is imported, it is fully supported, including trimming the clip, playout of the clip, using the clip in playlists, and exporting the clip.

AVC-Intra formats

Format	Sampling	Frame Rate	Data Rate	Other
AVC-Intra 50 1440x1080i	4:2:0	29.97, 25	50 Mbps	Requires licenses or hardware for support on different K2 Solo 3G system models.
AVC-Intra 50 960x720p	4:2:0	59.94, 50	50 Mbps	
AVC-Intra 100 1920 x 1080i	4:2:2	29.97, 25	100 Mbps	
AVC-Intra 100 1280 x 720p	4:2:2	59.94, 50	100 Mbps	
AVC-Intra 100 1920 x 1080p	4:2:2	59.94, 50	200 Mbps	

AVCHD/H.264 formats

The following formats are for AVCHD and PitchBlue content. These are only supported for play output (decode) on AVCHD. A license is required. Record input (encode) is not supported.

Format	Sampling	Frame Rate	Data Rate	Other
720x480i	4:2:0	29.97	4-50	H.264-style open GoP. GoP length up to 30 frames. Up to 4 B-frames between anchor frames.
	4:2:2	29.97	4-50	
720x512i	4:2:2	29.97	4-50	

Format	Sampling	Frame Rate	Data Rate	Other
720x576i	4:2:0	25	4-50	
	4:2:2	25	4-50	
720x608i	4:2:2	25	4-50	
1920x1080i	4:2:0	29.97, 25	24 Mbps max.	
	4:2:2	29.97, 25	24 Mbps max.	
1440x1080i	4:2:0	29.97, 25	24 Mbps max.	
	4:2:2	29.97, 25	24 Mbps max.	
1280x720p	4:2:0	59.94, 50	24 Mbps max.	
	4:2:2	59.94, 50	24 Mbps max.	

AVC-LongG formats

The following formats are for AVC - LongG content. These are only supported for play output (decode). A license is required. Record input (encode) is not supported.

Format	Sampling	Frame Rate	Data Rate	Other
AVC-Ultra G6 1920x1080i	4:2:0	59.94, 50	6 Mbps	LongG
AVC-Ultra G6 1280x720p	4:2:0	59.94, 50	6 Mbps	
AVC-Ultra G12 1920x1080i	4:2:0	59.94, 50	12 Mbps	
AVC-Ultra G12 1280x720p	4:2:0	59.94, 50	12 Mbps	
AVC-Ultra G25 1920x1080i	4:2:2	59.94, 50	25 Mbps	
AVC-Ultra G25 1280x720p	4:2:2	59.94, 50	25 Mbps	
AVC-Ultra G50 1920x1080i	4:2:2	59.94, 50	50 Mbps	
AVC-Ultra G50 1280x720p	4:2:2	59.94, 50	50 Mbps	

Avid DNxHD formats

The following formats are for Avid DNxHD content. These are supported for record input (encode) and play output (decode). A Summit 3G Codec board with a K2-XDP2-DNX-2CH license is required.

Format	Frame Rate	Data Rate	Bits	Other
1920x1080i	29.97	220 Mbps	10	Avid DNxHD 220x
	29.97	220 Mbps	8	Avid DNxHD 220
	29.97	145 Mbps	8	Avid DNxHD 145
	25	184 Mbps	10	Avid DNxHD 185x
	25	184 Mbps	8	Avid DNxHD 185
	25	121 Mbps	8	Avid DNxHD 120
1280x720p	59.94	220 Mbps	10	Avid DNxHD 220x
	59.94	220 Mbps	8	Avid DNxHD 220
	59.94	145 Mbps	8	Avid DNxHD 145
	50	175 Mbps	10	Avid DNxHD 175x
	50	175 Mbps	8	Avid DNxHD 175
	50	116 Mbps	8	Avid DNxHD 115

Proxy/live streaming formats

The proxy files and streams created by a K2 Solo 3G system conform to industry standards, as follows.

Video: MPEG-4 Part 2

Format	Frame Rate	Data Rate (Mbps)	Other
320x240p	29.97, 25	1.5 Mbps	GOP 1 second
384x288p	29.97, 25	1.5 Mbps	GOP 1 second
512x288p	29.97, 25	1.5 Mbps	GOP 1 second

Audio: MPEG-4 Part 3 AAC-LC, 64 kbps, 48 kHz

Proxy file: MPEG-4 Part 12 Fragmented MP4 Movie

Live streaming: SDP files and RTP/RTCP streams are compliant with the following RFCs:

- RFC 3350, RFC 4566, RFC 3016, RFC 3640, RFC 5484, MPEG-4 Part 8

Playout of multiple formats

The K2 Solo 3G system automatically handles material of various types and formats as specified in the following sections:

Playout on K2 Summit/Solo

For a given frame rate, you can play SD clips of any format back-to-back on the same timeline. Both 16:9 and 4:3 SD aspect ratio formats can be played on the same timeline. Refer to video codec description earlier in this section for a list of the supported formats.

On channels with the XDP (HD) license, for similar frame rates (25/50 fps or 29.97/59.95 fps), SD material transferred or recorded into the K2 Solo 3G system along with its audio is up-converted when played on a HD output channel. Likewise, HD material is down-converted along with its audio when played on an SD output channel. HD and SD clips can be played back-to-back on the same timeline, and aspect ratio conversion is user configurable.

The K2 Solo 3G system supports mixed clips with uncompressed and compressed (PCM, AC3, and Dolby) audio on the same timeline.

25/50 fps conversions on HD K2 Solo 3G system models

The following specifications apply to K2 Solo 3G system channels with the XDP (HD) license.

		Converted SD format	**Converted HD format**	**Converted HD format**
		625 at 25 fps	**1080i at 25 fps**	**720p at 50 fps**
Source SD format	**625 at 25 fps**	No conversion	Up-convert SD to HD	Up-convert SD to HD
Source HD format	**1080i at 25 fps**	Down-convert HD to SD	No conversion	Cross-convert from 1080i to 720p
	720p at 50 fps	Down-convert HD to SD	Cross-convert from 720p to 1080i	No conversion

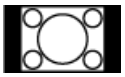
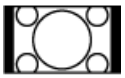
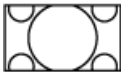
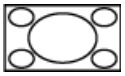
29.97/59.95 fps conversions on HD K2 Solo 3G system models

The following specifications apply to K2 Solo 3G system channels with the XDP (HD) license.

		Converted SD format	**Converted HD format**	**Converted HD format**
		525 at 29.97 fps	**1080i at 29.97 fps**	**720p at 59.94 fps**
Source SD format	**525 at 29.97 fps**	No conversion	Up-convert SD to HD	Up-convert SD to HD
Source HD format	**1080i at 29.97 fps**	Down-convert HD to SD	No conversion	Cross-convert HD to HD
	720p at 59.94 fps	Down-convert HD to SD	Convert HD to HD	No conversion

Aspect ratio conversions on HD K2 client

The following specifications apply to K2 Solo 3G system channels with the XDP (HD) license.

Source aspect ratio	Source image	Conversion option	Conversion description	Converted aspect ratio	Converted image
4:3		Bar	The 4:3 aspect ratio is maintained, centered on the screen, with black bars filling the left and right portions of the 16:9 display.	16:9	
		Half Bar	The picture aspect ratio is maintained, but the image is slightly enlarged. The top and bottom of the image are slightly cropped, and thin black bars fill the left and right portions of the 16:9 display.	16:9	
		Crop	The picture aspect ratio is maintained, but the image is enlarged so that it horizontally fills the HD display. The top and bottom of the 4:3 SD image are cropped to fit in the 16:9 display.	16:9	
		Stretch	The picture aspect ratio is distorted. The image fills the screen vertically without cropping, and is stretched horizontally to fill the 16:9 display. This conversion up-converts Full Height Anamorphic (FHA) 16:9 SD material.	16:9	
16:9		Bar	The 16:9 aspect ratio is maintained, centered on the screen, with black bars filling the top and bottom portions of the 4:3 display.	4:3	
		Half Bar	The picture aspect ratio is maintained, but the image is slightly enlarged. The left and right sides the image are slightly cropped, and thin black bars fill the top and bottom portions of the 4:3 display.	4:3	
		Crop	The picture aspect ratio is maintained, but the image is enlarged so that it vertically fills the SD display. The left and right sides of the 16:9 HD image are cropped to fit in the 4:3 SD display	4:3	

Source aspect ratio	Source image	Conversion option	Conversion description	Converted aspect ratio	Converted image
		Stretch	The picture aspect ratio is distorted. The image fills the screen horizontally without cropping, and is stretched vertically to fill the 4:3 display. This conversion generates Full Height Anamorphic (FHA) 16:9 SD material.	4:3	

Active Format Description (AFD) specifications

NOTE: This topic applies to K2 Summit/Solo systems.

Active Format Description (AFD) settings automatically determine the proper aspect ratio to use for up- and down-conversions, based on the AFD information embedded in the clip metadata. If no AFD was set on the incoming SDI input, you can assign the AFD setting in K2 AppCenter. A related setting, aspect ratio conversion (ARC), makes settings in K2 AppCenter on a clip-by-clip basis or per channel basis but does not embed settings in clip metadata.

About Active Format Description

The AFD is defined during production. By inserting metadata about the aspect ratio into the vertical ancillary data, AFD can define the aspect ratio of the signal as it progresses through ingest, editing, up/down conversion and playout. If the aspect ratio is altered during processing, then the AFD passed on downstream might need to be modified to ensure the correct aspect ratio is obtained.

NOTE: If ARC leads to unsupported active video format (postage stamp), the new AFD code will be the 'undefined' value of 0000.

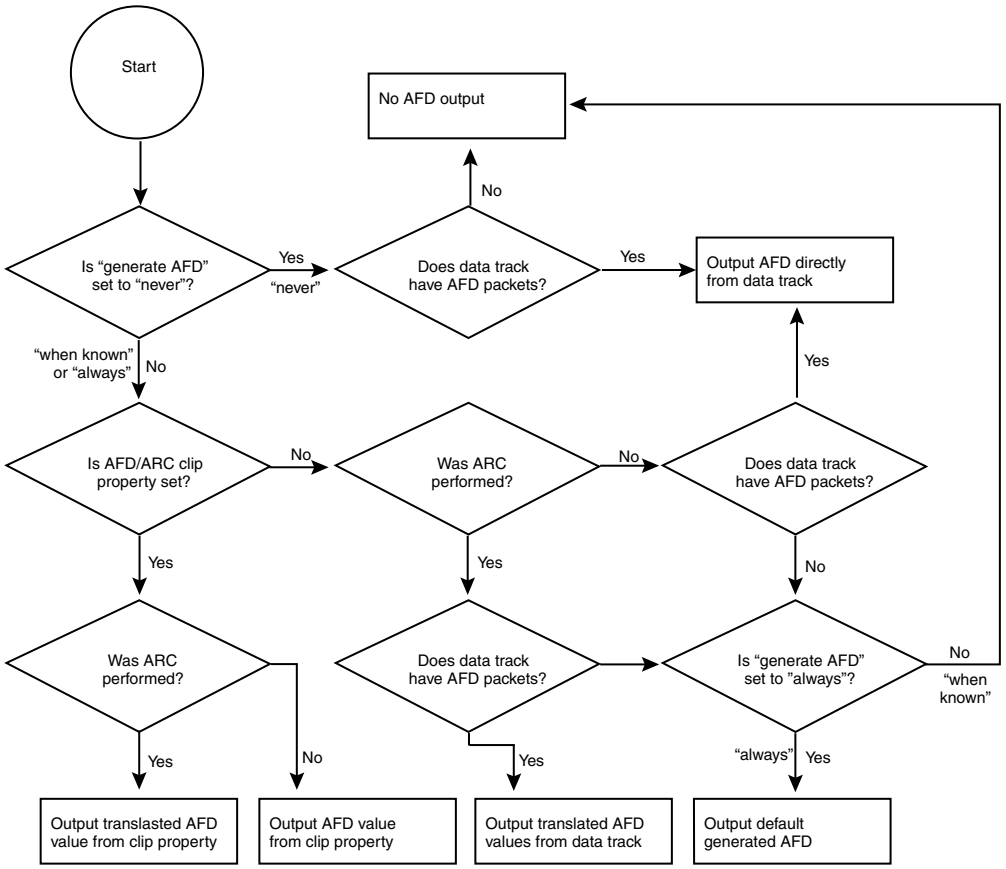
The playback Aspect Ratio Conversion (ARC) is prioritized according to the following table:

Playback aspect ratio conversion priority	
1	Clip property (ARC or AFD-based conversion rules)
2	Output channel (ARC configuration property)

NOTE: Bar data is not supported on the K2 system.

AFD output flowchart

The K2 Solo 3G system determines AFD code values in output as illustrated by the following flowchart.



Storing AFD on K2 Summit/Solo systems

The K2 Summit/Solo system stores clip metadata in clip properties and uses this data throughout the workflow. You can modify the AFD setting in AppCenter.

You can store AFD in a data track. Grass Valley recommends selecting this for HD clips; if using SD, this is optional. This method takes more storage (it is approximately equal to four tracks of audio) but this method enables AFD and CC/Teletext support for HD.

Ingesting SDI

An SDI video signal stores AFD in the vertical ancillary data. The K2 Solo 3G system processes the signal as follows:

- If present, the AFD setting from two seconds into the file is copied into the clip properties. This is the default K2 system behavior and occurs unless you set it to **No** in Configuration Manager.
- If selected, the ANC data is copied into the K2 data track.

Using AFD with file transfers

The following tables describe the AFD file priorities and the AFD behavior with GXF and MXF transfers.

File transfer AFD priority	
1	AFD from the MXF or GXF metadata is copied to the K2 clip properties.
2	If the MXF stream contains an ancillary data track with AFD ancillary data packets and Active Format Descriptor attribute of the Generic Picture Essence descriptor in the MXF header metadata is absent, then the AFD value for the K2 clip is derived from the AFD ancillary data packet located around 2 seconds into the material. That AFD value is then copied to the K2 clip properties.
3	If there is no AFD in the MXF, the GXF, or the data track, then no AFD is set.

GXF Export: (both AFD and ARC values inserted into XML of stream)	
Condition	**Description**
Exported to K2 system that does not support AFD	AFD setting is ignored, but setting is retained with clip ARC settings apply
Exported to K2 system that supports AFD	AFD overrides ARC settings

GXF Import	
Condition	**Description**
Imported from K2 system that does not support AFD	ARC converted to AFD
Imported from K2 system that supports AFD	AFD overrides ARC settings

MXF Export	
Condition	**Description**
AFD from clip property added to properties of the video in the header metadata	If clip property is not set, do not add property in stream
AFD from data track in stream's ancillary data	No change required

ARC is K2 specific and therefore not included in MXF transfers.

MXF Import	
Imported stream has AFD in the header metadata	AFD is stored in the clip property setting of the clip
Imported stream has AFD in the data track	AFD is stored in the clip property setting of the clip. (AFD is taken from the ancillary data two seconds from the beginning, or, if the clip is less than 2 seconds long, from the last valid AFD.)
Imported stream has no AFD	No AFD

ARC is K2 specific and therefore not included in MXF transfers.

Default generated AFD values

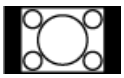
Default AFD values are generated when the three following conditions are met:

- The AFD output setting in the Configuration Manager is set to **Always**
- The clip does not have AFD in the data track, and
- The clip does not have AFD specified in its clip properties

Under these conditions, default AFD is generated and inserted, based on ARC performed and the source material format. Default generated AFD settings are described in the table below.

Default generated AFD values when up-converting to HD

Source image is presumed based on the conversion that has been selected.

Source aspect ratio	Presumed source image	Conversion option	Converted AFD and aspect ratio	Converted image
16:9 HD		No conversion	AFD = 1010 AR = 16:9 HD	
16:9 SD		Scale up Crop vertical	AFD = 1010 AR = 16:9 HD “crop”	
		Scale up	AFD = 1010 AR = 16:9 HD	
		Scale up Crop vertical Pillarbox	AFD = 1011 AR = 16:9 HD “half bars”	
4:3 SD		Scale up Pillarbox	AFD = 1011 AR = 16:9 HD “bars”	

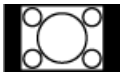
Default generated AFD values when down-converting to SD

Source image is presumed based on the conversion that has been selected.

Source aspect ratio	Presumed source image	Conversion option	Converted AFD and aspect ratio	Converted image
4:3 SD not widescreen		No conversion	AFD = 1001 AR = 4:3 SD	
16:9 SD widescreen		No conversion (only if ARC set to ‘stretch’)	AFD = 1010 AR = 16:9 SD	

Source aspect ratio	Presumed source image	Conversion option	Converted AFD and aspect ratio	Converted image
16:9 HD		Scale down letterbox	AFD = 1010 AR = 4:3 SD "bars"	
		Scale down Crop horizontal	AFD = 1001 AR = 4:3 SD "crop"	
		Scale down	AFD = 1010 AR = 16:9 SD "stretch"	
		Scale down Crop horizontal Letterbox	AFD = 1011 AR = 4:3 SD "half bars"	

Supported conversions from SD to HD using AFD

Source AFD and aspect ratio	Source image	Conversion performed	Converted AFD and aspect ratio	Converted image
AFD = 1010 AR 4:3 SD		Scale up crop vertical	AFD = 1010 AR 16:9 HD	
AFD = 1000 or 1001 AR 4:3 SD		Scale up pillarbox	AFD = 1001 AR 16:9 HD	
AFD = 1010 AR 16:9 SD		Scale up	AFD = 1010[4] AR 16:9 HD	
AFD = 1011 AR = 4:3 SD		Scale up Crop vertical pillarbox	AFD = 1011 AR 16:9 HD	

[4] You can change the default converted value of AFD = 1010 to be AFD = 1001. This setting is in K2 AppCenter Configuration Manager play channel video settings.

Supported conversions from HD to SD using AFD

Source AFD and aspect ratio	Source image	Conversion performed	Converted AFD and aspect ratio	Converted image
AFD = 1000 or 1010 AR = 16:9		Scale down letterbox	AFD = 1010 AR = 4:3[5]	
AFD = 1001 AR = 16:9		Scale down crop horizontal	AFD = 1001 AR = 4:3	
AFD = 1010 AR = 16:9		Scale down	AFD = 1010 AR = 16:9[6]	
AFD = 1011 AR = 16:9		Scale down Crop horizontal letterbox	AFD = 1011 AR = 4:3	
AFD = 1111 AR = 16:9		Scale down crop horizontal	AFD = 1001 AR = 4:3	

VBI/Ancillary/data track specifications

This section contains topics about data carried in the media file.

VBI/Ancillary/data track definitions

Terms in this section are defined as follows:

Ancillary data	Ancillary data (ANC data) as specified in this section is primarily a means by which timecode, Closed Captioning, and Teletext information is embedded within the serial digital interface. Other Type 2 ancillary data packets are stored and played back without modification. Ancillary data is standardized by SMPTE 291M.
Closed Captioning (CC)	Line 21 NTSC Closed Captioning as defined in EIA-608 and used as a subset of EIA-708. EIA-708 has been updated and renamed to CEA-708. Includes other Line 21 services such as V-Chip.
Teletext (TT)	Teletext System B subtitles as defined ETSI EN 300 706 and other documents. The Australian standard for digital TV is Free TV Operational Practice OP-47. It has been ratified as SMPTE RDD 8.
Captioning	Denotes both NTSC Closed Captioning and Teletext subtitling.

[5] When play channel video settings Aspect Ratio is set to "Standard (4:3)"
[6] When play channel video settings Aspect Ratio is set to "Widescreen (16:9)"

Luma/Chroma VBI support on K2 Summit/Solo

Record and playout of VBI is supported for both Luma and Chroma. However, a given line of VBI data can be stored as either Luma or Chroma, but not both.

VBI data support on K2 Summit/Solo

The following table applies when in Configuration Manager, the Data Track settings are configured as:

- Record ancillary data: No

Or as:

- Record ancillary data: Yes
- Record Uncompressed VBI and captioning data to track: No

Use these Data Track settings to retain compatibility with legacy systems, such as the Profile XP Media Platform.

Video format	Compressed VBI	Uncompressed VBI	Captioning	Comments
DVCPRO25 525 line (NTSC)	Not supported	Not supported by DVCPRO25 format	CC supported, as native to DVCPRO25. VCHIP data supported.	—
DVCPRO25 625 line (PAL)	Not supported	Not supported by DVCPRO25 format	TT not supported as VBI data.	
DVCPRO50 525 line (NTSC)	Supported for playout	Not supported by DVCPRO50 format	CC supported, as native to DVCPRO50 (compressed VBI). VCHIP data supported.	—
DVCPRO50 625 line (PAL)	Supported for playout	Not supported by DVCPRO50 format	TT supported, as native to DVCPRO50 (compressed VBI).	—
DVCAM 525 line (NTSC)	Not supported	Not supported by DVCAM format	CC supported, as native to DVCAM.	—
DVCAM 625 line (PAL)	Not supported	Not supported by DVCAM format	TT not supported as VBI data.	—

Video format	Compressed VBI	Uncompressed VBI	Captioning	Comments
MPEG-2 525 line (NTSC)	Supported as 16 lines per field. Range: 7–22	Supported for record. Not supported for playout.	CC supported and always on. Not selectable.	—
MPEG-2 625 line (PAL)	Supported as 16 lines per field. Range: 7–22	Supported for record. Not supported for playout.	TT supported only as compressed or uncompressed VBI.	—
MPEG-D10 525 line (NTSC)	Supported	Not supported by D10 format.	CC supported, as native to D10.	—
MPEG-D10 625 line (PAL)	Supported	Not supported by D10 format.	TT supported, as native to D10.	—

Data track support on K2 Summit/Solo SD channels

The following table applies to SD channels when in Configuration Manager the Data Track settings are configured as follows:

- Record ancillary data: Yes
- Record Uncompressed VBI and captioning data to track: Yes

Video format	Data	Supported as follows:
525 line (NTSC)	Closed Captioning	Stored in EIA-708 packets. On playback, modulate to VBI line 21.
625 line (PAL)	Teletext	Stored in OP-47 packets. On playback, modulate to VBI line specified in OP-47 packet.
All supported SD formats	Uncompressed VBI	Selectable per line. Limited to 5 lines. The 5 line limit does not include any lines used for CC or TT. Can select either Luma or Chroma for each line, but not both.
	Ancillary timecode	Ancillary timecode is preserved only. No timecode track is constructed from ancillary timecode data. The timecode track is not inserted as ancillary timecode on playout.

Data track support on K2 Summit/Solo HD channels

On channels with the XDP (HD) license, the data track can contain ancillary data and other types of data. Luma ancillary data packets are stored. Chroma ancillary data packets are not supported.

Data	Supported as follows:
Ancillary timecode	For record, selectable to use VITC or LTC ancillary timecode as timecode source. For playout, selectable to insert recorded timecode track as ancillary data VITC or LTC timecode packets. If the recorded timecode track is inserted as VITC ancillary timecode and VITC ancillary timecode packets are already stored on the data track, then the recorded timecode track overrides the stored VITC ancillary timecode packets. If the recorded timecode track is inserted as LTC ancillary timecode and LTC ancillary timecode packets are already stored on the data track, then the recorded timecode track overrides the stored LTC ancillary timecode packets.
Vertical interval ancillary data packets	Extracted at input and stored on an ancillary data track. Upon playout, the data packets are inserted into the video stream on specified lines. Maximum 8 packets per field. CC and TT supported as native to format.

Captioning system support

An API is provided for access to captioning data, allowing Closed Captioning and Teletext systems to produce timecode correlated captions for an existing K2 clip.

CEA 608 to CEA 708 DTV CC Transcoder and FCC requirements

Federal Communications Commission (FCC) rules incorporate sections of industry standards EIA-708 and EIA-608. The K2 Summit/Solo system fulfills the requirement for older materials that do not have DTV CC. If SD material has EIA-608 CC present, the K2 Summit/Solo system can be configured so that when it up-converts the material the EIA-708 packet contains the EIA-608 data plus the DTV CC transcoded from EIA-608.

DTV CC transcoding is enabled on a per channel basis in the Configuration Manager under **Channel Configuration**. By default, transcoding is disabled and the behavior is the same as prior software releases that did not support this transcoding. When enabled, transcoding is applied to any CEA 708 packets played out to either 1080i or 720p outputs (NTSC timing only). Transcoding happens for the following cases:

- SD clips are recorded with CC on the data track.
- SD MPEG clips with CC in the MPEG user data.
- DVCPRO25 clips with CC in the DV frame.
- HD clips with CEA 708 packets on the data track that have Line 21 data is present and DTV CC is absent.

CEA 608 commands from the above sources are converted to CEA 708 DTV CC commands that generate caption presentations that are similar to the original CEA 608 captions. The appearance is similar but not the same due to the differences in fonts, text positioning, etc.

This applies to up-conversion only. HD material should already have compliant EIA-708 packets.

About privately defined data packets

In ancillary data, the K2 Solo 3G system supports data defined by a private organization. This is data that is not defined and registered with SMPTE.

For example, if a facility puts privately defined data as special "triggers" in their stream for downstream devices, these triggers are preserved on record and transfer and played with field accuracy when needed. SMPTE standard data is supported as well as the privately defined data, for fully compliant, field accurate data track support.

Data bridging of VBI information on K2 Summit/Solo HD channels

On channels with the XDP (HD) license, data is bridged as follows:

Source format	Source data	Conversion ——>	Converted format	Converted data
SD 525 line	Closed-captioning (CC) on line 21 (EIA-608) can be stored as UserData[7] CC packets or UserData VBI Line21 (Uncompressed VBI Line21)	Up-convert	HD	Ancillary Closed Caption EIA-708-B packets
	EIA-708	Up-convert	HD	EIA-708
SD 625 line	Teletext (except as below)	No up-conversion to HD		
	5 lines of VBI Teletext in OP-47 packets	Up-convert	HD	OP-47 ancillary data packet in SD data track file. SD Teletext is in ancillary data location as specified in OP-47 packet.
SD 625 line 525 line	Ancillary data	Up-convert	HD	Moved to valid lines
HD	EIA-708 & 608 Ancillary data packets	Down-convert	SD	Closed-captioning on line 21 (EIA-608 standard).
HD	Teletext as OP-47 packets	Down-convert	SD	Output as VBI waveforms on lines specified in OP-47 packet or as specified by "Teletext Output Lines" data track settings in AppCenter Configuration Manager.
HD 1080i	Ancillary data	Cross-convert	HD 720p	Moved to valid lines.
HD 720p	Ancillary data	Cross-convert	HD 1080i	Moved to valid lines. Any data on lines 21-25 is moved to line 20 on 1080i output.

Line mapping of ancillary data packets on K2 Summit/Solo HD channels

On channels with the XDP (HD) license, you can use "Output OP-47 packet on line" data track settings in AppCenter Configuration Manager to specify that all OP-47 packets are output on the selected video line during playout.

[7] UserData CC packets always on. If CC exists, it is recorded and played back. MPEG UserData can be played out but not recorded.

Source format	Source data	Line mapping ——>	Playout format	Converted data
HD 1080i	OP-47 packets, as specified by DID and SID, on a line valid for 1080i	Maps to	HD 1080i (same as source)	OP-47 packets on a different line valid for 1080i.
HD 720p	OP-47 packets, as specified by DID and SDID, on a line valid for 720p	Maps to	HD 720p (same as source)	OP-47 packets on a different line valid for 720p.

PitchBlue/H.264 ancillary data and timecode

The K2 Summit/Solo system extracts captioning as defined by ATSC a/72 embedded in the video information of H.264 material during ingest. The system plays this information during H.264 playout.

Timecode for a PitchBlue import is striped timecode (continuous timecode) that starts at 00:00:00:00 as required for a PitchBlue workflow.

This functionality supports the PitchBlue workflow. However, the functionality applies to all H.264 material, not only PitchBlue material.

Internationalization

When you enable internationalization on a K2 Solo 3G system, you can name your media assets in a local language. The K2 Solo 3G system supports the local language name as specified in the following table.

System	Internationalization support
Keyboard input and display	• English • Chinese • Japanese • French • German • Spanish • Cyrillic (Russian) • Portuguese • Korean
Media database	• All external views of movie assets can be represented as wide-file names. • AppCenter runs in Unicode. • Only movie assets and searchable User Data keys are Unicode.
Media file system	• Support for Kanji and wide-character file and folder names. • File-folder representation of movie are internationalized, as well as the QuickTime reference file it contains. • Key names (V:\media) remain unchanged, but are Unicode.
K2 Summit/Solo applications	• Movie assets are described in Unicode. • Application user interfaces are Unicode compliant.
Protocols	Refer to "Remote control protocols" in the "Configuring the K2 System" section of this Topic Library.
FTP transfers	Refer to "FTP internationalization" in the "Configuring the K2 System" section of this Topic Library.

Names of media assets and bins must conform to the naming specifications for assets and bins.

Limitations for creating and naming assets and bins

Media assets and bins must conform to the following specifications.

Characters not allowed in asset and bin names

Position	Character	Description
Anywhere in name	\	backward slash
	/	forward slash
	:	colon
	*	asterisk
	?	question mark

Position	Character	Description
	<	less than
	>	greater than
	%	percent sign
	|	pipe
	"	double quote
At beginning of name	~	tilde
		space
At the end of name		space

Asset and bin name limitations

The maximum number of characters in an asset path name, including the bin name, is 259 characters. This includes separators such as "\" and parts of the path name that are not visible in AppCenter. The file system limits the number of bytes in a name as well as the number of characters. The values in this table apply to names in English and other languages referred to in ISO 8859-1. The full count of 259 characters might not be available with some other character sets.

	Asset name, bin name, and path			
Sections of an asset/path name	**The rest of the path name** (i.e. everything apart from the bin and asset names)	Bin name	Asset media directory and extension	Asset name and extension
Naming limitation	This part of the path name is not visible in AppCenter.	The bin name can be up to 227 characters (which would leave room for only a 1-character asset name)	This part of the path name is not visible in AppCenter. The directory name is the same as the asset name. 4 characters are reserved for the extension.	The extension is not visible in AppCenter. At least 25 characters are reserved for the asset name and extension, even if they are not all used.
Example	`\media`	`\mybin1\mybin2`	`\MyVideo.cmf`	`\MyVideo.xml`

The following examples show how a path name would appear in AppCenter and in the file system.

In AppCenter:

`V:\mybin1\mybin2\MyVideo`

In the file system:

`V:\media\mybin1\mybin2\MyVideo.cmf\MyVideo.xml`

Bin nesting limitations

The K2 media database supports nine levels of nested bins. This includes the top level (first) bin. Exceeding this specification results in a database error. When creating a bin do not create a bin at level ten or deeper.

For example:

- The following is supported:
  ```
  default\en\fr\es\de\it\be\dk\cn
  ```
- The following is not supported:
  ```
  default\en\fr\es\de\it\be\dk\cn\jp
  ```

Video network performance

K2 systems support streaming transfers to and from K2 Solo 3G system, K2 Media Clients, K2 SANs, Profile XP Media Platforms, or any device that supports General Exchange Format (GXF) as described in SMPTE 360M.

Parameter	Specification	Comments
Transfer bandwidth per internal storage K2 Solo 3G system	Up to 50 MBytes per second	—
Transfer bandwidth per K2-SVR-100	Up to 90Mbytes per second	Depending on system design
Transfer bandwidth per K2-SVR-NH10GE	Up to 600Mbytes per second	Depending on system design
Maximum concurrent transfers per transfer engine	4 to 10, configurable on SAN	Additional transfers are queued.
Minimum delay from start of record to start of transfer	20 seconds in actual time (not content duration)	This applies to both 60Hz timing and 50Hz timing.
Minimum delay between start of transfer into destination and start of play on destination	20 seconds in actual time (not content duration)	—

About file interchange mechanisms on K2 systems

K2 Summit, Solo, and SAN systems can send and receive files as follows:

- File based import/export — This is based on a file that is visible from the operating system. For example, AppCenter import/export features are file based.
- HotBin import/export — This is file based import/export, with automated features that are triggered when a clip is placed in a bin. Some HotBin functionality requires licensing.
- FTP stream — This is file interchange via File Transfer Protocol (FTP).

GXF interchange specification

This specification applies to GXF file transfer, import, and export on K2 Summit, Solo, and SAN systems.

Streaming between online K2 systems supports complex movies and agile playlists of mixed format.

Formats are supported are as follows:

Supported formats		Notes
Video	DVCPRO25	—
	DVCPRO50	—
	DVCPRO HD	Super Slo-Mo requires software version 7.1. x or higher
	DVCAM	—
	MPEG-2	Includes all MPEG-2 formats (IMX, XDCAM, etc.) that can be stored on a K2 system
	AVC-Intra	—
	H.264	Playable on K2 Summit 3G system only. Can transfer to systems with K2 software version 8.x and higher.
	Avid DNxHD	Playable on K2 Summit 3G system only. Can transfer to systems with K2 software version 8.x and higher.
Audio	48 kHz	—
	16 bit, 24 bit	—
	PCM, Dolby-E, AC-3	—
Data	VBI	—
	Ancillary	—

Interchange mechanisms are supported as follows:

Mechanism		Support
File based	Import	Yes
	Export	Yes
FTP stream	Import	Yes
	Export	Yes

Related Topics

Limitations with complex media types on page 292

MXF interchange specification

This specification applies to MXF file transfer, import, and export on K2 Summit, Solo, and SAN systems.

MXF supports simple clips with a single video track only.

Formats are supported are as follows:

Supported formats		Notes
Video	DVCPRO25	—
	DVCPRO50	—
	DVCPRO HD	Super Slo-Mo requires software version 7.1. x or higher
	DVCAM	—
	D10	See MXF export behavior for eVTR style D10AES3.
	MPEG-2	Includes all MPEG-2 formats (IMX, XDCAM, etc.) that can be stored on a K2 system
	AVC-Intra	—
	Avid DNxHD	Playable on K2 Summit 3G system only. Can transfer to systems with K2 software version 8.x and higher.
Audio	48 kHz	—
	16 bit, 24 bit	—
	PCM, Dolby-E, AC-3	—
Data	VBI	MXF supports either ancillary data packets or VBI lines in the data track but not both, so if ancillary data packets and VBI lines have been recorded into the K2 clip's data track, then the VBI lines will be dropped from the MXF data track on an MXF export.
	Ancillary	—

Interchange mechanisms are supported as follows:

Mechanism		Support
File based	Import	Yes
	Export	Yes
FTP stream	Import	Yes
	Export	Yes

With a special export option, you can export a completed continuous (loop) record clip as MXF or QuickTime, with the result being a flattened stream file. Recording must be complete before you export the clip, however you can make sub-clips while record is underway and export the sub-clips. For this feature, MPEG-2 long GoP is not supported.

Related Topics

Limitations with complex media types on page 292

MXF export behavior on K2 systems

Upon MXF export the K2 system checks clip structure for specifications as they apply to industry standard formats such as Sony XDCAM (SMPTE RDD-09) and Sony eVTR style (SMPTE ST 386). If specifications match, the media is exported as the appropriate format.

The K2 system allows you to override the MXF export behavior so that the exported MXF file no longer match the specifications for the industry-standard format. For example, you can export a clip containing more audio tracks than constrained by the specific MXF standard for the maximum number of audio tracks in a D10AES3 channel. If you export a clip with such an override, the K2 will generate a generic MXF op1a file (instead of the default D10 or XDCAM constrained MXF file).

About MXF with DIDs and SDIDs

You can import and export MXF containing ANC packets and VBI lines as specified in SMPTE ST 436. The K2 system extracts the ANC packets or VBI lines to the K2 clip's data track.

MXF Export Type

When importing and exporting MXF the K2 system behaves as follows, in relation to the MXF Export Type setting in K2Config or in K2 AppCenter:

- The MXF Export Type setting applies to all MXF exports on the K2 system. There is one setting for one K2 system. The K2 system can be a stand-alone K2 Summit/Solo system or a K2 SAN. If a K2 SAN, the one setting applies to the K2 Media Server with role of FTP server that handles exports for all SAN-attached K2 Summit systems.
- For export, the K2 system must be set to one of the following MXF Export Types:
  - **377M**: SMPTE ST 377:2004 compliant. Ensures compatibility with older products.
  - **377-1**: SMPTE ST 377-1:2009 compliant.
- By default the K2 system is set to SMPTE ST 377:2004. This setting is only applicable to the MXF op1a import and export.
- The SMPTE ST 377:2004 setting is recommended for compatibility with older systems which do not support SMPTE ST 377-1:2009.
- The following format does not support SMPTE ST 377-1:2009 export. Therefore the format is always exported as SMPTE ST 377:2004, regardless of the MXF Export Type setting:
  - D10 media
- For import, both SMPTE ST 377:2004 and SMPTE ST 377-1:2009 are supported, regardless of the MXF Export Type setting. The MXF Export Type setting affects export only.

AMWA AS-02 interchange

The K2 system behaves as follows in relation to the Advanced Media Workflow Association (AMWA) AS-02 version 1.0: 2011 MXF Versioning Specification:

- The K2 system supports the AS-02 specification with no customizations
- Supports import of AS-02 content
- Plays media imported with AS-02
- Exports media to AS-02 content
- Requires license K2-ExtendedFileServices.

Related Topics

Limitations with complex media types on page 292

QuickTime interchange specification

This specification applies to QuickTime file transfer, import, and export on K2 Summit, Solo, and SAN systems.

The following are not supported:

- Sequences and lists
- Lists of mixed formats or containing empty tracks, such as tracks that do not contain recorded media

Formats are supported are as follows:

Supported formats		Notes
Video	DVCPRO25	—
	DVCPRO50	—
	DVCPRO HD	Super Slo-Mo requires software version 7.1.x or higher
	DVCAM	—
	AVC-Intra	—
	D10/IMX	—
	XDCAM-HD	—
	XDCAM-EX	—
	XDCAM-HD422	—
	H.264	Playable on K2 Summit 3G system only. Can transfer to systems with K2 software version 8.x and higher.
	Avid DNxHD	—
Audio	48 kHz	
	16 bit, 24 bit PCM	
Data	None	—

Interchange mechanisms are supported as follows:

Mechanism		Support
File based	Import	Yes
	Export	Yes
FTP stream	Import	No
	Export	No

With a special export option, you can export a completed continuous (loop) record clip as MXF or QuickTime, with the result being a flattened stream file. Recording must be complete before you export the clip, however you can make sub-clips while record is underway and export the sub-clips. For this feature, MPEG-2 long GoP is not supported.

Related Topics

Limitations with complex media types on page 292

QuickTime video and key import specification

This specification applies to importing a QuickTime file with an alpha channel. This is a licensed feature.

The imported file must be QuickTime 32 with alpha RLE 32-bit raster encoding, as produced by the Apple Animation Codec.

Supported video formats for import are as follows:

Format		Scan	Frame Rate
SD video	720 x 480	Interlaced	29.97
	720 x 512	Interlaced	29.97
	720 x 576	Interlaced	25
	720 x 608	Progressive	25
HD video	1920 x 1080	Interlaced	29.97, 25
	1280 x 720	Progressive	59.94, 50

Supported audio formats for import are as follows:

Format		
Audio tracks (if present)	48 kHz	Mono or stereo
	16 bit, 24 bit	
	PCM	

Interchange mechanisms are supported as follows:

Mechanism		Support
File based	Import	Yes

Mechanism		Support
	Export	No
FTP stream	Import	No
	Export	No

When K2 software imports a file that meets the above requirements, it creates a K2 clip with two video tracks, in formats as follows:

Format			Frame Rate	Data Rate
SD video	D10/IMX	720 x 512	29.97	50 CBR
	D10/IMX	720 x 608	25	50 CBR
HD video	AVC-Intra 100	1920 x 1080	29.97, 25	100 Mbps
	AVC-Intra 100	1280 x 720	29.97, 25	100 Mbps

Audio tracks, if present are imported.

Timecode data is imported as K2 striped timecode. The first timecode value is the starting value and subsequent timecode is continuous.

The import process consumes system resource since this involves video transcoding. Be aware of this if running other resource intensive processes during import.

QuickTime reference files

The following formats are supported as QuickTime reference files:

- DV
- AVC-Intra
- XDCAM-EX
- XDCAM-HD
- XDCAM-HD 422
- IMX
- Avid DNxHD

MPEG interchange specification

This specification applies to MPEG import on K2 Summit, Solo, and SAN systems.

Formats are supported are as follows:

Supported formats		Notes
Video	MPEG-2	Supports import of MPEG-2 program and transport streams. If the transport stream contains multiple programs, the first detected program in the transport stream is imported as a K2 clip.

Supported formats		Notes
	H.264	AVCHD /H.264 is K2 Summit 3G system only. Import only supported.
Audio	48kHz	—
	MPEG-1 (layer 1 & 2)	—
	SMPTE 302M AES3 LPCM	—
	AC-3	—
	AVCHD DVD VOB LPCM	AVCHD /H.264 is K2 Summit 3G system only. Import only supported.
	DVD/VOB AC-3	—
Data	ATSC a/53 captions	For MPEG-2 imports.
	ATSC a/72 captions	For H.264 imports.
	SMPTE RDD-11 ancillary data	—

Interchange mechanisms are supported as follows:

Mechanism		Support
File based	Import	Yes
	Export	No
FTP stream	Import	Yes
	Export	No

Related Topics

Limitations with complex media types on page 292

P2 interchange specification

This specification applies to P2 file transfer, import, and export on K2 Summit, Solo, and SAN systems.

Formats are supported are as follows:

Supported formats		Notes
Video	AVC - LongG	
	AVC-Intra	
	DVCPRO25	

Supported formats		Notes
	DVCPRO50	
	DVCPRO HD	
	DVCAM	
Audio	48 kHz	All audio tracks on the clip being exported have to be of the same type to comply with the P2 file format. For instance, exporting a clip with some PCM 16 audio tracks and others PCM 24 is not supported.
	16 bit, 24 bit PCM	

Interchange mechanisms are supported as follows:

Mechanism		Support	
File based	Import	Yes	Directory structure as specified by P2
	Export	Yes	
FTP stream	Import	Yes	For AVC – LongG MXF file format only
	Export	No	

Related Topics

Limitations with complex media types on page 292

WAV audio interchange specification

This specification applies to WAV import on K2 Summit, Solo, and SAN systems.

Formats are supported are as follows:

Supported formats		Notes
Video	NA	—
Audio	48 kHz	—
	16 bit stereo PCM	
Data	NA	—

Interchange mechanisms are supported as follows:

Mechanism		Support
File based	Import	Yes
	Export	No
FTP stream	Import	No
	Export	No

Media file system performance on K2 systems

This section specifies media operations on K2 systems. On a K2 SAN, these specification are qualified at channel counts up to 48 channels. Performance on larger systems is not tested.

Record-to-play specifications

The following tables specify the minimum length of time supported between recording on one channel and cueing the same clip for playout on another channel. Live play mode is available only on a K2 Summit/Solo system with the AppCenter Pro license. On a K2 SAN, Live play mode is not supported with record-to-play on different K2 clients or on a K2 SAN with Live Production mode not enabled.

Standalone K2 Solo 3G system

Formats	Live play	Normal play
DV	0.5 seconds	6.0 seconds
MPEG-2 I-frame, AVC-Intra	0.75 seconds	6.25 seconds
MPEG-2 long GoP, XDCAM	1.0 seconds	6.50 seconds

Live Play on K2 SAN with Live Production mode enabled

Formats	Record-to play on same K2 Summit System
DV	0.5 seconds
MPEG-2 I-frame, AVC-Intra	0.75 seconds
MPEG-2 long GoP, XDCAM	1.0 seconds

Normal play on K2 SAN with Live Production mode enabled

Formats	Record-to play on same K2 Summit System	Record-to play on different K2 Summit Systems
DV	6.0 seconds	8.0 seconds
MPEG-2 I-frame, AVC-Intra	6.25 seconds	8.25 seconds
MPEG-2 long GoP, XDCAM	6.50 seconds	8.50 seconds

Normal play on K2 SAN with Live Production mode not enabled

Formats	Record-to play on same K2 Summit System	Record-to play on different K2 Summit Systems
All formats	10 seconds	20 seconds

Other media file system specifications

Parameter	Stand-alone K2 Solo 3G system	K2 SAN
Maximum number of clips[8]	20,000	50,000
Maximum length continuous record	24 hours	24 hours
Off-speed play range for audio scrub[9]	-2x to +2x	-1.5x to +1.5x
Off-speed play range for insertion of MPEG user data and/or ancillary data on playout	0 to +1.2	0 to +1.2
Minimum duration between recordings	10 seconds	10 seconds
Minimum duration between start of clip import and clip play	10 seconds	10 seconds

Transition effects formats and limitations

Transition (mix) effects are supported on K2 Solo 3G system as follows.

Transition effects on first generation K2 Solo 3G system

	DV	AVC-Intra	MPEG-2 I-frame	MPEG-2 long GoP
DV	Yes	No	No	No
AVC-Intra	No	Yes	No	No
MPEG-2 I-frame	No	No	Yes	No
MPEG-2 long GoP	No	No	No	No

When adding transitions to all events in a playlist for an on-the-fly (the **Go To** feature) pause or transition, limitations on the time for the length of the transition are as follows:

- 0.5 second or less on first generation K2 Solo 3G system

Transition effects on K2 Summit 3G system

	DV	AVC-Intra	AVCHD/H.264	MPEG-2 I-frame	MPEG-2 long GoP	Avid DNxHD	AVC - LongG
DV	Yes	No	No	No	No	No	No
AVC-Intra	No	Yes	Yes	No	No	No	No
AVCHD/H.264	No	Yes	Yes	No	No	No	No

[8] The maximum number of clips is based on clips with 16 or less audio tracks. Large quantities of clips with more than 16 audio tracks proportionally reduce the maximum number of clips.

[9] Dolby audio tracks muted during off-speed play

MPEG-2 I-frame	No	No	No	Yes	No	No	No
MPEG-2 long GoP	No	No	No	No	Yes	No	No
Avid DNxHD	No	No	No	No	No	Yes	No
AVC - LongG	No	No	No	No	No	No	Yes

When adding transitions to all events in a playlist for an on-the-fly (the **Go To** feature) pause or transition, limitations on the time for the length of the transition are as follows:

- 0.5 second or less on K2 Summit 3G systems

Protocols supported

AMP, VCDP, and BVW protocols are supported.

Transfer compatibility with K2 Summit/Solo

When transferring material between a K2 Summit/Solo and other Grass Valley products, you must consider the specifications of the different products. The following tables illustrate some of these considerations. In these tables, source material is assumed to have been recorded on the source device.

Transfer compatibility with K2 Media Client

Transfer	Material transferred	Compatibility
From K2 Summit/Solo to K2 Media Client	DVCPRO25, DVCPRO50	Playout supported.
	DVCPRO HD	Not supported
	MPEG	Supported
	AVC-intra	Not supported
	H.264	Not supported
	Avid DNxHD	Not supported
From K2 Media Client to K2 Summit/Solo	All types of material supported, according to the SD and/or HD capability.	

Transfer compatibility with Profile XP Media Platform

Transfer	Material transferred	Compatibility
From K2 Summit/Solo to Profile XP Media Platform	DVCPRO25, DVCPRO50	Playout supported.
	DVCPRO HD	Not supported

Transfer	Material transferred	Compatibility
	MPEG-2 HD 4:2:0 80 Mb or less MPEG-2 SD 4:2:2, XDCAM-HD422, XDCAM-EX	Supported. Can be played out.
	MPEG-2 720p MPEG-2 HD 4:2:2 XDCAM-HD HDV 1440x1080	Supported for storage only. Transfer is successful but playout not supported.
	AVC-intra	Not supported
	H.264	Not supported
	Avid DNxHD	Not supported
From Profile XP Media Platform to K2 Summit/Solo	All types of material supported, according to the SD and/or HD capability of the model.	

Data compatibility between K2 Summit/Solo and PVS models

When material is transferred between a PVS Profile XP Media Platform and a K2 Solo 3G system, data is supported as follows:

Transferring from PVS (source) to K2 Summit/Solo with HD license (destination)

Source format	Source data	SD playout data support on destination	HD playout data support on destination
DVCPRO25	Closed captioning	Yes	Yes
	Ancillary data	No	No
DVCPRO50	Closed captioning in compressed VBI	Yes	No
	Ancillary data	Yes	Yes
DVCPRO50	Compressed VBI	Yes	No
SD MPEG-2	Uncompressed VBI	Yes	Yes, with data bridging for CC only. Other VBI lines are discarded.
	Closed captioning	Yes	Yes. Ancillary data packets
	Compressed VBI	Yes	Yes, if enabled
	Ancillary data	Yes	Yes
HD MPEG-2	Ancillary data	Yes	Yes

Transferring from K2 Summit/Solo (source) to PVS (destination)

Source format	Source data	SD playout data support on destination	HD playout data support on destination
DVCPRO25, DVCPRO50	Any supported on K2 Summit/Solo	Yes	NA
DVCPRO HD	Any supported on K2 Summit/Solo	NA	NA
AVC-Intra	Any	NA — AVC-Intra not supported on PVS	
H.264	Any	NA — H.264 not supported on PVS	
Avid DNxHD	Any	NA — Avid DNxHD not supported on PVS	
SD MPEG-2	Any data recorded with Profile compatible setting[10].	All supported	Yes
	Uncompressed VBI and captioning on data track	Not supported. Do not attempt to transfer to PVS.	
	Compressed VBI	Yes	Yes, with data bridging for CC only. Other VBI lines are discarded.
	Uncompressed VBI	Yes	No, except for bridging of CC data, which requires Profile software v5.4.9.
HD MPEG-2	Ancillary data	Yes. CC bridging requires data-bridging SDI board.	Yes.

Control Point PC system requirements

If you are building your own Control Point PC, the machine you choose must meet the following requirements. These requirements assume that the PC is dedicated to its function as the host for Grass Valley product control and configuration applications. You should not run other applications on the PC that could interfere with system performance.

Control Point PC system requirements are as follows:

Requirements	Comments
Operating System	Microsoft Windows (Must be a U.S. version) 64-bit: • Windows 7 • Server 2008 R2
RAM	Minimum 512 MB, 1 GB recommended

[10] When Record ancillary data = No or when Record Uncompressed VBI and captioning data to track = No

Requirements	Comments
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 4.0
Sun Java 2 Runtime Environment	Version 1.5.0_11, Version 1.6.0 or higher. Required for the HP Ethernet Switch configuration interface, which is used for K2 SAN (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.
Quicktime	Version 7 or higher
Acrobat Reader	Version 8 or higher

Find software at Internet locations such as the following:

- http://msdn.microsoft.com/en-us/netframework/default.aspx
- http://java.sun.com/javase/downloads/index.jsp
- http://www.microsoft.com/downloads/details.aspx?FamilyId=3144B72B-B4F2-46DA-B4B6-C5D7485F2B42&displaylang=en
- http://www.apple.com/quicktime/download/
- http://get.adobe.com/reader/

Super Slo-Mo camera formats

Formats specified for output by Super Slo-Mo cameras are supported as follows:

Camera	Format	Frame Rate (Hz)	Speed support
Grass Valley LDK8000 SportElite HD Camera	• 720p • 1080i	• 50/59.94/100/119.88 • 50/59.94/100/119.88	2x;
Grass Valley LDK8300 Camera	• 720p • 1080i	• 50/59.94/100/119.88/150/179.82 • 50/59.94/100/119.88/150/179.82	2x; 3x
Grass Valley LDX HiSpeed Camera	• 720p • 1080i	• 50/59.94/150/179.82 • 50/59.94/150/179.82	3x
Grass Valley LDX XtremeSpeed Camera	• 720p • 1080i • 1080p	• 50/59.94/150/179.82/300/359.64 • 50/59.94/150/ 179.82/300/359.64 • 50/59.94/150/179.82	• 3x in 720p; 1080i; 1080p • 6x in 720p; 1080i
Sony 3300	• 720p • 1080i	• 50/59.94/150/179.82 • 50/59.94/150/179.82	3x

MIB specifications

This section specifies Management Information Base (MIB) information for monitoring K2 devices with the Simple Network Management Protocol (SNMP). The Grass Valley NetCentral product uses this protocol. This information is intended for SNMP developers. MIB files can be obtained from the Grass Valley Developers website.

In addition to the MIBs specified in this section, a K2 device might support other MIBs based on third party software/hardware. To determine whether other MIBs are supported by the operating system or independent hardware/software vendors, perform a “MIB walk” operation on the K2 device using conventional SNMP utilities and determine MIBs supported.

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

K2 client MIBs

Grass Valley MIBs

MIB	Description
gvg-reg.mi2 (GVG-REG)	Grass Valley SMI enterprise namespace

MIB	Description
gvg-element.mi2 (GVG-ELEMENT-MIB)	Common object definitions for a Grass Valley device. • Generic device tracking information • SNMP trap target configuration • Generic IO/signal status information
gvg-prod.mi2 (GVG-PROD-REG)	Product sysObjectOID registrations for the Grass Valley devices
gvg-drs.mi2 (GVG-DRS-MIB)	Video disk recorder/server status information
gvg-tcm.mi2 (GVG-TCM-MIB)	Media transfer (import/export) statistical information
gvg-manclient.mi2 (GVG-MANCLIENT-MIB)	SAN client status information. Available only when the K2 client is connected to a SAN.

Other MIBs

MIB	Description
RFC1213-MIB.mib (RFC1213-MIB)	MIB-2 support as implemented by Microsoft for the Windows operating system.
hostmib.mib (HOST-RESOURCES-MIB)	Generic system information as implemented by Microsoft for the Windows operating system
lmmib2.mib (LanMgr-Mib-II-MIB)	Generic Windows networking, user account and service information as implemented by Microsoft for the Windows operating system
SUPERMICRO-SMI.my (SUPERMICRO-SMI)	Motherboard electromechanical sensor information (motherboard temperature hotspots, CPU fan, voltages, etc.)
SUPERMICRO-HEALTH-MIB.my (SUPERMICRO-HEALTH-MIB)	
MEGARAID.mib (RAID-Adapter-MIB)	Internal RAID-1 SCSI drive and controller information

K2 Media Server MIBs

Grass Valley MIBs

MIB	Description
gvg-reg.mi2 (GVG-REG)	Grass Valley SMI enterprise namespace
gvg-element.mi2 (GVG-ELEMENT-MIB)	Common object definitions for a Grass Valley device. • Generic device tracking information • SNMP trap target configuration
gvg-prod.mi2 (GVG-PROD-REG)	Product sysObjectOID registrations for the Grass Valley devices
gvg-ssr.mi2 (GVG-SSR-MIB)	K2 Storage roles configured for the server by the K2 System Configuration application and their status information
gvg-sbs.mi2 (GVG-SBS-MIB)	K2 iSCSI Bridge and TOE (TCP Offload Engine) related status information. Available only if the K2 Media Server has the iSCSI Bridge role.
gvg-manfsm.mi2 (GVG-MANFSM-MIB)	Video File System and Clip Database (FSM) related status information. Available only if the K2 Media Server has role(s) of media file system server and/or database server.
gvg-tcm.mi2 (GVG-TCM-MIB)	Media transfer (import/export) statistical information. Available only if the K2 Media Server is configured to be a transfer/FTP/hotbins server.
gvg-manclient.mi2 (GVG-MANCLIENT-MIB)	SAN client status information. Available only when the K2 Media Server is a media system and/or database client. For example, if the K2 Media Server has the role of FTP server only, then it must be a media file system/database client to another K2 Media Server that is the media file system/database server.

Other MIBs

MIB	Description
RFC1213-MIB.mib (RFC1213-MIB)	MIB-2 support as implemented by Microsoft for the Windows operating system.
hostmib.mib (HOST-RESOURCES-MIB)	Generic system information as implemented by Microsoft for the Windows operating system

MIB	Description
lmmib2.mib (LanMgr-Mib-II-MIB)	Generic Windows networking, user account and service information as implemented by Microsoft for the Windows operating system
mssql.mib (MSSQLSERVER-MIB)	Microsoft SQL Server information
10892.mib (MIB-Dell-10892)	Dell PowerEdge chassis related electro-mechanical status information
arymgr.mib (ArrayManager-MIB)	Dell RAID1 system disk (PERC) and controller information

K2 Appliance (Generic Windows computer based) MIBs

For details on the hardware/chassis running the K2 Appliance, check the chassis vendor's MIBs.

Grass Valley MIBs

MIB	Description
gvg-reg.mi2 (GVG-REG)	Grass Valley SMI enterprise namespace
gvg-element.mi2 (GVG-ELEMENT-MIB)	Common object definitions for a Grass Valley device. • Generic device tracking information • SNMP trap target configuration
gvg-prod.mi2 (GVG-PROD-REG)	Product sysObjectOID registrations for the Grass Valley devices
gvg-ssr.mi2 (GVG-SSR-MIB)	K2 Storage roles configured for the server by the K2 System Configuration application and their status information
gvg-tcm.mi2 (GVG-TCM-MIB)	Media transfer (import/export) statistical information. Available only if the K2 Media Server is configured to be a transfer/FTP/hotbins server.
gvg-manclient.mi2 (GVG-MANCLIENT-MIB)	SAN client status information. Available only when the K2 appliance is a media system and/or database client.

Other MIBs

MIB	Description
RFC1213-MIB.mib (RFC1213-MIB)	MIB-2 support as implemented by Microsoft for the Windows operating system.
hostmib.mib (HOST-RESOURCES-MIB)	Generic system information as implemented by Microsoft for the Windows operating system
lmmib2.mib (LanMgr-Mib-II-MIB)	Generic Windows networking, user account and service information as implemented by Microsoft for the Windows operating system

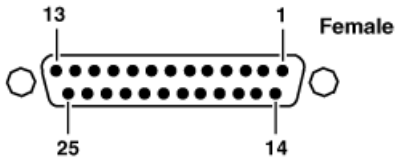
Connector pinouts

K2 Solo 3G system connector pinouts

The following sections describe K2 Solo 3G system rear panel connector pinouts.

AES Audio

Pinouts for each channel's AES Audio DB25 connector are as follows:



Pin #	Signal	Description
1	IN_P<0>	Channel Input 1&2 positive
2	IN_P<1>	Channel Input 3&4 positive
3	IN_P<2>	Channel Input 5&6 positive
4	IN_P<3>	Channel Input 7&8 positive
5	OUT_P<0>	Channel Output 1&2 positive
6	OUT_P<1>	Channel Output 3&4 positive
7	OUT_P<2>	Channel Output 5&6 positive
8	OUT_P<3>	Channel Output 7&8 positive
9	NO_C	NO_C
10	GND	GND

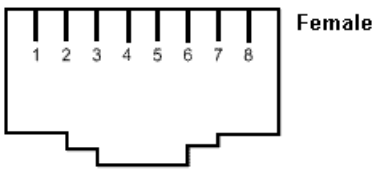
Pin #	Signal	Description
11	NO_C	NO_C
12	GND	GND
13	GND	GND
14	IN_N<0>	Channel Input 1&2 negative
15	IN_N<1>	Channel Input 3&4 negative
16	IN_N<2>	Channel Input 5&6 negative
17	IN_N<3>	Channel Input 7&8 negative
18	OUT_N<0>	Channel Output 1&2 negative
19	OUT_N<1>	Channel Output 3&4 negative
20	OUT_N<2>	Channel Output 5&6 negative
21	OUT_N<3>	Channel Output 7&8 negative
22-25	GND	GND

The optional audio cable has connections as follows:

RS-422 connector pinouts K2 Summit 3G

The K2 Summit 3G Production Client RS-422 interface conforms to ANSI/SMPTE 207M-1997 standard (SMPTE 422).

Pinouts for the individual RJ45 connectors are as follows:



Pin #	Signal	Description
1	+TXD	Differential Transmit Data (high) (out TXB)
2	-TXD	Differential Transmit Data (low) (out TXA)
3	+RXD	Differential Receive Data (high) (in RXB)

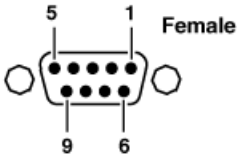
Pin #	Signal	Description
4	GND	Signal Ground
5	GND	Signal Ground
6	-RXD	Differential Receive Data (low) (in RXA)
7	GND	Signal Ground
8	GND	Signal Ground

Balanced signals are placed on twisted wire pairs within a standard CAT5 or CAT3 cable.

RS-422 connector pinouts first generation K2 Solo 3G system

The first generation K2 Solo 3G system RS-422 interface conforms to ANSI/SMPTE 207M-1997 standard (SMPTE 422).

Pinouts for the individual DB9 connectors are as follows:

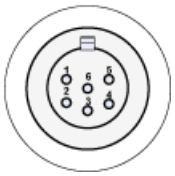


Pin #	Signal	Description
1	GND	Frame Ground
2	-TXD	Differential Transmit Data (low)
3	+RXD	Differential Receive Data (high)
4	GND	Transmit Signal Common
5	NC	Spare
6	GND	Receive Signal Common
7	+TXD	Differential Transmit Data (high)
8	-RXD	Differential Receive Data (low)
9	GND	Signal Ground

LTC connectors pinouts

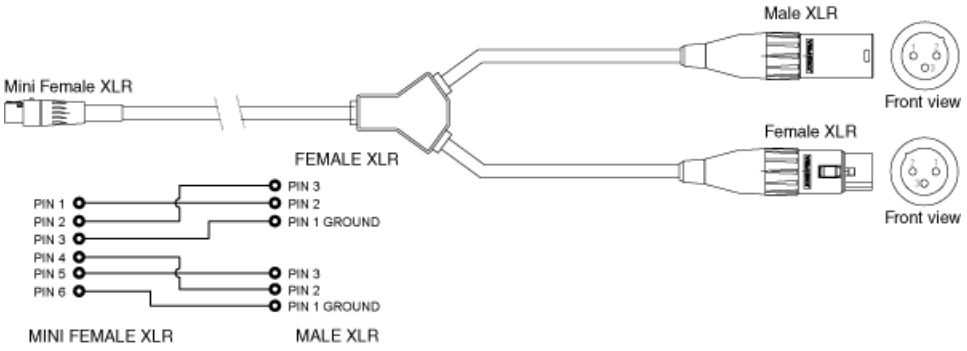
The K2 Solo 3G system LTC panel connector provides balanced linear timecode input and output connections. The interface conforms to SMTPE 12M Linear Timecode.

On the K2 Solo 3G system there is one 6 pin Switchcraft TRA6M Mini-XLR male connector for each channel. Pinouts are as follows:

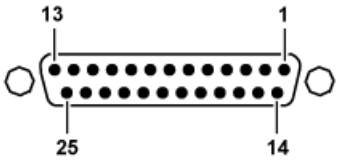


Pin #	Signal	Description
1	IN_P<0>	
2	IN_N<0>	
3	GND	Frame Ground
4	OUT_P<0>	
5	OUT_N<0>	
6	GND	Frame Ground

The mini-XLR to XLR LTC cable has connections as follows:



GPI I/O connector pinouts



Pin	Signal
1	Output 1
2	Output 2
3	Output 3

Pin	Signal
4	Output 4
5	Output 5
6	Output 6
7	Output 7
8	Output 8
9	Output 9
10	Output 10
11	Output 11
12	Output 12
13	Ground
14	Input 1
15	Input 2
16	Input 3
17	Input 4
18	Input 5
19	Input 6
20	Input 7
21	Input 8
22	Input 9
23	Input 10
24	Input 11
25	Input 12

K2 Media Server connector pinouts

The following sections describe K2 Media Server rear panel connector pinouts.

Redundant server heartbeat serial cable

Take care to use the proper serial cable to interconnect redundant K2 Media Servers that take the role of file system/database servers. This cable supports the heartbeat mechanism whereby the servers monitor each other's health. It is a 9 pin serial cable, but it is not a standard RS-232 null modem cable. The heartbeat cable is supplied with your system (Grass Valley part number 174-8137-00) and has a pin configuration as follows:

1 – 4

2 – 3

3 – 2

4 – 1&6

5 – 5

6 – 4

7 – 8

8 – 7

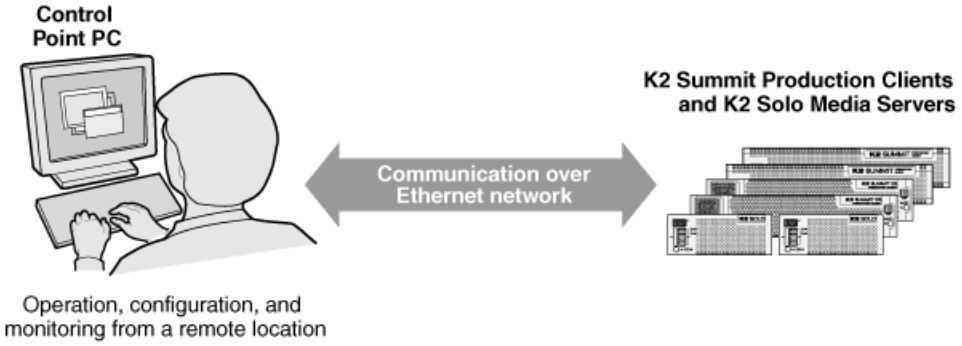
9 – No Connect

Configuring the K2 system

Product description

About K2 systems

The K2 Solo 3G system is a cost-effective Broadcast Enterprise Server that incorporates IT server platform and storage technologies to deliver a networked solution to facilities for ingest, playout, news integration, sports, and media asset management. Each K2 system model is a comprehensive platform that provides a suite of user applications, system tools, and the largest range of third-party interactivity in the industry.



The K2 Solo 3G system is designed for “headless” operation from a remote control point using Grass Valley Control Point software. You can also use the Microsoft Windows Remote Desktop Connection application on your PC to connect to the K2 system for configuration or administration.

The K2 Solo 3G system is further described in the following topics. Also refer to topics on Transmission models for information unique to those products.

K2 Summit 3G system features

The following features apply to the K2 Summit 3G Production Client:

- Windows 7 64-bit embedded operating system.
- Embedded Security for protection against viruses and other unauthorized programs.
- Bidirectional channels (channel can be either an input channel or it can be an output channel).
- Two or four channels per chassis.
- SDI video inputs and outputs.
- AES/EBU or embedded audio inputs and outputs.
- Standard Definition (SD) video formats and High Definition (HD) video formats.
- Support for DV, MPEG-2, AVCHD/H.264, AVC-Intra, AVC - LongG, and Avid DNxHD. For details regarding licenses, hardware support, and video codec specifications, refer to related topics in the "Using K2 AppCenter" section of the K2 Topic Library.
- 3G codec module hosts codec option cards that are programmable for multiple formats and functions.

- Mixed format playback of SD or HD clips on the same timeline.
- Up/down/cross HD/SD conversion (e.g. SD and HD clips ingested, then played back as SD or HD clips) or as a different SD or HD format (e.g. 720p to 1080i).
- 4K, Super Slo-Mo, Multi-cam, and 3D/Video + Key features are available as part of the ChannelFlex Suite.
- 4K/UHD workflow and 4K/UHD Pan & Zoom using the GV DynoZoom software.
- High endurance SSD internal storage for 6-in/2-out configuration, 6x Super Slow Motion (SSM), and 4K/UHD workflow.
- VGA monitoring capability.
- Redundant power supply, cooling fans for reliability.
- 2.5 inch media storage drives.
- mSATA SSD system drive.
- Type IV CPU carrier module with 8 GB RAM.
- USB 3.0 interface for file exchange. (In K2 Summit 3G system only).
- Ability to create nested bins, i.e. sub-bins within bins.
- Freeze mode can be frame or field.
- Various video mix effects (e.g. dissolves between two video and audio tracks on the same channel, or fade thru matte color).
- Remote operation and configuration via AppCenter.
- Gigabit Ethernet.
- AMP, VDCP, and BVW remote control protocols supported.
- Remote control over RS-422 or Ethernet.
- Low-resolution proxy files created during record and live streaming from SDI In/out are available as part of the AppCenter Pro and Elite licenses.
- RAID media storage.
- Stand-alone internal storage, stand-alone external direct-connect storage, and external shared (SAN) storage.

K2 Summit system features

The following features apply to the first-generation K2 Summit Production Client:

- Bidirectional channels (channel can be either an input channel or it can be an output channel).
- Two or four channels per chassis.
- SDI video inputs and outputs.
- AES/EBU or embedded audio inputs and outputs.
- Standard Definition (SD) video formats and High Definition (HD) video formats.
- Mixed format playback of SD or HD clips on the same timeline.
- Up/down/cross HD/SD conversion (e.g. SD and HD clips ingested, then played back as SD or HD clips) or as a different SD or HD format (e.g. 720p to 1080i).
- VGA monitoring capability.
- Redundant power supply, cooling fans for reliability.
- 3.5 inch media storage drives.
- CompactFlash system drive.
- Ability to create nested bins, i.e. sub-bins within bins.

- Freeze mode can be frame or field.
- Various video mix effects (e.g. dissolves between two video and audio tracks on the same channel, or fade thru matte color).
- Remote operation and configuration via AppCenter.
- Gigabit Ethernet.
- AMP, VDCP, and BVW remote control protocols supported.
- Remote control over RS-422 or Ethernet.
- Super Slo-Mo, Multi-cam, and 3D/Video + Key features are available as part of the ChannelFlex Suite.
- Low-resolution proxy files created during record and live streaming from SDI In/out are available as part of the AppCenter Pro and Elite licenses. This requires the Type II carrier module.
- RAID media storage.
- Stand-alone internal storage, stand-alone external direct-connect storage, and external shared (SAN) storage.

K2 Solo 3G system features

The following features apply to the K2 Solo 3G Media Server:

- Windows 7 64-bit embedded operating system.
- Embedded Security for protection against viruses and other unauthorized programs.
- Bidirectional channels (channel can be either an input channel or it can be an output channel).
- Two channels per chassis.
- SDI video inputs and outputs.
- AES/EBU or embedded audio inputs and outputs.
- Standard Definition (SD) video formats and High Definition (HD) video formats.
- Support for DV, MPEG-2, AVCHD/H.264, AVC-Intra, AVC - LongG, and Avid DNxHD. For details regarding licenses, hardware support, and video codec specifications, refer to related topics in the "Using K2 AppCenter" section of the K2 Topic Library.
- 3G codec module. Codec option card not supported on K2 Solo 3G system.
- Mixed format playback of SD or HD clips on the same timeline.
- Up/down/cross HD/SD conversion (e.g. SD and HD clips ingested, then played back as SD or HD clips) or as a different SD or HD format (e.g. 720p to 1080i). Aspect ratios are adjusted.
- VGA monitoring capability.
- Compact Flash System drive.
- Type IV CPU carrier module with 8 GB RAM.
- USB 3.0 interface for file exchange.
- Ability to create nested bins, i.e. sub-bins within bins.
- Freeze mode can be frame or field.
- Various video mix effects (e.g. dissolves between two video and audio tracks on the same channel, or fade thru matte color).
- Remote operation and configuration via AppCenter.
- Gigabit Ethernet.
- AMP, VDCP, and BVW remote control protocols supported.
- Remote control over RS-422 or Ethernet.

- ExpressCard.
- Super Slo-Mo, Multi-cam, and 3D/Video + Key features are available as part of the ChannelFlex Suite.
- Low-resolution proxy files created during record and live streaming from SDI In/out are available as part of the AppCenter Pro and Elite licenses.
- Internal media storage.
- Support for Dyno S.

K2 Solo system features

The following features apply to the first-generation K2 Solo Media Server:

- Bidirectional channels (channel can be either an input channel or it can be an output channel).
- Two channels per chassis.
- SDI video inputs and outputs.
- AES/EBU or embedded audio inputs and outputs.
- Standard Definition (SD) video formats and High Definition (HD) video formats.
- Mixed format playback of SD or HD clips on the same timeline.
- Up/down/cross HD/SD conversion (e.g. SD and HD clips ingested, then played back as SD or HD clips) or as a different SD or HD format (e.g. 720p to 1080i). Aspect ratios are adjusted.
- VGA monitoring capability.
- CompactFlash system drive.
- Ability to create nested bins, i.e. sub-bins within bins.
- Freeze mode can be frame or field.
- Various video mix effects (e.g. dissolves between two video and audio tracks on the same channel, or fade thru matte color).
- Remote operation and configuration via AppCenter.
- Gigabit Ethernet.
- AMP, VDCP, and BVW remote control protocols supported.
- Remote control over RS-422 or Ethernet.
- ExpressCard.
- Super Slo-Mo, Multi-cam, and 3D/Video + Key features are available as part of the ChannelFlex Suite.
- Low-resolution proxy files created during record and live streaming from SDI In/out are available as part of the AppCenter Pro and Elite licenses. This requires the Type II carrier module.
- RAID 0 internal media storage.

K2 Summit/Solo formats, models, licenses, and hardware support

Formats are supported as in the following tables.

Table 10: First-generation K2 Summit/Solo system

Formats	Compression	1x	Multi-Cam, 3D/Video + Key	3x Super Slo-Mo	4K
SD	DV	Encode/decode	Encode/decode	Not supported.	Not supported.
	MPEG-2	Decode is standard. Encode requires codec option card.	Decode is standard. Encode requires codec option card.	Not supported.	Not supported.
	AVCHD	Not supported.	Not supported.	Not supported.	Not supported.
1080i/720p	DV	Encode/decode. Requires HD license.	Encode/decode. Requires HD license.	Encode/decode. Requires HD license.	Not supported.
	MPEG-2	Decode is standard. Encode requires codec option card. Requires HD license.	Decode is standard. Encode requires codec option card. Requires HD license.	Not supported.	Not supported.
	AVC-Intra	Encode/decode. Requires codec option card. Requires HD license.	Encode/decode. Requires codec option card. Requires HD license.	Not supported.	Not supported.
	AVCHD	Not supported	Not supported	Not supported	Not supported.
	AVC - LongG	Not supported	Not supported	Not supported	Not supported.
	Avid DNxHD	Not supported	Not supported	Not supported	Not supported.
1080p	AVC-Intra Class 100	Not supported	Not supported	Not supported	Not supported.

To add support for additional formats, contact your Grass Valley representative for upgrade information.

Table 11: K2 Summit 3G system

Formats	Compression	1x	3x Super Slo-Mo, Multi-Cam, 3D/Video + Key	6x Super Slo-Mo	4K
SD	DV	Encode/decode	Encode/decode	Not supported.	Not supported.
	MPEG-2	Encode/decode	Encode/decode. Requires codec option card.	Not supported.	Not supported.

Formats	Compression	1x	3x Super Slo-Mo, Multi-Cam, 3D/Video + Key	6x Super Slo-Mo	4K
	AVCHD/H.264	Decode only. Requires AVC license.	Not supported	Not supported	Not supported.
1080i/720p	DV	Encode/decode. HD license is required.	Encode/decode. HD license is required.	Encode/decode. Requires codec option card, plus HD and 6xSSM licenses. Requires K2 Summit 3G chassis with 2.5” hard drives for one channel or high endurance solid state drives for full features with two channels.	Not supported.
	MPEG-2	Encode/decode. HD license is required.	Encode/decode. Requires codec option card. HD license is required.	Not supported.	Not supported.
	AVC-Intra	Encode/decode. Requires HD and AVC licenses.	Encode/decode. Requires HD and AVC licenses.	Encode/decode. Requires codec option card, plus HD, 6xSSM and AVC licenses. Requires K2 Summit 3G chassis with 2.5” hard drives for one channel or high endurance solid state drives for full features with two channels.	Not supported.

Formats	Compression	1x	3x Super Slo-Mo, Multi-Cam, 3D/Video + Key	6x Super Slo-Mo	4K
	AVCHD/H.264	Decode only. Requires HD and AVC licenses.	Not supported	Not supported	Not supported.
	AVC - LongG	Decode only. Requires HD and AVC licenses.	Not supported	Not supported	Not supported.
	Avid DNxHD	Encode/decode. Requires HD and DNxHD licenses.	Encode/decode. Requires HD and DNxHD licenses.	Not supported	Not supported.
1080p	AVC-Intra Class 100	Encode/decode. Requires HD, 3G and AVC licenses.	Encode/decode. Requires codec option card, plus HD, 3G and AVC licenses.	Not supported	Encode/decode. Requires codec option cards and high endurance solid state drives. Requires HD, 3G, 4K and AVC licenses.

Table 12: K2 Solo 3G system

Formats	Compression	1x	Multi-Cam, 3D/Video + Key	3x Super Slo-Mo	4K
SD	DV	Encode/decode	Encode/decode	Not supported.	Not supported.
	MPEG-2	Encode/decode	Not supported	Not supported	Not supported.
	AVCHD/H.264	Decode only. Requires AVC license.	Not supported	Not supported	Not supported.
1080i/720p	DV	Encode/decode. HD license is required.	Encode/decode. HD license is required.	Encode/decode. HD license is required.	Not supported.
	MPEG-2	Encode/decode. HD license is required.	Not supported	Not supported	Not supported.
	AVC-Intra	Encode/decode. Requires HD and AVC licenses.	Encode/decode. Requires HD and AVC licenses.	Encode/decode. Requires HD and AVC licenses.	Not supported.

Formats	Compression	1x	Multi-Cam, 3D/Video + Key	3x Super Slo-Mo	4K
	AVCHD/H.264	Decode only. Requires HD and AVC licenses.	Not supported	Not supported	Not supported.
	AVC - LongG	Decode only. Requires HD and AVC licenses.	Not supported	Not supported	Not supported.
	Avid DNxHD	Encode/decode. Requires HD and DNxHD licenses.	Encode/decode. Requires HD and DNxHD licenses.	Encode/decode. Requires HD and DNxHD licenses.	Not supported.
1080p	AVC-Intra Class 100	Encode/decode. Requires HD and 3G licenses.	Not supported	Not supported	Not supported.

Features of internal storage models

K2 Summit/Solo systems have media drives as follows:

- First generation K2 Summit system — Up to eight media drives
- K2 Summit 3G system — Up to twelve media drives
- K2 Solo Media Server — Two media drives
- K2 Solo 3G Media Server — Two media drives

This makes the internal storage K2 system a self-contained, stand-alone unit, with no external devices for storage connections required. You can transfer media in and out of the internal storage K2 system via Gigabit Ethernet. You can also export media to a mapped drive or USB-attached storage. With the K2 Solo Media Server, you can also export media via an ExpressCard.

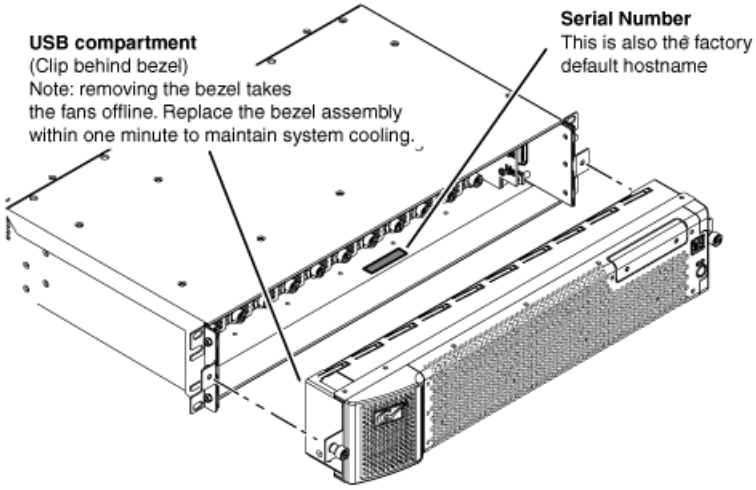
Features of external storage models

The external storage K2 Summit system contains only the system drive. There are no media drives in an external storage K2 Summit system. There are two types of external storage for media, as follows:

- Shared storage — Multiple external storage K2 Summit systems connect to the K2 SAN via Gigabit Ethernet or Fibre Channel to share a common pool of storage.
- Direct-connect storage — A single K2 Summit system with the optional Fibre Channel board installed connects directly to its own external (non-shared) RAID storage device. This makes the direct-connect K2 Summit system a self-contained, stand-alone unit, with no additional devices for storage connections required. You can transfer media in and out of the direct-connect K2 Summit system via Gigabit Ethernet.

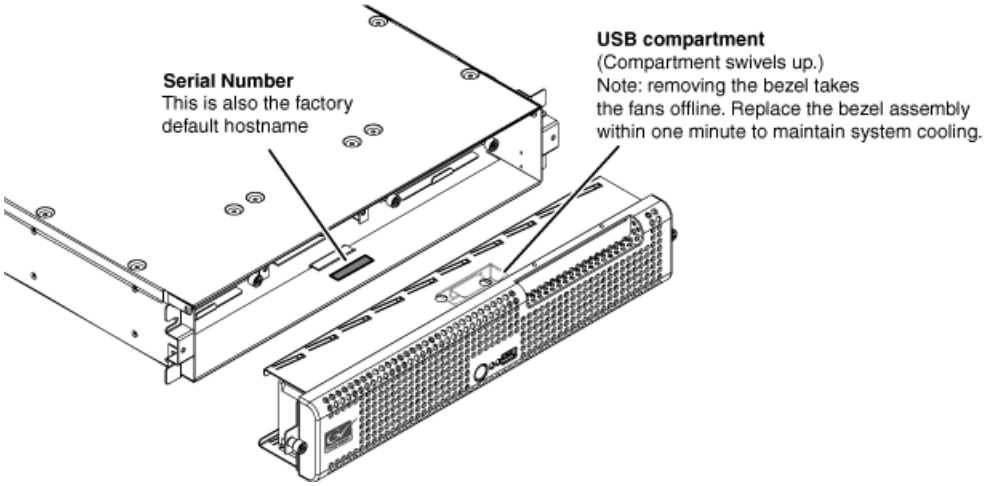
Product identification K2 Summit 3G

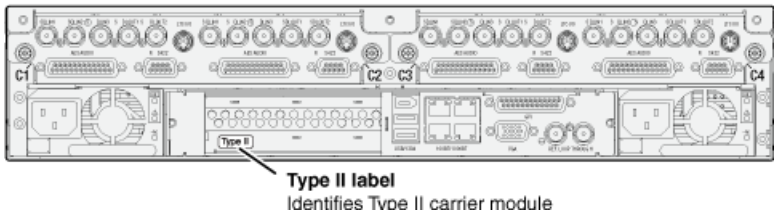
The K2 Summit 3G system has labels affixed to the chassis that provide product identification as illustrated:



Product identification first generation K2 Summit

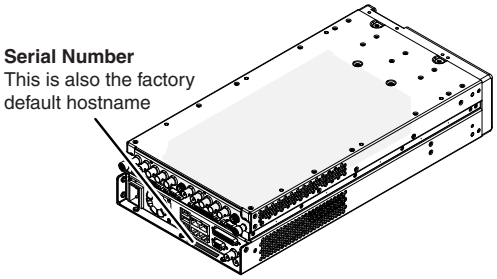
The first generation K2 Solo 3G system has labels affixed to the chassis that provide product identification as illustrated:





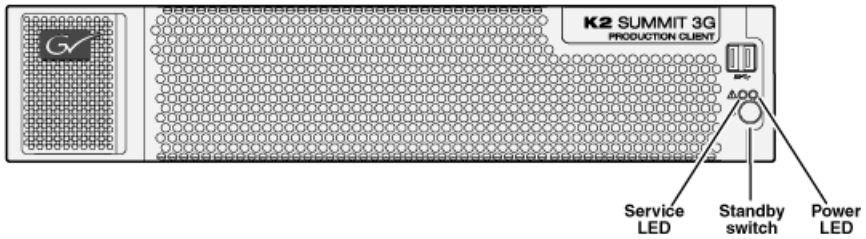
Product identification K2 Solo

K2 Solo 3G system have labels affixed to the chassis that provide product identification as illustrated:



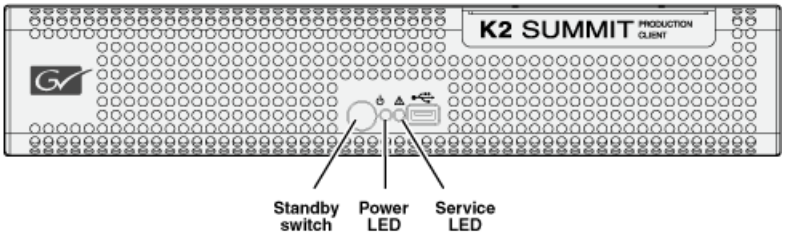
Front panel indicators K2 Summit 3G system

With the front bezel in place, the indicator LEDs are visible. The LEDs indicate the status of the machine. For example, when the Service LED is a steady yellow light, this could signify that one of the power cables is unplugged. For more information on indicator LEDs, see the "Servicing the K2 Summit system" section of the K2 Topic Library.



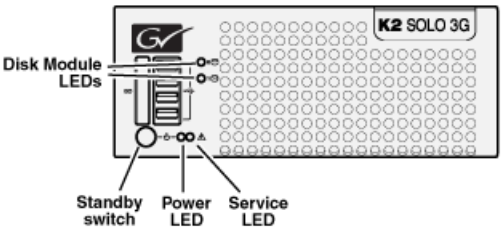
Front panel indicators first-generation K2 Summit

With the front bezel in place, the indicator LEDs are visible. The LEDs indicate the status of the machine. For example, when the Service LED is a steady yellow light, this could signify that one of the power cables is unplugged. For more information on indicator LEDs, see the service manual for your K2 product.



Front panel indicators K2 Solo

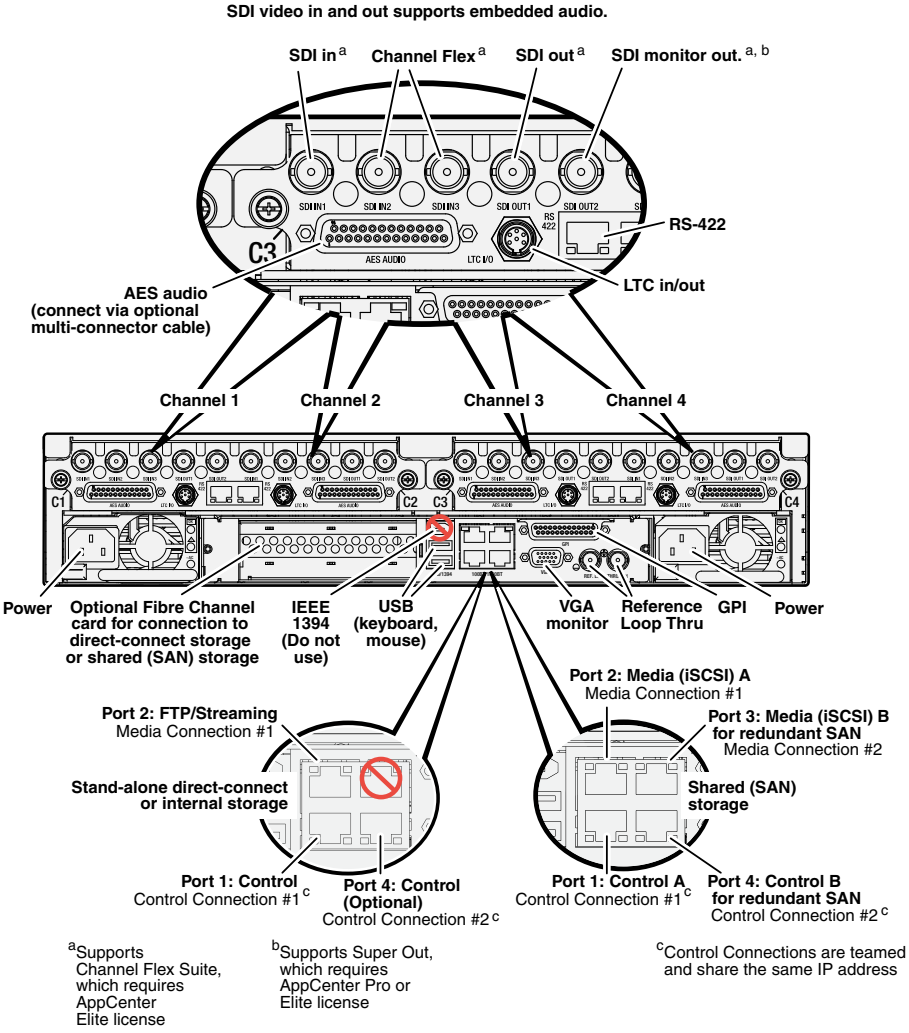
Both the first-generation K2 Solo system and the K2 Solo 3G system have the same front panel indicators. With the front bezel in place, the indicator LEDs are visible. The LEDs indicate the status of the machine. For example, when the Service LED is a steady yellow light, this could signify that one of the power cables is unplugged. For more information on indicator LEDs, see the service manual for your K2 product.



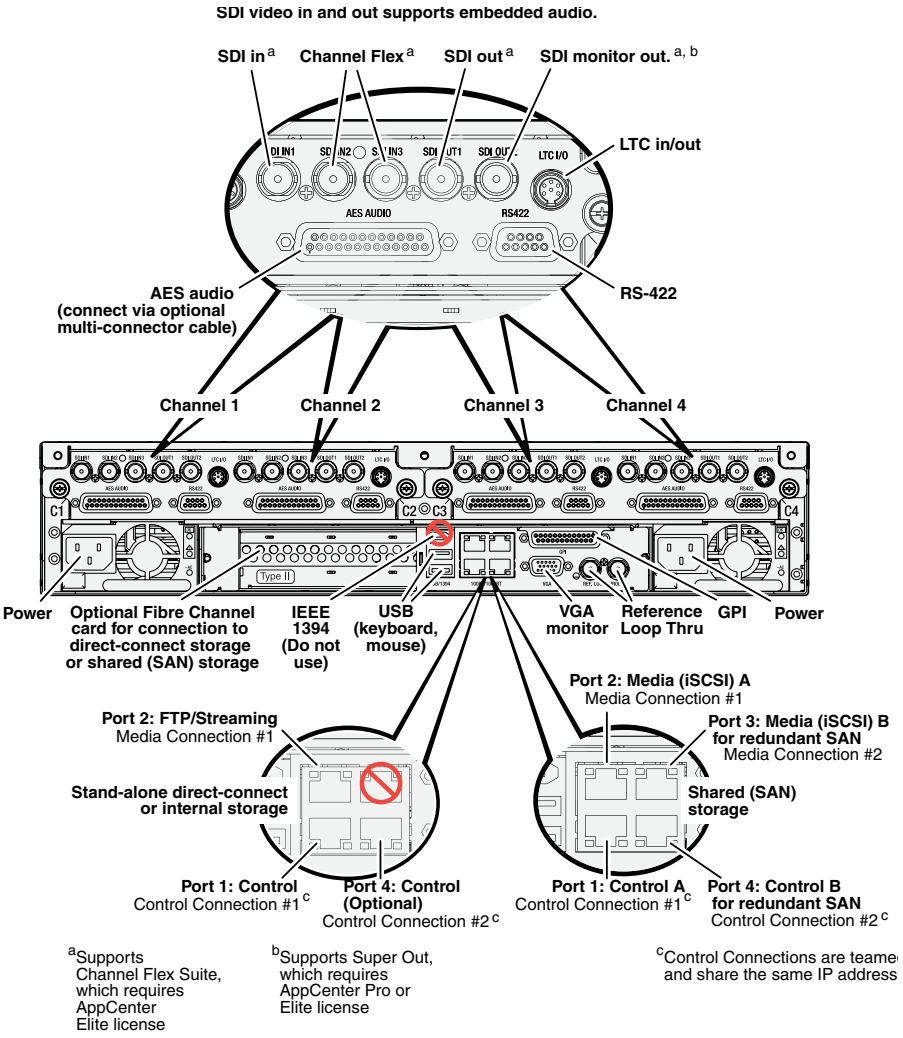
Rear panel view

The following illustrations identify the rear panel connectors and components.

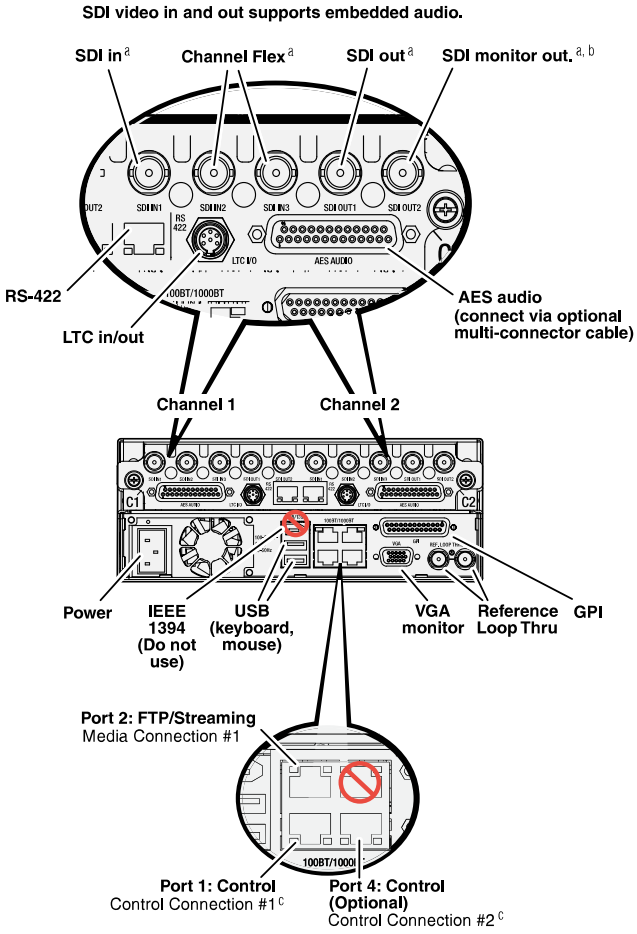
K2 Summit 3G models rear panel



K2 Summit first generation models rear panel



K2 Solo 3G Media Server rear panel

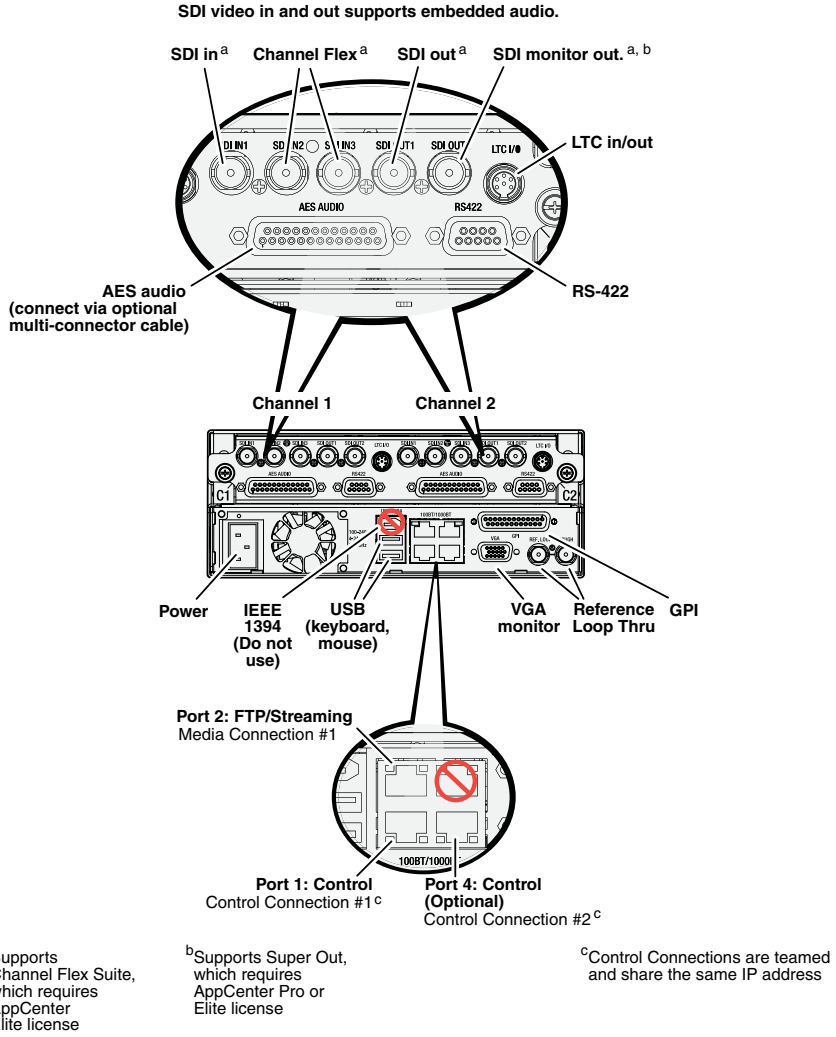


[a] Supports Channel Flex Suite, which requires AppCenter Elite license

[b] Supports Super Out, which requires AppCenter Pro or Elite license

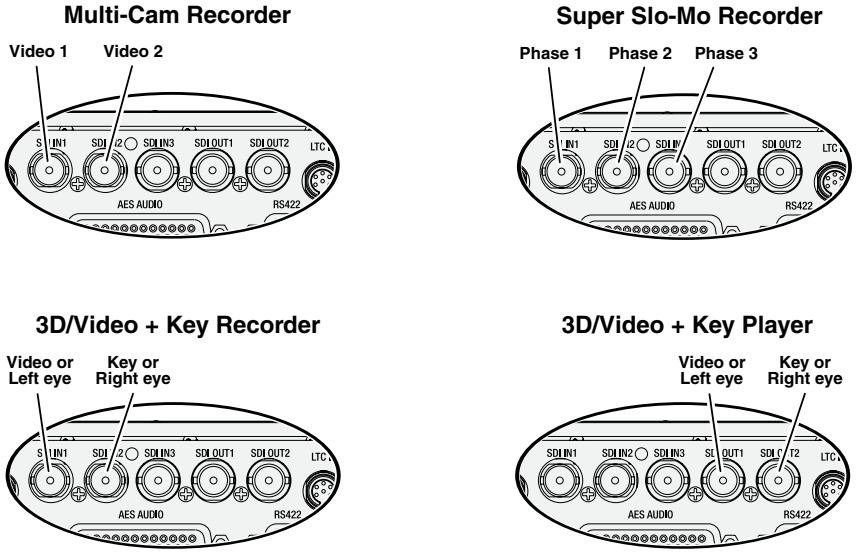
[c] Control Connections are teamed and share the same IP address

K2 Solo Media Server rear panel



ChannelFlex rear panel connections

ChannelFlex Suite features require the AppCenter Elite license. Super Slo-Mo also requires the HD license. When configured for these features, channel connections are as follows:



ChannelFlex Suite features do not support AVC-Intra Class 100.

Refer to the *K2 AppCenter User Manual* for more information on ChannelFlex Suite features.

Considerations for first startup out of box

When you receive a K2 system from the factory, one or more End User License Agreements (EULAs) appear on the screen at first startup. Software licensing agreements require that you accept these EULAs. When you do so, start up processes can proceed. This behavior occurs only at first startup. Subsequent startups do not exhibit this behavior.

K2 Summit/Solo system overview

The K2 Solo 3G system are purpose-built clients based on COM Express compact computer with dedicated systems to provide the video disk recorder functionality. This section explains the major architectural blocks.

Application System

The K2 Summit Production Client and K2 Solo Media Server application system architecture uses the COM Express form factor to provide functionality similar to that of standard PC-type computers. The carrier module contains a CPU module, built in Ethernet, and USB ports. On the K2 Summit Production Client, the carrier module also includes one PCIe board slot for expansion.

The Application system uses a Windows embedded operating system upon which all internal storage K2 system applications run for configuration and control of the unit.

Real Time System

Each channel hosts a complete Real Time system that provides the core video disk recorder functionality. Primary components are as follows:

- Dedicated processor for media access and processing.
- Codec circuits responsible for encoding/decoding video and processing audio and timecode, including the media-related input and output connectors.

The Real Time system uses a dedicated operating system. This operating system manages all the hardware involved in controlling the flow of video, audio, timecode, genlock, and GPI in and out of the K2 system.

Media control and processing

The following section explains how the Application system and the Real Time system work together to provide K2 system functionality.

The high processing requirements of digital video can overwhelm the processor on a standard desktop PC, resulting in wait-times that destroy the video's essential real-time aspect. The K2 system avoids this problem by providing dedicated systems that isolate processing needs. The components that work together to provide this functionality are as follows:

Application system — Dedicated to control, configuration, and networking functions that do not require real-time accuracy. The Application system has the following components:

- Application software provides the user interface for operating the K2 system. The software runs as Windows programs.
- The Media File system manages clips. It includes a database that associates the clip with its video, audio, and timecode files and a dedicated file system (separate from the Windows file system) that controls access to the raw data that makes up each file. Any reading and writing of clips, be it through play and record operations or through file transfers and media streaming, is managed by the database. The database and file system run as Windows programs.

Storage system — Includes the media disk drives, controllers, drivers, and adapters necessary for access and movement of the data. While the primary data flow is within the overall control of the Real Time system, some components and their communication pathways cross over into the Application system. For example, the media drives appear as the V: drive to the Windows operating system.

Real Time system — Manages the media flow between the Storage system and the inputs and outputs. The Real Time system has dedicated processors and time-sensitive mechanisms to serve media processing needs while maintaining real-time accuracy.

When you control play and record operations from within the Application system you trigger a chain of events that eventually crosses over into the Real Time system and results in media access. The following sequence is an example of this type of chain of events:

1. A user operates the Player application to play a particular clip. The Player application asks the Media File system for permission to access the clip. The Media File system grants access. In shared storage models, the Media File system enforces shared storage policies in order to grant the access. When access is granted, the Player application initiates play access to the clip.
2. The database identifies the files that make up the clip and the file system instructs the Storage system to open access to the files.
3. The Storage system finds the raw data and opens the appropriate read access. At this point both the Application system and the Real Time system are involved. Windows controls the media drives and controllers, so the Real Time system makes file requests to Windows and it causes the data to be transferred to buffers on the Real Time processor. The data is then available to the Real Time system so that it can be processed at exactly the right time.
4. The Real Time system processes the media, decompresses it, adjusts its timing, and moves it as required to play the clip as specified by the user.

Loop through, E to E, and feeds

Behaviors related to input signals routed to output connectors are described in the following topics.

Recording synchronous and asynchronous feeds

For best results in all workflows, use synchronous feeds, defined as follows:

- All outputs are locked to the house reference
- All inputs are genlocked to the house reference and at zero time

The K2 Summit Production Client and K2 Solo Media Server can record inputs that are asynchronous, with the following considerations:

- The encoder clock and the audio clock are derived from the input signal, which enables frame accurate recording of all inputs.
- Outputs are timed to the reference and if no reference is present, the output runs free.
- If the input video rate does not equal the output video rate (asynchronous) then video tearing or jumping can occur when input/output synch is critical, such as in the following:
  - K2 TimeDelay
  - SD-00 or Summit E-to-E (LoopThru) mode
  - HD-00 Loopback

Loop through on K2 Summit/Solo

The Player/Recorder application has a “E-to-E (LoopThru) mode” selection on the Control menu. This mode applies when the channel is under local AppCenter control as well as when it is under remote control, for all protocols.

This “E-to-E (LoopThru) mode” feature allows you to monitor the video that is being recorded. The video is routed back essentially untouched. Any audio or timecode that is on the input video stream is still there on the loop through output. The K2 Summit/Solo system and the loop through videos must be locked to a video reference for the loop through feature to work properly. This “E-to-E

(LoopThru) mode" feature should not be confused with true E to E. True E to E is not supported on the K2 Summit/Solo system.

When "E-to-E (LoopThru) mode" is not selected, the channel behaves as follows:

- "PB" is displayed on the channel pane, next to the Timecode Source indicator.
- When no clip is loaded, black plays out.
- When a record operation stops, Recorder becomes Player and the clip remains in the Player. The clip's last frame plays out.

When "E-to-E (LoopThru) mode" is selected, the channel behaves as follows:

- "EE" is displayed on the channel pane, next to the Timecode Source indicator.
- When no clip is loaded, the signal that is currently present at the channel input plays out.
- When a record operation stops, Recorder stays Recorder and the clip remains in the Recorder. The signal that is currently present at the channel input plays out.

Ports used by K2 services

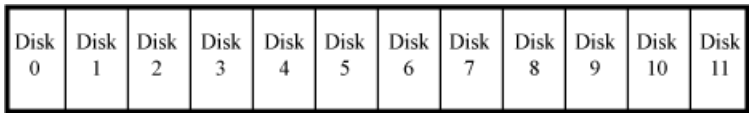
The following ports are used by the applications and system tools of the K2 family of products:

20	TCP: Used by mpgsession.exe, mxfsession.exe, gxfsession.exe, or ftpd.exe for FTP.
21	TCP: Used by ftpd.exe for FTP data.
81	Protocol: TCP. Used by SNFS for GUI (Java). User starts at port 81, redirected to 443.
161	UDP: Used by snmp.exe for SNMP.
162	UDP: Used by snmptrap.exe for SNMP trap.
443	Protocol: TCP. Used by SNFS for GUI (Java).
1062	Protocol: TCP. Used by SNFS for Blockpool. Both ports 1062 and 1063 if HA primary.
1063	Protocol: TCP. Used by SNFS for Blockpool. Both ports 1062 and 1063 if HA primary.
1070	Used by SNFS for GUI (Java connection to Linter).
1070	Used by SNFS for GUI (Java connection to Linter).
1527	Protocol: TCP. Used by SNFS for GUI (Java connection to derby database).
3389	TCP: Used by Remote Desktop for use by SiteConfig.
3811	Protocol: TCP. Used by Grass Valley AppService for 3rd party applications to communicate using AMP protocol. Used by SDB Server and GV STRATUS Rundown outgoing AMP communication to control playout channels.
5164	Protocol: TCP. Used by SNFS for fsmpm, IOPS.
5189	Protocol: TCP. Used by SNFS for HA Manager. Symbol HAMGR_DEFAULT_PORT.
8080	Protocol: TCP. Traffic: HTTP. Used by GV STRATUS Summit Services. Used by WCF service provided by the GV STRATUS Workflow Engine. Used by WCF service provided by the GV STRATUS Rules Engine.

8100	HTTP/TCP: Used by Macintosh systems for the SabreTooth licensing web service to check out licenses
8732	Protocol: TCP. Traffic: HTTP. Used by Site Config data service .
8733	Protocol: TCP. Traffic: HTTP. Used by K2 Config data service .
8734	Protocol: TCP. Traffic: HTTP. Used by Site Config data service .
8735	Protocol: TCP. Traffic: HTTP. Used by K2 Config data service.
14500	Protocol: TCP. Used by SNFS for snpolicyd.
18262	TCP: Used by GV ProductFrame Configuration Service, ProductFrame Discovery Agent Service for use by SiteConfig. Used by GV NetConfig Service. gv-pf. UDP: Used by GV NetConfig Service. gv-pf.
18263	UDP: Used by ProductFrame Discovery Agent Service for GV NetConfig Device Broadcast/Unicast Protocol. Used by SiteConfig. Sent by ControlPoint, received by Devices
18264	UDP: Used by ProductFrame Discovery Agent Service for GV NetConfig Controller Protocol. Used by SiteConfig. Sent by Devices, received by ControlPoint
20566	Protocol: TCP. Used by SNFS for MySQL. Only used internally on an MDC.
31820	Protocol: UDP. Used for live streaming from K2 Summit/Solo systems. This is the default base for UDP ports, with the range being 31820 to 31827. Other ranges are possible, depending on the UDP port base configured on the K2 Summit/Solo system.
49168	HTTP/TCP: Used by Grass Valley K2 Config for K2Config application connection between a control point PC and the K2 system device configured. Used for most functions.
49169	TCP: Used by Grass Valley K2 Config for K2Config application connection between a control point PC and the K2 system device configured. Used for a few functions that require longer time periods.
49170	HTTP: Used by Grass Valley Transfer Queue Service for Transfer Manager connection between source system and destination system.
49171	TCP: Used by Grass Valley AppService for AppCenter connection between control point PC and K2 client/Solo.
49172	HTTP: Used by Grass Valley Storage Utility Host for connection for Storage Utility between the control point PC and the K2 system being configured.
50872	UDP: Used by K2 Appcenter to discover K2 systems on the network.
60001	Protocol: TCP. Used by ACSLS Tape Libraries. Related to SNFS.
60002	Protocol: TCP. Used by ACSLS Tape Libraries. Related to SNFS.

RAID drive numbering K2 Summit 3G system

In the K2 Summit 3G system, internal RAID drives are numbered as follows. This numbering is displayed in Storage Utility.

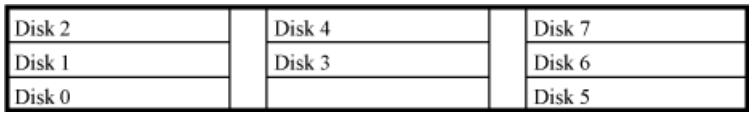


Drives are configured as RAID 1.

Drive numbering	Explanation
Disk 0	These two RAID drives make up LUN 0.
Disk 1	
Disk 2	These two RAID drives make up LUN 1.
Disk 3	
Disk 4	These two RAID drives make up LUN 2.
Disk 5	
Disk 6	These two RAID drives make up LUN 3.
Disk 7	
Disk 8	These two RAID drives make up LUN 4.
Disk 9	
Disk 10	These two RAID drives make up LUN 5.
Disk 11	

RAID drive numbering first generation K2 Summit system

In the first generation K2 Solo 3G system, internal RAID drives are numbered as follows. This numbering is displayed in Storage Utility. You cannot see the labeling on the K2 Summit Production Client chassis RAID drive when you remove the fan module.



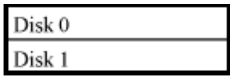
Drive numbering	Explanation
Disk 0	When configured as RAID 1, these two RAID drives make up LUN 0.
Disk 1	
Disk 2	When configured as RAID 1, these two RAID drives make up LUN 1.
Disk 3	

Drive numbering	Explanation
Disk 4	When configured as RAID 1, these two RAID drives make up LUN 2.
Disk 5	
Disk 6	When configured as RAID 1, these two RAID drives make up LUN 3.
Disk 7	

When drives are configured as RAID 0, each drive is considered its own LUN. As such, the order of LUNs and drive numbers as displayed in Storage Utility does not always correlate with the position of drives in the chassis.

RAID drive numbering K2 Solo system

In the K2 Solo 3G system, internal RAID drives are numbered as follows.



NOTE: **K2 Solo 3G system** ***drives are always configured as RAID 0.***

When drives are configured as RAID 0, each drive is considered its own LUN. As such, the order of LUNs and drive numbers as displayed in Storage Utility does not always correlate with the position of drives in the chassis.

Overview of K2 System Tools

Configuration Manager

The Configuration Manager is the primary configuration tool for a K2 Solo 3G system. It makes settings that apply to the overall internal storage K2 Solo 3G system as well as settings that apply to individual channels.

Configuration Manager settings are stored in a database. When the K2 Solo 3G system starts up it reads the current settings from the database and configures itself accordingly. When you modify a setting in Configuration Manager you must save the setting in order to update the database and reconfigure the K2 Solo 3G system.

You can also save settings out of Configuration Manager into a configuration file, which is a stand-alone XML file. Likewise, you can load settings into Configuration Manager from a configuration file. However, you must use Configuration Manager as the means to save the settings to the database before the settings actually take effect. Configuration files are not linked directly to the database.

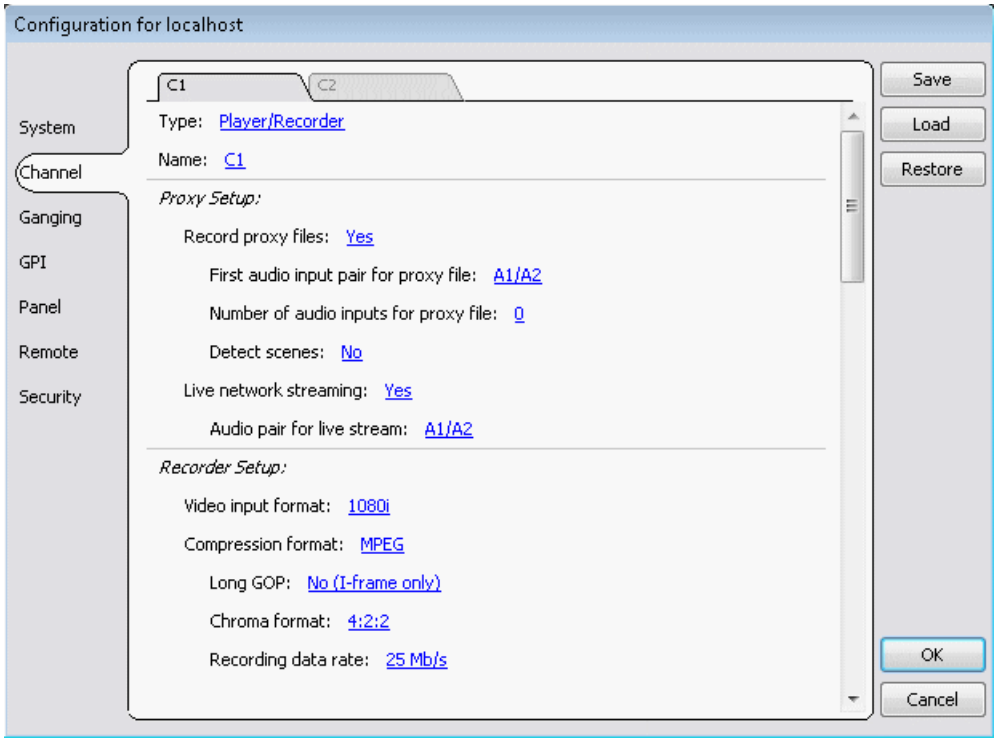
You can use configuration files as a means to back up your settings. You can also use configuration files to save several different groups of customized settings, each with a unique name, so that you can quickly load settings for specialized applications.

If you save a configuration file and then upgrade your K2 system software, there can be compatiblity issues. If the upgraded software version has new features, the saved configuration file might not be compatible.

Accessing Configuration Manager

You access Configuration Manager through the K2 AppCenter application from the local K2 Solo 3G system or from the Control Point PC.

To access the configuration settings, open AppCenter and select **System | Configuration**.



Saving and restoring Configuration Manager settings

Settings can be saved as a configuration file. You can save any number of uniquely named custom configuration files. You can load a configuration file to restore system settings.

To save custom settings:

1. In the Configuration Manager, click the **Save** button.

   The Save As dialog opens.

2. Use the up arrow or select folders to navigate to the folder in which you want to save the configuration file.
3. Enter a name for the configuration file.

   Do not name the file *Default*Config.xml, as this name is reserved for the factory default configuration file. Otherwise, standard Windows 2000 and up file naming restrictions apply.

4. Click **Save** and **Close**.

To restore custom settings:

1. If you want to save current settings, you should save them as a configuration file before continuing.
2. In the Configuration Manager, click the **Load** button.

   The Open dialog opens.
3. Use the up arrow or select folders to navigate to the custom configuration file.
4. Select the custom configuration file.
5. Click **Open**.

   The custom settings are loaded into Configuration Manager, but they have not been saved and put into effect.
6. Click **OK** to save and apply settings, and to close the Configuration Manager.

Restoring default Configuration Manager settings

You can restore factory default settings as follows:

- Restore some individual settings or groups of settings by selecting the **Default** button which appears below the settings in the configuration screen.
- Restore all the settings in Configuration Manager at once to their default values as explained in the following procedure.

1. If you want to save current settings you should do so before proceeding.
2. In the Configuration Manager dialog, click **Restore**.

   The default settings are loaded into Configuration Manager, but they have not yet been saved and put into effect.
3. Click **OK** to save settings and close Configuration Manager.

K2Config

The K2 System Configuration application (K2Config) is the primary tool for configuring systems in the category of a K2 SAN, which include online or production K2 SANs, K2 Nearline systems, and GV STRATUS Proxy Storage systems. Once the devices of the storage system are cabled and are communicating on the control network, you can do all the configuration required to create a working K2 SAN using the K2Config application. When you use SiteConfig for network configuration, you can import the SiteConfig system description file into the K2Config application to get you started with your SAN configuration.

After your K2 SAN is initially installed and configured, if you need to reconfigure the system you should do so using SiteConfig and the K2Config application. This enforces consistent policy and sequencing for configuration tasks, which makes the system easier to maintain and aids in troubleshooting should a problem arise.

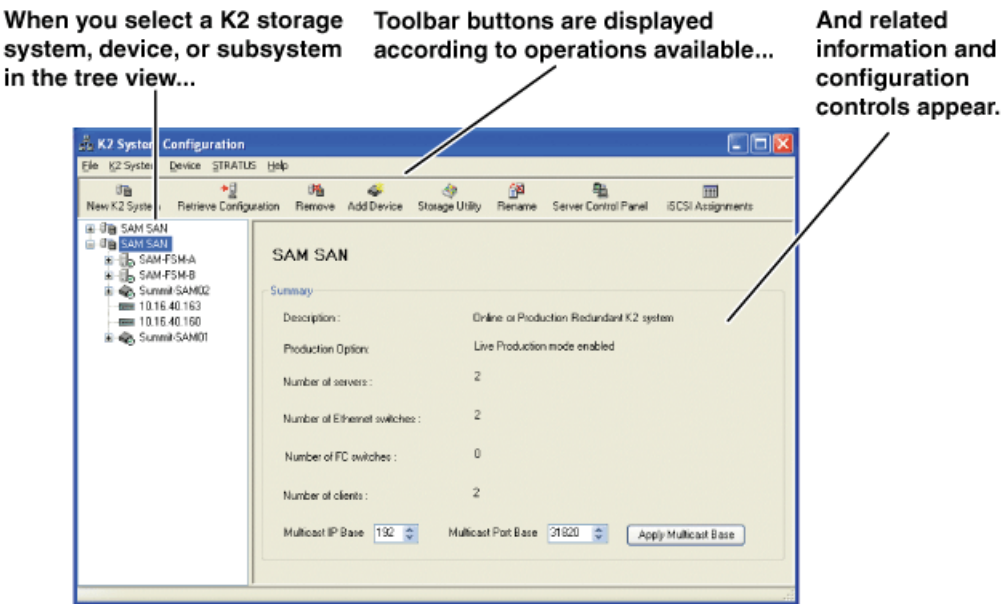
The K2Config application runs on a control point PC and accesses the devices of the K2 SAN via the control network. You can configure the devices of the K2 SAN as follows:

- SAN-attached K2/Summit systems and K2 Media Server — These devices are configured directly by the K2Config application.
- K2 RAID storage devices — The K2Config application launches a remote instance of Storage Utility, which configures RAID storage devices. Storage Utility components run on the K2 Media Server and the configuration actually takes place via the Fibre Channel connection between the K2 Media Server and the RAID storage device.
- Ethernet switches — The K2Config application can launch a switch's web-based configuration application.

You can expand and select nodes in the tree view to view K2 SANs, individual devices, and configuration settings. The configuration file is saved on the V: drive, along with the media files in the shared storage system. The configuration file is updated and saved whenever you change a configuration using the K2Config application. That is why you must always use the K2Config application to change settings on the storage system, so the most recently changed configurations will always be stored in the configuration file and displayed.

Opening the K2Config application

1. On the control point PC open the K2Config application shortcut on the desktop. The K2Config application log in dialog box opens.
2. Log in using the designated administrator account for configuring K2 SAN devices.
3. The K2Config application opens.



If you have one or more K2 SANs currently configured, the K2Config application displays the systems in the tree view.

If you have not yet configured a K2 SAN, the K2Config application opens with the tree view blank.

Storage Utility for standalone K2 Solo 3G system

There are two versions of Storage Utility:

- Storage Utility for the K2 SAN
- Storage Utility for stand-alone K2 systems

This manual explains Storage Utility for stand-alone K2 Solo 3G system. Refer to the *K2 SAN Installation and Service Manual* to learn about Storage Utility for the K2 SAN.

NOTE: For shared storage, run Storage Utility only via the* K2Config *application.

The Storage Utility is your primary access to the media file system, the media database, and the media disks of the K2 Solo 3G system for configuration, maintenance, and repair. It is launched from the K2 AppCenter application.

⚠ ***CAUTION: Use the Storage Utility only as directed by a documented procedure or by Grass Valley Support. If used improperly, the Storage Utility can render your K2 system inoperable or result in the loss of all your media.***

NOTE: Do not use the MegaRAID utility on a K2 system. This utility is for use by qualified Grass Valley Service personnel only. When this utility is opened it scans the SCSI bus and interferes with record and play operations.

Remote Desktop Connection

You can use the Microsoft Windows Remote Desktop Connection application to make a remote connection to a Grass Valley system that runs the Windows operating system.

Take the following into consideration when connecting to K2 systems:

- Before you can use the Remote Desktop Connection, you need network access and permissions to connect to the K2 system.
- You can use either the name or the IP address to access the K2 system.
- Do not use the Remote Desktop Connection to access the PC running the Control Point software or to access the AppCenter application; results may be unreliable.
- Take care when accessing an online K2 system on which media access is underway. The additional load on network and system resources could cause unpredictable results.
- Lack of robust video/graphic support can cause video display problems. Remote desktop connections can interrupt proxy and live streaming. AppCenter video monitoring is not supported through Remote Desktop Connection.

Accessing Remote Desktop Connection

1. Do one of the following:
   - Click the **Start** button on the Windows task bar
   - Press the Windows key on the keyboard.
2. Select **Programs | Accessories | Communications | Remote Desktop Connection**.

   The Remote Desktop dialog box opens.

3. Enter the name or IP address of the system to which you are making the remote connection and click **Connect**.

About SiteConfig

SiteConfig is Grass Valley's tool for network configuration and software deployment. SiteConfig is a ProductFrame application. ProductFrame is an integrated platform of tools and product distribution processes for system installation and configuration.

You can use SiteConfig as a stand-alone tool for planning and system design, even before you have any devices installed or cabled. You can define networks, IP addresses, hostnames, interfaces, and other network parameters. You can add devices, group devices, and modify device roles in the system.

As you install and commission systems, SiteConfig runs on a designated PC. It discovers devices, configures their network settings, and manages host files. SiteConfig also manages software installations and upgrades and provides a unified software package with compatible versions for deployment across multi-product systems.

You should use SiteConfig for network configuration and software deployment at installation and throughout the life of the system in your facility. This enforces consistent policy and allows SiteConfig to keep a record of changes, which makes the system easier to maintain and aids in troubleshooting should a problem arise.

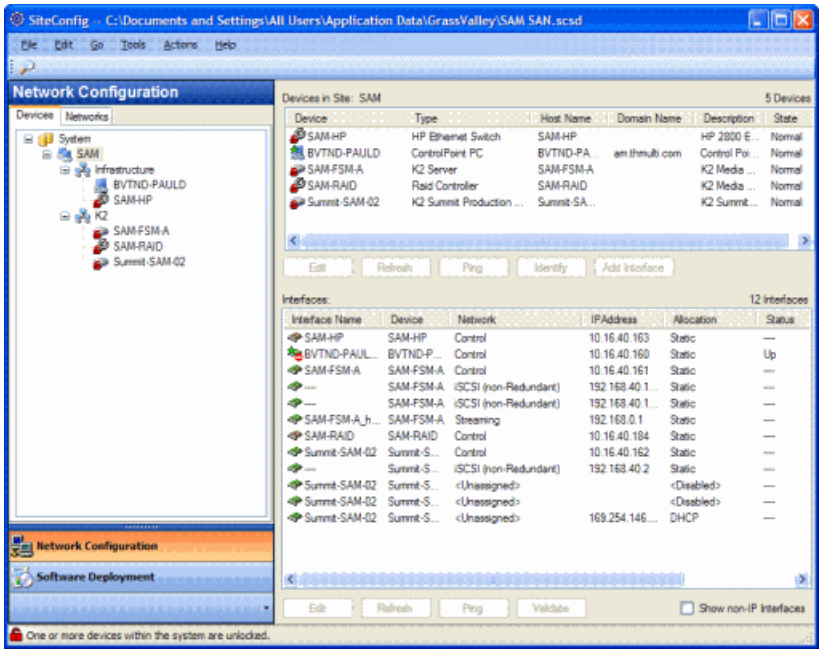
SiteConfig displays information from a system description file, which is an XML file.

Opening SiteConfig

1. Do one of the following: Use the SiteConfig shortcut on the Windows desktop or in the Start menu to open SiteConfig.
   - On the Windows desktop, click the **Grass Valley SiteConfig** shortcut. 
   - On the Windows **Start** menu, in the **Grass Valley** folder, click the **SiteConfig** shortcut. 
2. SiteConfig opens as follows:
   - If you have previously opened SiteConfig, the SiteConfig main window opens with the most recently used system description loaded.
   - If you have not previously used SiteConfig or if SiteConfig does not have access to a system description file, you are prompted to create a new system description or to import an existing system description.
3. Respond as appropriate.

SiteConfig main window

The SiteConfig main window is as follows:



The left side of the screen shows the tree view of the currently loaded system description. The Network Configuration and Software Deployment buttons at the bottom of the tree view activate either the network configuration workspace or the software deployment workspace.

The network configuration workspace on the left has two tabs: a Devices tab to display the tree of devices in the system and a Networks tab to show the hierarchy of networks defined in the system.

The software deployment workspace also has two tabs: a Devices tab that displays the same tree view of devices but provides information about the software roles assigned to the devices and the software currently installed on devices. The Deployment Groups tab provides the interface to manage software deployment tasks.

Select an item in the tree and the view on the right side of the screen shows details about the item selected. Select a site or group to show information about all the items that fall under the selected item.

Right-click an item to access a context menu of operations.

Icon overlays on items and tooltips provide status and warning feedback.

Grass Valley Recommended Deployment and Monitoring Solutions

To maximize up-time, a maintenance strategy must provide the ability to easily identify the root cause of an unanticipated hardware or software failure and to quickly compile failure data. The ability to proactively predict failures and to quickly notify those who can rectify them makes the maintenance strategy even more powerful. Grass Valley has a long history of building the necessary functionality into critical broadcast products. Beginning with Grass Valley's longstanding monitoring application NetCentral and progressing to the next generation tool GV GUARDIAN, remote monitoring and proactive predictive failure analysis are important contributors to Grass Valley

system solutions. Both NetCentral and GV GUARDIAN run on commercial off-the-shelf server PCs, such as the K2 system control point PC. Grass Valley and 3rd party devices report status via Window Messaging, Simple Network Management Protocol (SNMP), or syslog to the NetCentral or GV GUARDIAN application. Each application provides easy to use, fully autonomous remote monitoring to predict errors, provide proactive notifications, and centrally consolidate error logs and hardware failure information. Grass Valley recommends using a remote monitoring tool like NetCentral or GV GUARDIAN. With NetCentral, and even more so with GV GUARDIAN, you can maximize your up-time with less manpower, as compared to manual system monitoring. Watching for indicator lights, physically scanning logs, and other manual monitoring is far more time consuming, more error-prone, and much less accurate. If you have an existing NetCentral installation you install a NetCentral device provider on the NetCentral server PC for each type of device you are monitoring. Refer to NetCentral product documentation for installation and operating instructions. With GV GUARDIAN, only SNMP MIBs are required. Separate device providers are not necessary. Refer to the on-line GV GUARDIAN Topic Library for information.

System connections and configuration

About networks

The following section describe networks as they apply to K2 systems. Also refer to the *K2 SAN Installation and Configuration Guide* for more detailed information about K2 SAN networking.

Control network description

The control network is for communication between devices and components. It does not have real-time media traffic or streaming/FTP media traffic. The control network traffic must be separated from the streaming/FTP network traffic and the media (iSCSI) network traffic. This separation may be provided by different subnets, VLANs, or physical switch fabrics. The control network and the streaming/FTP network, if on different subnets, may be on the same VLAN. The control network and the media (iSCSI) network must not be on the same VLAN. Static IP addresses with name resolution via host files are recommended for the control network.

Streaming/FTP network description

The streaming/FTP network is for media transfers and FTP traffic. The streaming/FTP network network traffic must be separated from the control network traffic and the media (iSCSI) network traffic. This separation may be provided by different subnets, VLANs, or physical switch fabrics. The control network and the streaming/FTP network, if on different subnets, may be on the same VLAN. The control network and the media (iSCSI) network must not be on the same VLAN. Static IP addresses with name resolution via host files are recommended for the streaming/FTP network. Hostnames of network adapters that are dedicated to the streaming/FTP network must be aliased in the hosts file with the `_he0` suffix. This directs the streaming traffic to the correct port.

Media (iSCSI) network description

The media network is exclusively for real-time iSCSI traffic on a K2 SAN. It must be on a different subnet than the control network and the streaming/FTP network. Furthermore, its traffic is kept

physically separate from that of other networks. This separation is provided by dedicated ports, cables, and by a dedicated VLAN on the Ethernet switch or by separate switches. Static IP addresses are required for the media network. Name resolution is not necessary, so media network IP addresses are not required in host files.

Network considerations and constraints

- If your GV STRATUS system is on a domain, all servers and client PCs on that system that have any interaction with Grass Valley components must be logged on to Windows with a domain user account. Do not use a local user account.
- Do not use any 10.1.0.n or 10.2.0.n IP addresses. These are used by the K2 RAID maintenance port and must be reserved for that purpose. If these addresses are otherwise used, maintenance port communication errors occur.

Network connections

Use the information in this section as appropriate to connect the Gigabit (1GBaseT) Ethernet network for your application:

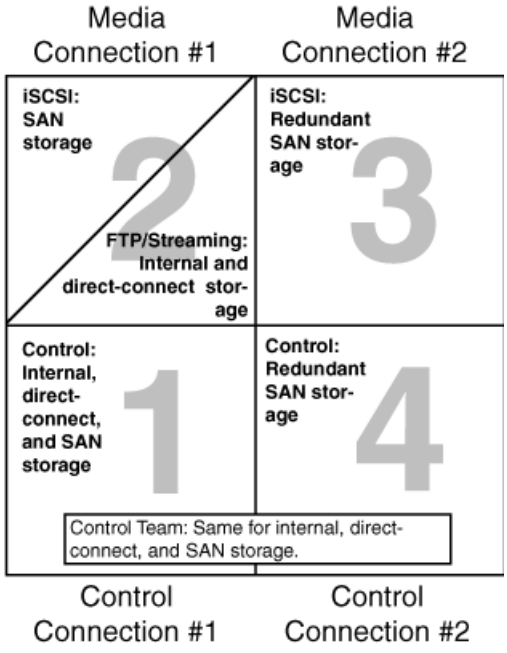
Ethernet cable requirements

For making Ethernet connections, cabling must meet the following requirements:

- Use CAT5e or CAT6 cables. The maximum cable length is 50 meters for CAT5e and 100 meters for CAT6.

About network ports

When you receive a K2 Summit Production Client or K2 Solo Media Server from the factory, it has a specific network configuration, including a loopback adapter and two of the four Gigabit Ethernet ports configured as a teamed pair. The Gigabit Ethernet ports, as viewed when looking at the rear panel, are represented in the following illustration.

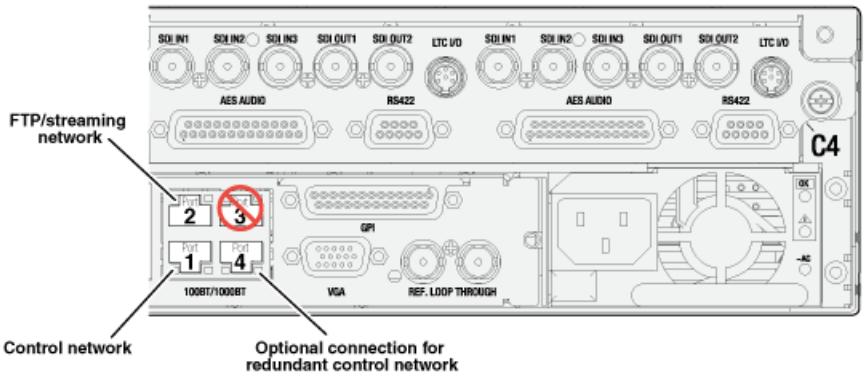


The K2 Solo Media Server is not supported for SAN (shared storage) connection.

Making network connections

Connect network ports as appropriate for the K2 Solo 3G system storage option as in the following illustrations. In these illustrations the first generation K2 Solo 3G system is shown. Connections are identical on the K2 Summit 3G system.

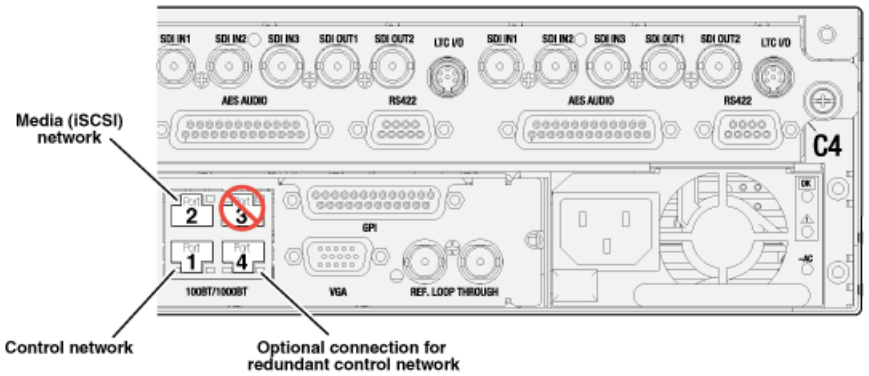
Stand-alone storage K2 Summit/Solo network connections



On a K2 Solo Media Server, an internal storage K2 Summit system, or a direct-connect storage K2 Summit system, connect the control network to port 1, which is the first port of the control team. If you have a FTP/streaming network, connect that network to port 2. Port 3 is not used. In most cases

port 4, which is the second port of the control team, is not used, although it is available to provide additional redundancy for the control network connection.

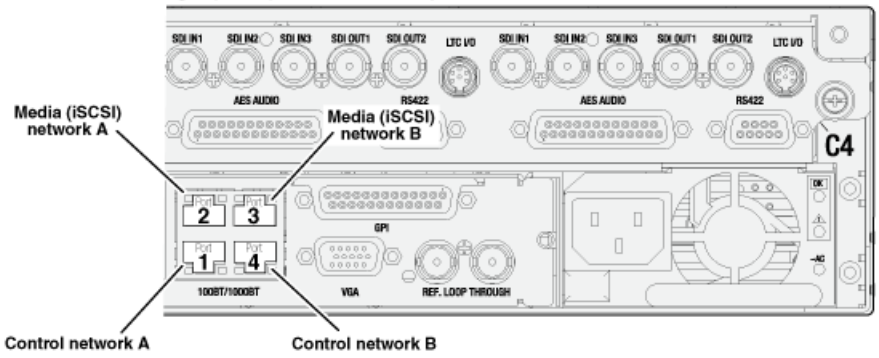
Basic shared storage (SAN) K2 Summit system network connections



On a non-redundant shared storage (SAN) K2 Summit system, connect the control network to port 1, which is the first port of the control team. Port 2 must be connected to the media (iSCSI) network. Port 3 is not used. Port 4, which is the second port of the control team, is not used except as follows: Port 4 may be used only if you extend your control network to provide the same redundancy as that of a redundant K2 SAN.

Refer to topics in this document for more information.

Redundant shared storage (SAN) K2 Summit system network connections



On a redundant shared storage (SAN) K2 Summit system, you must connect both ports of the control team. Connect control network connection A to port 1 and control network connection B to port 4. You must also connect both media ports. Connect port 2 to the A media network and port 3 to the B media network. The media ports must not be teamed, as doing so interferes with failover functionality.

Refer to topics in this document for more information.

Network configuration

This section contains instructions for configuring network connections.

About network functionality

K2 networks support the following:

- Remote control and configuration of the internal storage K2 system using AppCenter from a Control Point PC.
- Remote control of the internal storage K2 system using devices and applications software developed for the K2 system that use industry standard remote control protocols over Ethernet.
- Stream media transfers between K2 systems and other supported Grass Valley systems. Streaming transfers allow loading and playing a clip before the transfer is complete.
- Standard data network capability.
- General networking tasks such as file sharing and mapping network drives.

The procedures in this section guide you to relevant settings, but do not instruct you on the specific settings required for your network. It is assumed that you understand Ethernet networks in general and your particular network needs and that you can apply that understanding to make the required settings using standard Windows procedures. If you need help with these procedures, contact your network administrator.

Refer to the *K2 SAN Installation and Service Manual* for network configuration procedures for shared storage K2 clients.

About modifying or restoring network settings

Before configuring network settings, consider the following:

- Loopback adapter — When you receive a K2 Summit Production Client, a K2 Solo Media Server, or a K2 Media Client from the factory, it has a loopback adapter installed. The loopback adapter allows the media file system to continue operating if an Ethernet cable is disconnected. Do not modify the loopback adapter. If you need to restore the loopback adapter, refer to the Service Manual for your K2 product.

  The loopback IP address is 192.168.200.200. Keep that IP address reserved on your network. Do not assign it to any other device. If this causes conflicts with your existing network, consult your Grass Valley representative.
- Hostname changes — If you change the host name, remote AppCenter and other systems could have difficulty connecting. On a shared storage K2 client, Grass Valley strongly recommends that you do not change the host name or IP address unless following the documented procedure. For more information, refer to the *K2 SAN Installation and Service Manual*.
- Restoring factory default network settings — Several settings are configured at the factory and should never be modified. If you suspect settings have been changed, you should reimage the K2 system to restore settings. Refer to the Service Manual for your K2 product for recovery image and network configuration procedures.

Configure network settings for a stand-alone K2 systems

Stand-alone K2 systems with internal or direct-connect storage ship from the factory DHCP configured. If your control network has DHCP/DNS and you are satisfied to use the factory default host name (which is the serial number), then no local configuration of the control connection is required.

If the Windows network settings need to be configured, you must have Windows administrator security privileges on the K2 system.

1. Access the Windows desktop on the K2 system. You can do this locally with a connected keyboard, mouse, and monitor or remotely via the Windows Remote Desktop Connection.
2. Open the Network Connections Control Panel.
3. Continue with standard Windows procedures to configure the TCP/IP protocol properties. You can set up the network using DHCP, DNS, WINS, or other standard networking mechanisms.

   ***NOTE: On small networks or networks with certain security policies a DHCP server or domain name server (DNS) might not be available. In this case you can set up a static IP address and create a host file on each* K2 system.**

4. Configure the control connection on the K2 system as follows:
   a) Configure the network connection with the following name:

      Control Team

      The control team is GigE ports 1 (Control Connection #1) and 4 (Control Connection #2) on the rear panel.

      ⚠ ***CAUTION: Under no circumstances should you modify the loopback adapter. The loopback IP address is 192.168.200.200. Keep that IP address reserved on your network. Don't assign it to any other device. If this causes conflicts with your existing network, consult your Grass Valley representative.***

5. Configure the FTP/streaming connection (if needed) on the K2 system.

   This connection must have an IP address that is on a different subnet from the control connection. There are special name resolution requirements for the FTP/streaming network.

   Configure as follows:

   a) Configure the network connection with the following name:

      Media Connection #1

      This is GigE port 2 on the rear panel.

6. If prompted, shutdown and restart Windows.
7. If you are going to FTP/stream video between K2 systems, configure for streaming video between K2 systems; otherwise, the K2 system is ready for standard data networking tasks.

Streaming video between K2 systems

It is required that FTP/streaming traffic be on a separate subnet from control traffic and, in the case of a K2 SAN with shared storage K2 clients, separate from media (iSCSI) traffic. To reserve bandwidth and keep FTP/streaming traffic routed to dedicated ports, IP addresses for FTP/streaming ports must have double name resolution such that hostnames are appended with the "_he0" suffix. You can use host tables or another mechanism, such as DNS, to provide the name resolution. This directs the streaming traffic to the correct port.

In most K2 systems, network name resolution is provided by host tables, which are found in hosts files. The following procedure describes how to set up hosts tables to provide name resolution for both the control network and the FTP/streaming network. If you are using other mechanisms for

name resolution, use the host table examples here to guide you. For shared storage K2 clients, also refer to the *K2 SAN Installation and Service Manual* for a discussion of host tables.

Setting up the K2 system for FTP/streaming transfer has the following network requirements:

- For stand-alone internal storage K2 systems, the K2 machine is the source/destination for FTP/streaming transfers. FTP/streaming traffic uses the FTP GigE port (Media Connection #1) on the K2 client.
- For K2 Summit Production Clients or K2 Media Clients with shared storage on a K2 SAN, a K2 Media Server is the source/destination for FTP/streaming transfers. FTP/streaming traffic uses the FTP GigE port on the K2 Media Server. No transfers go to/from the shared storage K2 client directly.
- Some kind of name resolution process must be followed. You have the following options:
  - Set up hosts files located on each networked device so that you reference host names through the hosts files.
  - Edit the DNS entries. See your network administrator.
- The host name of all peer K2 systems and Profile XP systems must be added to a Remote host registry using the K2 AppCenter Configuration Manager.
- To import to or export from a K2 system, both the source and destination must be in the same domain.

Set up hosts files

Set up a hosts file located in `C:\WINDOWS\system32\drivers\etc\hosts` on each K2 system. If you include the names and addresses of all the systems on the network, then you can copy this information to all the machines instead of entering it in the hosts file on each machine.

To provide the required name resolution for the FTP/streaming network, in the hosts file each system that is a transfer source/destination has its host name listed twice: once for the control network and once for the FTP/streaming network. The host name for the streaming network has the extension "_he0" after the name. The K2 systems use this information to keep the FTP/streaming traffic separate from the control traffic.

For FTP transfers to/from a K2 SAN, transfers go to/from K2 Media Servers that have the role of FTP server. No transfers go directly to/from the shared storage K2 clients that are on the K2 SAN. So in the hosts file, you must add the "he_0" extension to a K2 Media Server hostname and associate that hostname with the K2 Media Server's FTP/streaming network IP address.

1. Open Notepad or some other text editor. When you open the text editor you must right-click and select **Run as administrator**.
2. In the text editor, open the following file:

   `C:\WINDOWS\system32\drivers\etc\hosts`

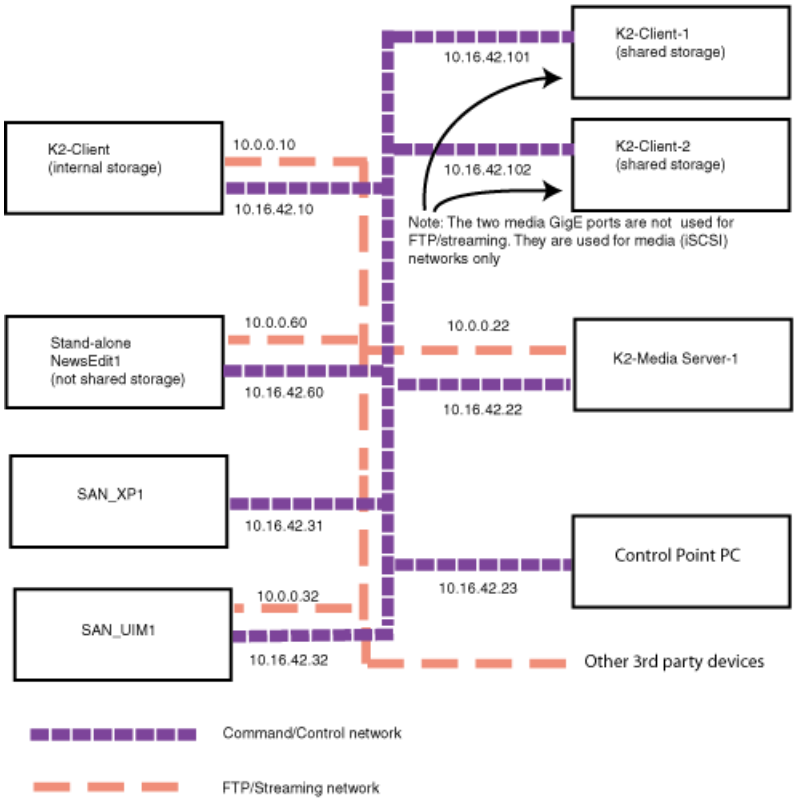
3. Enter text in two lines for each K2 system that is a transfer source/destination.
   a) Type the IP address for the control network, then use the TAB key or Space bar to insert a few spaces.
   b) Type the machine name, such as `K2-Client`. This sets up the host file for resolving the machine name on the control network. The machine name must not have any spaces in it.
   c) On the next line, type the IP address for the FTP/streaming network, then use the TAB key or Space bar to insert a few spaces.
   d) Type the machine name followed by the characters "_he0". Be sure to use the zero character, not the letter 'o'. Refer to the following example:

```
00.16.42.10   K2-Client
00.0.0.10     K2-Client_he0
```

4. For systems that are not a transfer source/destination, the second line (for the FTP/streaming network) is not required.
5. If there are UIM systems on the FTP/streaming network, make sure you follow the UIM naming conventions. Refer to the *UIM Instruction Manual*.
6. Once you have added the host names for the all the systems on the networks for which the host file provides name resolution, save the file and exit the text editor.
7. Copy the hosts file onto all the other machines to save you editing it again.
8. Add host names to AppCenter to enable streaming.

Sample K2 client configuration and hosts file

The following diagram illustrates one possible configuration setup, including a K2 system with stand-alone storage, K2 clients with shared (SAN) storage, and other Grass Valley systems.



The following example shows the contents of a default Windows hosts file with new lines added that match the IP addresses and host names in the previous sample diagram.

All lines beginning with a # are comments and can be ignored or deleted.

```
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# For example:
# 102.54.94.97     rhino.acme.com # source server
# 38.25.63.10      x.acme.com   # x client host

127.0.0.1          localhost

10.16.42.10        K2-Client
10.0.0.10          K2-Client_he0

10.16.42.101       K2-Client-1
10.16.42.102       K2-Client-2

10.16.42.22        K2-MediaServer-1
10.0.0.22          K2-MediaServer-1_he0

10.16.42.23        ControlPointPC

10.16.42.60        NewsEdit1
10.0.0.60          NewsEdit1_he0
```

```
10.16.42.31         SAN_XP1
10.0.0.32           SAN_XP1_he0 SAN_UIM1_he0
10.16.42.32         SAN_UIM1
```

Add host names to AppCenter to enable streaming

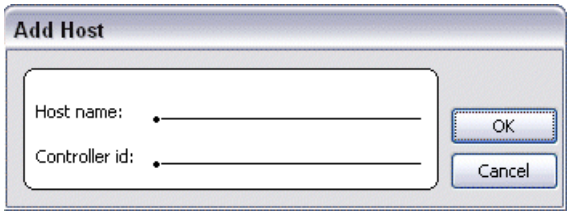
In K2 AppCenter, you must add the host names of all peer K2 systems on the network that support streaming transfers. Adding host names is required to allow selection of networked K2 systems in the AppCenter user interface and to provide a successful network connection for streaming. The host names added appear in the "Import" and "Send to" dialog boxes.

NOTE: By default, the K2 system host name is the same as the Windows operating system computer name.

1. Open AppCenter for the K2 client.
2. In the AppCenter toolbar, select **System**, then choose **Configuration**.
3. Select the **Remote** tab.

   The Remote Settings dialog box displays, showing any network host names that have been added.
4. Select **Add**, to open the Add Host dialog box, then do the following:
   a) Select the Host name field, then enter the computer name of a peer K2 system.

      Make sure to enter the exact computer name. Any differences will result in being unable to connect to the K2 system.



   b) If you are using VDCP remote protocol to perform video network transfers, use the following steps to add a unique Controller ID for each host. Otherwise, you can ignore this step and proceed to the next step.

      - Select controller id field.
      - Enter the controller ID of the K2 system, then select **OK**. Use a number between 1 and 255 that is not assigned to any other K2 system.

   c) Select **OK** in the Add Host dialog box.
5. Repeat the previous step for the remaining K2 systems.
6. In the Configuration dialog box, select **OK** to save settings.

Once the host names are added, the K2 system is ready for streaming operation. For information on transfer compatibility and supported formats, refer to K2 system specifications. For procedures on transferring media, refer to the *K2 AppCenter User Manual*.

NOTE: If you have trouble, try using the ping utility in the Windows command prompt using either the IP address or host name. Troubleshoot as needed. Also, refer to the Service Manual for your K2 system for troubleshooting procedures.

Configuring Server 2008 for domain

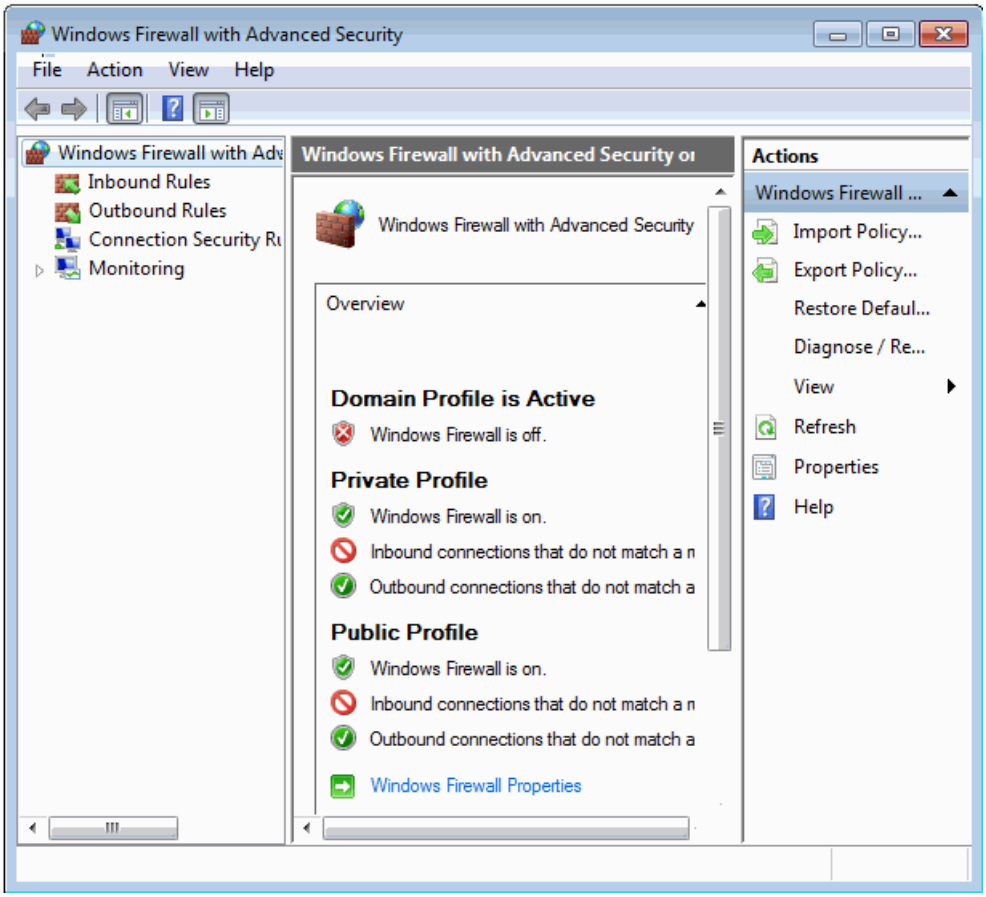
This topic applies to Grass Valley servers with a base disk image created prior to mid-2011. Server disk images created after that time do not require this special configuration.

Systems with the Microsoft Windows Server 2008 R2 operating system require special configuration. A server must have its firewall disabled for proper K2 system operation. This includes the Windows firewall that has different profiles for workgroup, domain, etc. You must do the following steps to disable the firewall.

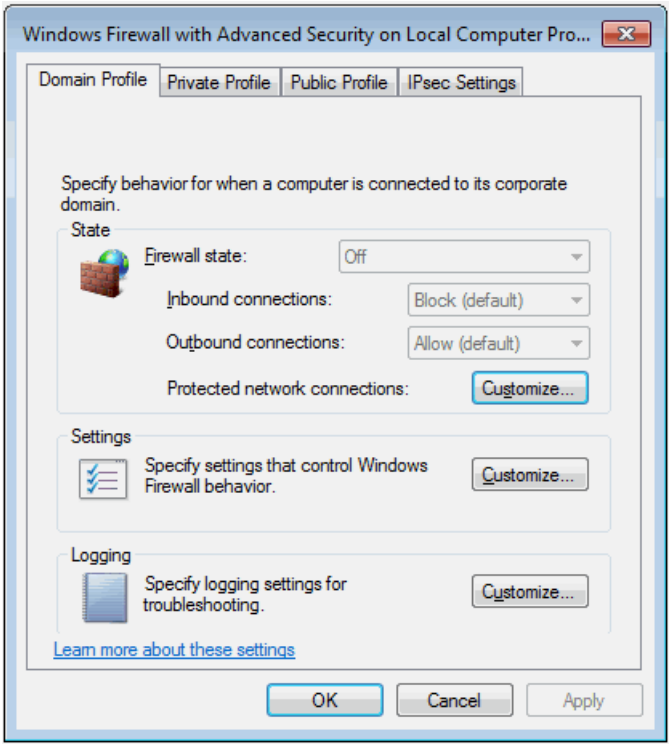
1. Log in to the server with Windows administrator privileges.
2. From the Windows desktop click **Start** and in the **Search programs and files** box type the following and then press **Enter**.

   `wf.msc`

   The Windows Firewall with Advanced Security window opens.



3. At the bottom of the Overview section, click **Windows Firewall Properties**.
   The Properties dialog box opens.



4. On the **Domain Profile** tab, set **Firewall state** to **Off**.
5. On the **Private Profile** tab, set **Firewall state** to **Off**.
6. On the **Public Profile** tab, set **Firewall state** to **Off**.
7. Click **OK** to save settings and close.

Using FTP for file transfer

This section contains topics about the K2 FTP interface.

About the K2 FTP interface

The K2 FTP interface has the following modes:

- Movie mode — FTP operations are performed on assets in the K2 media database. This is the mode on a K2 systems with a media database, such as online/production K2 SANs and stand-alone K2 Summit systems.
- File mode — FTP operations are performed on files. This is the mode on systems without a media database, such as Nearline K2 SANs.

The K2 FTP interface can run in the movie mode and the file mode simultaneously.

On online/production K2 SANs and stand-alone K2 Summit systems, FTP clients can log into the K2 FTP server using credentials for Windows user accounts that are registered on the K2 system. When such accounts are used, the K2 FTP server exposes “virtual” folders at the FTP root. A virtual folder exists for each video file format that is supported by the FTP server. Navigation to one of these virtual folders allows an FTP client to get or put clips in that file format.

In addition, the K2 FTP server supports reserved user login names that directly places the FTP client in a particular mode of operation. The FTP login names and their modes are as follows:

movie FTP gets/puts supported for K2 clips in the GXF file format; the clip's root becomes the FTP root.

mxfmovie FTP gets/puts supported for K2 clips in the MXF file format; the clip's root becomes the FTP root

mpegmovie FTP puts supported for MPEG program and transport streams; the clip's root becomes the FTP root

video_fs Pinnacle FTP emulation mode

k2vfs All FTP operations supported on generic files on the K2 system's media file system; media file system root becomes the FTP root.

You can use Internet Explorer to access the FTP interface to see an example.

The K2 FTP server runs on K2 Media Server that has the role of FTP server. While it also runs on the K2 Solo Media Server, stand-alone storage K2 Summit Production Clients and K2 Media Clients, it is important to understand that it does not run on shared storage K2 clients. When you FTP files to/from a K2 SAN, you use the FTP server on the K2 Media Server, not on the K2 client that accesses the shared storage on the K2 SAN.

If clips are created by record or streaming on a K2 file system such that media files have holes/gaps, i.e. unallocated disk blocks, in them, then that clip represents a corrupt movie that needs to be re-acquired. The K2 system handles corrupt movies of this type on a best-effort basis. There is no guarantee that all available media, especially media around the edges of the holes/gaps, is streamed.

You can also apply K2 security features to FTP access.

When using FTP in a shared storage environment, ensure that all FTP communication takes place on the FTP/streaming network, and not on the Control network.

Limitations with complex media types

Depending on the system software versions of source and destination devices, it is possible that lists or programs containing mixed video formats or compression types, or mixed audio types cannot stream to other devices, nor can they be exported to a file. Refer the "About This Release" section of the K2 Topic Library for the specific software versions for details.

Exporting in GXF preserves sequences and lists in their original form.

For other formats, exporting sequences and lists with uniform video and audio types generates a file that represents a single continuous clip (a clip with no cuts), which is called "flattening". Flattening

a list preserves only the video and audio referenced by the list – all control features such as looping, transitions and mix effects are lost.

Flattening export is not supported for sequences and lists containing mixed video and audio types or lists and sequences containing long GOP video tracks.

Transferring between different types of systems

While GXF transfer of media with mixed format (such as an agile playlist) is supported between K2 systems, it might not be supported between a K2 system and a non-K2 system, depending on system software versions. Refer to the release notes for the software version.

You can also use remote control protocols to initiate transfers.

Transfer mechanisms

You can move material between systems using the following mechanisms, each of which offers a different set of features:

- Manual mechanisms — These are the AppCenter transfer features. Refer to the K2 AppCenter User Manual for AppCenter instructions. When transferring between K2 systems you can browse and select files for transfer. When transferring between K2 systems and other types of systems, one or more of the following might be required, depending on software versions. Refer to release notes for the version information:
  - Specify the IP address, path, and file name to initiate a transfer.
  - Add the remote host in Configuration Manager before the transfer.
  - Enter machine names in compliance with UIM naming conventions.
- Automatic mechanisms, including the following:
  - K2 FTP interface — This interface supports transfers via third party FTP applications, such as automation systems. To demonstrate this, you can use Internet Explorer to transfer files between a PC and the FTP interface on a stand-alone K2 Summit Production Client or a K2 Media Server on the same network.
  - Remote control protocols — Industry standard remote control automation applications can initiate transfers. The protocol command must be sent to the K2 client. This applies to both stand-alone and shared storage K2 systems.

Related Topics

Configuring FTP Overwrite setting on page 158

FTP access and configuration

For basic LAN access, the following Grass Valley products can connect as an FTP client to the K2 FTP server with no special configuration required:

- K2 Summit Production Client
- K2 Media Client
- K2 Solo Media Server

- UIM-connected Profile XP Media Platform

For WAN access, contact your Grass Valley representative for assistance.

If the FTP client is not one of these Grass Valley products, contact the product's supplier or your network system administrator for assistance with configuring TCP window scaling. Any computer that connects as an FTP client to the K2 FTP server must have TCP window scaling enabled. Refer to http://support.microsoft.com/kb/q224829/ for more information on this feature. Never set Tcp1323Opts without setting TcpWindowSize. Also, Windows NT 4.0 does not support TCP window scaling, but will still communicate with Grass Valley products in a LAN environment.

FTP access by automation

Using FTP, third parties can initiate transfers between two K2 systems or between a K2 system and another FTP server. Transfers of this type are known as "passive" FTP transfers, or "server to server" transfers.

If you are managing transfers with this scheme from a Windows operating system computer, you should disable the Windows firewall on that computer. Otherwise, FTP transfers can fail because the Windows firewall detects FTP commands and can switch the IP addresses in the commands.

NOTE: You should disable the Windows firewall on non-K2 systems issuing passive FTP transfer commands.

FTP and media access security

The following systems host the K2 FTP interface:

- A stand-alone K2 system.
- A K2 Media Server that takes the role of FTP server

The way in which the K2 FTP interface applies media access security is explained in this section.

The K2 FTP interface uses the credential information for the current FTP session logon and checks it against the access control list for a K2 bin. This is the access control list that you set up through the Organize Bins dialog box in AppCenter. Any media access related operations such as get, put, dir, rename and delete are checked against the FTP session's logon credentials to access the media. For example, if an FTP session is denied access to List Bin Contents for bin A, then the session can not initiate a dir operation on bin A to list the contents of the bin. Furthermore, the session can not transfer clips into bin A using the put operation.

For the purpose of legacy support with older Profile systems, accounts for user movie or user mxfmovie are provided on the K2 system. There is also a video_fs account for Mac/FCP access. These accounts are automatically set up when you install K2 software version 3.2 or higher. Do not restrict access for these accounts. If your security policy requires restricting access to these accounts, contact Grass Valley Support.

On a K2 SAN, authentication takes place on the K2 Media Server. Setting up FTP security for specific local users and groups is not supported on a K2 SAN, with the exception of the local movie and mxfmovie accounts. However, you can set up FTP security for domain users and groups.

FTP overwrite

By default, the K2 FTP server does not allow overwriting a clip with the same name during a transfer. However you can set the FTP Overwrite setting in the Configuration Manager of K2 AppCenter.

If the K2 FTP server is configured for overwrites, it will implicitly delete a clip with the existing name and then proceed to create the new clip with the same name. If the delete operation fails (for reasons such as the clip was being used by a channel), the FTP transfer operation will also fail.

Configuring FTP Overwrite setting

1. In AppCenter, click **File | System | Configuration**.
   Configuration Manager opens.
2. In Configuration Manager, click the **System** tab.
3. In FTP settings, for the **Allow FTP Overwrites** setting, select one of the following:
   - **Yes**: Clips with existing names get overwritten during an FTP put operation.
   - **No**: An FTP put operation specifying an existing clip name causes the FTP put operation to fail. (This is the default behavior)
4. Click **OK** to apply the setting.

   For more information, see topics in the "Configuring the K2 System" section of this Topic Library.

Related Topics

Using FTP for file transfer on page 291

About FTP internationalization

The K2 FTP interface supports clip and bin names in non-English locales (international languages) as follows:

- Non-ASCII localized characters represented as UTF-8 characters.
- All FTP client/server commands are in ASCII.
- The named movie asset is Unicode 16-bit characters
- The K2 FTP client converts between Unicode and UTF-8 strings explicitly.

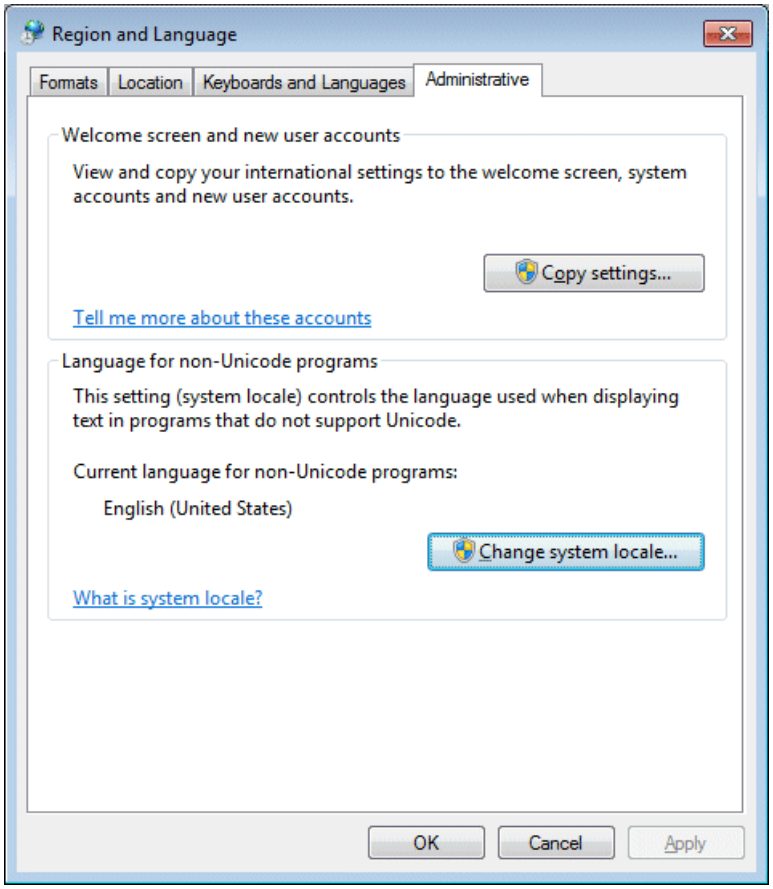
Also refer to “Internationalization” section in the "Configuring the K2 System" section of this Topic Library.

The Microsoft FTP client (the ftp.exe program which users run from a Windows console or DOS prompt) does not convert from a Unicode string to a UTF-8 string. Instead, it passes the Unicode string directly to the FTP server which can cause errors. To avoid these errors, in the FTP command, every reference to the clip path must be in UTF-8.

A specific language setting is required on the computer that hosts the K2 FTP interface. This requirement applies to a K2 Media Server, K2 Solo Media Server, and a stand-alone K2 client, as they all host the K2 FTP interface.

Setting the FTP language

1. Open the **Regional and Language** control panel.



2. On the **Administrative** tab make sure "Current language for non-Unicode programs" is set to **English (United States)**.
3. If you made a change click **Apply** and **OK**, and when prompted restart the computer to put the change into effect.

FTP access by Internet Explorer

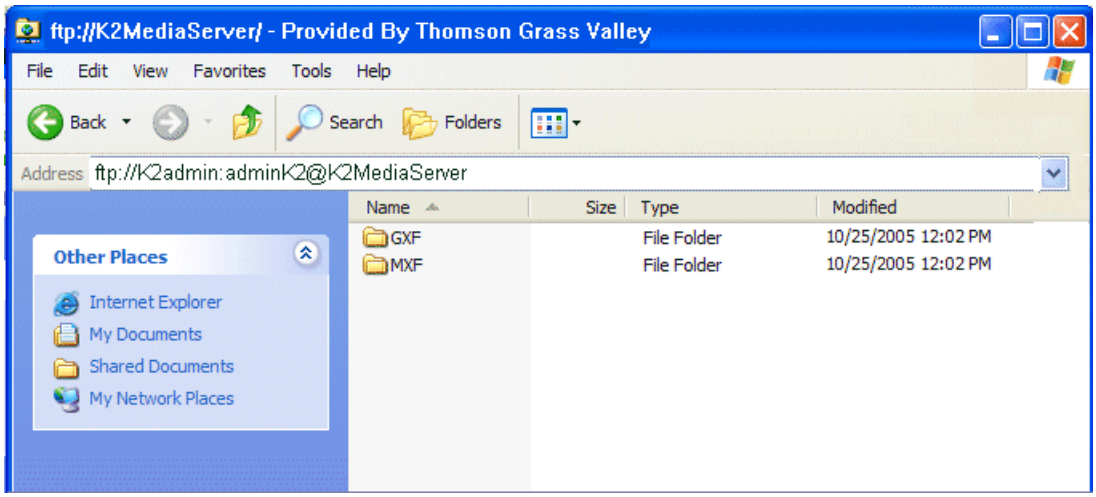
You can use Internet Explorer to transfer files via FTP between a PC and the FTP interface on a stand-alone K2 system or a K2 Media Server, so long as both source and destination machines are on the same network.

While the K2 FTP interface supports local languages, some international characters are not displayed correctly in Internet Explorer. Use only English language characters with Internet Explorer.

To access FTP using Internet Explorer, use the following syntax in the Address field: `ftp://<username:password@hostname>`. The username/password can be any account set up on the machine hosting the FTP interface. The hostname can be the name of a stand-alone K2 client

or it can be the name of a K2 Media Server. (You cannot make a FTP connection to a K2 client with shared storage or to a K2 Control Point PC.)

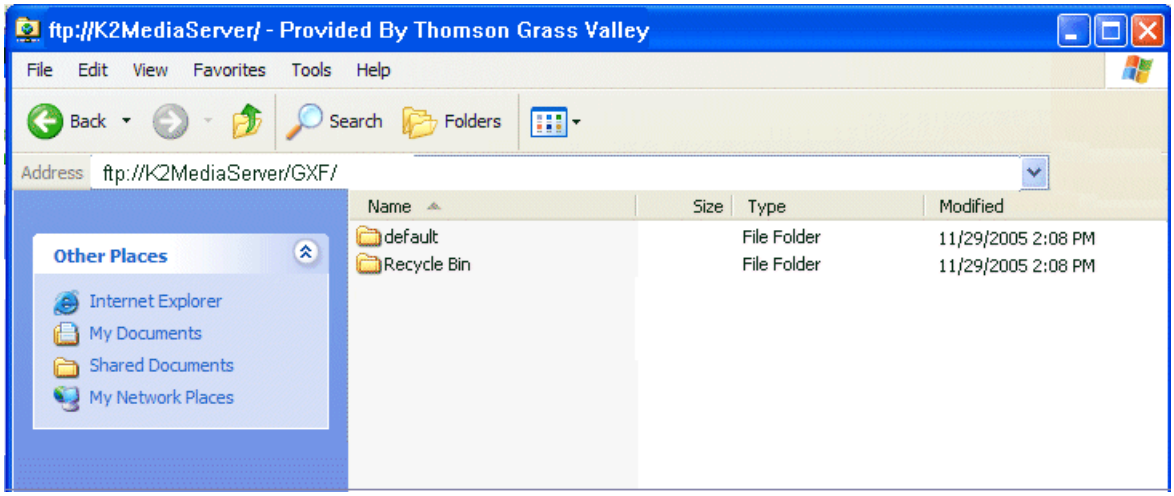
Once you have logged in, the two virtual directories are displayed.



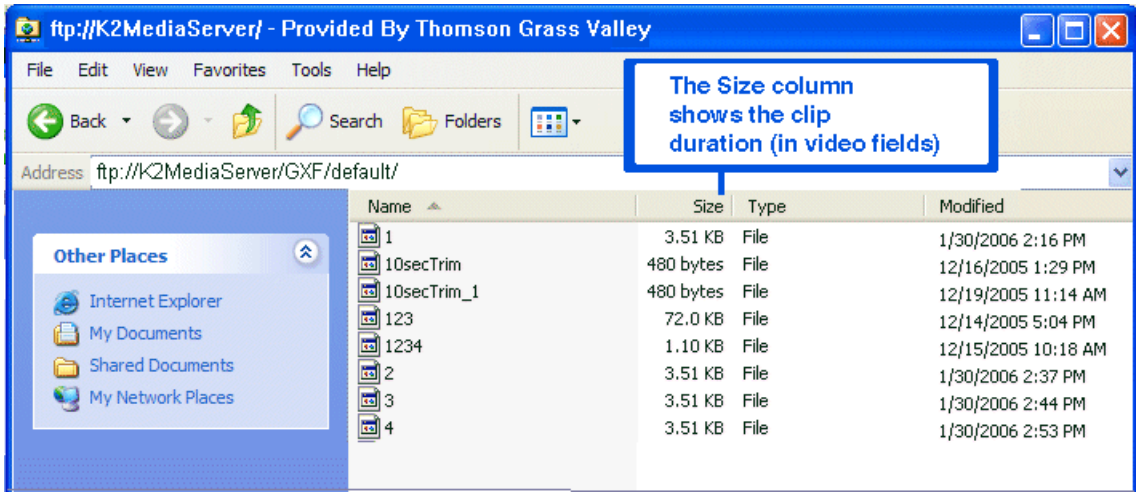
GXF — General Exchange Format (SMPTE 360M). This is the standard Grass Valley file interchange format. Refer to specifications later in this manual for media types supported.

MXF — Media Exchange Format (SMPTE 377M). Refer to specifications later in this manual for media types supported.

Inside the GXF and MXF folders you can see contents of the system.



The subfolders are organized in typical Windows fashion, with columns denoting the file's name, size, etc. The Size column refers to the clip duration (in video fields).



You can use Internet Explorer to drag a file from your stand-alone K2 system or K2 Media Server and drop it in a folder on your PC. You can also drag a file from your PC and drop it in the appropriate folder on your stand-alone K2 system or K2 Media Server.

Be careful not to mix files from the two types of file interchange formats. GXF files can only be transferred to the GXF folder, and MXF files can only be transferred to the MXF folder. If you try to drop a clip into the incorrect folder, the transfer fails. For example, *clip1.gxf* can be dropped into the *K2-MediaSVR/GXF/default/* folder, but not into the *K2-MediaSVR/MXF/default/ folder*.

FTP commands supported

The following table lists the FTP commands that the K2 FTP interface supports.

FTP command name	FTP command description	K2 FTP support
USER	User Name	Supported
PASS	Password	Supported
ACCT	Account	Not supported
CWD	Change working directory	Supported
CDUP	Change to parent directory	Supported
SMNT	Structure mount	Not supported
REIN	Reinitialize	Not supported
QUIT	Logout	Supported
PORT	Data port	Supported
PASV	Passive	Supported
TYPE	Representation type	Supported
STRU	File structure	Not supported
MODE	Transfer mode	Not supported

FTP command name	FTP command description	K2 FTP support
RETR	Retrieve	Supported
STOR	Store	Supported
STOU	Store unique	Not supported
APPE	Append (with create)	Not supported
ALLO	Allocate	Not supported
REST	Restart	Not supported
RNFR	Rename From	Supported
RNTO	Rename To	Supported
ABOR	Abort	Supported
DELE	Delete	Supported
RMD	Remove directory	Supported
MKD	Make directory	Supported
PWD	Print working directory	Supported
LIST	List	Supported. Reports clip size in number of video fields.
NLST	Name List	Supported
SITE	Site Parameters	Supported
SYST	System	Supported
SIZE	Size of file (clip)	Supported. Reports an approximated clip size in bytes. The size is the estimated size of the clip in the K2 system, not the byte size that K2 exports in the FTP get operation.
STAT	Status	Supported
HELP	Help	Supported
NOOP	No Operation	Supported

Using FTP on a K2 Nearline SAN

A K2 Nearline SAN is considered an "offline" system, as it has no media database and is not capable of direct playout of media. On this type of system the K2 FTP interface operates in file mode. Therefore, procedures that apply to "online" K2 SANs do not globally apply to the Nearline SAN. This includes procedures for streaming, import, export, and FTP.

The rules for transferring to/from a K2 Nearline SAN are as follows:

- Transfer files only. Streaming media, as in AppCenter's Import/Send to | Stream feature, is not supported.

- Passive FTP mode is supported. You must use this mode for FTP transfers.
- In addition to FTP transfers, you can also map shared drives and use basic Windows networking to move files to/from a Nearline storage system.
- You should use the dedicated K2 FTP/streaming network.

Additional information about Nearline FTP is as follows:

- K2 FTP protocol supports clip and bin names in non-English locales (international languages) using UTF-8 character encoding. Refer to specifications for internationalization.
- The Nearline FTP interface operates in file mode so it does not have GXF and MXF folders to support format-specific functionality, as does the K2 FTP interface in movie mode for "online" K2 systems. This means the Nearline FTP interface treats all files, including GXF and MXF, as generic files with no particular consideration for any file format.

Using reference files

When you create a simple K2 clip on a K2 system, K2 software can create a corresponding reference file. The reference file is stored in a directory in the clip's folder on the V: drive. You can configure the software to create QuickTime reference files or no reference files. The following topics provide information about reference files on K2 systems.

About QuickTime reference files

The following formats are supported as QuickTime reference files:

- DV
- AVC-Intra
- XDCAM-EX
- XDCAM-HD
- XDCAM-HD 422
- IMX
- Avid DNxHD

The K2 clip must be a simple clip in order to create the reference file. With the QuickTime reference file you can open the K2 clip with QuickTime tools, such as Final Cut Pro, for playback and editing. For some formats the QuickTime tool does not provide default support, so you must configure the tool as necessary to support the format. The QuickTime tool must be run on another system. Running the QuickTime player or other QuickTime tools on the K2 system is not supported. You have options for connections, access, and software to support your workflow requirements.

Configuring reference file type on a standalone K2 Summit/Solo system

1. In AppCenter, click **File | System | Configuration**.
   Configuration Manager opens.
2. In Configuration Manager, click the **System** tab.

3. In Reference Files settings, for the **Reference file type** setting, select one of the following:
   - None — K2 software does not create reference files.
   - QuickTime — K2 software creates QuickTime reference files.
4. Click **OK** to apply the setting.
5. Restart the standalone K2 Solo 3G system to put the change into effect.

Configuring reference file type on a K2 SAN system

1. In the K2Config application, for the K2 Media Server with role of file system server, access the File System Server Configuration page as follows:
   - On a SAN that is already configured, in the tree view click **File System Server**.
   - On a SAN that is not yet fully configured, work through the Configure K2 Server wizard until you reach the File System Server Configuration page.
2. On the File System Server Configuration page select one of the following:
   - No reference file — K2 software does not create reference files.
   - QuickTime reference file — K2 software creates QuickTime reference files.
3. Click **Check** to apply the setting.
4. Manage the required K2 Media Server restart as follows:
   - On a SAN that is already configured, you must restart the K2 Media Server to put the change into effect. Follow the restart procedure appropriate for the basic or redundant K2 SAN.
   - On a SAN that is not yet fully configured, continue to work through the Configure K2 Server wizard. The restart at the end of the configuration process is sufficient.

If a redundant K2 SAN, you must configure similarly and restart both K2 Media Servers with role of file system server.

MXF Export Type

When importing and exporting MXF the K2 system behaves as follows, in relation to the MXF Export Type setting in K2Config or in K2 AppCenter:

- The MXF Export Type setting applies to all MXF exports on the K2 system. There is one setting for one K2 system. The K2 system can be a stand-alone K2 Summit/Solo system or a K2 SAN. If a K2 SAN, the one setting applies to the K2 Media Server with role of FTP server that handles exports for all SAN-attached K2 Summit systems.
- For export, the K2 system must be set to one of the following MXF Export Types:
  - **377M**: SMPTE ST 377:2004 compliant. Ensures compatibility with older products.
  - **377-1**: SMPTE ST 377-1:2009 compliant.
- By default the K2 system is set to SMPTE ST 377:2004. This setting is only applicable to the MXF op1a import and export.
- The SMPTE ST 377:2004 setting is recommended for compatibility with older systems which do not support SMPTE ST 377-1:2009.

- The following format does not support SMPTE ST 377-1:2009 export. Therefore the format is always exported as SMPTE ST 377:2004, regardless of the MXF Export Type setting:
  - D10 media
- For import, both SMPTE ST 377:2004 and SMPTE ST 377-1:2009 are supported, regardless of the MXF Export Type setting. The MXF Export Type setting affects export only.

Configuring MXF Export Type on a standalone K2 Summit/Solo system

1. In AppCenter, click **File | System | Configuration**.
   Configuration Manager opens.
2. In Configuration Manager, click the **System** tab.
3. In MXF Export settings, for the **MXF Export Type** setting, select one of the following:
   - **377M**: SMPTE ST 377:2004 compliant. Ensures compatibility with older products.
   - **377-1**: SMPTE ST 377-1:2009 compliant.
4. Click **OK** to apply the setting.
5. Restart the standalone K2 Solo 3G system to put the change into effect.

Configuring MXF Export Type on a K2 SAN system

1. In the K2Config application, for the K2 Media Server with role of FTP server, access the FTP Server Configuration page as follows:
   - On a SAN that is already configured, in the tree view click **FTP Server**.
   - On a SAN that is not yet fully configured, work through the Configure K2 Server wizard until you reach the FTP Server Configuration page.
2. On the FTP Server Configuration page select one of the following:
   - **377M**: SMPTE ST 377:2004 compliant. Ensures compatibility with older products.
   - **377-1**: SMPTE ST 377-1:2009 compliant.
3. Manage the required K2 Media Server restart as follows:
   - On a SAN that is already configured, you must restart the K2 Media Server to put the change into effect. Follow the restart procedure appropriate for the basic or redundant K2 SAN.
   - On a SAN that is not yet fully configured, continue to work through the Configure K2 Server wizard. The restart at the end of the configuration process is sufficient.

Quicktime and Final Cut Pro support

You can access K2 media as QuickTime for editing in Final Cut Pro, as explained in the following topics.

About connecting to K2 storage with Final Cut Pro

This topic describes the different ways you can access K2 media for editing with Final Cut Pro.

Connection types are as follows:

- iSCSI – This is a connection as a client to an iSCSI K2 SAN. The connection requires a K2 FCP Connect license and supporting software on the Macintosh system. The connection uses the K2 SAN's iSCSI Gigabit Ethernet network.

Access methods are as follows:

- Edit-in-place – With this method you edit the K2 media in Final Cut Pro across the network while the media is still in place in K2 storage. You can do this over any connection type.
- File transfer – With this method you transfer (copy) the K2 media to the Macintosh system and then edit it in Final Cut Pro across the network while the media is still in place in K2 storage. You can do this over any connection type. You can initiate the transfer as file copy over iSCSI, or via FTP.

With all access methods, after you are done editing the K2 media you export it back to K2 storage via a K2 HotBin.

Software components that support various workflows are as follows:

- K2 FCP Connect – This is a Grass Valley product that supports all connection types for optimal performance. It is a toolset that must be purchased, installed, licensed, and configured. It includes GV Connect, which is a Final Cut Pro plug-in. GV Connect supports edit-in-place and file transfer over iSCSI.

Refer to product release notes for information about connections, access, and software that apply to K2 storage and versions.

For detailed instructions refer to documentation as follows:

- iSCSI – Refer to the K2 FCP Connect documentation set, which includes the following documents:
  - K2 FCP Connect Installation Manual
  - K2 FCP Connect Release Notes
  - GV Connect User Manual

Operation guidelines

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

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

Export to K2 storage

When exporting media to K2 storage, 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 60 (50 for PAL).
   - If you are exporting 720p material the frame rate must be "Current" or 60.
   - If you are exporting 720p material for 1080i conversions the frame rate must be 60 (50 for PAL).

The HotBin imports the clip into the K2 system as K2 media. As a by-product of the import, the K2 system creates a QuickTime reference file for the new K2 media.

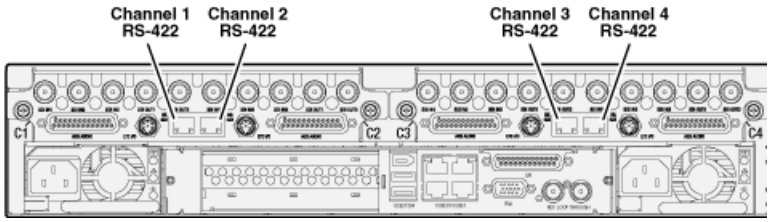
About QuickTime import delay

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, when you configure a K2 HotBin you can configure the QuickTime import delay setting. This setting 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 RS-422 K2 Summit/Solo 3G system

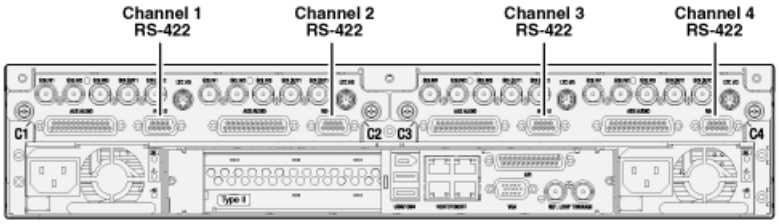
You can control the K2 system with remote control devices and software developed for the K2 system that use industry-standard serial protocols: AMP, BVW, and VDCP. Make RS-422 connections for protocol control as illustrated:



Refer to topics in the "Using K2 AppCenter" section of the K2 Topic Library to configure the K2 system for remote control.

Connecting RS-422 first generation Summit

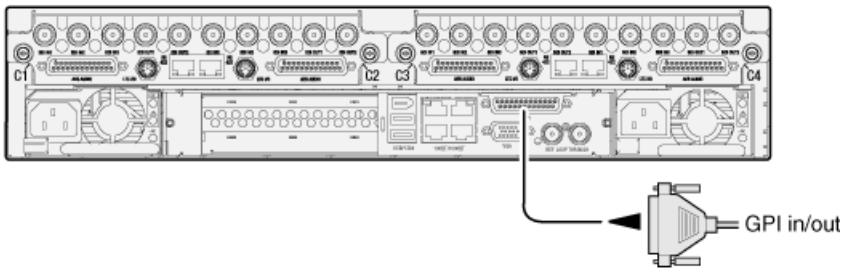
You can control the K2 system with remote control devices and software developed for the K2 system that use industry-standard serial protocols: AMP, BVW, and VDCP. Make RS-422 connections for protocol control as illustrated:



Refer to topics in the "Using K2 AppCenter" section of the K2 Topic Library to configure the K2 system for remote control.

Connecting GPI

The K2 Solo 3G system provides 12 GPI inputs, and 12 GPI outputs on a single DB-25 rear panel connector, as illustrated:



K2 Summit 3G system shown. Connection is identical on first generation K2 Solo 3G system.

Refer to topics in the "Using K2 AppCenter" section of the K2 Topic Library for GPI configuration procedures.

Import/export services

Using the HotBin capture service

This section contains topics about the K2 HotBin Import capture service.

About the HotBin capture service

The functionality of the HotBin service is provided by the Grass Valley Import Service. The HotBin service provides a way to automate the import of files as clips into the K2 media file system and database. This is similar to what happens when you manually import files one at a time using K2 AppCenter import features, except with the HotBin service the files are automatically imported. The HotBin service can import any file or stream type that is supported as a K2 file-based import.

By default, the service does not start automatically. If you have never configured or used the service, it is set to startup type Manual. When you configure the service for the first time, the service is set to startup type Automatic. However, if you upgrade or otherwise re-install your K2 System Software, the service is re-set to startup type Manual.

NOTE: Therefore, you must re-configure the service after K2 System Software upgrade/reinstall in order to set the startup type back to Automatic.

There is no Grass Valley license required specifically for the HotBin service.

Before you can use the HotBin service, it must be configured through the K2 Capture Services utility. The HotBin service must be configured on the K2 system that receives the imported media. The K2 system that receives the imported media can be a K2 Solo Media Server, a stand-alone K2 Summit Production Client, a stand-alone K2 Media Client, or the K2 Media Server with the role of primary FTP server on a K2 SAN.

Once configured, the HotBin service monitors a watched folder (a HotBin). The watched folder is a specified source directory on a source PC. The watched folder can be on a stand-alone K2 system, a K2 Media Server, a Windows PC, or a Macintosh. When files are placed in the watched folder, the HotBin service imports them as a clip into the specified destination bin. The destination bin is on the K2 system that receives the imported media and is within that K2 system's media file system and database.

The HotBin service automatically creates sub-directories in the watched folder (source directory), described as follows:

- Success — After the HotBin service successfully imports the files in the source directory into the destination bin on the K2 system, it then moves those files into the Success directory.
- Fail — If the HotBin service can not successfully import the files in the source directory into the destination bin on the K2 system, it moves the failed files into the Fail directory.
- Archive — If there are files in the source directory when the Hot Bin service first starts up, it does not attempt to import those files into the K2 system. Instead, it moves those files into the Archive directory. This occurs when you first configure the Hot Bin service, if you manually stop/start the Hot Bin service, and when you upgrade K2 system software.

Prerequisites for using the HotBin capture service

Before you can configure and use the HotBin capture service, the following requirements must be satisfied:

- K2 system software must be at version 3.2.56 or higher.

Use topics in this section as appropriate to satisfy prerequisites.

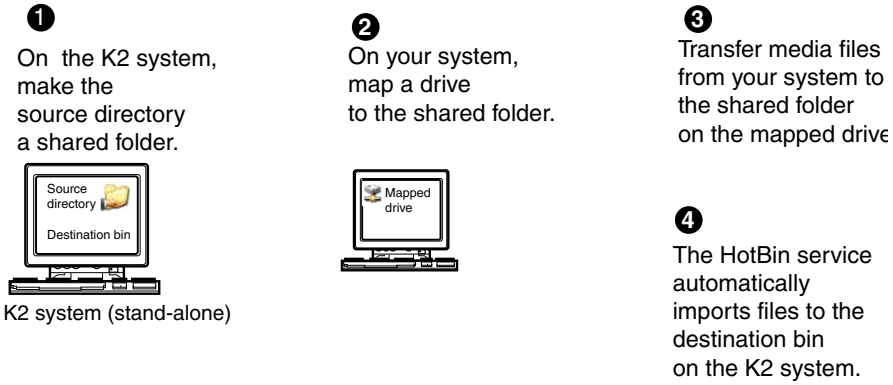
Considerations for using the HotBin capture service

When you are configuring and using the K2 HotBin capture service, bear in mind the following considerations:

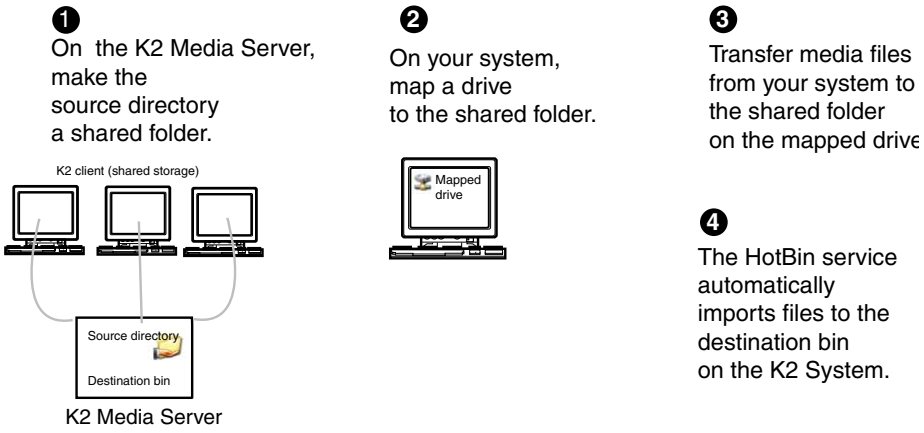
- You must be logged in with administrator privileges on the K2 system as well as having the appropriate security permissions to access the watched folder or bin.
- If you have multiple source folders (for import) or destination folders (for export) on external systems, use the same user account for all capture service access to all systems.
- If using the capture service on a K2 SAN, the K2 Capture Services utility and the import watched folder must be on a K2 Media Server that is also an FTP server.
- It is recommended that you keep the source directory and destination bin located on the local V: drive, which is their default location.
- Do not configure any other location with files that must be retained. When the HotBin service first starts up it removes files in the source directory.
- If you require that the source directory and destination bin be on different systems, system clocks must be synchronized. The Cleanup Frequency function depends on accurate system clocks.
- If you specify a destination bin name that does not yet exist, the K2 system creates it when files are transferred to it.
- Imports are serialized. For example, if you drop two clips into the watched folder for import, the capture service does not queue the second clip for import until the first clip is imported. This is different than the ordinary K2 transfer process.
- Capture service imports are serialized with other K2 transfers. For example, if fourteen items are already queued up from ordinary K2 transfers, and you drop content into the watched folder for import, the import triggered by the capture service becomes the fifteenth clip in the transfer queue.
- After the capture service imports media into K2 media storage successfully, the capture service immediately deletes the original media files from the watched folder. If the import fails, the original media files are retained in the watched folder for the number of days specified as the Cleanup Frequency.
- The “Cleanup Frequency” (purge) feature deletes files in the Success sub-directory and in the Fail sub-directory. It does not delete files in the Archive sub-directory.
- Files in the Success, Fail, and Archive sub-directories are “hidden” files in Windows Explorer. To see these files you must select Show Hidden Files in the Windows Explorer Folder Options dialog box.

Grass Valley recommends that you use the HotBin service as demonstrated in the following diagram.

Using the HotBin service with a standalone K2 system



Using the HotBin service with a K2 SAN



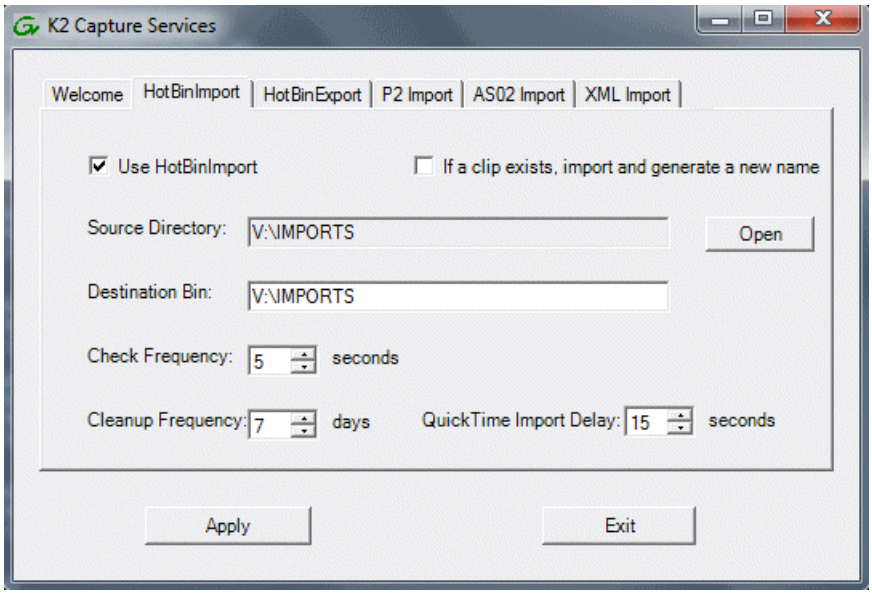
While not preferred, you can also use the HotBin service if the source directory is on another system. The following table lists the requirements for accessing a source directory located on various operating systems.

If your source directory is on:	...and the source directory is on a shared folder on a mapped drive, you need:
Another Windows system	• Administrator privileges for the K2 system • A user account with log-in service rights for your system
Macintosh operating system	• Privileges as listed above. • The identical user name and password on both systems. For example, if you have a Macintosh user named Jane, you would need to have a user named Jane on your Windows system with the same password. From the Windows Control Panel, select **Administrator Tools | Local Security Policy | User Rights Assignment | Log on as service** and click **Add New User**.

Configuring the HotBin Capture Service

NOTE: Once configured, the service deletes files in the watched folder or bin (source) that are older than the specified cleanup frequency.

1. From the **Start** menu, access the **All Programs** menu and select **Grass Valley \| K2 Capture Services**. The K2 Capture Services utility dialog box is displayed.
2. Click the **HotBinImport** tab.



3. Select **Use HotBinImport**.

4. To retain the current version of a clip at the destination that is named the same as a clip you are importing, select **If a clip exists, import and generate a new name**.

   The Hotbin service increments the file name of the imported clip so it does not overwrite the clip at the destination.

5. Enter the paths to the source directory and destination bin. If the source directory does not currently exist, it will automatically be created.

   NOTE: Do not configure the source directory to be a location with files that must be retained. When the HotBin service first starts up it removes files in the source directory.

6. For Check Frequency, it is recommended that you accept the default value. This value specifies how often you want the capture service to check the source directory for new files.
7. For the Cleanup Frequency, it is recommended that you accept the default value. This value specifies the maximum age of files in the source directory. The capture service deletes files that are older than this age.
8. If the source directory is not on the local K2 system, a User Account dialog box displays. Enter the user information that you use to access the source directory. If part of a domain, enter the domain name.
9. If necessary, configure QuickTime Import Delay.

   This setting adjusts 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 setting is 15 seconds.

10. When your capture service settings are complete, click **Apply**.

    If prompted, restart the K2 system.

The HotBin service checks the source directory for files. If files are present, the HotBin service moves them to the Archive sub-directory. It does not import the files into the destination bin on the K2 system.

Place files in the source directory to trigger the Hot Bin import processes.

HotBin capture service components

The following table describes the components that support K2 HotBin capture service functionality.

Name	Description
Grass Valley Import Service	This is the service that provides the functionality for a K2 capture service. It is the service that automatically creates the K2 clip from the media files in the watched folder (source directory) and puts the K2 clip in the K2 media storage (destination bin).
K2 Capture Services utility	Configures K2 capture services.
Source directory	This is the watched folder. It is a standard file system directory. When media files are placed in this directory, the capture service automatically creates a K2 clip in the K2 media storage. By default, the location of the source directory is `V:/IMPORTS`.
Check frequency	Determines how often (in seconds) the watched folder is checked for new files.

Name	Description
Cleanup frequency	Determines how long (in days) a file remains in the watched folder. A file with a file-creation date older than the specified number of days is deleted.
Destination bin	The clip bin in the K2 media storage that receives the K2 clip created by the capture service. The destination bin is in the K2 media database and appears in AppCenter as a media bin. By default, its location is `V:/IMPORTS`.

Using the XML Import capture service

This section contains topics about the K2 XML Import capture service.

About the XML Import capture service

The K2 XML Import capture service provides a way to have media automatically imported into a K2 system when it is pushed to the K2 system by a third party application. The XML Import capture service has a watched folder. The watched folder is a standard file system directory that can be recognized by the Windows operating system. You transfer the media to the directory using the third party application.

By default, the service does not start automatically. If you have never configured or used the service, it is set to startup type Manual. When you configure the service for the first time, the service is set to startup type Automatic. However, if you upgrade or otherwise re-install your K2 System Software, the service is re-set to startup type Manual. Therefore, you must re-configure the service after K2 System Software upgrade/reinstall in order to set the startup type back to Automatic.

After all the media files are finished being transferred to the watched folder, the third party application then transfers an XML file to the watched folder. This XML file defines the media files and specifies how they are to be assembled to create a K2 clip. When the XML file finishes transferring to the watched folder, the capture service goes into action and validates the XML file to make sure it has the proper structure. If the XML file is valid, the capture service then does the necessary processing to create the clip in the K2 media storage. The media is then available as a K2 clip, ready for playout.

The K2 XML Import capture service and its watched folder must be on a K2 system that hosts the K2 FTP interface, as follows:

- Stand-alone K2 system— When media files and the XML file are pushed to the watched folder, the capture service creates a K2 clip in the internal storage or direct-connect media storage of the K2 system. The watched folder must be on the K2 system's V: drive.
- K2 Media Server with role of FTP server — When media files and the XML file are pushed to the watched folder, the capture service creates a K2 clip in the shared media storage of the K2 SAN. The watched folder must be on the K2 Media Server's V: drive.

Prerequisites for using the XML Import capture service

Before you can configure and use the XML Import capture service, the following requirements must be satisfied:

- K2 system software must be at a version that supports the XML Import capture service. Refer to the "About This Release" section of the K2 Topic Library for information on XML Import capture service version compatibility.
- The K2 XML Import capture service must be licensed on the stand-alone K2 system or K2 Media Server. This is a Grass Valley software license.
- The application that pushes the media files and XML file to the watched folder must provide valid files according to K2 XML Import capture service requirements. Developers of applications can contact Grass Valley Developer Support for more information

Use topics in this section as appropriate to satisfy prerequisites.

Considerations for using the XML import capture service

When you are configuring and using the K2 XML Import capture service, bear in mind the following considerations:

- You must be logged in with administrator privileges on the K2 system as well as having the appropriate security permissions to access the watched folder or bin.
- If using the capture service on a K2 SAN, the K2 Capture Services utility and the import watched folder must be on a K2 Media Server that is also an FTP server.
- After the capture service imports media into K2 media storage successfully, the capture service immediately deletes the original media files from the watched folder. If the import fails, the original media files are retained in the watched folder for the number of days specified as the Cleanup Frequency.
- The transfer of the media files, then the XML file, must be 100% complete before the K2 XML Import capture service begins to create the clip in K2 media storage.

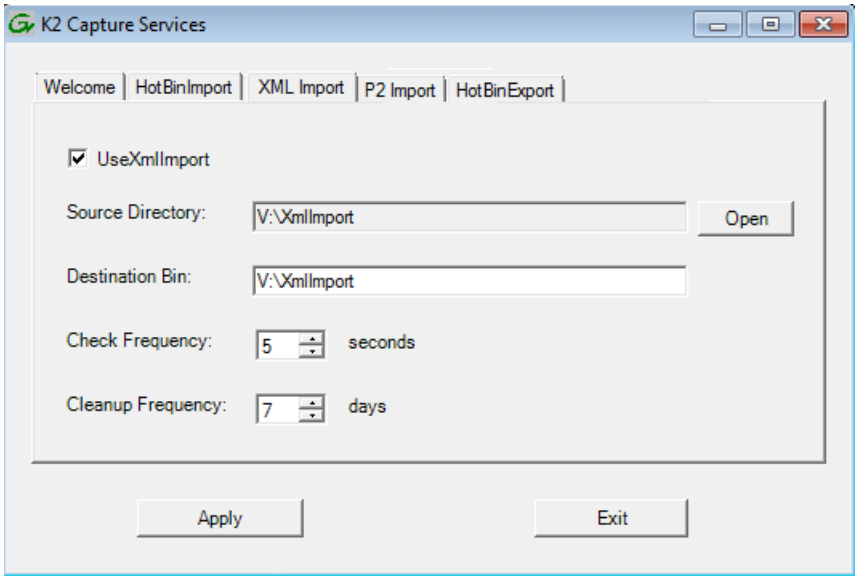
Configuring the XML Import Capture Service

NOTE: Once configured, the service deletes files in the watched folder or bin (source) that are older than the specified cleanup frequency.

1. From the **Start** menu, access the **All Programs** menu and select **Grass Valley | K2 Capture Services**.

   The K2 Capture Services utility dialog box is displayed.

2. Click the **XML Import** tab.



3. Select **UseXMLImport**.

   If you have not yet licensed the XML Import capture service, a "…start the process of getting a license now?" message appears. Follow on-screen instructions to obtain a license. After licensing, restart the K2 Capture Services utility and continue with this procedure.

4. Enter the paths to the source directory and destination bin, which are defined as follows:

   - Source Directory — This is the watched folder. It is a standard file system directory. It must be on the K2 system's V: drive. When valid media is placed in this directory, the capture service automatically creates a K2 clip in the K2 media storage.
   - Destination Bin — The clip bin in the K2 media storage that receives the media processed by the capture service. The destination bin is in the K2 media database and it appears in AppCenter as a media bin. The bin must be on the K2 system's V: drive. If you specify a destination bin name that does not yet exist, the K2 system creates it when the K2 clip is created.

5. For Check Frequency, it is recommended that you accept the default value. This value specifies how often you want the capture service to check the source directory for new files.
6. For the Cleanup Frequency, it is recommended that you accept the default value. This value specifies the maximum age of files in the source directory. The capture service deletes files that are older than this age.
7. When your capture service settings are complete, click **Apply**.

   If prompted, restart the K2 system.

The service checks the source directory for any files that are beyond the specified cleanup age and deletes them from the directory.

Testing the XML Import Capture Service

1. Place media files into the watched folder.
2. On the K2 System, open Windows Explorer, browse to the watched folder and verify that files have completed the transfer. The transfer must be 100% complete before the capture service triggers the processes to create the K2 clip.
3. Place a valid XML file into the watched folder.
4. On the K2 System, open Windows Explorer, browse to the watched folder and verify that XML file has completed the transfer. The transfer must be 100% complete before the K2 XML Import capture service triggers the processes to create the K2 clip.
5. After the K2 clip is created, verify that the media appears in the destination bin.
6. Play to verify success.

XML Import capture service components

The following table describes the components that support K2 XML Import capture service functionality.

Name	Description
Grass Valley Import Service	This is the service that provides the functionality for a K2 capture service. It is the service that automatically creates the K2 clip from the media files in the watched folder (source directory) and puts the K2 clip in the K2 media storage (destination bin).
K2 Capture Services utility	Configures K2 capture services.
Source directory	This is the watched folder. It is a standard file system directory. When media files are placed in this directory, the capture service automatically creates a K2 clip in the K2 media storage. By default, the location of the source directory is `V:\XmlImport`.
Check frequency	Determines how often (in seconds) the watched folder is checked for new files.
Cleanup frequency	Determines how long (in days) a file remains in the watched folder. A file with a file-creation date older than the specified number of days is deleted.
Destination bin	The clip bin in the K2 media storage that receives the K2 clip created by the capture service. The destination bin is in the K2 media database and appears in AppCenter as a media bin. By default, its location is `V:\XmlImport`.

Using the P2 capture service

This section contains topics about the K2 P2 Import capture service.

About the P2 capture service

The K2 P2 Import capture service provides a way to have P2 media automatically imported into a K2 system. The K2 P2 Import capture service supports importing DV and AVC-Intra content based on the P2 MXF OP-ATOM files, as well as AVC LongG content based on the P2 MXF OP1B files.

The P2 Import capture service has a watched folder. The watched folder is a standard file system directory that can be recognized by the Windows operating system. You transfer the media to the directory and it is imported into the K2 system.

By default, the service does not start automatically. If you have never configured or used the service, it is set to startup type Manual. When you configure the service for the first time, the service is set to startup type Automatic. However, if you upgrade or otherwise re-install your K2 System Software, the service is re-set to startup type Manual.

NOTE: Therefore, you must re-configure the service after K2 System Software upgrade/reinstall in order to set the startup type back to Automatic.

The watched folder receives the nested directories that define P2 media for one clip or multiple clips. All the P2 audio files, video media files and P2 XML files must be transferred to the watched folder. All P2 media files (MXF files) need to be copied first into the appropriate folders. After the media files have been copied, the P2 clip XML file must be copied into it's appropriate folder. The presence of the XML file triggers the P2 import capture service to begin importing the content. If the P2 file is valid, the capture service then does the necessary processing to create the clip in the K2 media storage. The media is then available as a K2 clip, ready for playout.

The K2 P2 Import capture service and its watched folder must be on a K2 system that hosts the K2 FTP interface, as follows:

- Stand-alone K2 system — When media files and the P2 files are pushed to the watched folder, the capture service creates a K2 clip in the internal storage or direct-connect media storage of the K2 system. The watched folder must be on the K2 system's V: drive.
- K2 Media Server with role of FTP server — When media files are pushed to the watched folder, the capture service creates a K2 clip in the shared media storage of the K2 SAN. The watched folder must be on the K2 Media Server's V: drive.

Prerequisites for using the P2 capture service

Before you can configure and use the P2 Import capture service, the following requirements must be satisfied:

- K2 system software must be at a version that supports the P2 Import capture service. Refer to the "About This Release" section of the K2 Topic Library for information on P2 Import capture service version compatibility.
- The K2 P2 Import capture service must be licensed on the stand-alone K2 system or K2 Media Server. This is a Grass Valley software license.
- The Panasonic storage device that is the source of the P2 media must be on a separate PC and all Panasonic drivers must exist on that PC.
- The directories/file transferred to the watched folder must be valid files according to P2 requirements.

- The K2 system also supports playback of P2 AVC-Intra clips. This requires that the AVC-Intra codec card to be installed.

Use topics in this section as appropriate to satisfy prerequisites.

Considerations for using the P2 capture service

When you are configuring and using the K2 P2 Import capture service, bear in mind the following considerations:

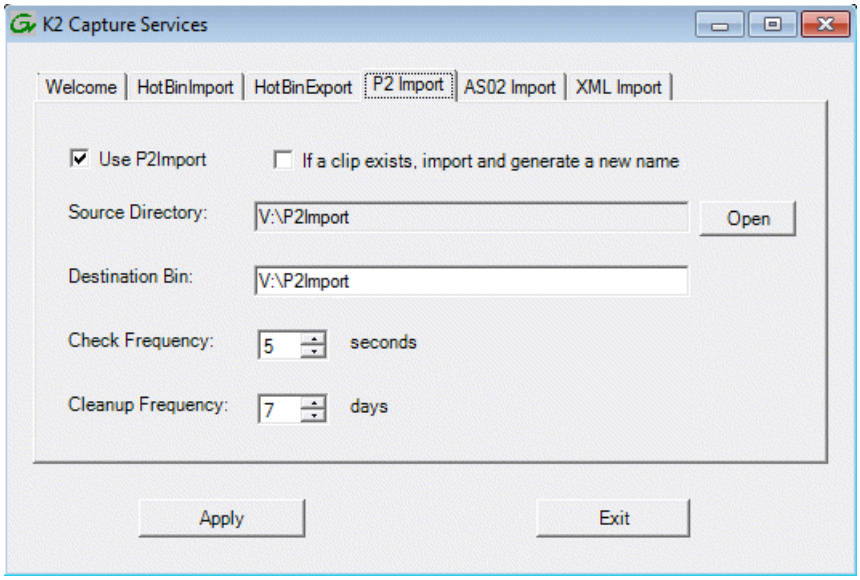
- You must be logged in with administrator privileges on the K2 system as well as having the appropriate security permissions to access the watched folder or bin.
- If you have multiple source folders (for import) or destination folders (for export) on external systems, use the same user account for all capture service access to all systems.
- If using the capture service on a K2 SAN, the K2 Capture Services utility and the import watched folder must be on a K2 Media Server that is also an FTP server.
- You can share the K2 V: drive, so that the Panasonic storage device can access via CIFS.
- P2 content can be dragged/dropped onto the V: drive watch folder from a Panasonic storage device.
- After the capture service imports media into K2 media storage successfully, the capture service immediately deletes the original media files from the watched folder. If the import fails, the original media files are retained in the watched folder for the number of days specified as the Cleanup Frequency.
- The transfer of the directories/files must be 100% complete before the capture service begins to create the clip in K2 media storage.
- P2 content is imported as follows:
  - A simple clip with striped timecode is created.
  - Video (DV, AVC-Intra, or H.264) track is imported and added to the clip
  - Audio tracks are imported and added to the clip
  - There is no P2 Import of metadata into the clip
  - An ancillary data track is imported only for P2 AVC LongG content.

Configuring the P2 Capture Service

NOTE: Once configured, the service deletes files in the watched folder or bin (source) that are older than the specified cleanup frequency.

1. From the **Start** menu, access the **All Programs** menu and select **Grass Valley | K2 Capture Services**.
   The K2 Capture Services utility dialog box is displayed.

2. Click the **P2 Import** tab.



3. Select **Use P2Import**.

   If you have not yet licensed the P2 Import capture service, a "…start the process of getting a license now?" message appears. Follow on-screen instructions to obtain a license. After licensing, restart the K2 Capture Services utility and continue with this procedure.

4. To retain the current version of a clip at the destination that is named the same as a clip you are importing, select **If a clip exists, import and generate a new name**.

   The Hotbin service increments the file name of the imported clip so it does not overwrite the clip at the destination.

5. Enter the paths to the source directory and destination bin, which are defined as follows:

   - Source Directory — This is the watched folder. It is a standard file system directory. It must be on the K2 system's V: drive. When valid media is placed in this directory, the capture service automatically creates a K2 clip in the K2 media storage.
   - Destination Bin — The clip bin in the K2 media storage that receives the media processed by the capture service. The destination bin is in the K2 media database and it appears in AppCenter as a media bin. The bin must be on the K2 system's V: drive. If you specify a destination bin name that does not yet exist, the K2 system creates it when the K2 clip is created.

6. For Check Frequency, it is recommended that you accept the default value. This value specifies how often you want the capture service to check the source directory for new files.
7. For the Cleanup Frequency, it is recommended that you accept the default value. This value specifies the maximum age of files in the source directory. The capture service deletes files that are older than this age.
8. When your capture service settings are complete, click **Apply**.

   If prompted, restart the K2 system.

The service checks the source directory for any files that are beyond the specified cleanup age and deletes them from the directory.

Testing the P2 Capture Service

1. Place P2 directories/files into the watched folder.
2. On the K2 System, open Windows Explorer, browse to the watched folder and verify that files have completed the transfer. The transfer must be 100% complete before the capture service triggers the processes to create the K2 clip.
3. After the K2 clip is created, verify that the media appears in the destination bin.
4. Play to verify success.

P2 capture service components

The following table describes the components that support K2 P2 Import capture service functionality.

Name	Description
Grass Valley Import Service	This is the service that provides the functionality for a K2 capture service. It is the service that automatically creates the K2 clip from the media files in the watched folder (source directory) and puts the K2 clip in the K2 media storage (destination bin).
K2 Capture Services utility	Configures K2 capture services.
Source directory	This is the watched folder. It is a standard file system directory. When media files are placed in this directory, the capture service automatically creates a K2 clip in the K2 media storage. By default, the location of the source directory is `V:\P2Import`.
Check frequency	Determines how often (in seconds) the watched folder is checked for new files.
Cleanup frequency	Determines how long (in days) a file remains in the watched folder. A file with a file-creation date older than the specified number of days is deleted.
Destination bin	The clip bin in the K2 media storage that receives the K2 clip created by the capture service. The destination bin is in the K2 media database and appears in AppCenter as a media bin. By default, its location is `V:\P2Import`.

Using the AS02 capture service

This section contains topics about the K2 AS02 Import capture service.

About the AS-02 capture service

The K2 AS-02 Import capture service provides a way to have AS-02 media automatically imported into a K2 system. The AS-02 Import capture service has a watched folder. The watched folder is a standard file system directory that can be recognized by the Windows operating system. You transfer the media to the directory and it is imported into the K2 system.

By default, the service does not start automatically. If you have never configured or used the service, it is set to startup type Manual. When you configure the service for the first time, the service is set to startup type Automatic. However, if you upgrade or otherwise re-install your K2 System Software, the service is re-set to startup type Manual. Therefore, you must re-configure the service after K2 System Software upgrade/reinstall in order to set the startup type back to Automatic.

The watched folder receives the nested directories that define AS-02 media. After all the directories/files are finished being transferred to the watched folder, the capture service goes into action and validates the AS-02 media to make sure it has the proper structure. If the AS-02 file is valid, the capture service then does the necessary processing to create the clip in the K2 media storage. The media is then available as a K2 clip, ready for playout.

The K2 AS-02 Import capture service and its watched folder must be on a K2 system that hosts the K2 FTP interface, as follows:

- Stand-alone K2 system — When media files and the AS-02 files are pushed to the watched folder, the capture service creates a K2 clip in the internal storage or direct-connect media storage of the K2 system. The watched folder must be on the K2 system's V: drive.
- K2 Media Server with role of FTP server — When media files are pushed to the watched folder, the capture service creates a K2 clip in the shared media storage of the K2 SAN. The watched folder must be on the K2 Media Server's V: drive.

Prerequisites for using the AS-02 capture service

Before you can configure and use the AS-02 Import capture service, the following requirements must be satisfied:

- K2 system software must be at a version that supports the AS-02 Import capture service. Refer to the "About This Release" section of the K2 Topic Library for information on AS-02 Import capture service version compatibility.
- K2 Extended File Services must be licensed on the stand-alone K2 system or K2 Media Server. This is a Grass Valley software license.
- The directories/file transferred to the watched folder must be valid files according to AS-02 requirements.

Use topics in this section as appropriate to satisfy prerequisites.

Considerations for using the AS-02 capture service

When you are configuring and using the K2 AS-02 Import capture service, bear in mind the following considerations:

- You must be logged in with administrator privileges on the K2 system as well as having the appropriate security permissions to access the watched folder or bin.
- If you have multiple source folders (for import) or destination folders (for export) on external systems, use the same user account for all capture service access to all systems.
- If using the capture service on a K2 SAN, the K2 Capture Services utility and the import watched folder must be on a K2 Media Server that is also an FTP server.

- After the capture service imports media into K2 media storage successfully, the capture service immediately deletes the original media files from the watched folder. If the import fails, the original media files are retained in the watched folder for the number of days specified as the Cleanup Frequency.
- The transfer of the directories/files must be 100% complete before the capture service begins to create the clip in K2 media storage.

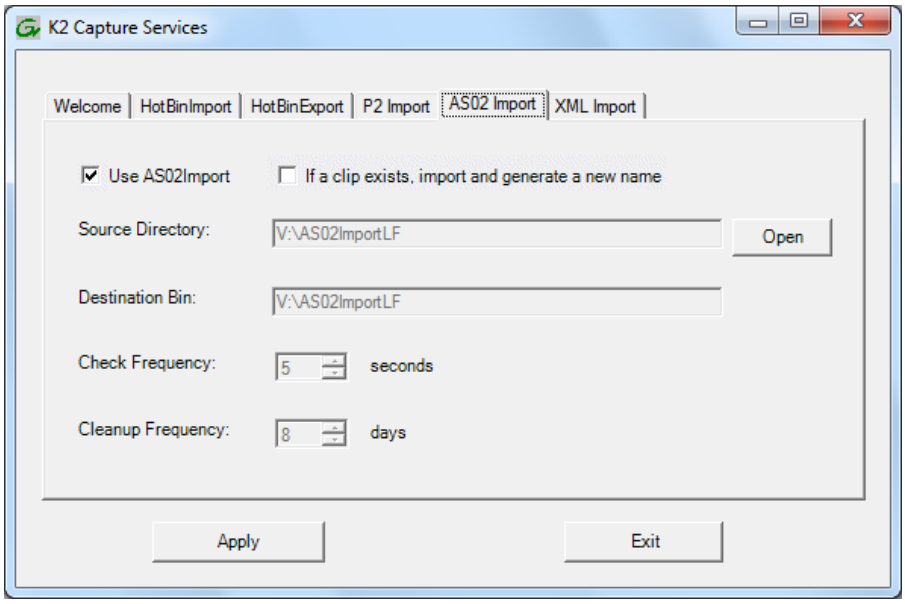
Configuring the AS-02 Capture Service

NOTE: Once configured, the service deletes files in the watched folder or bin (source) that are older than the specified cleanup frequency.

1. From the **Start** menu, access the **All Programs** menu and select **Grass Valley | K2 Capture Services**.

   The K2 Capture Services utility dialog box is displayed.

2. Click the **AS02 Import** tab.



3. Select **Use AS02Import**.

   If you have not yet licensed the AS-02 Import capture service, a "…start the process of getting a license now?" message appears. Follow on-screen instructions to obtain a license. After licensing, restart the K2 Capture Services utility and continue with this procedure.

4. To retain the current version of a clip at the destination that is named the same as a clip you are importing, select **If a clip exists, import and generate a new name**.

   The Hotbin service increments the file name of the imported clip so it does not overwrite the clip at the destination.

5. Enter the paths to the source directory and destination bin, which are defined as follows:
   - Source Directory — This is the watched folder. It is a standard file system directory. It must be on the K2 system's V: drive. When valid media is placed in this directory, the capture service automatically creates a K2 clip in the K2 media storage.
   - Destination Bin — The clip bin in the K2 media storage that receives the media processed by the capture service. The destination bin is in the K2 media database and it appears in AppCenter as a media bin. The bin must be on the K2 system's V: drive. If you specify a destination bin name that does not yet exist, the K2 system creates it when the K2 clip is created.
6. For Check Frequency, it is recommended that you accept the default value. This value specifies how often you want the capture service to check the source directory for new files.
7. For the Cleanup Frequency, it is recommended that you accept the default value. This value specifies the maximum age of files in the source directory. The capture service deletes files that are older than this age.
8. When your capture service settings are complete, click **Apply**.

   If prompted, restart the K2 system.

The service checks the source directory for any files that are beyond the specified cleanup age and deletes them from the directory.

Testing the AS-02 Capture Service

1. Place AS-02 directories/files into the watched folder.
2. On the K2 System, open Windows Explorer, browse to the watched folder and verify that files have completed the transfer. The transfer must be 100% complete before the capture service triggers the processes to create the K2 clip.
3. After the K2 clip is created, verify that the media appears in the destination bin.
4. Play to verify success.

Importing AS-02 clips

1. For each AS-02 clip, create a sub-directory in the AS-02 watched folder and name the bin with the clip name.

   The clip name can be the same as the AS-02 clip that you want to import, or a different name if desired.

   For example, name the bin as **ClipX**.
2. In the sub-bin, create another bin and name it with the same name of the folder containing tracks or media files of the AS-02 clip that you want to import.

   For example if the folder of tracks and media files for the AS-02 clip is named **Tracks**, you must name the sub-bin as **Tracks** as well. The file path is `V:\AS02watchedfolder\ClipX\Tracks`
3. Copy all media files of the AS-02 clip into the bin.

   NOTE: All copied media files must have the same name as media files in the original AS-02 clip.

4. After all media files are copied, copy the AS-02 MXF version file into the bin with the clip name.

   The transfer starts when K2 AS02 capture service detects the AS-02 MXF version file. The newly created bin and sub-bin will be deleted after the transfer is complete.

5. Repeat above steps for all AS-02 clips that you want to import into the K2 system.

AS-02 capture service components

The following table describes the components that support K2 AS-02 Import capture service functionality.

Name	Description
Grass Valley Import Service	This is the service that provides the functionality for a K2 capture service. It is the service that automatically creates the K2 clip from the media files in the watched folder (source directory) and puts the K2 clip in the K2 media storage (destination bin).
K2 Capture Services utility	Configures K2 capture services.
Source directory	This is the watched folder. It is a standard file system directory. When media files are placed in this directory, the capture service automatically creates a K2 clip in the K2 media storage.
Determines how often (in seconds) the watched folder is checked for new files.	
Cleanup frequency	Determines how long (in days) a file remains in the watched folder. A file with a file-creation date older than the specified number of days is deleted.
Destination bin	The clip bin in the K2 media storage that receives the K2 clip created by the capture service. The destination bin is in the K2 media database and appears in AppCenter as a media bin.

Using the Export capture service

This section contains topics about the K2 Export capture service.

About the Export capture service

The Export capture service provides a way to have media automatically exported from a K2 system. The capture service has a watched bin. The watched bin is a K2 storage system bin. You place the media in the bin and it is exported from the K2 system.

By default, the service does not start automatically. If you have never configured or used the service, it is set to startup type Manual. When you configure the service for the first time, the service is set to startup type Automatic. However, if you upgrade or otherwise re-install your K2 System Software, the service is re-set to startup type Manual. Therefore, you must re-configure the service after K2 System Software upgrade/reinstall in order to set the startup type back to Automatic.

You configure the watched bin to export the K2 media as your desired clip format. After you place the K2 clip in the watched bin, the capture service goes into action and validates the media to make sure it has the proper structure for the desired file format. If it is valid, the capture service then does the necessary processing to export the clip to the destination folder.

The Export capture service and its watched bin must be on a K2 system that hosts the K2 FTP interface, as follows:

- Stand-alone K2 system — When you place a K2 clip in the watched bin, the capture service exports the clip from the internal storage or direct-connect media storage of the K2 system. The watched bin must be on the K2 system's V: drive.
- K2 Media Server with role of FTP server — When you place a K2 clip in the watched bin, the capture service exports the clip from the shared media storage of the K2 SAN. The watched bin must be on the K2 Media Server's V: drive.

Prerequisites for using the Export capture service

Before you can configure and use the Export capture service, the following requirements must be satisfied:

- The K2 system must support the clip format you plan to export. This could require specific hardware and/or licenses.
- K2 system software must be at a version that supports the Export capture service. Refer to the "About This Release" section of the K2 Topic Library for information on Export capture service version compatibility.
- The capture service must be licensed on the stand-alone K2 system or K2 Media Server. This is a Grass Valley software license.

Use topics in this section as appropriate to satisfy prerequisites.

Considerations and requirements for using the Export capture service

When you are configuring and using the Export capture service, do the following:

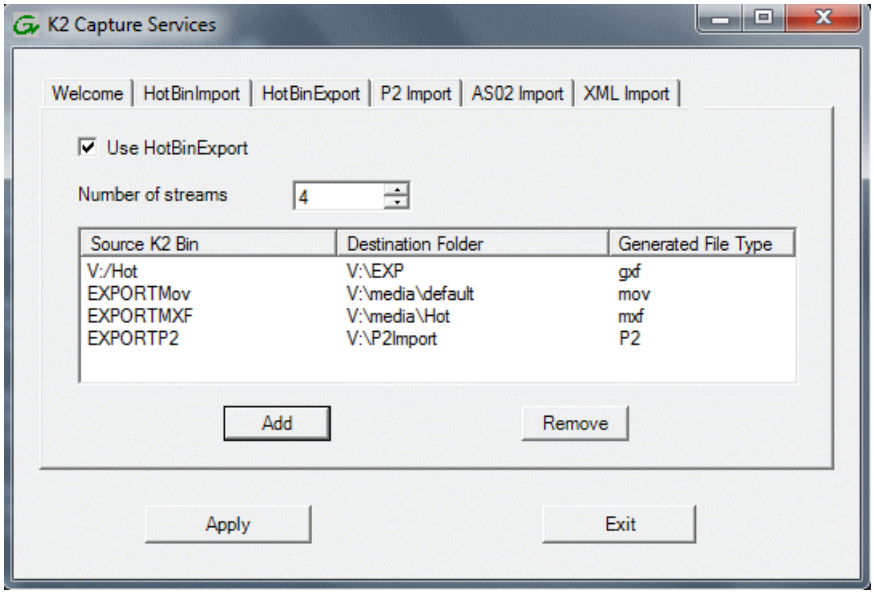
- You must be logged in with administrator privileges on the K2 system as well as having the appropriate security permissions to access the watched folder or bin.
- If the destination folder (for export) is on a remote machine, you must configure the "movie" user account as a local user account on that machine. The "movie" user account is not supported as a domain administrator account. Configure the account as follows:
  - Username: `movie`
  - Password: `M0vieK2M0vie`

  The password uses the number zero character, not the letter O character.
- If the destination folder (for export) is on a remote machine, the local K2 Summit system must be able to access the remote system with administrator level credentials. If on a domain, the account used to access the remote system must be a domain administrator account.
- If you have multiple source folders (for import) or destination folders (for export) on external systems, use the same user account for all capture service access to all systems.

- If using the export capture service on a K2 SAN, the K2 Capture Services utility must be on a K2 Media Server that is also an FTP server. If your K2 SAN has multiple FTP servers, the utility must be on the primary FTP server.

Configuring the Export Capture Service

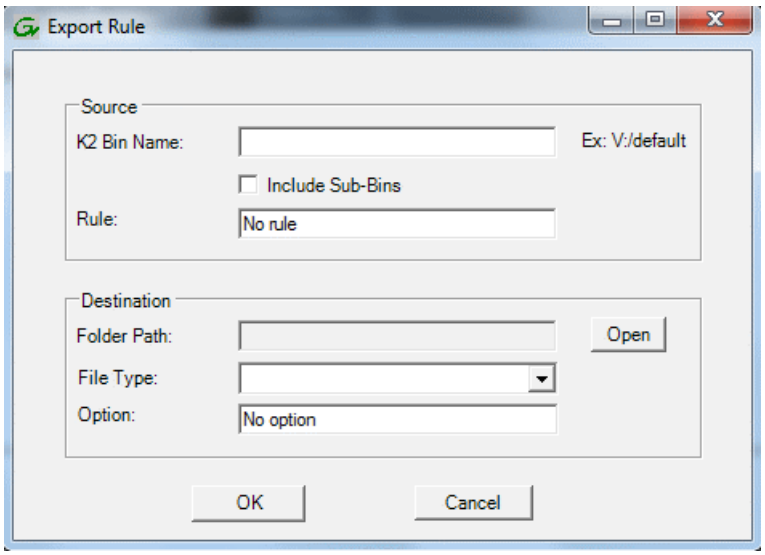
1. From the **Start** menu, access the **All Programs** menu and select **Grass Valley | K2 Capture Services**.
   The K2 Capture Services utility dialog box is displayed.
2. Click the **HotBinExport** tab.



3. Select **Use HotBinExport**.
   If you have not yet licensed the HotBin Export capture service, a "…start the process of getting a license now?" message appears. Follow on-screen instructions to obtain a license. After licensing, restart the K2 Capture Services utility and continue with this procedure.
4. Select the number of streams.
   Exports run serially. If you select one stream, only one export can occur at a time. If you select multiple streams, multiple exports can occur at one time.

5. Click **Add**.

   The Export Rule dialog box opens.



6. Configure as follows:

   - Source K2 Bin Name — Required. This is the watched bin. The bin must be on the K2 system's V: drive. It must be in the K2 media database and appears in AppCenter as a media bin. When valid clips are placed in this bin, the HotBin Export capture service automatically exports the clips.
   - Include Sub-Bins — Optional. When selected, clips are exported if they are in a bin nested inside the Source K2 Bin.
   - Rule — Do not configure this field. Leave the default value as it is.
   - Destination Folder Path — Required. This is a standard file system directory. It receives the files/directories exported by the Export capture service. If you specify a destination folder that does not yet exist, the K2 system creates it when exporting. If the destination folder is not on the local K2 system, you are prompted to enter user account credentials to access the source directory. You must enter user account credentials that have administrator level privileges on the remote system. If part of a domain, the user account must be a domain administrator account. When you enter a domain account, you must enter the domain name.

     NOTE: You must use the same user account for all capture service access to all systems.
   - File Type — Required. Select the file format in which K2 clips are exported.
   - Option — Do not configure this field. Leave the default value as it is.

7. Click **OK** to save settings and close the Export Rule dialog box.
8. Repeat previous steps to add additional Export HotBins.

Testing the Export Capture Service

1. Place the clips to export into the watched bin.
2. Verify that the media appears in the destination.

3. Play to verify success.

Export capture service components

The following table describes the components that support Export capture service functionality.

Name	Description
Grass Valley Import Service	This is the service that provides the functionality for the capture service. It is the service that automatically exports K2 clips from the K2 media storage.
K2 Capture Services utility	Configures K2 capture services.
Source K2 bin	This is the watched bin. It is a bin in K2 media storage. When files are placed in this directory, the capture service automatically exports them from K2 media storage.
Destination folder	The folder that receives the files exported from the K2 media storage.

Licensing K2 capture service software

Licensing is required for K2 capture service software as follows:

- To use the XML Import capture service, you must obtain a XML Import capture service license from Grass Valley.
- To use the P2 Import capture service, you must obtain a P2 Import capture service license from Grass Valley.
- To use the Export capture service, you must obtain an Export capture service license from Grass Valley.

Licenses are requested through the K2 License Wizard and managed through the SabreTooth License Manager, which are installed with K2 system software.

1. To start the licensing process, open the K2 Capture Services utility and on the tab for your capture service, select the "Use…" checkbox.

   If you do not yet have a license, a "…start the process of getting a license now?" message appears.

2. Click **Yes** and **OK** to open the K2 License Wizard for the type of license. Refer to *K2 Release Notes* for procedures and information on obtaining and managing licenses.

PitchBlue workflow considerations

The K2 Solo 3G system supports the H.264 format used in the PitchBlue workflow. However, you must consider the intended PitchBlue workflow when using this H.264 media, as it is not supported for general purpose use outside of the PitchBlue workflow.

The K2 Solo 3G system ingests the PitchBlue material without any error correction. The material often has anomalies, such as incomplete last frame, that the K2 Solo 3G system accepts as-is. When PitchBlue plays out this material under VDCP automation control, it plays the known-good material only. The automation playout system tracks the portions of the imported PitchBlue content for playout by interacting with the traffic and other related playout automation components. Anomalies

can be identified so that they are not played out. In this way, the automation playout system avoids the errors that would otherwise occur if the material were used for general purpose playout without automation control.

Therefore, you must adhere to the complete PitchBlue workflow from ingest through playout for all PitchBlue material. Do not attempt to play out PitchBlue material except as part of the prescribed PitchBlue workflow.

NOTE: Playing out PitchBlue material in any other way can cause errors.

Pinnacle support

The K2 system can automatically convert Pinnacle material into K2 clips as part of a FTP transfer or a HotBin import, as described in the topics in this section.

Pinnacle material that can be converted

A Pinnacle clip is stored as a folder on a Pinnacle MediaStream server. The folder structure for its MPEG program/system stream based content is as follows:

```
<folder> clipname
  <file> header (contains Pinnacle clip metadata)
  <file> ft (Pinnacle version of "Frame Index Table")
  <file> info (File used to hold automation specific data. Not
  used by Pinnacle.)
  <file> std (The MPEG program or system stream -
  essence/media)
```

You have the following options for the Pinnacle material to convert:

- Convert only the media essence (the std file).
- Convert the metadata along with the media essence.

Pinnacle import mechanisms

You have the following options for import/transfer mechanisms:

- K2 HotBin import — This method converts only the media essence. It does not convert the Pinnacle clip metadata. You drop the Pinnacle clip's std file into a K2 HotBin. Then the K2 HotBin process imports, converts, and creates a K2 clip. The K2 clip is available for playout when the process is complete.
- K2 FTP import — This method converts only the media essence. It does not convert the Pinnacle clip metadata. Your third-party FTP client connects to the K2 FTP server as a normal K2 FTP session and puts the Pinnacle clip's std file.
- Pinnacle emulation K2 FTP import — This method converts the Pinnacle clip metadata along with the media essence. Your third-party automation vendor or FTP client connects to the K2 FTP server with the Pinnacle specific login, creates a new directory, and puts the Pinnacle clip files in the new directory. The K2 FTP server creates a corresponding K2 clip. The K2 clip is available for playout while the content is being transferred. The K2 clip contains timecode, mark in/out points, and other metadata as defined by the Pinnacle clip metadata.

Enabling Pinnacle import

Before you import your Pinnacle material, familiarize yourself with the configuration options in the following procedure.

1. To import Pinnacle material, create the following registry value:

```
HKEY_LOCAL_MACHINE\Software\Grass Valley Group\Streaming
REG_DWORD "ImportPinnacleStreams" = 1
```

   Without this registry value, the K2 system does not handle the import correctly.

2. Do one of the following:

   - If do not want to import captions and timecode from your Pinnacle material, skip the remainder of this procedure. No further configuration is necessary.
   - If you want to import captions and timecode from your Pinnacle material, continue with this procedure. Read each step carefully and proceed only if you are sure that your Pinnacle material is suitable.

3. To optionally import VITC from Pinnacle clips, proceed with this step as appropriate.

   - If you know that VITC was not recorded on your Pinnacle material in the Pinnacle-private uncompressed VBI data, skip to the next step. Do not create a registry value.
   - If you know that your Pinnacle material was recorded with VITC as Pinnacle-private uncompressed VBI lines and you want to preserve this timecode when you import the content into the K2 system, then create the following registry key:

```
HKEY_LOCAL_MACHINE\Software\Grass Valley Group\Streaming
REG_DWORD "ExtractPinnacleVitc" = 1
```

   This instructs the K2 system to extract and preserve the VITC.

4. To optionally import captions from Pinnacle clips, proceed with this step as appropriate.

   - If you know that captions were not recorded on your Pinnacle material in the Pinnacle-private uncompressed VBI data, skip the remainder of this procedure. Do not create a registry value.
   - If you know that your Pinnacle material was recorded with closed captions or teletext data as Pinnacle-private uncompressed VBI lines and you want to preserve the captions when you import the content into the K2 system, then create the following registry key:

```
HKEY_LOCAL_MACHINE\Software\Grass Valley Group\Streaming
REG_DWORD "ExtractPinnacleCaptions" = 1
```

   This instructs the K2 system to extract and preserve the captions.

When you are no longer using the K2 system to import Pinnacle material, you can delete all of the above registry values that you created to support the import.

Importing via K2 Hot Bin

1. If you have not already done so, configure a K2 HotBin.
2. Rename the Pinnacle clip's *std* file with your desired K2 clip name and a **.mpg* extension.

3. Drop the file in the K2 HotBin.

Importing via K2 FTP

1. With your third-party FTP client, connects to the K2 FTP server as a standard K2 FTP session.
2. Use the FTP `put` command to transfer the Pinnacle clip's *`std`* file with your desired K2 clip name.

   Use the following example as a guideline:

```
ftp mx-proto-b14
Connected to mx-proto-b14.
220 FTP Server (1, 0, 0, 1) ready.
User (mx-proto-b14:(none)): administrator
331 Password required for user administrator.
Password:
230 Logged in, and aspect successfully set to MOVIE, stream mode GXF.
ftp> bin
200 Type set to IMAGE.
ftp> put std /MPG/V:/default/646405_IMX30_ MXF_IPN
200 PORT command okay.
150 Opening MOVIE mode data connection for
/explodedFile/V:/default/646405_IMX30_ MXF_IPN.
226 Transfer complete.
ftp: 54547968 bytes sent in 14.05Seconds 3883.25Kbytes/sec.
ftp> quit
221 Goodbye.
```

Importing via Pinnacle emulation K2 FTP

1. With your third-party automation vendor or FTP client, connect to the K2 FTP server as follows:

   FTP username: video_fs

   FTP password: .video_fs

   The username and password are case sensitive.
2. Create a directory named for the Pinnacle clip.

3. Put the following Pinnacle clip files in the directory in the following order:

   header

   ft

   info (optional)

   std

   Use the following example as a guideline:

```
J:\>ftp mx-proto-b14
Connected to mx-proto-b14.
220 FTP Server (1, 0, 0, 1) ready.
User (mx-proto-b14:(none)): video_fs
331 Password required for user video_fs.
Password:
230 Logged in, and aspect successfully set to MOVIE, stream mode PIN.
ftp> bin
200 Type set to IMAGE.
ftp> mkdir pinnacle_clip
250 Command "XMKD pinnacle_clip" succeeded.
ftp> cd pinnacle_clip
250 Change of directory to explodedFile/V:/default/pinnacle_clip
successful, xfer mode PIN.
ftp> put header
200 PORT command okay.
150 Opening MOVIE mode data connection for header.
226 Transfer complete.
ftp: 132 bytes sent in 0.00Seconds 132000.00Kbytes/sec.
ftp> put ft
200 PORT command okay.
150 Opening MOVIE mode data connection for ft.
226 Transfer complete.
ftp: 393216 bytes sent in 0.11Seconds 3574.69Kbytes/sec.
ftp> put std
200 PORT command okay.
150 Opening MOVIE mode data connection for
/explodedFile/V:/default/pinnacle_clip.
226 Transfer complete.
ftp: 56097960 bytes sent in 16.25Seconds 3452.18Kbytes/sec.
ftp> quit
221 Goodbye.
```

Specifications for Pinnacle support

- Pinnacle clips do not indicate timecode as drop-frame. The K2 import assumes non-drop-frame values.
- The time-code used in the header file and recorded into the MPEG Video GOP header starts out as 00:00:00:00 by default. If the option to extract VITC is not enabled, or no VITC is detected on import, timecode extracted from the MPEG Video GOP manifests as the timecode track for the imported K2 clip.
- Pinnacle servers preserve non-MPEG-1 (Musicam) audio as Pinnacle-private elementary streams within the program stream *std* file. Pinnacle clips allow up to 8 channels of audio. On import the K2 system detects the private stream audio packets when they are present and generates the appropriate K2 audio track(s).

- When importing Pinnacle content recorded as an MPEG1 system stream, any Pinnacle-private audio from MPEG2 program stream based clips is lost.
- The K2 system supports extraction of the following kinds of Pinnacle-private audio:
  - PCM-16, PCM-20 (PCM-20 is converted into PCM-24 on import)
  - DolbyE and AC-3
- If you enable the option via registry key, the K2 system examines specific VBI lines when it detects Pinnacle-private VBI lines, as follows:
  - Line 21 (default, can be overridden via registry) is examined for the presence of close captioning or SDP teletext. If detected, this is appropriately de-modulated into EIA-608 close caption or OP-47 subtitling packets and inserted as ancillary data packets into an ancillary data track on the imported clip.
  - Line 19-PAL and 14-NTSC (default, can be overridden via registry) is examined for the presence of VITC. If detected, this is appropriately de-modulated into SMPTE 12M compliant time-code values which is inserted as time-code values into the time-code track on the imported clip.
- The following applies to the Pinnacle emulation K2 FTP import:
  - All supported FTP commands, with the exception of those mentioned below, respond as they do for a conventional K2 FTP session. For instance, commands such as renames and deletes operate on K2 clips, directory listings reveal K2 clips and bins, and so on.
  - Navigation (`cd`) to K2 bins is allowed. By default, the *`default`* K2 bin is projected as the FTP root.
  - The `MKD/XMKD` command does not create a K2 bin for the argument specified, but merely retains the argument as the name of the K2 clip to be created based on following `STOR` commands.
  - The `CWD/XCWD` command does not allow navigation to a K2 bin. If the Pinnacle clip name used in a previous MKD command is used as an argument to `CWD`, the K2 FTP server does not internally navigate to that "bin", but rather merely returns a success status.
  - The `STOR` command only honors `ft`, `std`, or `header` as arguments, or filenames with a *`.mxf`* extension. When the K2 FTP server receives data for the *`std`* file it creates a K2 clip with the name issued by a previous `MKD/XMKD` command.

Compressed VBI import

The K2 system can be set up to import Standard Definition (SD) Compressed VBI closed captioning. The feature can be useful for workflows that include SD clips from Profile XP and other video servers, or for facilities transitioning from SD to HD. If you are interested in this feature, contact Grass Valley Support to determine if it is appropriate for your system design. If appropriate, Grass Valley Support can provide you with the instructions to enable the feature.

About compressed VBI import processes

The K2 system extracts closed captioning by decoding the compressed video. The K2 system then inserts the extracted closed captioning as an SD ancillary data track into the K2 clip. These processes occur as the material is being transferred into the K2 system.

These processes take place on the K2 device performing the import. This can be a stand-alone or SAN K2 system. During these import processes the CPU consumption on the system performing

the import is higher than with conventional imports. Take this into consideration when planning to use this feature.

Compressed VBI import specifications

The compressed VBI import is supported as follows:

- SD MPEG only.
- All forms of import are supported, such as FTP, automation protocols, AppCenter, Capture services, and InSync.
- GXF, MXF, MPEG, and MOV imports extract closed captioning from SD 720x512 video.
- D-10/IMX SD MPEG video is supported
- SD 525 line (NTSC) closed captioning is supported
- SD 625 line (PAL) teletext is not supported
- The first SD video track encountered is processed for compressed VBI. Multiple video tracks are not processed.
- If the incoming video contains compressed VBI lines but closed caption data is not present, the resultant K2 clip has an ancillary data track containing “blank” closed caption data. On playout, the blank closed caption data is inserted into the video, but no closed caption is displayed for the video.
- If an MPEG program/transport stream contains both ATSC Closed Captioning inserted into the MPEG picture user data and compressed VBI lines, the K2 system ignores the compressed VBI lines and processes for the ATSC Closed Captioning instead.
- The K2 system does not process the incoming video when the following occurs:
  - The video does not contain compressed VBI lines
  - The video already contains an ancillary data track
  - The video is High Definition (HD)
  - The video is a GXF complex movie, such as a program or a playlist.

Managing Stand-alone Storage

About the internal storage system

A K2 Solo 3G system with internal drives for media storage is a self-contained, stand-alone unit, with no external devices for storage, audio, or video connections required.

K2 Summit 3G internal storage system

The storage system on an internal storage first generation K2 Solo 3G system includes the following:

mSATA — The mSATA SSD boot media on the front interconnect board serves as the system drive. The Windows operating system, applications, and other standard computer software components reside on the system drive.

RAID drives — There are slots for twelve 2.5 inch RAID drives, located behind the front bezel assembly in the front of the unit. These drives are for media storage. Twelve media drives are available. Media data is written or “striped” across media drives in a continuous fashion, which

makes them a “stripe group”. This media stripe group appears as the V: drive to the Windows operating system.

Disk controller board — The disk controller board provides the RAID functionality for the internal disks. It is mounted vertically in the front of the unit. K2 Summit 3G systems with direct-connect storage or shared SAN storage do not contain a disk controller board, as RAID disks are in the external RAID storage devices.

RAID 1 — Drives configured as RAID 1 provide redundancy. The two disks in a RAID 1 LUN are redundant partners. Any single disk in a LUN can fail and disk access can continue. When a disk fails, error messages in the AppCenter StatusPane inform you of the problem. You can then replace the failed disk. The data is rebuilt on the replacement disk and redundancy is restored.

RAID 0 — Media drives configured as RAID 0 offer no redundancy. If any single RAID 0 media drive fails, all data is lost on all media drives.

First generation K2 Summit internal storage system

The storage system on an internal storage first generation K2 Solo 3G system includes the following:

Compact Flash — The Compact Flash boot media serves as the system drive. The Windows operating system, applications, and other standard computer software components reside on the system drive.

RAID drives — There are slots for eight 3.5 inch RAID drives, located behind the front bezel assembly in the front of the unit. These drives are for media storage. Eight media drives are available. RAID 0 is available as an option from the factory. Media data is written or “striped” across media drives in a continuous fashion, which makes them a “stripe group”. This media stripe group appears as the V: drive to the Windows operating system.

Disk controller board — The disk controller board provides the RAID functionality for the internal disks. It is mounted horizontally in the front center of the unit. K2 Solo 3G systems with direct-connect storage or shared SAN storage do not contain a disk controller board, as RAID disks are in the external RAID storage devices.

RAID 1 — Drives configured as RAID 1 provide redundancy. The two disks in a RAID 1 LUN are redundant partners. Any single disk in a LUN can fail and disk access can continue. When a disk fails, error messages in the AppCenter StatusPane inform you of the problem. You can then replace the failed disk. The data is rebuilt on the replacement disk and redundancy is restored.

RAID 0 — Media drives configured as RAID 0 offer no redundancy. If any single RAID 0 media drive fails, all data is lost on all media drives.

K2 Solo Media Server internal storage system

The storage system on a K2 Solo Media Server includes the following:

Compact Flash — The Compact Flash boot media serves as the system drive. The Windows operating system, applications, and other standard computer software components reside on the system drive.

RAID drives — A K2 Solo Media Server contains 2 disk modules. Media data is written or “striped” across media drives in a continuous fashion, which makes them a “stripe group”. This media stripe group appears as the V: drive to the Windows operating system. Disks are configured as RAID 0,

so you cannot remove and replace a disk module while the K2 Solo Media Server is operational. If a disk fails, you lose all media.

Disk controller board — The disk controller board provides the RAID functionality for the internal disks.

RAID 0 — Media drives configured as RAID 0 offer no redundancy. If any single RAID 0 media drive fails, all data is lost on all media drives.

About the direct-connect storage system

A K2 Solo 3G system that is directly connected to an external K2 RAID storage device for media storage is a self-contained, stand-alone unit.

The storage system on direct-connect storage K2 Solo 3G system includes the following:

System Drive — Compact Flash (first generation Summit) or mSATA (Summit 3G) boot media serves as the system drive. The Windows operating system, applications, and other standard computer software components reside on the system drive.

Fibre Channel card — The direct-connect K2 Solo 3G system has a direct Fibre Channel connection to external K2 RAID. The K2 Solo 3G system must have the optional Fibre Channel card installed to support this connection.

There are no internal RAID drives or a disk controller board in a direct-connect storage K2 Solo 3G system.

RAID 5 — Drives configured as RAID 5 provide redundancy. There are six disks in one RAID 5 LUN. A disk in a LUN can fail and disk access can continue. When a disk fails, error messages in the AppCenter StatusPane inform you of the problem. You can then replace the failed disk. The data is rebuilt on the replacement disk and redundancy is restored.

Using Storage Utility

This section contains topics about using Storage Utility for stand-alone internal storage.

About Storage Utility

You can use Storage Utility for general maintenance tasks on a stand-alone internal storage K2 system. Refer to the Service Manual for your K2 product for repair procedures, such as those required to replace a failed drive.

NOTE: Do not run Storage Utility on a shared storage (SAN) K2 client. For shared storage, run Storage Utility only via the K2 System Configuration application, as explained in the K2 SAN Installation and Service Manual.

The Storage Utility runs on either the local K2 system or from a Control Point PC. In both cases the Storage Utility's primary functionality is hosted by the K2 system. The Storage Utility uses the connection to the RAID disks for access and configuration.

A stand-alone K2 system runs in either an online mode or an offline mode. These modes are required for Storage Utility operations. Online/offline modes are as follows:

- Online mode — This is the stand-alone K2 system's normal operating mode. When the stand-alone K2 system is in the online mode and you open Storage Utility, you can stay in this mode while you view the devices, LUNs, and disks of the internal storage system, but you can not configure the storage system. However, some operations are available that do not configure the storage system, such as identify a drive (flash the drive LEDs), get controller logs, disable a drive, and force a drive to rebuild.
- Offline mode — In this mode the stand-alone K2 system channels are disconnected and all media access operations are disabled. You are prompted to put the stand-alone K2 system into offline mode when you select an operation that configures the storage system. When the stand-alone K2 system is in the offline mode you can configure the storage system and perform all Storage Utility operations. When you exit Storage Utility you can put the stand-alone K2 system back into online mode.

⚠ ***CAUTION: Use the Storage Utility only as directed by a documented procedure or by Grass Valley Support. If used improperly, the Storage Utility can render your K2 system inoperable or result in the loss of all your media.***

Opening Storage Utility

There are two ways to open Storage Utility for work on a stand-alone K2 system, as explained in the following sections.

Opening Storage Utility through AppCenter

Unless prevented by a system problem, you should always open Storage Utility through AppCenter. When you do this your AppCenter login permissions are passed to Storage Utility, so you do not have to log in to Storage Utility separately.

If you are running AppCenter on the local K2 system, as Storage Utility opens it connects to the storage system of that local K2 system. If you are running AppCenter on a control point PC, as Storage Utility opens it connects to the storage system of the K2 system that hosts the channel currently selected in AppCenter.

1. Open AppCenter, either on the local K2 system or on the control point PC and log in.

   Make sure you log in to AppCenter with appropriate privileges, as this log in is passed to Storage Utility. Administrator-level permission is necessary for most Storage Utility operations. If you log in with user-level permissions, the Storage Utility menu item is disabled.

2. If you are running AppCenter from a control point PC and you have channels from multiple K2 systems in your channel suite, select a channel from the stand-alone K2 system whose storage you intend to configure with Storage Utility. This is important as Storage Utility automatically connects to the K2 system that hosts the currently selected channel.

   NOTE: Make sure you are connecting to a stand-alone K2 system. You should never connect Storage Utility directly to a K2 client that uses shared (SAN) storage.

3. From the AppCenter **System** menu, select **Storage Utility**.

   Storage Utility opens.

4. If you are connecting from a control point PC, you should verify that you are connected to the correct K2 system. To verify this, use the Identify feature to flash the disks on the K2 system.

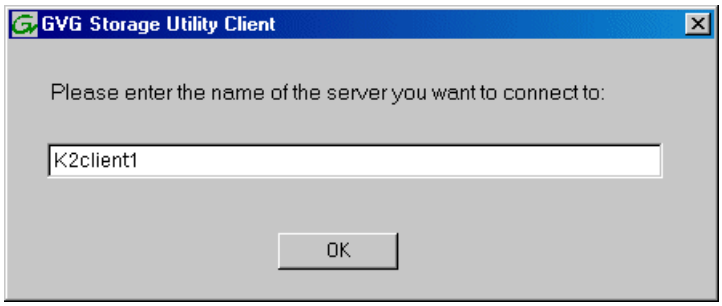
Opening Storage Utility Independently

Do not open Storage Utility independently unless there is a problem that prevents you from opening it through AppCenter.

1. Open the Storage Utility shortcut on the Windows desktop or from the Windows Start Menu at **Programs | Grass Valley | Storage Utility**.

   A dialog box opens in which you specify the machine to connect to with Storage Utility.

   NOTE: Make sure you are connecting to a stand-alone K2 system. You should never connect Storage Utility directly to a K2 client that uses shared storage.

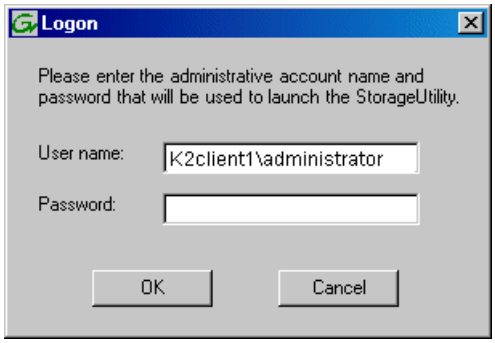


2. Enter the name or IP address of the K2 system for which you intend to use Storage Utility. If you are opening Storage Utility on a local K2 system, enter the name of that K2 system. Click **OK**.

   The Storage Utility logon dialog box opens.

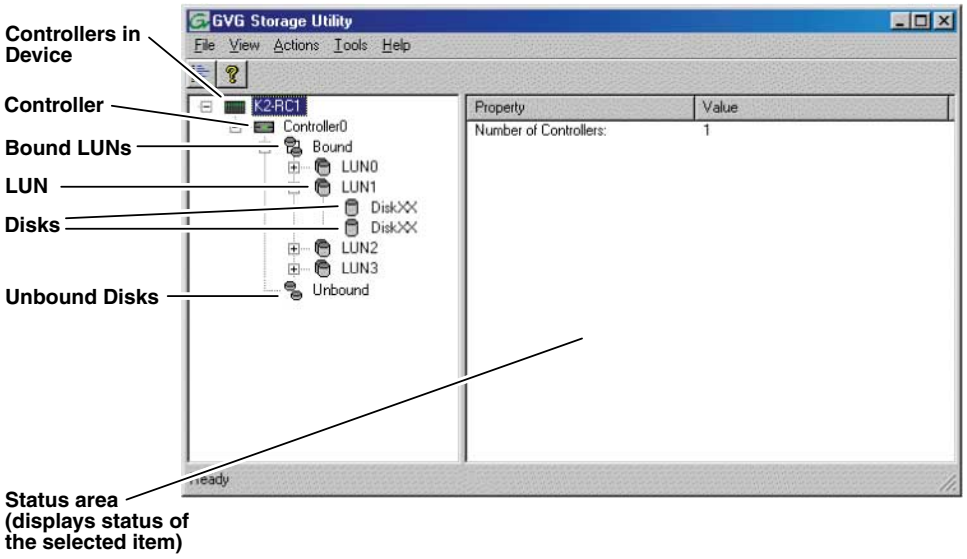
3. Logon to Storage Utility. Make sure you log in with appropriate privileges. Administrator-level permission is necessary for most Storage Utility operations. For user name, you might need to enter the machine name as the domain to successfully log in.

   Storage Utility opens.



4. If you are connecting from a control point PC, you should verify that you are connected to the correct K2 system. To verify this, use the Identify feature to flash the disks.

Overview of Storage Utility



The Storage Utility user interface includes a tree view in the left-hand pane, and a status information area displayed in the right-hand pane. The tree view displays the hardware that makes up the storage system connected. The context menus in the tree view are used to configure storage. The right-hand status pane displays information about the item selected in the tree view. The tree view hierarchy is as follows:

Controllers in Device — Provides a logical grouping of RAID Controllers by device.

Controller — Represents the RAID Controllers found. These are numbered in the order discovered. The controller icon represents both RAID Controller A and, if installed, RAID Controller B. To determine if an optional RAID Controller B is installed, select the Controller icon in the tree view, then examine the status pane for peer status.

Bound LUNs — Expanding the Bound node displays all bound LUNs.

LUN — Represents a bound LUN. Expanding the LUN node displays the disk modules that make up the LUN.

UnBound disks — Expanding the UnBound node, displays all unbound disk modules.

Disks — Represents the disk modules.

The Storage Utility detects disks available and lists them on the opening screen.

Refer to the following procedures to use Storage Utility for maintenance tasks

Checking storage subsystem status

Some limited status information for storage subsystems is displayed in the Storage Utility. This can be helpful when configuring storage.

You can view status information by selecting items in the tree view.

Item in tree view	Status information displayed
Controllers in Device	Number of Controllers
Controller	Microcode Version
Bound	Number of LUNs
LUN	Binding Type, such as RAID 1 State (online or offline)
Disk	Firmware
	Vendor
	State
	Product ID
	Capacity
Unbound	Number of disks

Checking controller microcode

As explained in the previous section, to check controller microcode, select the controller in the tree view and the microcode version is displayed.

About identifying disks

The Identify feature allows you to flash the disk LEDs so that you can physically locate a specific disk module or group of disk modules that make up a LUN. Always use the disk identify feature before removing and replacing a failed disk module. Accidentally removing the wrong disk module can destroy all data on the disk drives.

You can also use this feature to verify the K2 system to which you are currently connected.

Identifying internal disks

1. Open Storage Utility and in the tree view expand all nodes so that all disks are displayed.
2. On the K2 Summit system, remove the front bezel assembly. On the K2 Solo Media Server, disk LEDs are visible without removing the bezel.

   NOTE: Replace the bezel assembly within one minute to maintain system cooling.

3. The tables below illustrates the position of drives as numbered in the K2 Solo 3G system chassis. Compare the drive number positions and the disk numbering displayed in Storage Utility to identify drive locations.

   K2 Summit 3G Production Client

Disk 0	Disk 1	Disk 2	Disk 3	Disk 4	Disk 5	Disk 6	Disk 7	Disk 8	Disk 9	Disk 10	Disk 11

   First generation K2 Summit Production Client

Disk 2		Disk 4		Disk 7
Disk 1		Disk 3		Disk 6
Disk 0				Disk 5

   K2 Solo Media Server

Disk 0
Disk 1

4. Position yourself so you can see the RAID drive LEDs.
5. Identify the disks in a LUN or identify a single disk, as follows:
   a) In the Storage Utility tree view, right-click a LUN or right-click a single disk, then select **Identify LUN** or **Identify Disk** in the context menu.

      A message box opens with a message that informs you that a disk or disks are blinking.

   b) View disks.

      The LEDs display an amber color flashing several times a second. This flashing pattern can stop automatically after a specific time interval, such as ten seconds.

   c) Verify the location of the disk or disks.

Get controller logs

1. In the tree view, select the controller.
2. Click **Actions | Get Controller Logs**.
3. A message informs you of the location of the logs.
4. Find the following files on the local K2 Summit/Solo system at *C:\logs*:

   tty.log

   ControllerEvents.log

Check disk mode pages

1. In the tree view, right-click the controller and select **Check DIsk Mode Pages**.

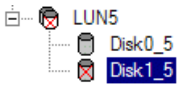
2. Messages report the results of the check. For each disk that has mode pages set incorrectly, click **Yes** when prompted "…restore the default mode page settings?".

Disabling a disk

1. In the tree view, right-click the disk and select **Advanced | Disable** and **OK** to confirm.

   A message "The drive is spinning down…Please wait" appears.

   If internal storage, the Service LED on the K2 system displays a flashing yellow pattern three time a second.
2. When the message "Operation succeeded…now safe to remove disk" appears, click **OK**.
3. The Storage Utility displays red Xs on tree view icons to represent a disk fault and a degraded LUN.



NOTE: On the K2 Media Client, remember that the LUN 0 (disks 0_0 and 0_1) is the system drive. Do not attempt disk operations on the system drive.

Forcing a disk to rebuild

With RAID 0 there is no RAID redundancy, so disks do not rebuild. With other RAID types, such as RAID 1, if media access (record/play) is underway, when you insert a media disk it automatically begins to rebuild. If there is no media access underway, to start the rebuild process either begin a media operation or use the following procedure:

1. In the tree view, identify the faulty disk . If the disk is not currently in the fault state, the Rebuild option is not available.
2. In the tree view, right-click the faulty disk and select **Rebuild**.
3. When the message "Succeeded to start rebuild…" appears, click **OK**.

   If internal storage, the Service LED on the K2 system displays a flashing pattern alternating yellow/green once a second.

Unbind LUN

With internal storage, you can only unbind one LUN at a time. Also make sure the controller is not busy with other processes, such as rebuilding a disk. If the controller is busy, the unbind LUN operation fails.

⚠ ***CAUTION: Unbinding destroys all data stored on disk modules.***

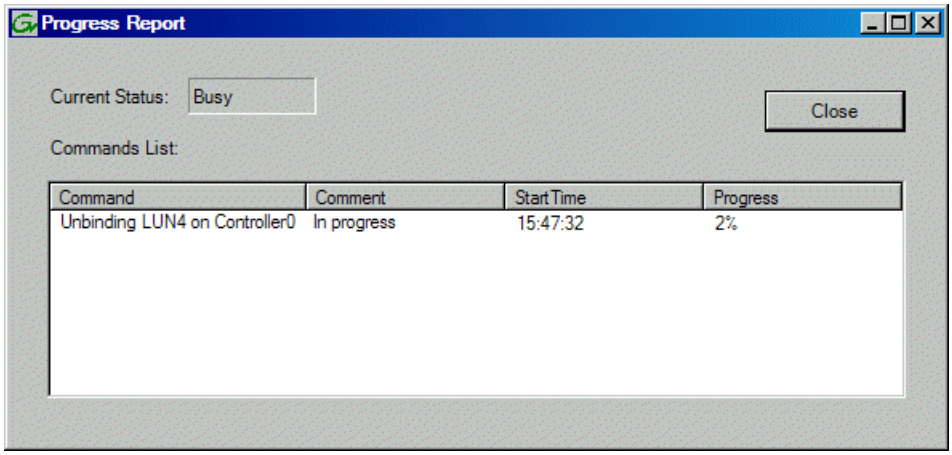
Refer to topics about direct-connect external storage before using this procedure on direct-connect systems.

1. In the tree view, right-click the LUN and select **Unbind LUN**.

2. If online, messages appear "…offline mode now?" and "…continue?". Click **Yes** to put the system in offline mode.

   AppCenter channels go offline.

3. When warning messages appear "…destroy all existing media…" and "Are you sure?", click **OK** to continue.
4. The Progress Report opens and displays unbind progress.



5. When progress reports 100% complete, the LUN is unbound.
6. Restart the K2 system.

NOTE: On the K2 Media Client, remember that the LUN 0 (disks 0_0 and 0_1) is the system drive. Do not attempt disk operations on the system drive.

Bind Luns

When you bind a LUN, you select one or more unbound disks and create a new LUN. The Storage Utility places this new LUN at the bottom of the list and numbers it accordingly. However, with internal storage, disk numbers are enforced by the chassis slot in which the disk resides. Therefore, depending on the number and sequence of LUNs created, it is possible that the LUN numbers and the disk numbers do not match. When you create a new file system, this mismatched numbering does not hamper functionality. However, to make the internal storage K2 system easy to service, you should retain the correct numbering sequence. To do this you must unbind all media LUNs and then bind disks in sequence. On a K2 Media Client, do not unbind LUN0, which is the system drive.

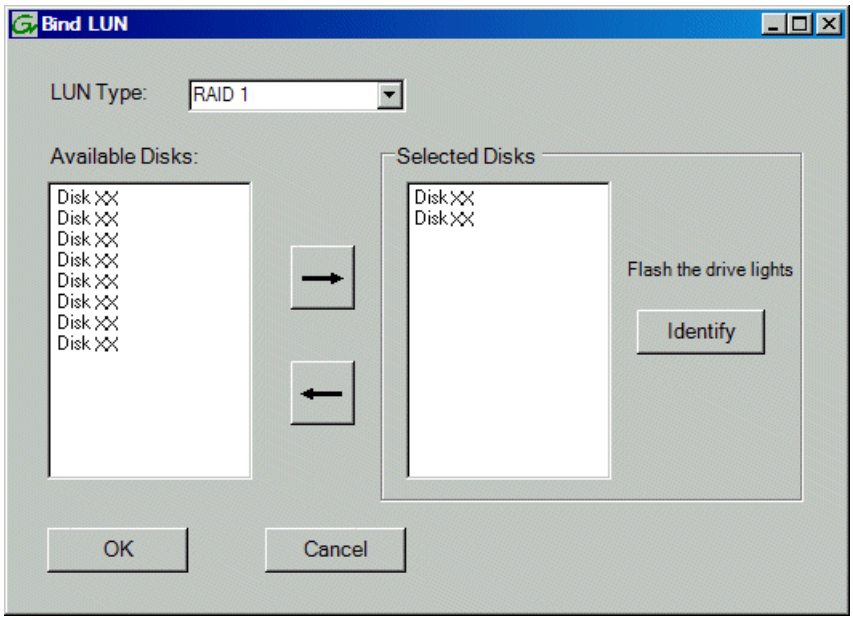
Refer to topics about direct-connect external storage before using this procedure on direct-connect systems.

1. In the tree view, right-click the **Unbound** node and select **Bind LUN**.

2. If online, messages appear "…offline mode now?" and "…continue?". Click **Yes** to put the system in offline mode.

   AppCenter channels go offline.

   The Bind LUN dialog box opens showing all unbound disks for the controller listed in the Available Disk list.



3. Make a selection in the LUN Type drop-down list and proceed as follows:

   - RAID 0 — For K2 Solo 3G systems. Optional for internal storage first generation K2 Summit systems and K2 Summit 3G systems.

     In the Available Disks list, select one media disk, then click the arrow button to add it to the Selected Disks list. K2 Solo Media Server supports RAID 0 only.

   - RAID 1 — For internal storage first generation K2 Summit systems and K2 Summit 3G systems.

     In the Available Disks list, select two contiguous disks, then click the arrow button to add them to the Selected Disks list. (TIP: Use 'shift-click' or 'control-click' to select disks.)

   - RAID 5 — For direct-connect storage on K2 Solo 3G systems.

     In the Available Disks list, select six contiguous disks, then click the arrow button to add them to the Selected Disks list. (TIP: Use 'shift-click' or 'control-click' to select disks.)

   NOTE: As an aid in identifying a disk module's physical location, select it in the Selected Disks list, then click Identify Disks. This causes the disk drive LED to flash.

4. Click OK to close the Bind LUN dialog box and begin the binding process.

   The Progress Report opens and displays binding progress.

5. Repeat the previous steps for remaining unbound disks. You do not need to wait until the first LUN is bound before you can start binding the next LUN. Multiple LUNs can be in the binding process all at the same time.

6. When progress reports 100% complete for all the LUNs that you are binding, proceed to the next step.
7. Restart the K2 system.
8. After binding one or more new LUNs, you must make a new file system.

Changing RAID type for internal storage

On an internal storage K2 Summit 3G system, you can change the internal media storage to be either RAID 1 or RAID 0, as follows:

- RAID 1 — Recommended for the "full" media drive option, which is eight drives on a first generation K2 Summit system. Not recommended for media drive options with fewer drives. With RAID 1, two media drives are configured as a mirrored pair to make one LUN. The capacity of each LUN is roughly equivalent to the capacity of one drive, so your total media storage capacity is approximately 50% of the sum total of all the drives. Since drives are mirrored in each LUN, your media is protected against drive failure. If a drive fails, the other drive in the LUN provides continued media access while you replace the failed drive.
- RAID 0 — Required on K2 Solo Media Server. With RAID 0 there is no mirroring, so your total media storage capacity is roughly equivalent to that of all drives combined. However, your media has no RAID protection against drive failure. If one media drive fails, the entire group of drives fails and you lose all your media.

Depending on your needs for capacity versus protection, you can change from one RAID type to another, as explained in the following procedure.

NOTE: This procedure loses all media.

1. If you need to retain media, transfer it to another K2 system or otherwise back it up.
2. Unbind all media LUNs.
3. Restart.
4. Bind media drives, as one of the following:
   - RAID 0 — Bind each media drive as a RAID 0 LUN.
   - RAID 1 — Bind the ten drives as five RAID 1 LUNs.
5. Restart.
6. Make a new file system.
7. If you backed up your media, you can now transfer it back.

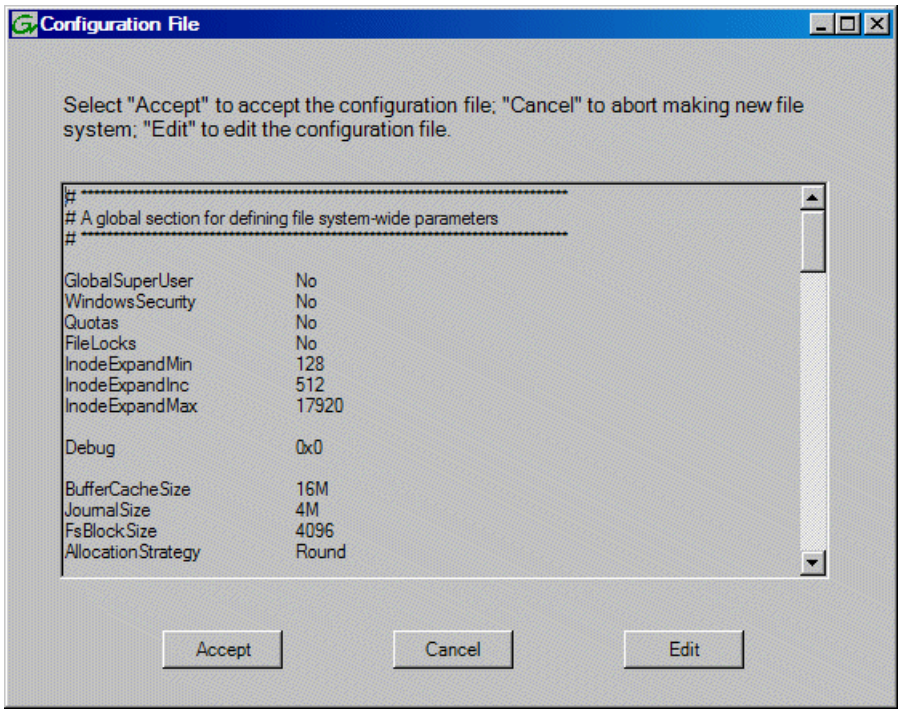
Making a new media file system on a K2 Summit/Solo

If your SNFS file system name is currently "default", when you make a new file system the name changes to "gvfs_hostname", where hostname is the name of the stand-alone K2 system. Also, Storage Utility creates unique disk labels, which is a requirement for compatibility with Dyno PA.

1. Click **Tools | Make New File System**.

2. If online, messages appear "…offline mode now?" and "…continue?". Click **Yes** to put the system in offline mode.

   AppCenter channels go offline. The Configuration File window opens.



3. You can view media file system settings, but do not attempt to change them. Click **Accept**.

   A "Making new file system. Please wait" message box displays progress.

4. When a message "Succeeded to make the new file system. The server will be restarted now" appears, click **OK** to restart.
5. If you have Macintosh systems accessing the stand-alone K2 system, you should check that the SNFS file system volume is configured correctly on the Macintosh systems. Refer to K2 FCP Connect procedures in the K2 FCP Connect Installation Manual.

Checking the media file system

- Media operations must be stopped. You must put the standalone K2 System offline as part of this procedure.

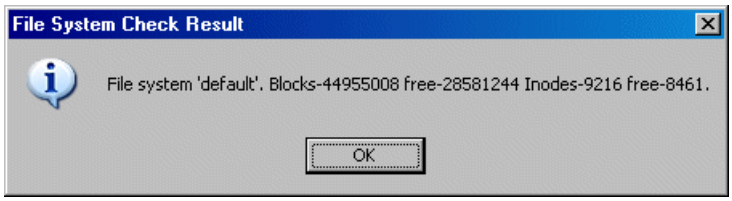
This procedure checks the media file system but retains current media files.

1. In Storage Utility, click **Tools | Check File System**.
2. If online, messages appear "…offline mode now?" and "…continue?". Click **Yes** to put the system in offline mode.

   AppCenter channels go offline.

3. A message box appears “Checking media file system. Please wait”. Observe progress.

   If problems are discovered they are reported. If the check process passes, when the process is complete a message appears to confirm success.



4. Click **OK** to dismiss the results.
5. Messages appear “…online mode now?” and “…continue?”. Do one of the following:

   - Click **Yes** to put the system in online mode. This is the recommended option in most cases. For example, even if you plan to next clean unreferenced files and/or movies, that operation requires that the system be online, so you should put it online now. When you click Yes, AppCenter channels go online.
   - Click **No** to keep the system in offline mode. This is not recommended for most cases. Only do this when you are sure that subsequent operations require the system to be offlline.

Your file system has been checked.

Cleaning unreferenced files and movies

- The standalone K2 system must be online. If K2 AppCenter channels are in the offline state, the clean unreferenced files/movies operations fail.

These procedures allow you to keep the media database and the media files in sync. You can check the movies (clips) in the media database for the references to media files that should be currently stored on the media disks. Likewise, you can check for media files that are not referenced by a movie in the media database. If you find any unreferenced files or movies, you can delete them.

Clean unreferenced files

1. In Storage Utility, click **Tools | Clean Unreferenced Files**.
2. A message box appears “…searching …Please wait”. Observe progress.
3. A message box reports results. Respond as follows:

   - If no unreferenced files are found, click **OK** to dismiss the results.
   - If unreferenced files are discovered, you are prompted to delete them. Click **Yes** to delete the files or **No** to leave the files intact.

The process writes a log file to `C:\profile\logFS.txt`, which you can check for more information.

Clean unreferenced movies

1. In Storage Utility, click **Tools | Clean Unreferenced Movies**.
2. A message box appears “…searching …Please wait”. Observe progress.

3. A message box reports results. Respond as follows:
   - If no unreferenced movies are found, click **OK** to dismiss the results.
   - If unreferenced movies are discovered, you are prompted to delete them. Click **Yes** to delete the movies or **No** to leave the movies intact.

The process writes log files to `C:\profile\cleanupDB.txt` and `C:\profile\MediaDB.txt`, which you can check for more information.

Downloading controller microcode

You might be instructed in K2 release notes to upgrade controller microcode. This allows you to take advantage of enhancements and benefit from improved performance and reliability.

To determine your current controller microcode version, select the controller in the Storage Utility tree view, then in the properties reported in the right-hand pane, note the controller microcode version. Use the following procedure if you need to download controller microcode.

1. Refer to *K2 Release Notes* to determine microcode types, versions, files, and any other special instructions regarding the particular controller microcode you are downloading.
2. In the Storage Utility, right-click the controller in the tree view, then select **Load Controller Microcode** in the context menu.
3. If online, messages appear "…offline mode now?" and "…continue?". Click **Yes** to put the system in offline mode.

   AppCenter channels go offline. The Open File dialog box opens.
4. In the Open File dialog box, browse to the desired microcode file, select the file.
5. Click **OK.**

   The Progress Report window appears showing the microcode download task and the percentage completion.
6. When finished, exit Storage Utility.
7. Put AppCenter channels back online.
8. Restart.

Downloading disk drive firmware

You might be instructed in K2 release notes to upgrade disk drive firmware. This allows you to take advantage of the disk drive enhancements and benefit from improved performance and reliability.

To determine your disk drive type and current firmware version, select a disk drive icon in the Storage Utility tree view, then note the drive properties reported in the right-hand pane. Use the following procedure if you need to download disk drive firmware.

NOTE: The disk drives are upgraded one at a time which can take as long as 2 minutes per drive. Take this into consideration when scheduling the upgrade.

1. Refer to *K2 Release Notes* to determine firmware types, versions, files, and any other special instructions regarding the particular disk drive firmware you are downloading.
2. In the Storage Utility, right-click a disk in the tree view, then select **Advanced | Download Disk Firmware** in the context menu.

3. If online, messages appear "…offline mode now?" and "…continue?". Click **Yes** to put the system in offline mode.

   AppCenter channels go offline. The Open File dialog box opens.

4. In the Open File dialog box, browse to the latest firmware file for your disks, select the file, and click **OK.**

   For internal drives, watch the lights on the drive to which you are downloading firmware. The lights flash as firmware loads. Wait until the lights have completed their flashing pattern. This can take several minutes.

   The Progress Report window appears showing the disk firmware download task and the percentage completion.

5. Repeat this procedure on each drive.
6. When finished, exit Storage Utility.
7. Put AppCenter channels back online.
8. Restart.

Placing the K2 system into online mode

If the stand-alone K2 system is in offline mode and you have completed your storage system configuration tasks, you have the following options to return the system to the online mode:

- Exit Storage Utility and bring channels online — If Storage Utility is closed, first open Storage Utility and then exit Storage Utility. When you exit Storage Utility you are prompted "…back to online mode?". Click **Yes**.

  After exiting Storage Utility, if AppCenter is open the channels remain offline. To bring channels online, if you are running AppCenter on a Control Point PC, select **System | Reconnect**. If you are running AppCenter on a local K2 system, close and reopen AppCenter.
- Restart the K2 system — Restarting automatically resets the system to online mode. When you log into AppCenter channels connect and come up online.

Managing stand-alone K2 systems with SiteConfig

About 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
☐	Select a PC to use as the SiteConfig control point PC	Review system requirements and network access requirements about installing SiteConfig.
☐	Install SiteConfig on the control point PC	—
☐	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.
☐	Add a control network to the site. You can also add a FTP/streaming network if desired	—
☐	Add a group for your K2 clients to the system description	—
☐	Add a placeholder K2 client to the system description for each of your actual K2 clients	—
☐	Configure the names of the placeholder K2 clients	—
☐	Configure the network interfaces of the placeholder K2 clients	Specify IP address ranges and other network details
☐	Discover your K2 clients	—
☐	Assign each discovered K2 client to its placeholder K2 client	—
☐	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.
☐	Add a control point PC placeholder device to the system description	—
☐	Discover the control point PC and assign it to the placeholder control point PC	—
☐	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.
☐	Ping each K2 client and the control point PC to test network communication	—

	Task	Comment
☐	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.
☐	Create a deployment group	—
☐	Add stand-alone K2 clients to the deployment group	—

System requirements for SiteConfig host 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 3 • Server 2003 • Vista Enterprise Service Pack 1 • Windows 7 • Server 2008 R2
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 4.0
Java JRE	1.3.1_12 and 1.4.2_05 or higher. Required for the HP Ethernet Switch configuration interface, which is used for K2 SANs.
XML	Microsoft XML 4 Service Pack 2 is required.

About installing SiteConfig

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

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

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

For a given system, there should be just one instance of SiteConfig managing the system.

Installing/upgrading SiteConfig

- The PC on which you are installing SiteConfg must meet system requirements.
- The PC must be connected to the LAN on which all the devices to be managed are connected.
- There must be no routed paths to the devices to be managed.

1. Procure SiteConfig installation files from the Grass Valley website or via other distribution mechanisms.

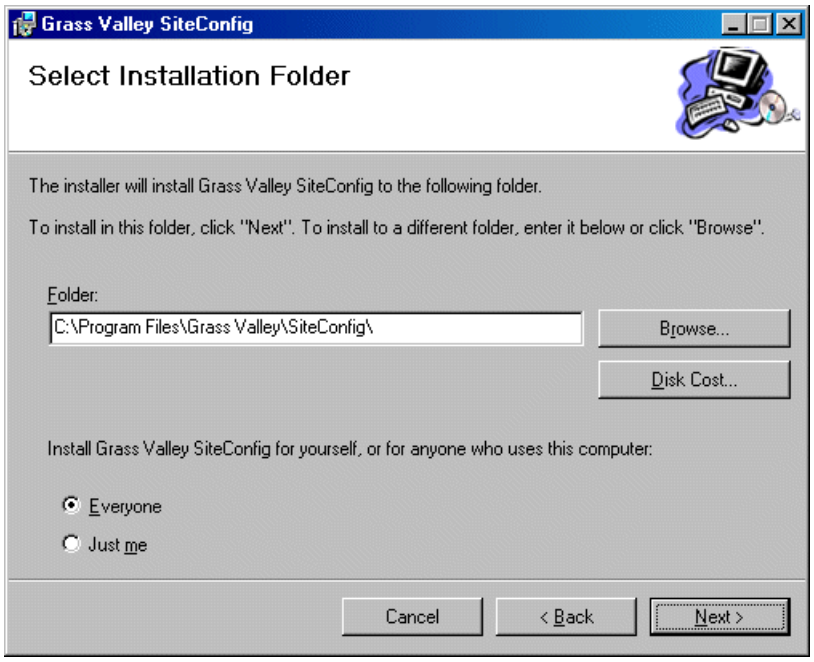
   The following directory and files are required to install SiteConfig:

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

2. If you already have a version of SiteConfig installed, go to Windows **Add/Remove Programs** and uninstall it.
3. Double-click *setup.exe*.

   The installation wizard opens.

4. Work through the wizard pages, clicking **Next** and **Finish**.



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

5. Open the Windows operating system Services control panel on the PC and look for an entry called " ProductFrame Discovery Agent".

   The Discovery Agent must be installed on the SiteConfig PC so that the PC can be discovered by SiteConfig and added to the system description as a managed device. This is necessary to ensure name resolution in SiteConfig's hosts file.

   The Discovery Agent is also known as the Network Configuration Connect Kit. For example, in Windows Add/Remove Programs, it can be displayed as either Network Configuration Connect Kit or SiteConfig Discovery Agent.

6. Proceed as follows:

   - If the Discovery Agent is not installed, navigate to the SiteConfig install location's Discovery Agent Setup subdirectory and double-click the `DiscoveryAgentServiceSetup.msi` file. This launches the setup program and installs the Discovery Agent. Follow the setup wizard to complete installation. A restart is required after installation. Then continue with the next step in this procedure.
   - If the Discovery Agent is already installed, continue with the next step in this procedure.

7. If not already configured, configure the SiteConfig PC with a valid Ethernet IP address for the LAN using Windows Network Connections.
8. If you are not going to be using SiteConfig to manage system hosts files, put the system hosts file on the SiteConfig PC.

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**.

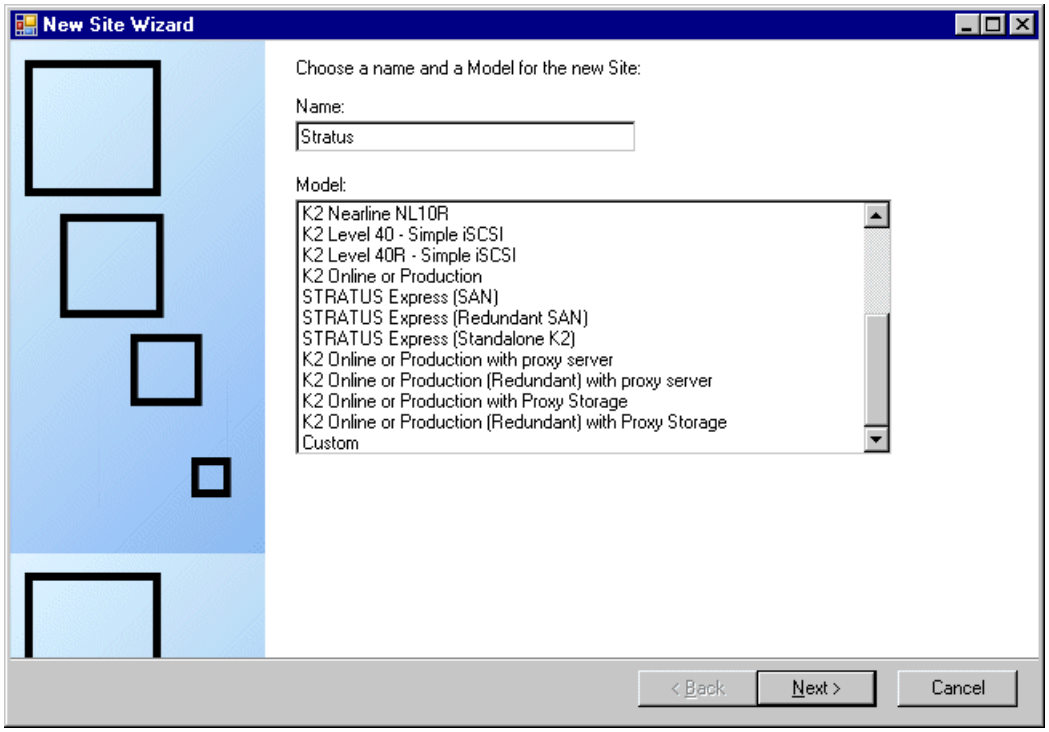
   The Create New System Description dialog box opens.
2. In the Create New System Description dialog box, enter the name of the file for the system description you are creating.

   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.

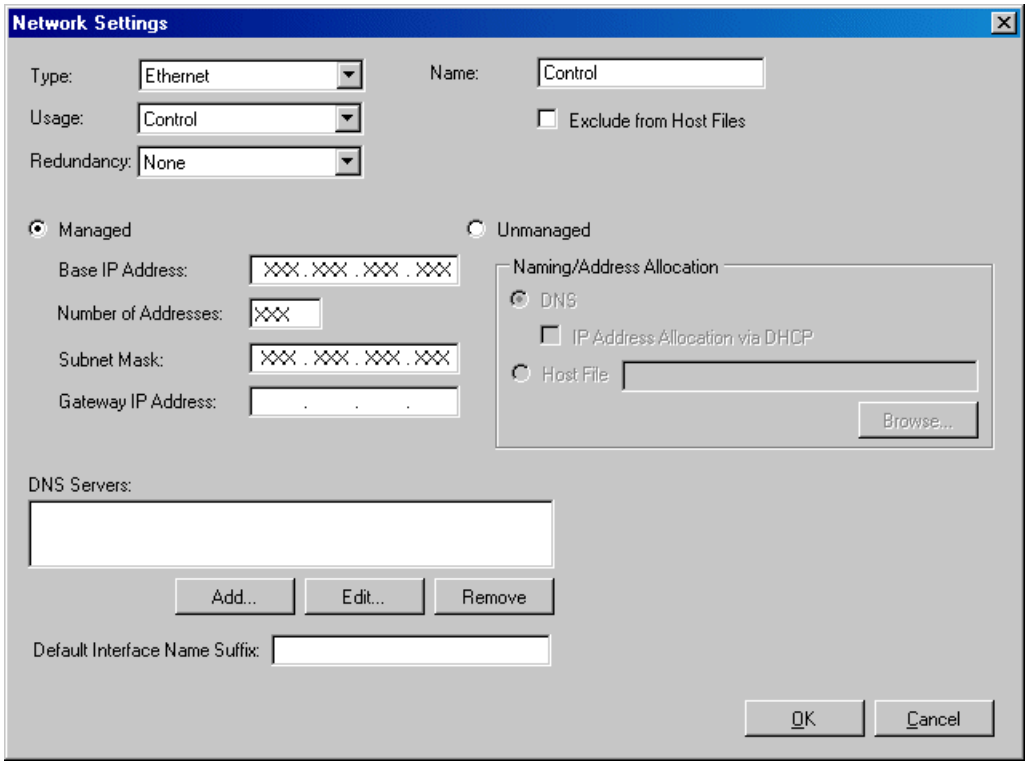
Creating the control network for stand-alone K2 clients

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	*Ethernet* is required
Usage	*Control* is required
Redundancy	*None* is required. This is true even on a redundant K2 SAN. (Only the iSCSI network is redundant on a redundant K2 SAN.)
Name	*Control* is recommended
Exclude from Host Files	*Unselected* is required
Managed	*Selected* 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	*Unselected* 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	*Ethernet* is required
Usage	*FileTransfer* is required
Redundancy	*None* is required. This is true even on a redundant K2 SAN. (Only the iSCSI network is redundant on a redundant K2 SAN.)
Name	*Streaming* is recommended
Exclude from Host Files	*Unselected* is required
Managed	*Selected* 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	*Unselected* is required. Related settings are disabled.
DNS Servers	Servers providing DNS for name resolution. Allowed.
Default Interface Name Suffix	*_he0* is required

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

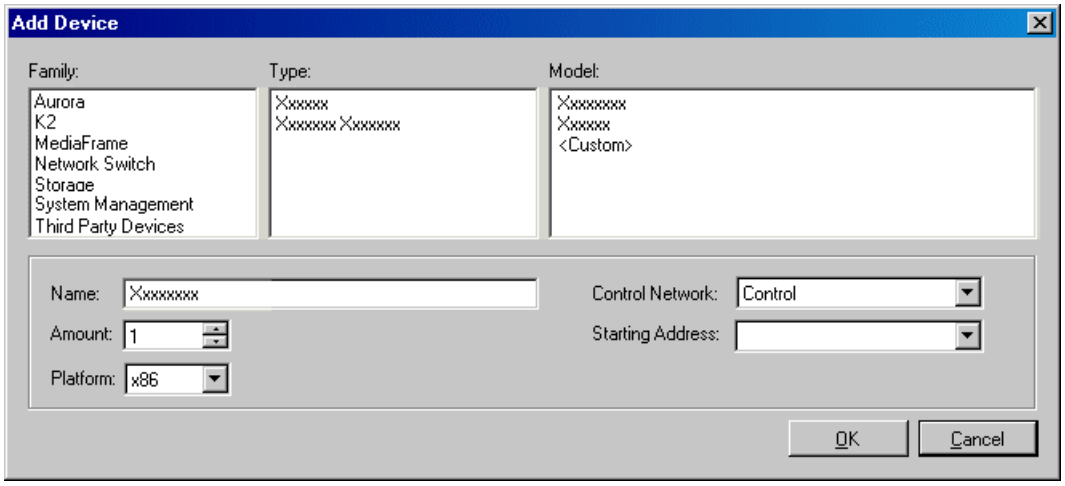
Adding a group

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

- The system description must contain a group.

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



2. Configure settings for the device you are adding as follows:
   - Family – Select **K2**.
   - Type – Select the appropriate type of K2 system.
   - Model – Select the model with the appropriate 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

- The system description must have a stand-alone K2 client that is a placeholder device.

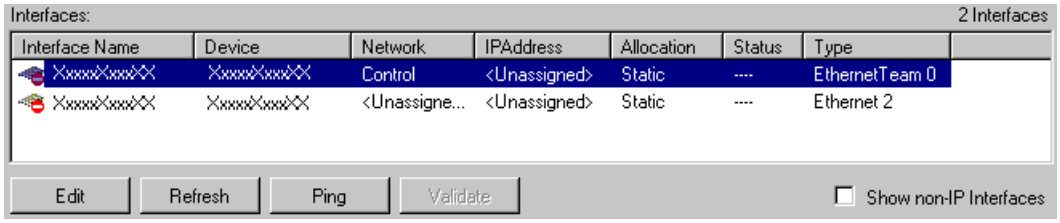
- The placeholder device must have one or more unmanaged network interfaces.

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.

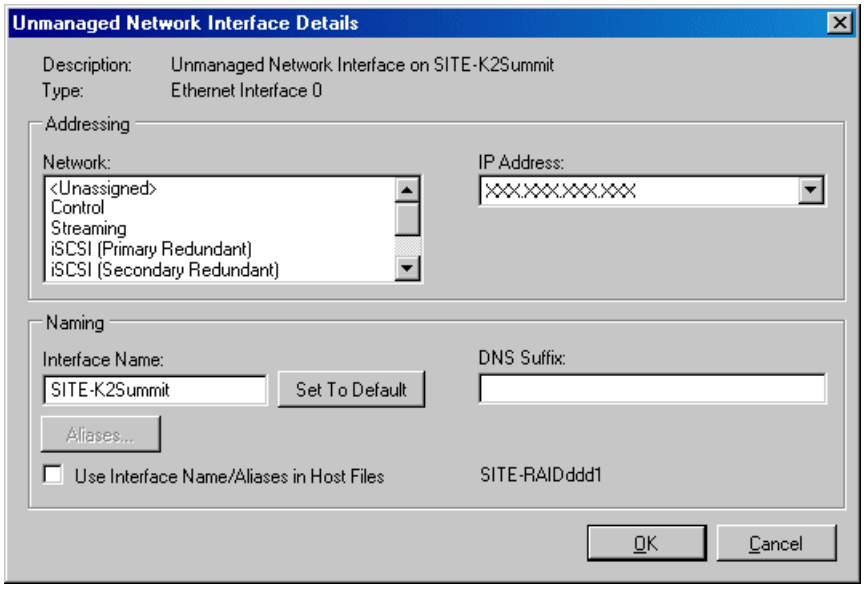
   The interfaces for that device are displayed in the interfaces list view.



   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	*Control* is required
IP Address	The IP address for this interface on the network. Required.
Interface Name	The device host name. Required.
Set to Default	Not recommended. Sets the interface name to SiteConfig default convention, based on the root Site name and device-type.
...use Interface Name/Aliases in Host Files...	*Unselected* is required. Since not selected, the default behavior occurs, which is to use the device host name in the hosts file.
Aliases	Not allowed
DNS Suffix	Allowed, if applicable to the network. The DNS suffix is added to the interface name.

4. Click **OK** to save settings and close.
5. 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	*Streaming* 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 *K2prod01*, then *K2prod01_he0* 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...	*Selected* is required
Aliases	Not allowed
DNS Suffix	Allowed, if applicable to the network. The DNS suffix is added to the interface name.

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

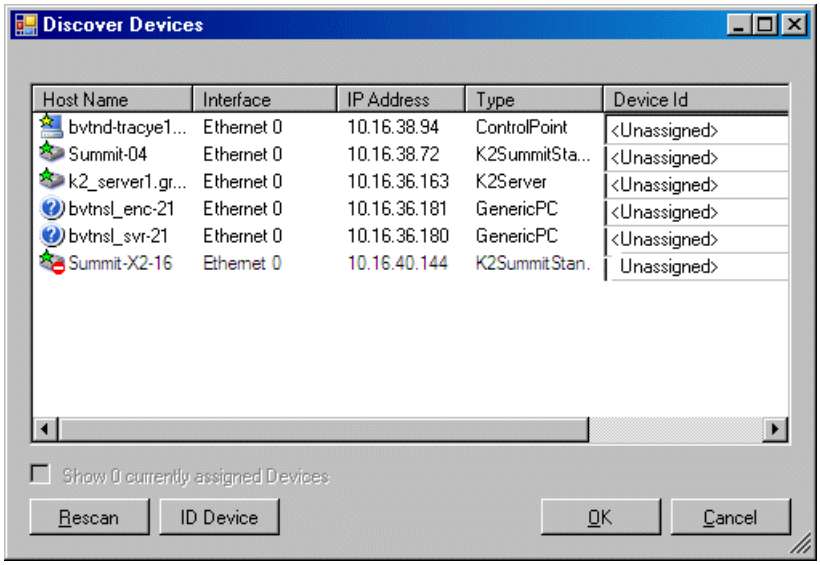
Discovering devices with SiteConfig

- The Ethernet switch or switches that support the control network must be configured and operational. If multiple switches, ISLs are connected and trunks configured.
- The PC that hosts SiteConfig must be communicating on the control network.

- There must be no routers between the PC that hosts SiteConfig and the devices to be discovered.
- Devices to be discovered must be Windows operating system devices, with SiteConfig support installed.
- Devices must be cabled for control network connections.
- If discovering a device with Microsoft Windows Server 2008 operating system, the device must have an IP address, either static or DHCP supplied.

1. Open SiteConfig.
2. In the toolbar, click the discover devices button.

   The Discover Devices dialog box opens.



   A list of discovered devices is displayed.

3. Click **Rescan** to re-run the discovery mechanism. You can do this if a device that you want to discover has its network connection restored or otherwise becomes available. Additional devices discovered are added to the list.

Assigning discovered devices

- Devices must be discovered by SiteConfig
- Discovered devices must not yet be assigned to a device in the system description
- The system description must have placeholder devices to which to assign the discovered devices.

1. If the Discovered Devices Dialog box is not already open, click the discover devices button.

   The Discover Devices dialog box opens.

2. Identify discovered devices.
   - If a single device is discovered in multiple rows, it means the device has multiple network interfaces. Choose the interface that represents the device's currently connected control connection. This is typically Ethernet ... 0.
   - If necessary, select a device in the list and click **ID Device**. This triggers an action on the device, such as flashing an LED or ejecting a CD drive, to identify the device.
3. To also view previously discovered devices that have already been assigned to a device in the system description, select **Show … currently assigned devices**.

   The currently assigned devices are added to the list. Viewing both assigned and unassigned devices in this way can be helpful to verify the match between discovered devices and placeholder devices.
4. In the row for each discovered device, view items on the Device Id drop-down list to determine the match with placeholder devices, as follows:
   - If SiteConfig finds a match between the device-type discovered and the device-type of one or more placeholder devices, it displays those placeholder devices in the list.
   - If SiteConfig does not find a match between the device-type discovered and the device-type of a placeholder device, no placeholder device is displayed in the list.
5. In the row for a discovered device, click the Device Id drop-down list and select the placeholder device that corresponds to the discovered device.

   If there is no corresponding placeholder device currently in the system description, you can select **Add** to create a new placeholder device and then assign the discovered device to it.
6. When discovered devices have been assigned, click **OK** to save settings and close.
7. In the **Network Configuration | Devices** tree view, select each of the devices to which you assigned a discovered device.

Modifying stand-alone K2 client managed network interfaces

- The physical device you are configuring must be discovered and must be assigned to a device in the SiteConfig system description.
- SiteConfig must have communication with the device.
- The device must be defined in the system description with an appropriate network interface.

Use this task to modify managed 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.

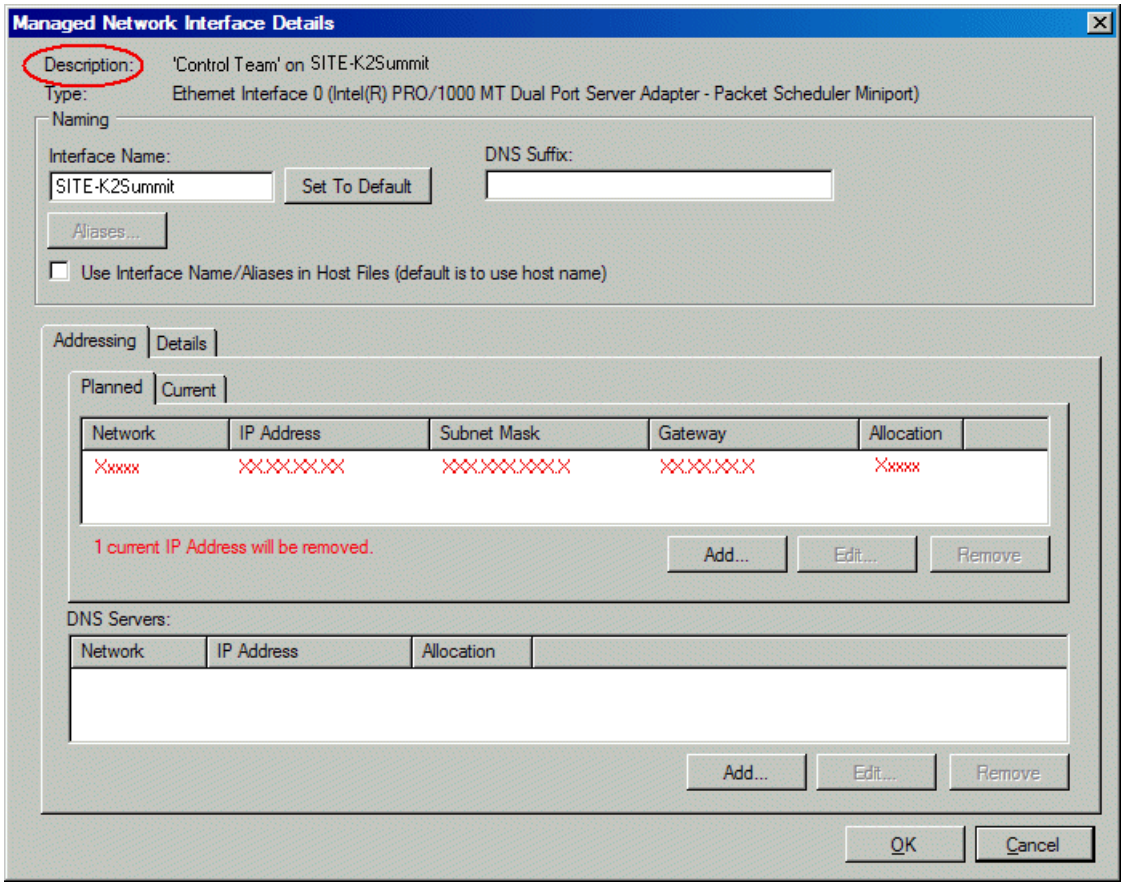
2. In the Interfaces list view determine the interface to configure, as follows:
   - Identify the interface with which SiteConfig is currently communicating, indicated by the green star overlay icon. This should be the control network interface.
   - Verify that the interface over which SiteConfig is 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. The control connection should always be the first port on the motherboard, except when you have a loopback connection.
   - Configure the control network interface first before configuring any of the other interfaces.
   - 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: Make sure that the device is unlocked in SiteConfig before proceeding. For a K2 Summit Production Client with K2 software at a version lower than 9.0, 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.

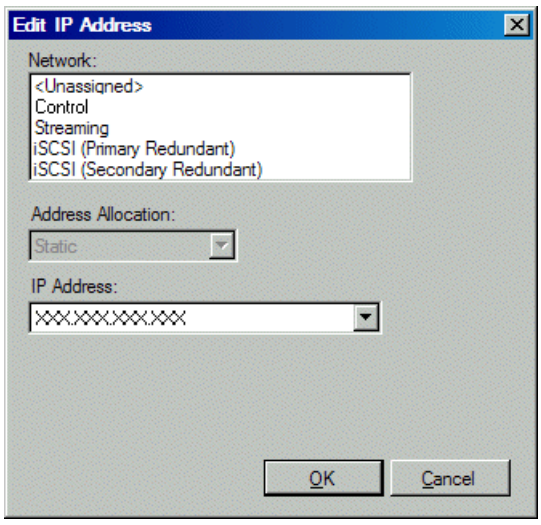
6. Configure naming settings as follows:

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
Use Interface Name/Aliases in Host Files	*Unselected* is required. Since not selected, the default behavior occurs, which is to use the device host name in the hosts file.

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	*Control* is required
Address Allocation	*Static* is recommended.
IP Address	The IP address for this interface on the network. Required.

      The networks listed in the Edit IP Address dialog box are those currently defined in the system description, with available settings restricted according to the network definition. If you require settings that are not available, you can close dialog boxes and go to the **Network Configuration | Networks** tab to modify network settings, then return to the Edit IP Address dialog box to continue.

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	*Selected* is required

14. 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.

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

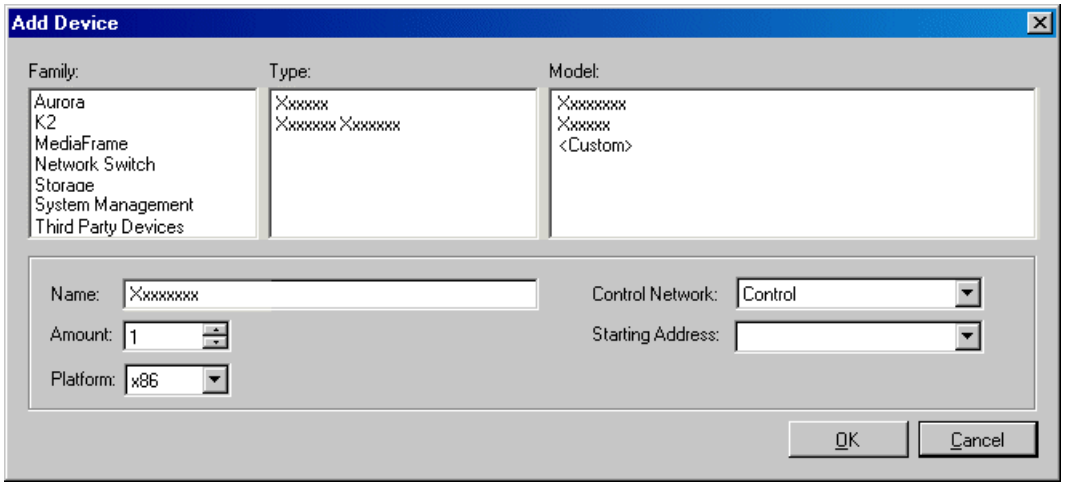
    A Contacting Device message box reports progress.

    NOTE: For a K2 Summit Production Client with K2 software at a version lower than 9.0, 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

- The system description must contain a group.

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



   The Add Device dialog box opens.

2. Configure settings for the device you are adding as follows:

   - Family – Select **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

- The SiteConfig control point PC must have the SiteConfig Discovery Agent installed. The Discovery Agent is also known as the Network Configuration Connect Kit. In Windows Add/Remove Programs, it can be displayed as either Network Configuration Connect Kit or SiteConfig Discovery Agent.
- The system description must contain a control point PC placeholder device.
- The placeholder's control network interface must be 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 must be the 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. Identify the state of buttons as follows:
   - If the host name is different than the device name, the **Set to Device Name** button is enabled.
   - If the host name is the same as the device name, the **Set to Device Name** button is disabled.
4. If enabled, click **Set to Device Name**.
   This changes the host name to be the same as the device name.
5. Click **OK**.
6. When prompted, restart the device.

Pinging devices from the PC that hosts SiteConfig

- The devices you are pinging must be in the SiteConfig system description.

You can send the ping command to one or more devices in the system description over the network to which the SiteConfig host PC is connected. Typically this is the control network.

1. In the **Network Configuration** | **Networks** tree view, select a network, site, or system node.
2. In the Devices list view, select one or more devices. Use Ctrl + Click or Shift + Click to select multiple devices.
3. Right-click the selected device or devices and select **Ping**.
   The Ping Devices dialog box opens and lists the selected device or devices.

The Ping Devices dialog box reports the progress and results of the ping command per device.

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 using SiteConfig

- Planned control network settings must be applied to control network interfaces and devices must be communicating on the control network as defined in the system description.
- Interfaces for networks that require name resolution via the hosts file, such as the FTP/streaming network, must have settings applied and must be communicating.
- Host names defined in the system description must be correct.
- The SiteConfig PC must be added to the system description so that it is included in the host tables generated by SiteConfig.

When you add or modify devices or their IP addresses in the SiteConfig system description, you should update host tables on all devices that use them.

1. In the **Network Configuration | Networks** tree view, select a network, site, or system node.
2. Click **View Hosts file**.

   A Hosts File Contents window opens that displays the contents of the hosts file as currently defined in the system description.
3. Verify the information in the hosts file.
4. Do one of the following:

   - If you are managing host table information yourself, click **Save As** and save a copy of the hosts file to a location on the control point PC. Then open the copy of the hosts file, copy the desired host table information from it, and paste it into your facility hosts file as desired. Then you can use your own process to distribute the facility hosts file to devices. Remember to distribute to the control point PC so that SiteConfig and other management applications such as K2Config can resolve network host names.
   - If SiteConfig is managing hosts files, do the following:

   NOTE: Writing hosts files to multiple devices consumes system resource and network bandwidth. Therefore it is recommended that you wait and do this after the system is complete and fully implemented, rather than updating hosts files incrementally as you discover/assign devices.

   a) In the **Network Configuration | Devices | Devices** list view, right-click a device to which you intend to write the hosts file and select **View Current Host File**.

      A Host File Contents window opens that displays the contents of the hosts file that is currently on that actual device.

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

   c) In the **Network Configuration | Devices | Devices** list view, right-click a device or use Ctrl + Click to select multiple devices, and select **Update Host File**.

      The current hosts file is overwritten with the hosts file as defined in the system description.

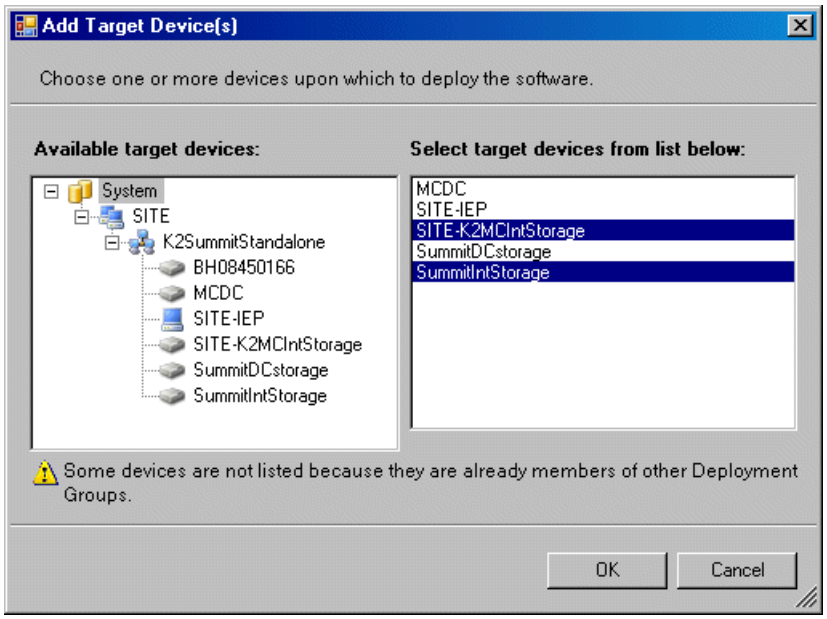
Configuring deployment groups

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

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

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

   The Add Target Device(s) wizard opens.



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

Managing K2 system software

About K2 system software

Check *K2 Release Notes* for the latest information about software.

K2 system software components are as follows:

- K2 Client: Installed on K2 Solo 3G system. Provides core functionality for all K2 Solo 3G system models.
- K2 Server: Installed on K2 Media Servers. Provides core functionality for all K2 Media Servers in all roles.
- Control Point: Installed on Control Point PCs. Provides remote control and configuration of K2 Solo 3G systems (both internal and external storage) as well as the K2 SAN.
- Media File System (SNFS): Installed on K2 Media Servers, stand-alone K2 Solo 3G systems, and shared storage (SAN) K2 Solo 3G system. Provides a dedicated file system for access to media data. Install only as instructed by release notes.

In addition, the following software is installed in special cases:

- Multi-Path I/O software — You must install this software on K2 Solo 3G systems that are part of a redundant K2 SAN and on K2 Solo 3G systems with direct-connect storage.

On a K2 SAN system, Grass Valley requires that you use SiteConfig to install K2 system software. On a standalone K2 Solo 3G system Grass Valley recommends SiteConfig but allows manual installation as well. You can access software on your K2 Solo 3G system's USB Recovery Flash Drive and via download from the Grass Valley website. On the USB Recovery Flash Drive, find SiteConfig `*.cab` files in the `ProductFrame` directory and find manual installation files in the `release` directory.

Software components installed

Each of the K2 installation packages installs software components that provide the functionality for various applications and system tools. The components installed are as follows:

Software	Components installed	Comments
K2 Client	Core system software	Provides the primary media functionality.
	AppCenter user interface	Allows you to operate AppCenter on the local machine.

Software	Components installed	Comments
	AppServer	Provides AppCenter functionality. It is accessed by both the remote AppCenter (on a Control Point PC) and the local AppCenter user interface.
	Storage Utility	Configures the media storage on internal storage K2 clients only. Do not run Storage Utility on shared storage K2 clients.
	K2 System Configuration	Installed only on shared storage models. Provides to the remotely connected K2 System Configuration application the ability to configure the local machine. You cannot run the K2 System Configuration user interface on the local K2 client.
	Multi-Path I/O	Installation files copied to K2 client but software not installed.
K2 Server	Core system software	Provides the primary media functionality.
	Storage Utility	Provides functionality for the remotely connected Storage Utility that runs on the Control Point PC. You should not run Storage Utility locally on the K2 Media Server.
	K2 System Configuration	Provides to the remotely connected K2 System Configuration application the ability to configure the local machine. You cannot run the K2 System Configuration user interface on the local K2 Media Server.
Control Point	AppCenter user interface	Connects to K2 clients for control and configuration of channels.
	K2 System Configuration user interface	Connects to K2 clients, K2 Media Servers, RAID storage, and Gigabit switches for configuration of the K2 SAN.
	Storage Utility	Connects to the K2 Media Server, and through the K2 Media Server to the RAID storage, for configuration of the media file system, media database, and RAID storage.

Installing Control Point software

If you are using the Grass Valley Control Point PC, it comes from the factory with software installed, so you should not need to install software.

If you intend to use a PC that you own as a Control Point PC, make sure that you choose a PC that meets system requirements for supporting Control Point software. Then install software and configure as follows:

1. Set up Windows user accounts according to your site's security policies. Refer to related topics in the "About This Release" section of the K2 Topic Library for the list of accounts and passwords.

2. Install the following software, as it is required to support K2 Control Point software:
   - MSXML 4.0
   - .NET Framework 1.1

   You can find this software on your K2 Solo 3G system's USB Recovery Flash Drive.
3. Install K2 Control Point PC software, as referenced earlier in this chapter.
4. It is recommended that you install the following software, so that you can accomplish a broad range of operational and administrative tasks from the control point PC:
   - Java Real Time Environment Update 7 or higher. Required for the HP Ethernet Switch configuration interface, which is used for K2 SANs (shared storage).
   - QuickTime 7, for local viewing of exported media. You can find this on your K2 Solo 3G system's USB Recovery Flash Drive.
   - Adobe Acrobat Reader, for reading documentation from the K2 Documentation Set.
5. Install SiteConfig. It is recommended that you use SiteConfig to manage stand-alone K2 Solo 3G systems. It is required that you use SiteConfig to manage K2 SANs.
6. Install SNMP manager software.

   Refer to related topics about Grass Valley recommended deployment and monitoring solutions in the "About This Release" section of the K2 Topic Library.
7. Create a backup image.

Installing K2 software

Except as noted in the preceding sections, when you receive your K2 Solo 3G system, you do not need to install software. The system has software pre-installed at the factory.

If you are upgrading software on a K2 Solo 3G system, refer to related topics in the "About This Release" section of the K2 Topic Library for that version of software for specific upgrade procedures. If you are upgrading a K2 SAN, you must use SiteConfig with the proper sequence and upgrade all K2 Media Servers and K2 Solo 3G systems to the same software version. Upgrade K2 Media Servers first, then K2 Solo 3G systems. Refer to related topics in the "About This Release" section of the K2 Topic Library for the complete explanation of the rules that apply to upgrading software on the K2 SAN.

Before upgrading K2 software, you should make a recovery image.

Pre-installed software

Software is pre-installed on K2 products when you receive them from the factory. Refer to related topics in the "About This Release" section of the K2 Topic Library for version updates.

Backup and recovery strategies

Find information on creating images, restoring from images, and other backup and recovery information as follows:

For this device…	Find information in this documentation:
K2 Solo 3G system	K2 Summit Service Manual
K2 Media Client	K2 Media Client Service Manual
K2 Solo Media Server	K2 Solo Media Server Service Manual
K2 Media Server	K2 SAN Installation and Service Manual
Control Point PC	Use procedures from a K2 Summit Service Manual

Administering and maintaining the K2 system

Licensing

Grass Valley continues to develop the K2 product family to better meet the needs of a wide range of customer requirements. As these developments become available, you can add the specific functionality you need with Grass Valley software licenses. Detailed procedures for installing licenses come with option kits or are included in release notes for K2 products. Contact your Grass Valley representative to learn more about the licensing structure and for purchasing information.

Software version licenses

At major software releases, significant new features are added. If you are licensed for the software release, you can upgrade your software and receive the benefits of the new features.

Licensable options

Optional applications, bundles of advanced features, and enhanced functionality are available as licensable options for K2 products. Refer to the *K2 Release Notes* for a list of options, and contact your Grass Valley representative to learn more about options.

Configuring K2 security

The section contains topics about K2 security.

Overview of K2 security features

K2 security features reference Windows operating system user accounts and groups on the local K2 system to determine permission levels. Depending on the account used to log on to the Windows operating system, to log on to K2 applications, or to otherwise authenticate system access, permission is granted for various levels of operational and media access.

K2 systems offer security features as follows:

- Windows operating system — Depending on the current Windows logon, permission is granted to make security and user account settings in the Windows operating system.

- K2 applications — Depending on the user account used to log on to the application, permission is granted to control and configure the application. These K2 applications include AppCenter, Storage Utility, and the K2 System Configuration application.
- Media access — There are three types of media access security, as follows:
  - Media access in AppCenter — You can set user permissions on the K2 bins that store your media. Then, depending on the current AppCenter logon, permission is granted for AppCenter operations on the media in the bins.
  - Media access via FTP — The user permissions set on K2 bins in AppCenter also determine access via FTP. Depending on the FTP session logon, permission is granted for FTP commands accessing the media in the bins.
  - Media access via protocols — The permissions set on K2 bins in AppCenter also determine access for channels controlled by protocols. Depending on the channel accessing the media, permission is granted for operations on the media in the bins.
- Channel access security — You can set user permissions for each channel. Then, depending on the current AppCenter logon or protocol operating a channel, permission is granted or denied to operate the channel.

Example: Setting up user access to bins

In this example User A requires a private bin in which only they can see media or have any access to media. User B requires a bin that provides media to other users, but prevents other users from modifying the media. To set up security features to meet these requirements, do the following:

Task	Documentation
Log on to the local K2 system with Windows administrator permissions.	*Passwords and security on Grass Valley systems* on page 32
Configure a “userA” account and a “userB” account on the local K2 client.	Use standard Windows procedures
Log on to AppCenter with GV administrator permissions.	*Passwords and security on Grass Valley systems* on page 32
Create a “userA_private” bin and a “userB_share” bin on the local K2 system.	*K2 AppCenter User Manual*
For bin “userA_private” configure an access control list with permissions as follows: • Create a group and add all users except user A to the group. For this group, set permissions to: Deny Full Control • userA: Allow Full Control	*Configuring media access security for K2 bins* on page 378

Task	Documentation
For bin “userB_share” configure an access control list with permissions as follows: • Create a group and add all users except user B to the group. For this group, set permissions to: Allow List Bin Contents, Allow Read, Deny Write, Deny Delete • userA: Allow Full Control	*Configuring media access security for K2 bins* on page 378
Log on to AppCenter as userA. Test userA access to bins. Log off.	—
Log on to AppCenter as userB. Test userB access to bins. Log off.	—

Example: Setting up user access to channels

In this example User A requires exclusive access to channels 1 and 2 and User B requires exclusive access to channels 3 and 4. To set up security features to meet these requirements, do the following:

Task	Documentation
Log on to the local K2 system with Windows administrator permissions.	*Passwords and security on Grass Valley systems* on page 32
Configure a “userA” account and a “userB” account on the local K2 client.	Use standard Windows procedures
Log on to AppCenter with GV administrator permissions.	*Passwords and security on Grass Valley systems* on page 32
For channels 1 and 2, configure access control lists with permissions as follows: • Create a group and add all users except user A to the group. For this group, set permissions to: Deny • userA: Allow	*About channel access security* on page 382
For channels 3 and 4, configure access control lists with permissions as follows: • Create a group and add all users except user B to the group. For this group, set permissions to: Deny • userB: Allow	*About channel access security* on page 382
Log on to AppCenter as userA. Test userA access to channels. Log off.	—
Log on to AppCenter as userB. Test userB access to channels. Log off.	—

Passwords and security on Grass Valley systems

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

The following table shows the different types of users and their privileges. Passwords are case sensitive.

	Windows administrator	Grass Valley product administrator	K2 product administrator	Grass Valley product user
User name	Administrator	GVAdmin	K2Admin	GVUser
Password	adminGV!	adminGV!	adminK2	userGV!
AppCenter Configuration Manager	Full access	Full access	Full access	Can view
AppCenter	Full access	Full access	Full access	Full access; requires an account on the K2 Summit/Solo system
Storage Utility	Full access	Full access	Full access	Can't access
K2Config	Full access	Full access	Full access	Can't access
Server Control Panel	Full access	Full access	Can view	Can view
Windows Operating System	Full access	Full access	Limited access (based on Windows user account privileges).	Limited access (based on Windows user account privileges)

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

Configuring media access security for K2 bins

The permissions you set on a K2 bin restricts access to the media in the bin via AppCenter operations, via FTP, and via protocol control of channels.

You can set permissions on a K2 bin as follows:

- Write — Allow access to rename or delete any of the clips located in the bin.
- Delete — Allow access to delete any of the clips located in the bin.
- Read — Allow access to the clips located in a bin, but deny the ability to modify the clips.

- List Bin Contents — Allow or deny access to explore the contents of the bin. This permission also controls access to transfer clips in/out of the bin and to perform search operations on the bin.
- Full Control — Allow or deny all of the above permissions plus the ability to modify the permissions on a bin.

As you configure permissions, take the following into account:

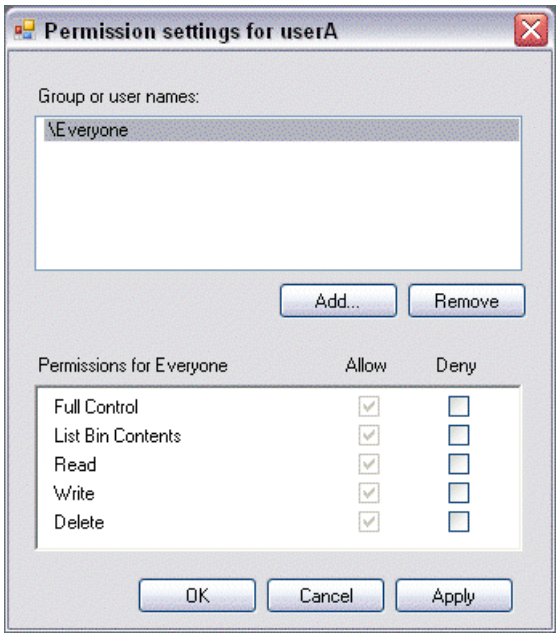
- In case of conflicts, the Deny permission always overrides the Allow permission.
- Do not restrict access for the *movie*, *mxfmovie*, and *video_fs* accounts. These accounts are used for access by applications and modifying permissions can cause applications and transfers to fail. If your security policy requires restricting access to these accounts, contact Grass Valley Support.
- By default, the "Everyone" group is set to Full Control, with all permissions allowed. When you create a new bin it has these default permissions applied automatically.
- Avoid using the "Everyone" group to restrict permissions. Doing so causes some or all operations to fail, regardless of the account currently logged on.
- The "system" user account must retain access to bins and files.
- Never deny any permissions to the user NT AUTHORITY\System.
- The user account that originally created a bin always retains the ability to modify permissions on that bin.

If you need to restrict access to a K2 bin that you have created, set up a media access control list on the bin, as instructed in the following procedure.

1. Make sure you are logged on to Windows and AppCenter with administrator privileges.
2. Create user accounts and bins as necessary to support your permission policies.
3. In the Clips pane, select the Current Bin drop-down list, then select **Organize Bins**. The Organize Bins dialog box opens.

4. Create a bin if necessary, or otherwise select the bin for which you are setting permissions and then click **Permission**. The Permission settings dialog box opens.

   NOTE: You can not set permissions on the default bin or on the Recycle bin.



5. Add users and groups to the access control list and set permissions as follows:
   a) Click **Add**. The Select Users or Groups dialog box opens. This is the standard Windows operating system interface to users and groups, so you can use standard Windows procedures. In the "Enter the object names…" box, you can enter the users or groups for which you want to set permissions, then click **OK**.
   b) In the Permission settings dialog box, select a user or group and then set permissions as desired.
6. Click **Apply**, **OK**, and **Close** to save settings and close dialog boxes.

AppCenter operations and media access security

AppCenter uses the credential information for the current AppCenter logon and checks it against the access control list for a K2 bin. This is the access control list that you set up through the Organize Bins dialog box in AppCenter. In this way, AppCenter determines whether to allow or deny operations on media in a K2 bin.

Once permissions are granted based on the current logon account, those permissions remain in place until that account logs off of AppCenter.

FTP and media access security

The following systems host the K2 FTP interface:

- A stand-alone K2 system.

- A K2 Media Server that takes the role of FTP server

The way in which the K2 FTP interface applies media access security is explained in this section.

The K2 FTP interface uses the credential information for the current FTP session logon and checks it against the access control list for a K2 bin. This is the access control list that you set up through the Organize Bins dialog box in AppCenter. Any media access related operations such as `get`, `put`, `dir`, `rename` and `delete` are checked against the FTP session's logon credentials to access the media. For example, if an FTP session is denied access to List Bin Contents for bin A, then the session can not initiate a `dir` operation on bin A to list the contents of the bin. Furthermore, the session can not transfer clips into bin A using the `put` operation.

For the purpose of legacy support with older Profile systems, accounts for user `movie` or user `mxfmovie` are provided on the K2 system. There is also a `video_fs` account for Mac/FCP access. These accounts are automatically set up when you install K2 software version 3.2 or higher. Do not restrict access for these accounts. If your security policy requires restricting access to these accounts, contact Grass Valley Support.

On a K2 SAN, authentication takes place on the K2 Media Server. Setting up FTP security for specific local users and groups is not supported on a K2 SAN, with the exception of the local `movie` and `mxfmovie` accounts. However, you can set up FTP security for domain users and groups.

K2 SANs and media access security

This section applies to media access security, not FTP security. Refer to the preceding section for information about FTP security.

On a K2 SAN, the users and groups referenced by media access security features are the users and groups on the connected K2 clients, not the K2 Media Server. Use domain users and groups rather than local users and groups. Media access security is not supported with Workgroup network configuration on a K2 SAN.

Protocol control of channels and media access security

Protocol security restricts a channel in its access to the media in a bin, regardless of what user is currently logged on to AppCenter. This is different than the other types of media access security, in which the security restricts the user (as currently logged on to AppCenter) in their access to the media in a bin, regardless of what channel is being used.

Nevertheless, permissions for protocol channels are still derived from user accounts. In AppCenter's Configuration Manager, on the Security tab you can associate a user account with a channel of protocol control. Based on that association, when a protocol controls the channel, AppCenter checks the credential information for the associated user account against the access control list for a K2 bin. This is the access control list that you set up through the Organize Bins dialog box in AppCenter. In this way, AppCenter determines whether to allow or deny that channel's operations on the media in the bin.

By default, protocols have administrator privileges for media access. In addition, protocols are always allowed access to a channel.

Associating a protocol channel with a user account

1. Make sure you are logged on to Windows and AppCenter with administrator privileges.
2. Create user accounts and bins as necessary to support your permission policies.
3. Click **System | Configuration**. Configuration Manager opens.
4. Click a channel tab.
5. Click the **Security** tab.
6. Enter the username, the password, and (if applicable) the domain for the user account that you are associating with the channel.

   When this channel is under protocol control and it accesses media in a bin for which permissions have been set, AppCenter makes the channel's access to the media equivalent to this user's access to the media.
7. Click **OK** to save Configuration Manager settings and close Configuration Manager.
8. Restart AppCenter to put the change into effect.

About channel access security

Channel access security restricts the user (as currently logged on to AppCenter) in their use of an AppCenter channel, regardless of what bin or what media is involved. This is different than media access security, in which the security restricts the user in their access to the media in a bin, regardless of what channel is being used.

You can set up an access control list for each channel through the channel's Permissions dialog box. AppCenter uses the credential information for the current AppCenter logon and checks it against the access control list for a channel. In this way, AppCenter determines whether to allow or deny access to the channel's controls.

When you set up a channel access control list, you select the permissions for the channel as follows:

Allow — The user can operate the channel. All channel controls are enabled.

Deny — The user can not operate the channel. The controls are not displayed on the channel pane.

If neither Allow nor Deny are selected permissions are inherited from the user's parent group.

You configure these permissions to apply to users and groups. By default, all channels have their permission set to allow access to "Everyone". In case of conflicts arising from a user belonging to multiple groups, the Deny permission always overrides the Allow permission.

When you log on to AppCenter on a local K2 system, permissions for all local channels are based on the single user logged on. Therefore channel permissions are enforced for just one user at a time across all local channels. If you require that channel permissions be enforced simultaneously for different users each accessing their own channel or channels on a single K2 system, those users must log on via a remote AppCenter channel suite from a Control Point PC. The remote AppCenter channel suite allows each channel to be operated by a different user.

Once permissions are granted based on the current logon account, those permissions remain in place until that account logs off of AppCenter.

If you need to restrict access to an AppCenter channel, configure channel access security by setting up a channel access control list.

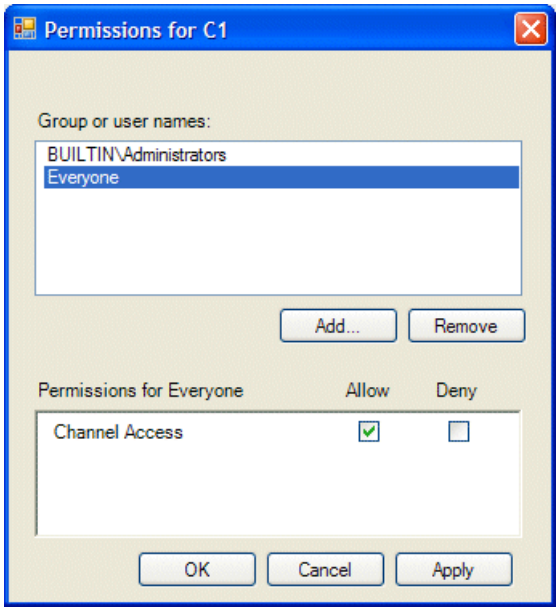
Setting up a channel access control list

1. Make sure you are logged on to Windows and AppCenter with administrator privileges.
2. Create user accounts and bins as necessary to support your permission policies.
3. Click **System | Configuration**. Configuration Manager opens.
4. Click a channel tab.
5. Click the **Security** tab.

   NOTE: Do not configure protocol user setup. This is for protocol media access security only and has nothing to do with channel access security.

6. Click **Permission**.

   The Permissions dialog box opens.



7. Add users and groups to the access control list and set permissions as follows:
   a) Click **Add**. The Select Users or Groups dialog box opens. This is the standard Windows operating system interface to users and groups, so you can use standard Windows procedures. In the "Enter the object names…" box, you can enter the users or groups for which you want to set permissions, then click **OK**.
   b) In the Permission settings dialog box, select a user or group and then set permissions as desired.

      Remember that by default, "Everyone" is set to Allow. You might need to change this in order to configure your permission policies.

   NOTE: You can not change permissions for the BUILTIN\Administrators account.

8. Click **Apply** and **OK** to save settings and close the Permissions dialog box.

9. Click **OK** to save Configuration Manager settings and close Configuration Manager.
10. Restart AppCenter to put the change into effect.

K2 and GV STRATUS security considerations

Access Control Lists (ACLs) specify individual user or group rights to specific system objects such as programs, processes, or files. K2 Summit systems enforce ACLs for security and permissions on K2 bins and channels, while the GV STRATUS system has its own mechanism for security. The GV STRATUS system always accesses the K2 Summit system via the internal system account, which by default is GVAdmin, and the K2 Summit system is configured by default to allow full access to that account. This is an important consideration to allow the systems to operate together. Therefore you must not change the default configuration of security and permissions on your K2 Summit systems that are part of your GV STRATUS system. This includes Windows operating system ACL settings and K2 AppCenter security/permission settings on bins and channels. Changing these settings could prevent the GV STRATUS system from accessing the K2 Summit system. Configure security using GV STRATUS security only. Do not configure K2 Summit security.

Understanding virus and security policies

Read the topics in this section for a better understanding of your system.

Windows operating system update policy

Grass Valley recognizes that it is essential to deploy Microsoft security patches to Windows operating system products as quickly as possible. As Grass Valley systems are used to meet the mission-critical requirements of your environment, it is imperative that these systems be kept up to date in order to maintain the highest level of security available. To that end, Grass Valley recommends that for standard-edition Windows operating system products, you install all high priority updates provided by Microsoft. In the unlikely event that one of these updates causes ill effects to a Grass Valley system, you are urged to uninstall the update and contact Grass Valley customer service as soon as possible. Grass Valley will investigate the incompatibility and, if necessary, provide a software update or work-around to allow the system to properly function with the Microsoft update in question.

Note that this policy applies to “High Priority” updates only. There are countless updates not classified as “High Priority” that are made available by Microsoft. If you believe that one or more of these other updates must be applied, contact Grass Valley prior to installation. This policy also applies to standard-edition (not embedded) operating systems only. Do not attempt to update an embedded Windows operating system in any way except as directed by Grass Valley for the specific product.

You should exercise common sense when applying updates. Specifically, do not download or install an update while a Grass Valley product is being used for mission-critical purposes such as play to air.

Embedded Security modes and policies

The Embedded Security solution protects against viruses and other unauthorized programs on the following Grass Valley systems:

- K2 Summit/Solo system

- All types/roles of K2 Media Server
- All types/roles of GV STRATUS server

Embedded Security prevents any unauthorized programs from running on the system. It contains a whitelist of programs that are authorized to run. Whenever a program attempts to run, it is checked against the whitelist. If the program is not on the whitelist, Embedded Security blocks the program from running. SiteConfig, and any software deployed by SiteConfig, is on the whitelist, so you do not need to manage Embedded Security in any way when using SiteConfig to deploy software. All versions of SiteConfig are compatible with Embedded Security.

When installing software manually (without SiteConfig) it might be necessary to manage Embedded Security. When necessary, you can put Embedded Security in Update mode. This mode allows you to manually install software that is not on the whitelist. Do not confuse Update mode with the idea that Embedded Security is "disabled". When in Update mode, Embedded Security is still active. While in Update mode, Embedded Security keeps track of any software you run or install and adds it to the whitelist. When you are done installing software and any required restarts, you must take Embedded Security out of Update mode so that it can protect the system. For software that requires a restart after installation, such as K2 system software and SNFS media file system software, Embedded Security must remain in Update mode until after the restart is complete.

No system restarts are required for entering or leaving Update mode, and a restart does not change the Update mode status. If in Update mode before a restart, the system remains in Update mode after a restart. You use the Embedded Security Manager to enter and leave Update mode.

The following policies apply to the Embedded Security:

- Use Update mode only as instructed by Grass Valley product documentation or as directed by Grass Valley Support. Do not do any other operations with Embedded Security Manager, unless under the direct supervision of Grass Valley Support.
- Do not keep Embedded Security in Update mode long-term, as Embedded Security does extra processing while in Update mode and eventually problems arise when attempting to run software.
- Make sure that Embedded Security is not in Update mode when using SiteConfig to install software. Update mode interferes with SiteConfig's automatic management of Embedded Security and causes problems running the software installed.
- Leave Embedded Security enabled for normal operation of your Grass Valley system. Do not disable Embedded Security except as instructed by Grass Valley product documentation or as directed by Grass Valley Support. Enabling and disabling Embedded Security requires a restart.
- Do not install any programs or modify any operating system settings unless approved by Grass Valley. By design, Embedded Security prevents any programs from being installed or from running that are not present when you receive the system new from Grass Valley. These Grass Valley systems are not general purpose Windows workstations. The applications and configuration have been specifically optimized on each system for its intended use as part of the Grass Valley system.
- While Embedded Security is the key anti-virus component on these systems, you should still follow the Grass Valley anti-virus scan policy and scan all the devices in your Grass Valley system to ensure viruses are not propagated between machines.

Embedded Security is part of the K2 Solo 3G system generic disk image and the K2 Media Server generic disk image compatible with K2 software version 9.0 or higher. Both K2 Media Servers and GV STRATUS servers use the same generic disk image, so GV STRATUS servers inherit the

Embedded Security solution. On K2 Solo 3G systems, the Embedded Security solution introduced with K2 software version 9.0 replaces the write filter from previous versions.

Grass Valley anti-virus scan policy

Grass Valley systems are based on the Microsoft Windows operating system. It is important to defend this system against virus or Spyware attacks. However, you must use a strategy that allows you to scan Grass Valley systems without interrupting media access. The Grass Valley Embedded Security solution on K2 and GV STRATUS systems is a qualified strategy. If you use Embedded Security on a device, do not use other anti-virus strategies on that device. Contact Grass Valley Support to determine the strategy best suited to your environment.

Network and firewall policies

The following protection policies are recommended:

- Where possible, the K2 system should be run in a closed and protected environment without network access to the corporate IS environment or the outside world.
- If the K2 system must operate in a larger network, Grass Valley recommends that access be through a gateway or firewall to provide anti-virus protection. The firewall should allow incoming HTTP (TCP port 80) connections for client and configuration connections to the K2 system inside the private network.
- Access to the K2 system should be controlled in order to limit the likelihood of malicious or unintended introduction of viruses.

About tri-level sync

The K2 Solo 3G system supports tri-level sync as a genlock reference source. The reference must be in an HD format and frame rate that is supported by the K2 Solo 3G system, as follows:

- Reference Standard: NTSC (59.97Hz)
  - 1080i 29.97
  - 720p 59.94
- Reference Standard: PAL (50Hz)
  - 1080i 25
  - 720p 50

The K2 Solo 3G system automatically detects, switches, and syncs to the reference. When you configure the reference standard for either NTSC (59.97Hz) or PAL (50Hz) in K2 AppCenter Configuration Manager, a restart is required to put the change into effect and the system starts with a SD reference format by default. It then attempts to detect a reference in a format and frame rate that is compatible with the current reference standard setting. When the K2 Solo 3G system detects a reference in a supported format, it automatically switches to that format. This allows the system to switch between SD and HD tri-level formats with frame rates that are compatible with the reference standard setting. When the K2 Solo 3G system locks to a new reference format, it saves the format and frame rate information, and upon restart it returns to the saved format and frame rate.

Do not use a progressive reference with an interlace output. For example, do not use 720p tri-level sync for interlace output formats (such as SD and 1080i). Output timing can be off by a field with this type of incompatibility.

The K2 Solo 3G system treats the following conditions as a loss of reference:

- No reference is present
- A reference in an unsupported format is present
- A reference in a supported format is present but it has a frame rate that is not compatible with the current reference standard setting.

In these cases the K2 Solo 3G system internal genlock flywheel provides a stable reference for the last reference set. The system reports this status in K2 AppCenter Configuration Manager Reference Standard by a black "Reference present" indicator.

Auto log on

If you set a K2 Media Client, a K2 Summit Production Client or a K2 Solo Media Server to automatically log on to the Windows operating system at startup, AppCenter honors this setting. This means that at startup AppCenter bypasses its log in dialog box and opens automatically. For more information about how to turn on automatic login in the Windows operating system, including security risks and procedures, refer to the related Microsoft knowledge base article.

Regional and language settings

On all K2 Summit Production Clients, K2 Media Clients, K2 Solo Media Servers and K2 Media Servers, in the Windows Control Panel “Region and Language”, there are special FTP internationalization requirements regarding the language for non-Unicode programs to support FTP transfers. Do not change these settings.

Checking RAM

You can determine the amount of Random Access Memory (RAM) on your K2 Solo 3G system's CPU module.

1. Connect the the K2 Solo 3G system's USB Recovery Flash Drive to the K2 Solo 3G system.
2. On the USB Recovery Flash Drive, locate and double-click the following:

   `CPUList.exe`

   A System Inventory window opens and displays information about the manufacturer, model, and amount of RAM on the CPU module.
3. Press **Enter** to close the System Inventory window.

Direct Connect Storage

About the direct-connect Fibre Channel card

The direct-connect K2 Summit Production Client or K2 Media Client has a direct Fibre Channel connection to external K2 RAID. The K2 client must have the optional Fibre Channel card installed to support this connection. This gives the K2 client the large storage capacity of the external RAID, yet its media related functionality is that of a “stand-alone” K2 client, similar to a K2 client with internal storage.

A K2 Summit Production Client's optional Fiber Channel card is a 8 Gb/s ATTO Fibre Channel card.

Setting up direct-connect K2 G10v2 RAID storage

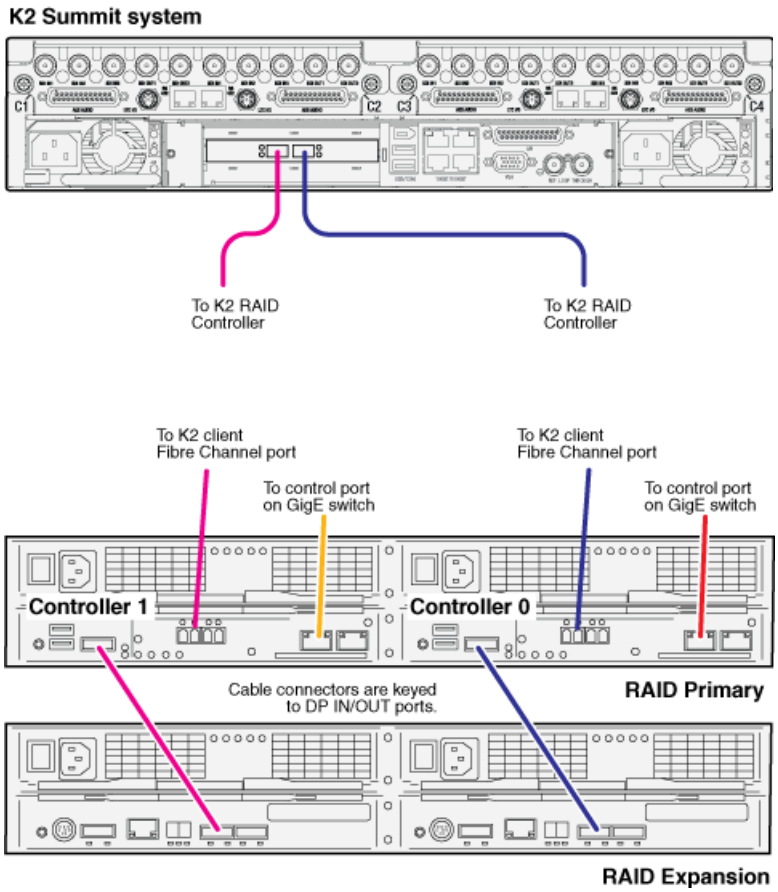
- For a 8 Gb/s Fibre Channel card on K2 Summit Production Client, RAID controllers must be configured for 8 Gb/s. This is the default configuration as shipped from Grass Valley.

The topic applies to K2 G10v2 (M100) RAID storage with direct connection to a K2 Solo 3G system system.

The following procedure is intending for the initial installation of a factory-prepared direct-connect system that you have ordered new from Grass Valley. If you are repurposing equipment or otherwise putting together direct-connect storage with equipment that is not factory-prepared, refer to the Service Manual for your model of K2 client for the complete restore/recover procedure.

As you work through the following procedure, refer as necessary to the *K2 SAN Installation and Service Manual* "Installing" chapters for information about cabling and configuring K2 RAID.

1. Connect the K2 Solo 3G system and RAID devices as shown in the following illustrations.



   Connect K2 Solo 3G system Fibre Channel ports to RAID controllers. Connect Fibre Channel port 1 to RAID controller 0. If you have the redundant controller, connect Fibre Channel port 2 to RAID controller 1.

   Connect RAID controller Management ports to control ports on a K2 GigE switch. If you have redundant switches, connect controller 0 to switch A and controller 1 to switch B.

   NOTE: The control network connection is required to support basic functionality such as gathering logs and loading controller microcode, as well as SNMP monitoring.

   Connect RAID controller Disk Port to the Expansion chassis Disk Port In 1 ports.

2. Connect power cables and power up the RAID devices. Refer to "Powering on K2 RAID" later in this chapter.
3. Connect remaining cables to the K2 Solo 3G system. Refer to the Quick Start Guide for the particular K2 Solo 3G system model for cabling details.
4. Start up the K2 Solo 3G system.

   The Windows initialization screen shows the progress bar but does not complete.

5. Power down the K2 Solo 3G system.

6. Disconnect all Fibre Channel cables from the K2 Solo 3G system.
7. Start up the K2 Solo 3G system and log in to Windows.
8. Uninstall Multi-Path I/O (MPIO) software as instructed by the topic later in this section.
9. Log in to Windows.
10. Power down the K2 Solo 3G system.
11. Reconnect one Fiber Channel cable.
12. Start up the K2 Solo 3G system and log on to Windows.
13. On the K2 Solo 3G system, open Storage Utility.
14. In Storage Utility, do the following:
    a) Configure network and SNMP settings for controllers.

       Refer to related topics about Grass Valley recommended deployment and monitoring solutions in the "About This Release" section of the K2 Topic Library.
    b) Bind the disks in the external RAID. Bind as RAID 5 or RAID 6, as specified by your system design.
    c) When the binding process completes, proceed to the next step.
15. Restart the K2 Solo 3G system and log in to Windows.
16. Reconnect the other Fiber Channel cable.
17. Install MPIO software as instructed by the topic later in this section.
18. In Storage Utility, make a new file system

    If you get a "…failed to remove the media database…" message, you can safely proceed.
19. Restart the K2 Solo 3G system and log in to Windows.
20. Open AppCenter and manually remove all clips and bins except the default bin and the recycle bin.
21. Uninstall and then reinstall both SNFS software and K2 Client software. Use the sequence and detailed procedure in the *K2 Release Notes* for the version of K2 Client software currently on the K2 Solo 3G system.
22. As you install K2 Client software, when you arrive at the Specify Target Type page, select **K2 with local storage**.
23. Restart the K2 Solo 3G system.

The K2 Solo 3G system is now ready for record/play operations.

NOTE: If you ever unbind LUNs, you must do the above procedure again, starting at step 5.

Setting up direct-connect K2 G10 RAID storage

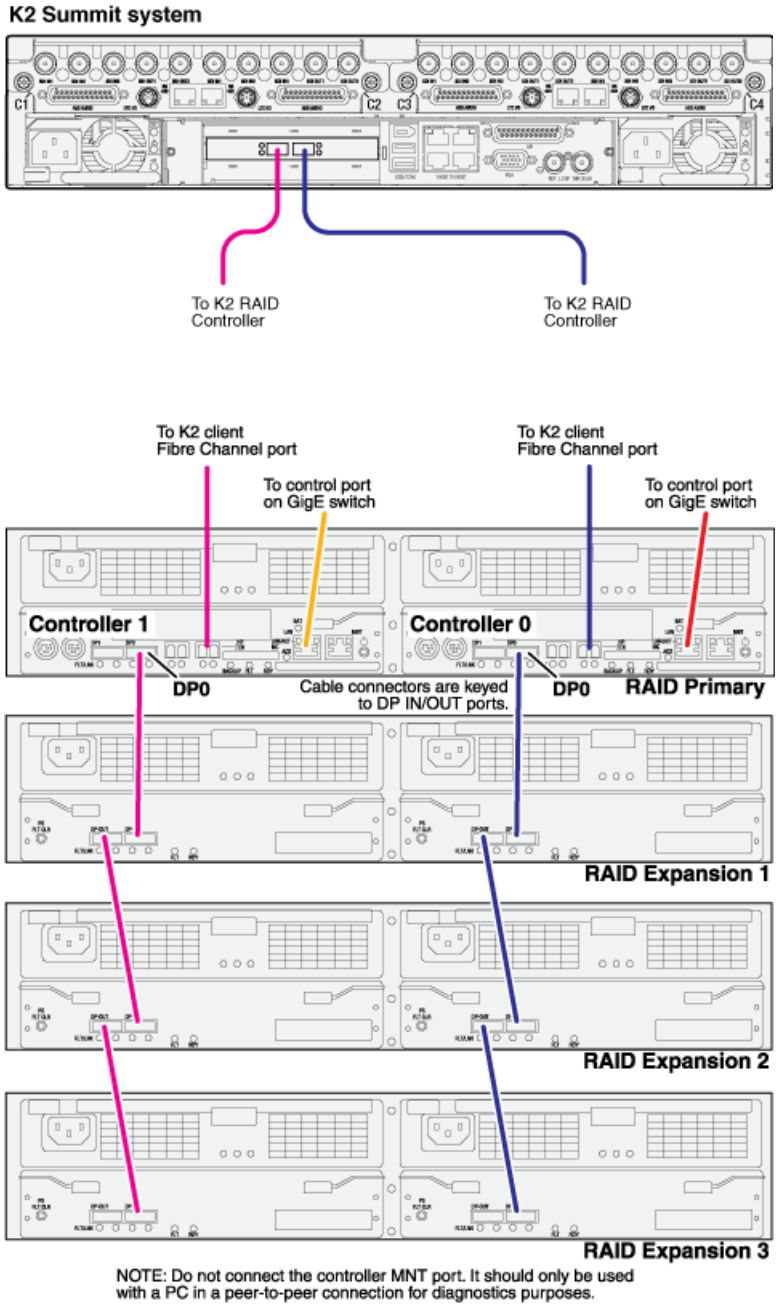
- For a 8 Gb/s Fibre Channel card on K2 Summit Production Client, RAID controllers must be configured for 8 Gb/s. This is the default configuration as shipped from Grass Valley.

The topic applies to K2 G10 (D4) RAID storage with direct connection to a K2 Solo 3G system system.

The following procedure is intending for the initial installation of a factory-prepared direct-connect system that you have ordered new from Grass Valley. If you are repurposing equipment or otherwise putting together direct-connect storage with equipment that is not factory-prepared, refer to the Service Manual for your model of K2 client for the complete restore/recover procedure.

As you work through the following procedure, refer as necessary to the *K2 SAN Installation and Service Manual* “Installing” chapters for information about cabling and configuring K2 RAID.

1. Connect the K2 client and RAID devices as shown in the following illustrations.



Connect K2 client Fibre Channel ports to RAID controllers. Connect Fibre Channel port 1 to RAID controller 0. If you have the redundant controller, connect Fibre Channel port 2 to RAID controller 1.

Connect RAID controller LAN ports to control ports on a K2 GigE switch. If you have redundant switches, connect controller 0 to switch A and controller 1 to switch B.

Connect RAID controller DP0 ports to the first Expansion chassis DP-IN ports.

Connect remaining Expansion chassis using DP-OUT and DP-IN ports.

2. Connect power cables and power up the RAID devices. Refer to "Powering on K2 RAID" later in this chapter.
3. Connect remaining cables to the K2 client. Refer to the Quick Start Guide for the particular K2 client model for cabling details.
4. Start up the K2 client.

   The Windows initialization screen shows the progress bar but does not complete.
5. Power down the K2 client.
6. Disconnect all Fibre Channel cables from the K2 client.
7. Start up the K2 client and log in to Windows.
8. Uninstall Multi-Path I/O (MPIO) software as instructed by the topic later in this section.
9. Log in to Windows.
10. Power down the K2 client.
11. Reconnect Fiber Channel cables.
12. Start up the K2 client and log on to Windows.
13. On the K2 client, open Storage Utility.
14. In Storage Utility, do the following:
    a) Configure network and SNMP settings for controllers.

       Refer to related topics about Grass Valley recommended deployment and monitoring solutions in the "About This Release" section of the K2 Topic Library.
    b) Bind the disks in the external RAID. Bind as RAID 5 or RAID 6, as specified by your system design.
    c) When the binding process completes, proceed to the next step.
15. Restart the K2 client and log in to Windows.
16. Install MPIO software as instructed by the topic later in this section.
17. In Storage Utility, make a new file system

    If you get a "…failed to remove the media database…" message, you can safely proceed.
18. Restart the K2 client and log in to Windows.
19. Open AppCenter and manually remove all clips and bins except the default bin and the recycle bin.
20. Uninstall and then reinstall both SNFS software and K2 Client software. Use the sequence and detailed procedure in the *K2 Release Notes* for the version of K2 Client software currently on the K2 client.
21. As you install K2 Client software, when you arrive at the Specify Target Type page, select **K2 with local storage**.
22. Restart the K2 client.

The K2 client is now ready for record/play operations.

NOTE: If you ever unbind LUNs, you must do the above procedure again, starting at step 5.

Uninstalling Multi-Path I/O Software on a direct-connect K2 system

The following procedure applies to direct-connect K2 systems.

The files for the Multi-Path I/O software are copied on to the K2 system when the K2 software is installed.

1. Access the Windows desktop on the K2 system.

   You can do this locally with a connected keyboard, mouse, and monitor or remotely via the Windows Remote Desktop Connection.

2. Stop all media access. If AppCenter is open, close it.
3. Click **Start | Run**, type `cmd` and press **Enter**.

   The MS-DOS command prompt window opens.

4. From the command prompt, navigate to the *`C:\profile\mpio`* directory.
5. Type one of the following at the command prompt:

   - If uninstalling on a 32-bit system:

     ```
     gdsminstall.exe -u c:\profile\mpio gdsm.inf Root\GDSM
     ```

   - If uninstalling on a 64-bit system:

     ```
     gdsminstall64.exe -u
     ```

6. Press **Enter**.

   The software is uninstalled. The command prompt window reports progress.

7. Restart the K2 system.

Installing Multi-Path I/O Software on a direct-connect K2 system

Before doing this task, if a K2 Solo 3G system with K2 software version lower than 9.0, make sure the write filter is disabled.

The following procedure is required for direct-connect K2 systems.

The files for the Multi-Path I/O software are copied on to the K2 system when the K2 software is installed.

1. Access the Windows desktop on the computer on which you are installing MPIO.

   You can do this locally with a connected keyboard, mouse, and monitor or remotely via the Windows Remote Desktop Connection.

2. Stop all media access. If AppCenter is open, close it.
3. Click **Start | Run**, type `cmd` and press **Enter**.

   The MS-DOS command prompt window opens.

4. From the command prompt, navigate to the *`C:\profile\mpio`* directory.
5. Type one of the following at the command prompt:

   - If installing on a 32-bit computer:

     ```
     gdsminstall.exe -i c:\profile\mpio gdsm.inf Root\GDSM
     ```

   - If installing on a 64-bit computer:

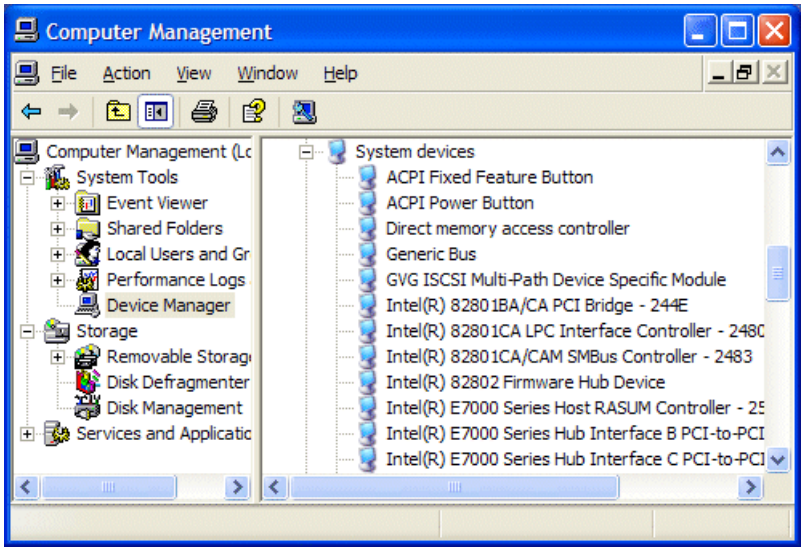
     ```
     gdsminstall64.exe -i
     ```

6. Press **Enter**.

   The software is installed. The command prompt window reports progress.

7. Restart the computer on which you installed MPIO.
8. After restart, to verify that the software is installed, on the Windows desktop right-click **My Computer** and select **Manage**.

   The Computer Management window opens.



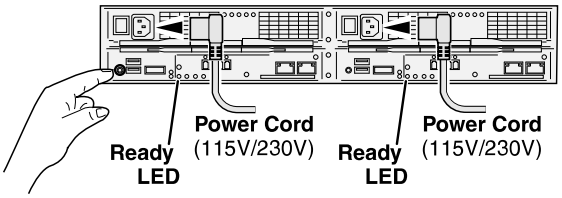
9. In the left pane select **Device Manager**.
10. In the right pane open the **System devices** node and verify that **GVG ISCSI Multi-Path Device Specific Module** is listed.

Powering on K2 G10v2 RAID

This topic applies to K2 G10v2 (M100) RAID.

1. Verify power and cabling.
2. Tap the power button on the controller, as shown.

   NOTE: Do not press and hold down the power button.



   If the RAID chassis has two controllers, you can tap the power button on either controller. You do not need to tap both power buttons.

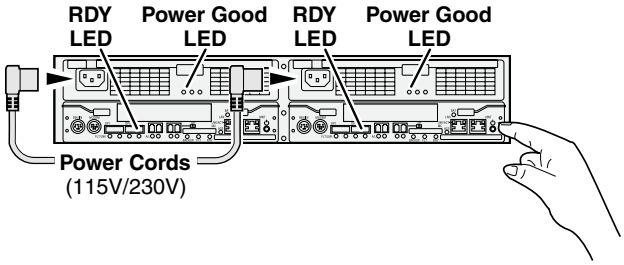
   Tapping the power button on a controller also powers on any connected Expansion chassis. There are no power buttons on Expansion chassis.

3. Wait while the primary RAID chassis performs self-test and initialization. This takes 6-8 minutes. While this is taking place, the Ready LED is illuminated with a steady on light.
4. Watch for the Ready LED to begin blinking at one second intervals. The LED might turn off and back on two times before starting the one second blink pattern. When the Ready LED is blinking at one second intervals, the self-test and initialization is complete and the chassis is ready for use.

Powering on K2 G10 RAID

This topic applies to K2 G10 (Condor) RAID.

1. Verify power and cabling.
2. Press and hold down the power button on the controller, as shown.



   If the RAID chassis has two controllers, you can press the power button on either controller. You do not need to press both power buttons.

   Pressing the power button on a controller also powers on any connected Expansion chassis. There are no power buttons on Expansion chassis.

3. Release the power button when the Power Good LED on the power supply is illuminated. This takes 1-3 seconds.
4. Wait while the primary RAID chassis performs self-test and initialization. This takes about four minutes. While this is taking place, the RDY LED is illuminated with a steady on light.
5. Watch for the RDY LED to begin blinking at one second intervals. The LED might turn off and back on two times before starting the one second blink pattern. When the RDY LED is blinking at one second intervals, the self-test and initialization is complete and the chassis is ready for use.

K2 Summit Transmission models

K2 Summit 3G Transmission models features

This chapter contains information that is unique to K2 Summit 3G Transmission Client models. Refer to other chapters for information that applies to all K2 Summit systems.

K2 Summit 3G Transmission Client models are optimized for playout, rather than record. Input/output configurations support the needs of playout applications. Higher efficiency MPEG-2 encoding

reduces bandwidth and increases storage capacity. The result is that the K2 Summit 3G Transmission Client models are restricted to a subset of K2 Summit system bit rates, formats, and other features.

The following feature lists contain features that are unique to K2 Summit 3G Transmission Client models. Features common to all K2 Summit models, both K2 Summit Production Client models and K2 Summit 3G Transmission Client models, are not listed here.

Features that all K2 Summit 3G Transmission Client models share are as follows:

- Records video with 16 channels of audio at 24bits/sample.
- Supports the following formats:
  - 720p/1080i – MPEG-2, XDCAM-HD, XDCAM-EX, XDCAM-HD422, AVC-Intra 50, AVC-Intra 100, DVCPROHD (DV100)
  - SD – MPEG-2, D10 (30,40,50), DVCAM, DVCPRO25/50
- Supports MPEG-2 formats at 100Mbps or less and other formats at 50Mbps or less.
- Supports FTP bandwidth up to 30 MB/second.

K2-XDT2-02 has the following features:

- One bi-directional and one playout only HD/SD channels.
- Channels are configurable as 1 x 1 or 0 x 2.
- Shared storage via iSCSI connection on a K2 SAN or can be configured with internal storage.

K2-KDT2-04 has the following features:

- Two bi-directional and two playout only HD/SD channels.
- Channels are configurable as 1 x 3, 2 x 2 or 0 x 4.
- Shared storage via iSCSI connection on a K2 SAN or can be configured with internal storage.

K2-XDT2-08-2TR1 has the following features:

- Two bi-directional and two playout only HD/SD channels.
- Channels are configurable as 1 x 3, 2 x 2 or 0 x 4.
- Internal storage with eight SAS media drives configured as RAID 1.

K2-XDP-2HDL has the following feature:

- Enables HD on a K2 Summit 3G codec board.

K2-XDP2-AVC-2CH has the following features:

- Enables AVC-Intra on a K2 Summit 3G codec board.
- Enables H.264 decoding on a K2 Summit 3G codec board.

K2-XDP2-DVHD-2CH has the following feature:

- Enables DVCPROHD encoding on a K2 Summit 3G codec board.

K2-XD1-BCH has the following feature:

- Enables bidirectional capability on an additional K2 Summit3G channel.

K2-XDT1-ME-2CH has the following feature:

- Enables the addition of mix effects on 2 channels for K2 Summit 3G Transmission Server.

K2 Summit 3G Transmission models channel configurations

The details of the channel configurations available on K2 Summit 3G Transmission Client models are as follows:

1 x 3 channels

Channel	Record	Play
1	X	X
2		X
3		X
4		X

2 x 2 channels

Channel	Record	Play
1	X	X
2		X
3	X	X
4		X

0 x 4 channels

Channel	Record	Play
1		X
2		X
3		X
4		X

1 x 1 channels

Channel	Record	Play
1	X	X
2		X

0 x 2 channels

Channel	Record	Play
1		X
2		X

K2 Summit 3G Transmission models requirements and restrictions

- Transition effects not supported
- AppCenter Elite not supported.
- ChannelFlex Suite inputs and outputs are not supported.
- Mobile environment not supported. The standard K2 Summit system random vibration specifications do not apply to the K2 Summit 3G Transmission Server models. Instead, random vibration specifications for K2 Summit 3G Transmission Server (internal storage) models are as follows:

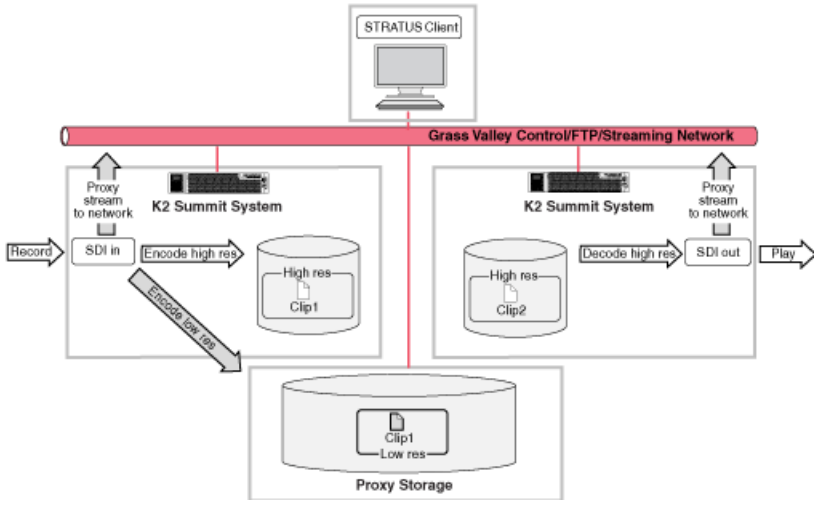
Characteristic	Specification
Random Vibration Operational	0.27 GRMS (5-500Hz)
Random Vibration Non-Operational	2.13 GRMS overall .015 g2/Hz (5-100Hz) .0075 g2/Hz (200-350Hz) .005256 g2/Hz (500 Hz)

Storage Utility procedures for K2 Summit 3G Transmission Server models

Storage Utility detects drive type/capacity and allows only those operations that are correct for the drive type/capacity. If you need to bind the internal drives, RAID 1 is recommended. This is the default configuration as received from the Grass Valley factory. However, Storage Utility allows you to bind as RAID 0 if you so choose.

Proxy/live streaming

Proxy and live streaming workflow overview



When licensed and configured, a K2 Summit system creates low-resolution representations of high-resolution media. Similar to PB/EE functionality, the K2 Summit System creates a live stream of low-resolution media at the SDI input and a live stream of low-resolution media at the SDI output, whether or not record/play operations are underway. These streams are multicast to the network and are available to applications on the network. When media is recorded, the K2 Summit system encodes a high resolution clip and a low resolution proxy clip. The system keeps these clips associated so any changes take effect simultaneously for both clips.

The GV STRATUS application accesses the low-resolution media over the network. When you monitor the K2 Summit system SDI inputs and outputs, the application displays the live stream. When you view an asset, the application displays the proxy representation of the asset. When you edit an asset, the K2 Summit system makes your changes on both the proxy and the high resolution asset.

About proxy/live streaming

The K2 Summit system writes proxy files to a CIFS share, using credentials for the internal system account, which by default is GVAdmin. A proxy file contains the video track, up to eight audio tracks, and timecode. The file is a fragmented MPEG-4 file, which can record/play in chunks. This allows you to play a growing proxy file while it is still recording.

Each K2 Summit system channel multicasts a low-resolution live stream. The K2 Summit system has an HTTP server over which it makes the SDP file available to applications that play the live stream.

A Type II, Type III, or Type IV CPU module is required to support proxy/live streaming.

An AppCenter Pro or AppCenter Elite license on the K2 Summit system enables proxy/live streaming. If licensed for AppCenter Pro, a live stream is available from each of the four channels. If licensed for AppCenter Elite, ChannelFlex features allow you to configure up to eight inputs/outputs, so up to eight live streams are similarly available. When a K2 Summit system is licensed, in Configuration Manager (a part of the K2 AppCenter application) you can configure proxy/live streaming for each channel. You can turn proxy file recording on or off, and you can turn live network streaming on or off. When you turn proxy file recording on, you can then select up to eight audio tracks to include in the proxy file. You can also turn automatic scene detection on or off. When you turn scene detection on, you can configure the minimum scene length. When you turn proxy live network streaming on, you can then select two audio tracks (one pair) to include in the proxy stream.

If licensed for AppCenter Elite, a ChannelFlex channel generates proxy/live streaming as follows:

- Multi-cam Recorder — Both high-resolution assets have their own proxy file. Two live streams are also available. If shared audio, the proxy file and live stream are generated as follows: the first input includes video, audio, and timecode; the second input includes video but does not include audio and timecode.
- 3D / Video + Key — Two live streams are available as follows: the first input/output includes video, audio, and timecode; the second input/output includes video but does not include audio and timecode. Proxy files are not created.
- Super Slo-Mo Recorder — A video-only proxy file and a video-only live stream are generated that are normal speed, which means that they are one half or one third the Super Slo-Mo record rate.

Proxy recording is not supported for continuous record mode.

Network switches and firewalls must be configured to allow the multicast live streaming traffic. IGMP Snooping must be enabled on the network that carries the low-resolution live streaming traffic.

The GV STRATUS product accesses proxy files through a shared CIFS folder. There is a limit to the number of proxy access connections on the server that hosts the share. Therefore full proxy recording is only supported using one of the recommended GV STRATUS configurations with a proxy server. Recording and storing proxy on the local media storage on a K2 Summit/Solo system is not recommended.

Proxy/live streaming formats

The proxy files and streams created by a K2 Solo 3G system conform to industry standards, as follows.

Video: MPEG-4 Part 2

Format	Frame Rate	Data Rate (Mbps)	Other
320x240p	29.97, 25	1.5 Mbps	GOP 1 second
384x288p	29.97, 25	1.5 Mbps	GOP 1 second
512x288p	29.97, 25	1.5 Mbps	GOP 1 second

Audio: MPEG-4 Part 3 AAC-LC, 64 kbps, 48 kHz

Proxy file: MPEG-4 Part 12 Fragmented MP4 Movie

Live streaming: SDP files and RTP/RTCP streams are compliant with the following RFCs:

- RFC 3350, RFC 4566, RFC 3016, RFC 3640, RFC 5484, MPEG-4 Part 8

Configuring proxy and live streaming settings

On the K2 Solo 3G system, configure proxy and live streaming settings as in the following sections. For complete information about proxy and live streaming, refer to related topics in the "Configuring the K2 System" section of this Topic Library.

Enable proxy files

1. In AppCenter, click **File | System | Configuration**.
   Configuration Manager opens.
2. In Configuration Manager, click the **Channel** tab.
3. Select a channel.
4. In Proxy Setup settings, set **Record proxy files** to **Yes**.
5. Select the audio included in the proxy file as follows:
   - Select the first audio input pair to include in the proxy file.
   - Select the number of audio inputs to include in the proxy file.

   The K2 Summit system includes audio pairs beginning with the first pair selected and then each subsequent audio pair up to the selected number of audio inputs.
6. If you want to the K2 Summit system to automatically detect scene changes and include them in the proxy file, do the following:
   - Set **Detect scenes** to **Yes**.
   - Select a minimum scene length. This is the length of time the K2 Solo 3G system waits after detecting a scene change to begin attempting to detect the next scene change.
7. Select another channel and configure as desired.
8. Click **OK** to apply the settings.

Enable live streaming

1. In AppCenter, click **File | System | Configuration**.
   Configuration Manager opens.
2. In Configuration Manager, click the **Channel** tab.
3. Select a channel.
4. In Proxy Setup settings, set **Live network streaming** to **Yes**.
5. Select the audio input pair to include in the proxy stream.
6. Select another channel and configure as desired.
7. Click **OK** to apply the settings.

Configure live streaming multicast

This task describes using AppCenter to configure multicast settings.

1. In AppCenter, click **File | System | Configuration**.
   Configuration Manager opens.
2. In Configuration Manager, click the **System** tab.
   These setting apply to all channels on the K2 Summit system.
3. In Proxy Setup settings, select the multicast IP base.
   The K2 Summit system applies channel-specific IP addresses from this base.
   Your choices are constrained to those specified by IANA for multicast.
4. Select the multicast port base.
   This is the first UDP port address for elementary streams.
5. Click **OK** to apply the settings.

Test proxy media generation

This test is valid for standalone K2 Summit systems. You can check the proxy media that the K2 Summit system generates. This can be helpful in troubleshooting situations where you need to verify that the proxy is available to other applications, such as the GV STRATUS application.

Use this procedure for test purposes only. Accessing proxy media as explained in this procedure is not supported for operational use.

1. Verify that in K2 AppCenter Configuration Manager, a K2 Summit system channel is enabled for live network streaming and for recording proxy files.
2. Verify that there is video available at the channel's SDI input.
3. Verify proxy live network streaming as follows:
   a) On the K2 Summit system, navigate to `V:\live streaming`.
   b) Identify the file that corresponds to the channel enabled for live network streaming.
      The file name is *`hostname_Cx.sdp`*, where *`x`* is the channel number.
   c) Double-click the file that corresponds to the channel enabled for live network streaming.
      QuickTime Player opens.
   d) View and verify the proxy video stream.

4. Verify recording proxy files as follows:
   a) Navigate to the proxy location.

      On a K2 Summit system that has not been configured to write proxy elsewhere, the location is *V:\proxy*. If configured by applications such as GV STRATUS to write proxy elsewhere, navigate to the configured location.

   b) While viewing the proxy location, start recording a new clip on the K2 Summit channel enabled for recording proxy files.

      The K2 Summit system creates a new folder at the proxy location. The folder is named with a long GUID.

   c) Stop the recording on the K2 Summit channel.
   d) In the new folder, double-click the *proxy.mp4* file.

      QuickTime Player opens.

   e) View and verify the proxy file.

Proxy/live streaming technical details

The K2 Summit system writes proxy files to the proxy location specified in the GV STRATUS Control Panel application. On the specified device the location is *V:\proxy*. For each clip recorded, the K2 system creates a directory and names it with the asset GUID, which is a long, unique string of characters. These directory names do not correspond to clip names or other human readable information. The directory contains the proxy files, which include the proxy video and audio files, as well as thumbnails files and a scene change file. The proxy video file is a fragmented MPEG-4 file. For test purposes, you can open the proxy file in a video player application that supports fragmented MPEG-4.

The K2 Summit system multicasts the low-resolution live stream using Real-time Transport Protocol, with UDP ports for the MPEG video with timecode and UDP ports for audio tracks, as defined by the Session Description Protocol (SDP). For each channel, the K2 system generates a **.sdp* file that contains the streaming media initialization parameters. The K2 system updates the file whenever you change the live streaming configuration. You can find these files on the K2 system at *V:\live streaming*. For test purposes, you can open a file in a text editor and read the IP addresses and ports assigned to the multicast session and other configuration information for the stream.

The K2 Summit system generates for each of its channels the specific live streaming network ports and IP addresses based on a port base and an IP address base. The port base is the first UDP port address for elementary streams. The IP address base is the first two octets in the IP address, as specified by the Internet Assigned Numbers Authority (IANA). By default, the port base is 31820 and the IP address base is 239.192.0.0. With these default bases, the range of network ports is UDP 31820 to 31827 , and the range of IP addresses is 239.192.x.x to 239.195.x.x. Grass Valley recommends that you use these default settings. However, if necessary for your site's network policies, you can also change the K2 system's default settings. You can configure the port base and the IP address base. Only IP addresses specified by IANA for multicast are allowed. Do not attempt to edit the **.sdp* files, as the K2 system generates them automatically whenever the system is restarted. If you change the IP address of the K2 system, you must restart in order to update the IP address in the **.sdp* file.

The K2 Summit system hosts a simple web server over which it delivers the live stream via HTTP. For test purposes, you can access the live stream by entering a URL of the following convention in a standard web browser:

`http://<httpservername>/live/<k2systemname>_<Cn>.sdp`

For example, to view the live stream from channel four on a K2 system named Summit01, the URL is `http://Summit01/live/Summit01_C4.sdp`. The http server name is the same as the name of the K2 system.

Remote control protocols

About remote control protocols

This section provides information for using remote control protocols to operate K2 Solo 3G systems. It is intended for use by installers, system integrators, and other persons responsible for setting up automation systems at a customer site.

For information about configuring AppCenter to enable protocol control of a K2 channel, refer to topics in the "Using K2 AppCenter" section of the K2 Topic Library.

Using AMP protocol to control K2 systems

Advanced Media Protocol (AMP) is an extension of the Odetics protocol.

AMP commands are available via Ethernet or RS-422 serial ports.

The automation setting for preroll should be at least 10 frames.

Preroll is 1 second for mixed compression format playout. Preroll is 10 frames for same compression format playout.

The AMP's socket interface uses IANA assigned port number 3811 for TCP.

In AppCenter, you must set a channel's options to enable protocol control of the channel. Subsequently, when the K2 Solo 3G system starts up, the channel is immediately available for protocol control. Manual log on is not required.

For channels in gang mode, the protocol must connect to the lowest numbered channel in the gang. This is required to support jog/shuttle of ganged channels.

AMP Two-Head Player Model

The AMP protocol supports the use of a *two-head player model* in that two clips can be loaded for playout, as follows:

- Current clip — The AMP "preset id" is the active clip.
- Preview clip — The AMP "preview preset id" is the preview clip. The preview clip becomes the current clip and begins playing when the current clip completes. When controlling AMP in Auto mode, the "in preset" (and "out preset") command should be sent before the Preview in commands.

Related specifications are as follows:

- A 3D/Video+Key player channel does not support a two-head player model.

Controlling transfers with AMP

Remote control automation applications can initiate transfers via AMP. The AMP command must be sent to the K2 Solo 3G system, not the K2 Media Server. This applies to both stand-alone and shared storage K2 systems.

If using AMP to initiate transfers between K2 systems and Profile XP systems, you must send the AMP command to the K2 system, not the Profile XP system. Transfers (both push and pull) are successful if the K2 system hosts the command. Transfers fail if the Profile XP system hosts the command.

Transfers initiated by AMP between K2 systems and M-Series iVDRs are not supported.

AMP channel designations

When using AMP protocol with Ethernet and the K2 Solo 3G system, the first port maps to the first channel, the second port maps to the second channel, and so on.

AMP internationalization

AMP supports UTF-8 2 and 3 byte characters. Unicode movie names pass through as opaque bits.

Using VDCP protocol to control K2 systems

Video Disk Control Protocol (VDCP) commands are available via RS-422 serial ports.

Preroll is 1 second for mixed compression format playout. Preroll is 10 frames for same compression format playout.

The K2 AppCenter Recorder application in protocol mode allows a default bin to be assigned to each record channel.

In AppCenter, you must set a channel's options to enable protocol control of the channel. Subsequently, when the K2 Solo 3G system starts up, the channel is immediately available for protocol control. Manual log on is not required.

For channels in gang mode, the protocol must connect to the lowest numbered channel in the gang. This is required to support jog/shuttle of ganged channels.

Loop-play mode on the K2 Solo 3G system is not supported under VDCP control.

The following categories of VDCP commands are not supported:

- Deferred (Timeline) Commands --these are the basic timeline commands but use the time specified by the PRESET STANDARD TIME
- Macro commands
- Archive Commands

- To control a given K2 channel, use only that channel's specific RS-422 rear panel connector. Send the VDCP "Open Port" and "Select Port" commands only to the RS-422 connector that is associated with the channel being controlled.

VDCP two-head player model

The VDCP protocol supports the use of a *two-head player model* in that two clips may be loaded for playout, as follows:

- Current clip — The VDCP "preset id" is the current clip.
- Preview clip — The VDCP "preview preset id" is considered the preview clip. When a play command is received, the preview clip becomes the active clip and begins playing after the preroll time has passed. If a play command has not been issued by the end of the clip, playout stops according to the VDCP end mode settings for that channel (last frame, black, first frame of preview clip).

Related specifications are as follows:

- A 3D/Video+Key player channel does not support a two-head player model.

Controlling transfers with VDCP

Remote control automation applications can initiate transfers via VDCP. The VDCP command must be sent to the K2 Solo 3G system, not the K2 Media Server. This applies to both stand-alone and shared storage K2 Solo 3G system.

If you are using VDCP to perform video network transfers, you must configure the K2 Solo 3G system so that there is a unique Controller ID for each host.

If using VDCP to initiate transfers between K2 systems and Profile XP systems, you must send the VDCP command to the K2 system, not the Profile XP system. Transfers (both push and pull) are successful if the K2 system hosts the command. Transfers fail if the Profile XP system hosts the command.

Transfers initiated by VDCP between K2 systems and M-Series iVDRs are not supported.

VDCP internationalization

VDCP does not support UTF-8 or Unicode, so use ASCII only for clip names and bin names.

PitchBlue workflow considerations

The K2 Solo 3G system supports the H.264 format used in the PitchBlue workflow. However, you must consider the intended PitchBlue workflow when using this H.264 media, as it is not supported for general purpose use outside of the PitchBlue workflow.

The K2 Solo 3G system ingests the PitchBlue material without any error correction. The material often has anomalies, such as incomplete last frame, that the K2 Solo 3G system accepts as-is. When PitchBlue plays out this material under VDCP automation control, it plays the known-good material only. The automation playout system tracks the portions of the imported PitchBlue content for playout by interacting with the traffic and other related playout automation components. Anomalies

can be identified so that they are not played out. In this way, the automation playout system avoids the errors that would otherwise occur if the material were used for general purpose playout without automation control.

Therefore, you must adhere to the complete PitchBlue workflow from ingest through playout for all PitchBlue material. Do not attempt to play out PitchBlue material except as part of the prescribed PitchBlue workflow.

NOTE: Playing out PitchBlue material in any other way can cause errors.

Using BVW protocol to control K2 systems

BVW commands are available via RS-422 serial ports.

A subset of BVW commands is supported through AppCenter in protocol mode.

Insert/Edit is not supported.

In AppCenter, you must set a channel's options to enable protocol control of the channel. Subsequently, when the K2 Solo 3G system starts up, the channel is immediately available for protocol control. Manual log on is not required.

For channels in gang mode, the protocol must connect to the lowest numbered channel in the gang. This is required to support jog/shuttle of ganged channels.

To set in and out points with BVW protocol, load clips only from the working bin.

Special considerations for automation vendors

The following information is provided for your convenience as you set up your chosen automation product to control K2 systems. Consult your automation vendor for complete information.

Harris settings

The Harris automation product uses VDCP protocol.

The following settings are required for the Harris automation product:

Setting	Mixed compression format playout	Same compression format playout	Comments
Disk Prerolls	1 second	10 frames	—
Frames to send Play early (Preroll Play)	1 second	10 frames	These two settings should be the same as the Disk Prerolls setting. However, if there is extra fixed latency in your RS-422 communication path, you might need to adjust the settings differently.
Frames to send Record early (Preroll Record)	1 second	10 frames	
Disk Port Comm Timeout	60 frames	60 frames	This is the minimum required by K2. Do not use the Harris default value, which is 10.

Setting	Mixed compression format playout	Same compression format playout	Comments
Back To Back Rec	Unchecked	Unchecked	K2 does not support this feature.

RS-422 protocol control connections

You can control the K2 Solo 3G system with remote control devices and software developed for the K2 system that use industry-standard serial protocols: AMP, BVW, and VDCP. (AMP protocols can also use Ethernet connections.) You can connect one RS-422 cable to each channel. Each RS-422 connection controls the channel to which it is connected only. Connect the RS-422 cabling as required, then refer to topics in the "Using K2 AppCenter" section of the K2 Topic Library to configure the K2 system for remote control.

Specifications for the RS-422 connection are as follows:

- Data Terminal Equipment (DTE)
- 38.4K Baud
- 1 Start bit
- 8 Data bits
- 1 Parity bit
- 1 Stop bit

Security and protocol control

The K2 security features can be configured to restrict protocol control of channels.

Specifications

K2 Summit Transmission models specifications

Refer to the section about K2 Summit Transmission models for specifications unique to that system. If a specification is not unique to a K2 Summit Transmission model, then the general K2 Solo 3G system specification found in this section applies.

AC power specification

Table 13: K2 Summit 3G AC power specification

Characteristic	Specification
Power supply	Dual, redundant
Mains Input Voltage	90 to 260V auto-range, 47-63Hz

Characteristic	Specification
Power consumption	450W typical (standalone) 390W typical (SAN client) Maximum AC current 8A @ 115VAC, 4A @ 230VAC

The specification is shown in the following table.

Table 14: First-generation K2 Summit AC power specification

Characteristic	Specification
Power supply	Dual, redundant
Mains Input Voltage	90 to 260V auto-range, 47-63Hz
Power consumption	350W typical (standalone) 300W typical (SAN-attached) Maximum AC current 7A @ 115VAC, 3.5A @ 230VAC

The specification is shown in the following table.

Table 15: First-generation K2 Solo and K2 Solo 3G Media Server AC power specification

Characteristic	Specification
Power supply	Single
Mains Input Voltage	100-240V, 50/60 Hz
Power consumption	180W typical Maximum AC current 4A @ 115VAC, 2A @ 230VAC

⚠ ***WARNING: Always use a grounded outlet to supply power to the system. Always use a power cable with a grounded plug, such as the one supplied with the system.***

Environmental specifications

The K2 Summit 3G system specification is shown in the following table:

Characteristic	Specification
Ambient Temperature Non-Operating	-40° to +60° C
Ambient Temperature Operating	10° to +40° C

Characteristic	Specification
Relative Humidity	Operating 20% to 80% from 10° to +40° C Non-Operating 10% to 85% from -30° to +55° C Do not operate with visible moisture on the circuit boards
Operating Altitude	To 10,000 feet IEC 950 compliant to 2000 meters
Storage Altitude	To 40,000 feet
Non-Operating Mechanical Shock	30G 11 ms trapezoid
Random Vibration Operational	0.27 GRMS (5-500Hz)
Random Vibration Non-Operational	2.38 GRMS overall .019 g2/Hz (5-100Hz) .009 g2/Hz (200-350Hz) .0065 g2/Hz (500 Hz)
Equipment Type	Information Technology
Equipment Class	Class 1
Installation Category	Category II Local level mains, appliances, portable equipment, etc.
Pollution Degree	Level 2 operating environment, indoor use only.

The first generation K2 Solo 3G system specification is shown in the following table:

Characteristic	Specification
Ambient Temperature Non-Operating	-40° to +60° C
Ambient Temperature Operating	10° to +40° C
Relative Humidity	Operating 20% to 80% from 10° to +40° C Non-Operating 10% to 80% from -30° to +60° C Do not operate with visible moisture on the circuit boards
Operating Altitude	To 10,000 feet IEC 950 compliant to 2000 meters
Storage Altitude	To 40,000 feet
Non-Operating Mechanical Shock	30G 11 ms trapezoid
Random Vibration Operational	0.27 GRMS (5-500Hz)

Characteristic	Specification
Random Vibration Non-Operational	2.38 GRMS overall .0175 g2/Hz (5-100Hz) .009375 g2/Hz (200-350Hz) .00657 g2/Hz (500 Hz)
Equipment Type	Information Technology
Equipment Class	Class 1
Installation Category	Category II Local level mains, appliances, portable equipment, etc.
Pollution Degree	Level 2 operating environment, indoor use only.

Specifications vary for transmission products.

Mechanical specifications

The K2 Summit 3G Production Client specification is shown in the following table

Dimension	Measurement
Height	3.5 in (89mm)
Width	17.6 in (447 mm)
Depth [11]	24.3 in (617 mm) total 23.0 in (585 mm) rack depth
Weight:	55.0 lbs (25.0 kg) maximum

The first generation K2 Summit Production Client specification is shown in the following table

Dimension	Measurement
Height	3.5 in (89mm)
Width	17.6 in (447 mm)
Depth [12]	24.3 in (617 mm) total 23.0 in (585 mm) rack depth
Weight:	53.0 lbs (24.0 kg) maximum

The K2 Solo Media Server specification is shown in the following table

Dimension	Measurement
Height	3.5 in (89mm)
Width	8.25 in (210 mm)
Depth	17.7 in (446 mm)
Weight:	16.5 lbs (7.5 kg)

[11] Adjustable rack-mounting ears accommodate different rack depth limitations.
[12] Adjustable rack-mounting ears accommodate different rack depth limitations.

Electrical specifications

The following sections describe the electrical specifications:

Serial Digital Video (SDI)

The K2 Summit/Solo system specification is shown in the following table

Parameter	Specification
Video Standard	SD: 525 Line or 625 Line component HD: 720p or 1080i
Number of Inputs	1 per channel standard. 2 or 3 per channel when licensed for ChannelFlex Suite.
Number of Outputs	2 per channel
Data format	Conforms to SMPTE 259M (SD) and 292M (HD)
Number of bits	10bits
Embedded Audio Input	SD data format conforms to SMPTE 259M (48kHz, 20bits) HD data format conforms to SMPTE 299 48 kHz (locked to video) and 16- or 24- bit PCM Compatible with AC-3 and Dolby-E
Embedded Audio Output	Output data format is 48 kHz 24-bit User can disable embedded audio on SDI output
Connector	BNC, 75 ohm, No loop-through
nominal Amplitude	800mV peak-to-peak terminated
DC Offset	0 +0.5V
Rise and Fall Times	SD: 400 - 1500ps; measured at the 20% and 80% amplitude points HD: less than 270ps
Jitter	less than 0.2UI peak-to-peak
Max Cable Length	SD 300 meters HD 125 meters
Return Loss	greater than or equal to 15db, 5Mhz to 1.485Ghz

Genlock Reference

The K2 Summit/Solo system specification is shown in the following table:

Characteristic	Description
Signal Type	NTSC/PAL Color Black Composite Analog
Connectors	2 BNC, 75 ohm passive loop through
Signal Amplitude Lock Range	Stays locked to +6 dB and -3 dB
Input Return Loss	Greater than or equal to 36 dB to 6MHz
Tri-level sync	Supported

System Timing

The K2 Summit/Solo system specification is shown in the following table. All delay values shown are relative to Black Reference.

Characteristic	Description
Encoder timing	Derived from the video input
Nominal Playback Output Delay	Adjustable (Default: Zero timed to reference genlock)
SD Output Delay Range (Independent for each play channel)	525 lines • Frames: 0 to +1 • Lines: 0 to +524 • Samples: 0 to +1715 clock samples
	625 lines • Frames: 0 to +3 • Lines: 0 to +624 • Samples: 0 to +1727 clock samples
HD Output Delay Range (Independent for each play channel)	1080i at 29.97 FPS (SMPTE ST 274:2008) • Frames: 0 to +1 • Lines: 0 to +1124 • Pixels: 0 to +2199
	1080p at 59.94 FPS (SMPTE ST 274:2008) • Frames: 0 to +1 • Lines: 0 to +1124 • Pixels: 0 to +2199
	720p at 59.94 FPS (SMPTE ST 296:2012) • Frames: 0 to +1 • Lines: 0 to +749 • Pixels: 0 to +1649

Characteristic	Description
	1080i at 25 FPS (SMPTE ST 274:2008) • Frames: 0 to +1 • Lines: 0 to +1124 • Pixels: 0 to +2639
	1080p at 50 FPS (SMPTE ST 274:2008) • Frames: 0 to +1 • Lines: 0 to +1124 • Pixels: 0 to +2639
	720p at 50 FPS (SMPTE ST 296:2012) • Frames: 0 to +1 • Lines: 0 to +749 • Pixels: 0 to +1979
Loop through/EE	The video, AES, and LTC inputs pass to the output connectors as loop through.

AES/EBU Digital Audio

The K2 Summit/Solo system specification is shown in the following table

Parameter	Specification
Standard	AES3
Audio Inputs	4 Channels per video input/output on DB-25. Supports 32 KHz to 96 KHz inputs, which are sample rate converted to 48 KHz, 16 bit, 20 bit, or 24 bit digital audio sources.
Audio Outputs	4 Channels per video output. Audio mapping is direct and fixed. AES outputs are active at all times. Audio is output using a 48kHz clock derived from the video reference. Supports 16- or 24-bit media. On playout, audio is synchronized with video as it was recorded. Compatible with AC-3 and Dolby-E
Input Impedance	110 ohms, balanced
Audio time shift	Configurable relative to video for both record and playout.

LTC Input/Output

The K2 Summit/Solo system specification is shown in the following table

Parameter	Specification
Standard	SMPTE 12M Longitudinal Time Code, AC coupled, differential input
Number of Inputs	1 per video input - Shared 6 pin conn. with output
Number of Outputs	1 per video output
Input Impedance	1K ohm
Output Impedance	110 ohm
Minimum Input Voltage	0.1 V peak-to-peak, differential
Maximum Input Voltage	2.5 V peak-to-peak, differential
Nominal Output Voltage	2.0 V peak-to-peak differential.
LTC Reader	LTC reader will accept LTC at rates between 1/30 and 80 times the nominal rate in either forward or reverse directions.
LTC Transmitter	LTC transmitter outputs LTC at the nominal frame rate for the selected standard at 1x speed, forward direction only.

VITC Input/Output

The K2 Summit/Solo system specification is shown in the following table.

Parameter	Specification
VITC waveform	lines 10-20 NTSC (525 Line); lines 10-22 PAL (625 Line) VITC is decoded on each SDI input and inserted on each SDI output. VITC Reader configurable for a search window (specified by two lines) or set to manual mode (based on two specified lines). VITC Writer inserts VITC data on two selectable lines per field in the vertical interval. The two lines have the same data. VITC is not decoded off of the video reference input.

RS-422 specification K2 Summit 3G system

The RS-422 interface conforms to ANSI/SMPTE 207M-1997 standard (SMPTE 422).

The K2 Summit/Solo system specification is shown in the following table.

Characteristic	Description
Number of Inputs/Outputs	1 per channel
Connector type	Female RJ45

RS-422 specification first generation K2 Summit/Solo system

The RS-422 interface conforms to ANSI/SMPTE 207M-1997 standard (SMPTE 422).

The K2 Summit/Solo system specification is shown in the following table.

Characteristic	Description
Number of Inputs/Outputs	1 per channel
Connector type	Female DB9 pin

GPI I/O specifications

The K2 Summit/Solo system specification is shown in the following table.

Characteristic	Description
Number of Inputs/Outputs	12 inputs and 12 outputs.
Connector type	Female DB 25pin
GPI Input	TTL 0-0.8 V Low; 2.4-5 V High; 1 mA external current sink
GPI Output	Max Sink Current: 100 mA; Max Voltage: 30 V Outputs are open drain drivers. Max. voltage when outputs are open = 45V Max. current when outputs are closed = 250mA Typical rise times approximately 625ns Typical fall times approximately 400ns

Operational specifications

This section contains specifications related to media operations.

Video codec description K2 Summit/Solo

First generation K2 Summit Production Client, K2 Summit 3G Production Client, and K2 Solo Media Server specifications are shown in the following tables. Licenses and/or hardware options are required to enable the full range of specifications.

DV formats

Format	Sampling	Frame Rate	Data Rate	Other
DVCAM 720x480i 720x576i	4:1:1/4:2:0	29.97, 25	28.8 Mbps	Conforms to IEC 61834

Format	Sampling	Frame Rate	Data Rate	Other
DVCPRO25 720x480i 720x576i	4:1:1	29.97, 25	28.8 Mbps	Conforms to SMPTE 314M
DVCPRO50 720x487.5i 720x585i	4:2:2	29.97, 25	57.6 Mbps	Conforms to SMPTE 314M
DVCPRO HD 1280x1080i 1440x1080i	4:2:2	29.97, 25	100 Mbps	Conforms to SMPTE 370M
DVCPRO HD 960x720p	4:2:2	59.94, 50	100 Mbps	Conforms to SMPTE 370M

MPEG-2 formats

Format	Sampling	Frame Rate	Data Rate (Mbps)	Other
720x480i	4:2:0	29.97	2-15	I-frame and long GoP
720x480i	4:2:2	29.97	4-50	I-frame and long GoP
720x512i	4:2:2	29.97	4-50	I-frame and long GoP
720x576i	4:2:0	25	2-15	I-frame and long GoP
720x576i	4:2:2	25	4-50	I-frame and long GoP
720x608i	4:2:2	25	4-50	I-frame and long GoP
D10/IMX 720x512i	4:2:2	29.97	30, 40, 50 CBR	I-frame only
1280x720p	4:2:0	59.94, 50	20-80	I-frame and long GoP
1280x720p	4:2:2	59.94, 50	20-100	I-frame and long GoP
D10/IMX 720x608i	4:2:2	25	30, 40, 50 CBR	I-frame only
1920x1080i	4:2:0	29.97, 25	20-80	I-frame and long GoP[13]
1920x1080i	4:2:2	29.97, 25	20-100	I-frame and long GoP
XDCAM-HD 1440x1080i	4:2:0	29.97, 25	18 VBR, 25 CBR, 35 VBR	Long GoP

[13] Decode of lower bit rate is possible

Format	Sampling	Frame Rate	Data Rate (Mbps)	Other
XDCAM-HD422 1920x1080i	4:2:2	29.97, 25	50 CBR	Long GoP
XDCAM-HD422 1280x720p	4:2:2	59.94, 50	50 CBR	Long GoP
XDCAM-EX 1920x1080i	4:2:0	29.97, 25	35 VBR	Long GoP
XDCAM-EX 1280x720p	4:2:0	59.94, 50	25 CBR, 35 VBR	Long GoP

K2 systems record closed GoP structure. If an open GoP clip is imported, it is fully supported, including trimming the clip, playout of the clip, using the clip in playlists, and exporting the clip.

AVC-Intra formats

Format	Sampling	Frame Rate	Data Rate	Other
AVC-Intra 50 1440x1080i	4:2:0	29.97, 25	50 Mbps	Requires licenses or hardware for support on different K2 Solo 3G system models.
AVC-Intra 50 960x720p	4:2:0	59.94, 50	50 Mbps	
AVC-Intra 100 1920 x 1080i	4:2:2	29.97, 25	100 Mbps	
AVC-Intra 100 1280 x 720p	4:2:2	59.94, 50	100 Mbps	
AVC-Intra 100 1920 x 1080p	4:2:2	59.94, 50	200 Mbps	

AVCHD/H.264 formats

The following formats are for AVCHD and PitchBlue content. These are only supported for play output (decode) on AVCHD. A license is required. Record input (encode) is not supported.

Format	Sampling	Frame Rate	Data Rate	Other
720x480i	4:2:0	29.97	4-50	H.264-style open GoP. GoP length up to 30 frames. Up to 4 B-frames between anchor frames.
	4:2:2	29.97	4-50	
720x512i	4:2:2	29.97	4-50	

Format	Sampling	Frame Rate	Data Rate	Other
720x576i	4:2:0	25	4-50	
	4:2:2	25	4-50	
720x608i	4:2:2	25	4-50	
1920x1080i	4:2:0	29.97, 25	24 Mbps max.	
	4:2:2	29.97, 25	24 Mbps max.	
1440x1080i	4:2:0	29.97, 25	24 Mbps max.	
	4:2:2	29.97, 25	24 Mbps max.	
1280x720p	4:2:0	59.94, 50	24 Mbps max.	
	4:2:2	59.94, 50	24 Mbps max.	

AVC-LongG formats

The following formats are for AVC - LongG content. These are only supported for play output (decode). A license is required. Record input (encode) is not supported.

Format	Sampling	Frame Rate	Data Rate	Other
AVC-Ultra G6 1920x1080i	4:2:0	59.94, 50	6 Mbps	LongG
AVC-Ultra G6 1280x720p	4:2:0	59.94, 50	6 Mbps	
AVC-Ultra G12 1920x1080i	4:2:0	59.94, 50	12 Mbps	
AVC-Ultra G12 1280x720p	4:2:0	59.94, 50	12 Mbps	
AVC-Ultra G25 1920x1080i	4:2:2	59.94, 50	25 Mbps	
AVC-Ultra G25 1280x720p	4:2:2	59.94, 50	25 Mbps	
AVC-Ultra G50 1920x1080i	4:2:2	59.94, 50	50 Mbps	
AVC-Ultra G50 1280x720p	4:2:2	59.94, 50	50 Mbps	

Avid DNxHD formats

The following formats are for Avid DNxHD content. These are supported for record input (encode) and play output (decode). A Summit 3G Codec board with a K2-XDP2-DNX-2CH license is required.

Format	Frame Rate	Data Rate	Bits	Other
1920x1080i	29.97	220 Mbps	10	Avid DNxHD 220x
	29.97	220 Mbps	8	Avid DNxHD 220
	29.97	145 Mbps	8	Avid DNxHD 145
	25	184 Mbps	10	Avid DNxHD 185x
	25	184 Mbps	8	Avid DNxHD 185
	25	121 Mbps	8	Avid DNxHD 120
1280x720p	59.94	220 Mbps	10	Avid DNxHD 220x
	59.94	220 Mbps	8	Avid DNxHD 220
	59.94	145 Mbps	8	Avid DNxHD 145
	50	175 Mbps	10	Avid DNxHD 175x
	50	175 Mbps	8	Avid DNxHD 175
	50	116 Mbps	8	Avid DNxHD 115

Proxy/live streaming formats

The proxy files and streams created by a K2 Solo 3G system conform to industry standards, as follows.

Video: MPEG-4 Part 2

Format	Frame Rate	Data Rate (Mbps)	Other
320x240p	29.97, 25	1.5 Mbps	GOP 1 second
384x288p	29.97, 25	1.5 Mbps	GOP 1 second
512x288p	29.97, 25	1.5 Mbps	GOP 1 second

Audio: MPEG-4 Part 3 AAC-LC, 64 kbps, 48 kHz

Proxy file: MPEG-4 Part 12 Fragmented MP4 Movie

Live streaming: SDP files and RTP/RTCP streams are compliant with the following RFCs:

- RFC 3350, RFC 4566, RFC 3016, RFC 3640, RFC 5484, MPEG-4 Part 8

Playout of multiple formats

The K2 Solo 3G system automatically handles material of various types and formats as specified in the following sections:

Playout on K2 Summit/Solo

For a given frame rate, you can play SD clips of any format back-to-back on the same timeline. Both 16:9 and 4:3 SD aspect ratio formats can be played on the same timeline. Refer to video codec description earlier in this section for a list of the supported formats.

On channels with the XDP (HD) license, for similar frame rates (25/50 fps or 29.97/59.95 fps), SD material transferred or recorded into the K2 Solo 3G system along with its audio is up-converted when played on a HD output channel. Likewise, HD material is down-converted along with its audio when played on an SD output channel. HD and SD clips can be played back-to-back on the same timeline, and aspect ratio conversion is user configurable.

The K2 Solo 3G system supports mixed clips with uncompressed and compressed (PCM, AC3, and Dolby) audio on the same timeline.

25/50 fps conversions on HD K2 Solo 3G system models

The following specifications apply to K2 Solo 3G system channels with the XDP (HD) license.

		Converted SD format	**Converted HD format**	**Converted HD format**
		625 at 25 fps	**1080i at 25 fps**	**720p at 50 fps**
Source SD format	**625 at 25 fps**	No conversion	Up-convert SD to HD	Up-convert SD to HD
Source HD format	**1080i at 25 fps**	Down-convert HD to SD	No conversion	Cross-convert from 1080i to 720p
	720p at 50 fps	Down-convert HD to SD	Cross-convert from 720p to 1080i	No conversion

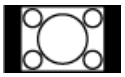
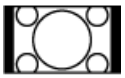
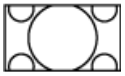
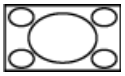
29.97/59.95 fps conversions on HD K2 Solo 3G system models

The following specifications apply to K2 Solo 3G system channels with the XDP (HD) license.

		Converted SD format	**Converted HD format**	**Converted HD format**
		525 at 29.97 fps	**1080i at 29.97 fps**	**720p at 59.94 fps**
Source SD format	**525 at 29.97 fps**	No conversion	Up-convert SD to HD	Up-convert SD to HD
Source HD format	**1080i at 29.97 fps**	Down-convert HD to SD	No conversion	Cross-convert HD to HD
	720p at 59.94 fps	Down-convert HD to SD	Convert HD to HD	No conversion

Aspect ratio conversions on HD K2 client

The following specifications apply to K2 Solo 3G system channels with the XDP (HD) license.

Source aspect ratio	Source image	Conversion option	Conversion description	Converted aspect ratio	Converted image
4:3		Bar	The 4:3 aspect ratio is maintained, centered on the screen, with black bars filling the left and right portions of the 16:9 display.	16:9	
		Half Bar	The picture aspect ratio is maintained, but the image is slightly enlarged. The top and bottom of the image are slightly cropped, and thin black bars fill the left and right portions of the 16:9 display.	16:9	
		Crop	The picture aspect ratio is maintained, but the image is enlarged so that it horizontally fills the HD display. The top and bottom of the 4:3 SD image are cropped to fit in the 16:9 display.	16:9	
		Stretch	The picture aspect ratio is distorted. The image fills the screen vertically without cropping, and is stretched horizontally to fill the 16:9 display. This conversion up-converts Full Height Anamorphic (FHA) 16:9 SD material.	16:9	
16:9		Bar	The 16:9 aspect ratio is maintained, centered on the screen, with black bars filling the top and bottom portions of the 4:3 display.	4:3	
		Half Bar	The picture aspect ratio is maintained, but the image is slightly enlarged. The left and right sides the image are slightly cropped, and thin black bars fill the top and bottom portions of the 4:3 display.	4:3	
		Crop	The picture aspect ratio is maintained, but the image is enlarged so that it vertically fills the SD display. The left and right sides of the 16:9 HD image are cropped to fit in the 4:3 SD display	4:3	

Source aspect ratio	Source image	Conversion option	Conversion description	Converted aspect ratio	Converted image
		Stretch	The picture aspect ratio is distorted. The image fills the screen horizontally without cropping, and is stretched vertically to fill the 4:3 display. This conversion generates Full Height Anamorphic (FHA) 16:9 SD material.	4:3	

Active Format Description (AFD) specifications

NOTE: This topic applies to K2 Summit/Solo systems.

Active Format Description (AFD) settings automatically determine the proper aspect ratio to use for up- and down-conversions, based on the AFD information embedded in the clip metadata. If no AFD was set on the incoming SDI input, you can assign the AFD setting in K2 AppCenter. A related setting, aspect ratio conversion (ARC), makes settings in K2 AppCenter on a clip-by-clip basis or per channel basis but does not embed settings in clip metadata.

About Active Format Description

The AFD is defined during production. By inserting metadata about the aspect ratio into the vertical ancillary data, AFD can define the aspect ratio of the signal as it progresses through ingest, editing, up/down conversion and playout. If the aspect ratio is altered during processing, then the AFD passed on downstream might need to be modified to ensure the correct aspect ratio is obtained.

NOTE: If ARC leads to unsupported active video format (postage stamp), the new AFD code will be the 'undefined' value of 0000.

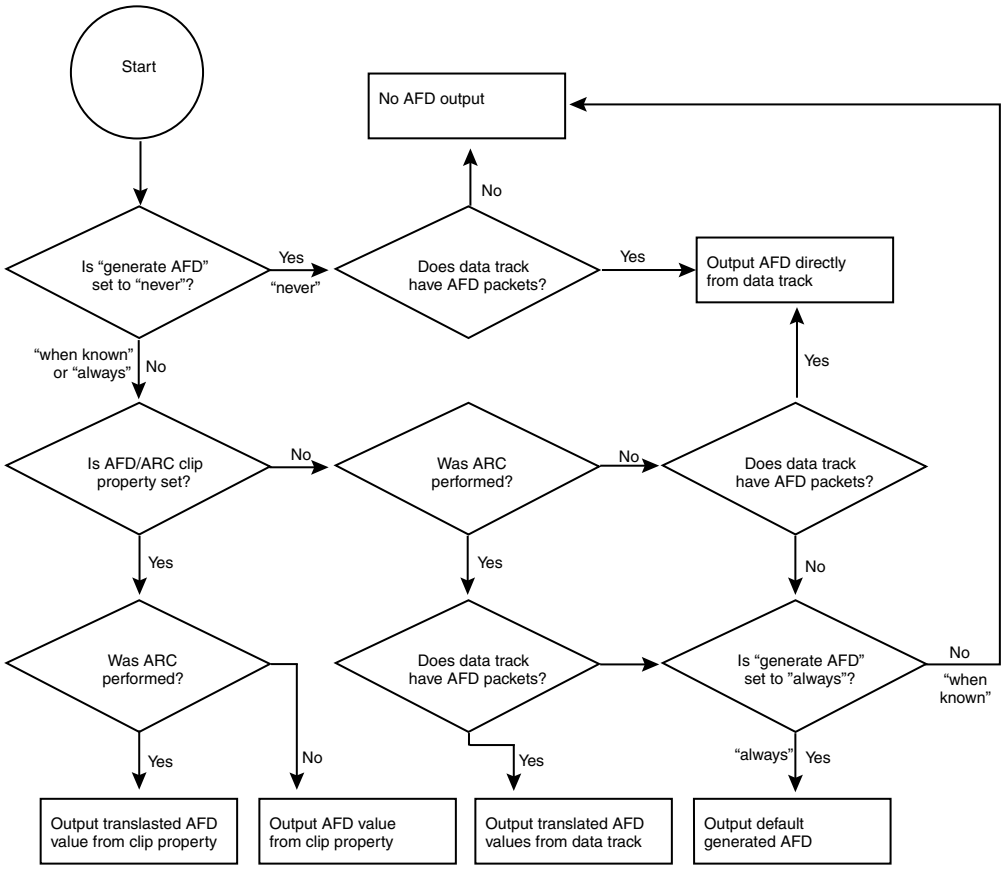
The playback Aspect Ratio Conversion (ARC) is prioritized according to the following table:

Playback aspect ratio conversion priority	
1	Clip property (ARC or AFD-based conversion rules)
2	Output channel (ARC configuration property)

NOTE: Bar data is not supported on the K2 system.

AFD output flowchart

The K2 Solo 3G system determines AFD code values in output as illustrated by the following flowchart.



Storing AFD on K2 Summit/Solo systems

The K2 Summit/Solo system stores clip metadata in clip properties and uses this data throughout the workflow. You can modify the AFD setting in AppCenter.

You can store AFD in a data track. Grass Valley recommends selecting this for HD clips; if using SD, this is optional. This method takes more storage (it is approximately equal to four tracks of audio) but this method enables AFD and CC/Teletext support for HD.

Ingesting SDI

An SDI video signal stores AFD in the vertical ancillary data. The K2 Solo 3G system processes the signal as follows:

- If present, the AFD setting from two seconds into the file is copied into the clip properties. This is the default K2 system behavior and occurs unless you set it to **No** in Configuration Manager.
- If selected, the ANC data is copied into the K2 data track.

Using AFD with file transfers

The following tables describe the AFD file priorities and the AFD behavior with GXF and MXF transfers.

File transfer AFD priority	
1	AFD from the MXF or GXF metadata is copied to the K2 clip properties.
2	If the MXF stream contains an ancillary data track with AFD ancillary data packets and Active Format Descriptor attribute of the Generic Picture Essence descriptor in the MXF header metadata is absent, then the AFD value for the K2 clip is derived from the AFD ancillary data packet located around 2 seconds into the material. That AFD value is then copied to the K2 clip properties.
3	If there is no AFD in the MXF, the GXF, or the data track, then no AFD is set.

GXF Export: (both AFD and ARC values inserted into XML of stream)	
Condition	**Description**
Exported to K2 system that does not support AFD	AFD setting is ignored, but setting is retained with clip ARC settings apply
Exported to K2 system that supports AFD	AFD overrides ARC settings

GXF Import	
Condition	**Description**
Imported from K2 system that does not support AFD	ARC converted to AFD
Imported from K2 system that supports AFD	AFD overrides ARC settings

MXF Export	
Condition	**Description**
AFD from clip property added to properties of the video in the header metadata	If clip property is not set, do not add property in stream
AFD from data track in stream's ancillary data	No change required

ARC is K2 specific and therefore not included in MXF transfers.

MXF Import	
Imported stream has AFD in the header metadata	AFD is stored in the clip property setting of the clip
Imported stream has AFD in the data track	AFD is stored in the clip property setting of the clip. (AFD is taken from the ancillary data two seconds from the beginning, or, if the clip is less than 2 seconds long, from the last valid AFD.)
Imported stream has no AFD	No AFD

ARC is K2 specific and therefore not included in MXF transfers.

Default generated AFD values

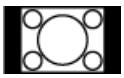
Default AFD values are generated when the three following conditions are met:

- The AFD output setting in the Configuration Manager is set to **Always**
- The clip does not have AFD in the data track, and
- The clip does not have AFD specified in its clip properties

Under these conditions, default AFD is generated and inserted, based on ARC performed and the source material format. Default generated AFD settings are described in the table below.

Default generated AFD values when up-converting to HD

Source image is presumed based on the conversion that has been selected.

Source aspect ratio	Presumed source image	Conversion option	Converted AFD and aspect ratio	Converted image
16:9 HD		No conversion	AFD = 1010 AR = 16:9 HD	
16:9 SD		Scale up Crop vertical	AFD = 1010 AR = 16:9 HD “crop”	
		Scale up	AFD = 1010 AR = 16:9 HD	
		Scale up Crop vertical Pillarbox	AFD = 1011 AR = 16:9 HD “half bars”	
4:3 SD		Scale up Pillarbox	AFD = 1011 AR = 16:9 HD “bars”	

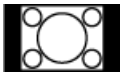
Default generated AFD values when down-converting to SD

Source image is presumed based on the conversion that has been selected.

Source aspect ratio	Presumed source image	Conversion option	Converted AFD and aspect ratio	Converted image
4:3 SD not widescreen		No conversion	AFD = 1001 AR = 4:3 SD	
16:9 SD widescreen		No conversion (only if ARC set to ‘stretch’)	AFD = 1010 AR = 16:9 SD	

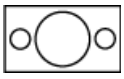
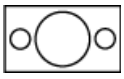
Source aspect ratio	Presumed source image	Conversion option	Converted AFD and aspect ratio	Converted image
16:9 HD		Scale down letterbox	AFD = 1010 AR = 4:3 SD "bars"	
		Scale down Crop horizontal	AFD = 1001 AR = 4:3 SD "crop"	
		Scale down	AFD = 1010 AR = 16:9 SD "stretch"	
		Scale down Crop horizontal Letterbox	AFD = 1011 AR = 4:3 SD "half bars"	

Supported conversions from SD to HD using AFD

Source AFD and aspect ratio	Source image	Conversion performed	Converted AFD and aspect ratio	Converted image
AFD = 1010 AR 4:3 SD		Scale up crop vertical	AFD = 1010 AR 16:9 HD	
AFD = 1000 or 1001 AR 4:3 SD		Scale up pillarbox	AFD = 1001 AR 16:9 HD	
AFD = 1010 AR 16:9 SD		Scale up	AFD = 1010[14] AR 16:9 HD	
AFD = 1011 AR = 4:3 SD		Scale up Crop vertical pillarbox	AFD = 1011 AR 16:9 HD	

[14] You can change the default converted value of AFD = 1010 to be AFD = 1001. This setting is in K2 AppCenter Configuration Manager play channel video settings.

Supported conversions from HD to SD using AFD

Source AFD and aspect ratio	Source image	Conversion performed	Converted AFD and aspect ratio	Converted image
AFD = 1000 or 1010 AR = 16:9		Scale down letterbox	AFD = 1010 AR = 4:3[15]	
AFD = 1001 AR = 16:9		Scale down crop horizontal	AFD = 1001 AR = 4:3	
AFD = 1010 AR = 16:9		Scale down	AFD = 1010 AR = 16:9[16]	
AFD = 1011 AR = 16:9		Scale down Crop horizontal letterbox	AFD = 1011 AR = 4:3	
AFD = 1111 AR = 16:9		Scale down crop horizontal	AFD = 1001 AR = 4:3	

VBI/Ancillary/data track specifications

This section contains topics about data carried in the media file.

VBI/Ancillary/data track definitions

Terms in this section are defined as follows:

Ancillary data	Ancillary data (ANC data) as specified in this section is primarily a means by which timecode, Closed Captioning, and Teletext information is embedded within the serial digital interface. Other Type 2 ancillary data packets are stored and played back without modification. Ancillary data is standardized by SMPTE 291M.
Closed Captioning (CC)	Line 21 NTSC Closed Captioning as defined in EIA-608 and used as a subset of EIA-708. EIA-708 has been updated and renamed to CEA-708. Includes other Line 21 services such as V-Chip.
Teletext (TT)	Teletext System B subtitles as defined ETSI EN 300 706 and other documents. The Australian standard for digital TV is Free TV Operational Practice OP-47. It has been ratified as SMPTE RDD 8.
Captioning	Denotes both NTSC Closed Captioning and Teletext subtitling.

[15] When play channel video settings Aspect Ratio is set to "Standard (4:3)"
[16] When play channel video settings Aspect Ratio is set to "Widescreen (16:9)"

Luma/Chroma VBI support on K2 Summit/Solo

Record and playout of VBI is supported for both Luma and Chroma. However, a given line of VBI data can be stored as either Luma or Chroma, but not both.

VBI data support on K2 Summit/Solo

The following table applies when in Configuration Manager, the Data Track settings are configured as:

- Record ancillary data: No

Or as:

- Record ancillary data: Yes
- Record Uncompressed VBI and captioning data to track: No

Use these Data Track settings to retain compatibility with legacy systems, such as the Profile XP Media Platform.

Video format	Compressed VBI	Uncompressed VBI	Captioning	Comments
DVCPRO25 525 line (NTSC)	Not supported	Not supported by DVCPRO25 format	CC supported, as native to DVCPRO25. VCHIP data supported.	—
DVCPRO25 625 line (PAL)	Not supported	Not supported by DVCPRO25 format	TT not supported as VBI data.	
DVCPRO50 525 line (NTSC)	Supported for playout	Not supported by DVCPRO50 format	CC supported, as native to DVCPRO50 (compressed VBI). VCHIP data supported.	—
DVCPRO50 625 line (PAL)	Supported for playout	Not supported by DVCPRO50 format	TT supported, as native to DVCPRO50 (compressed VBI).	—
DVCAM 525 line (NTSC)	Not supported	Not supported by DVCAM format	CC supported, as native to DVCAM.	—
DVCAM 625 line (PAL)	Not supported	Not supported by DVCAM format	TT not supported as VBI data.	—

Video format	Compressed VBI	Uncompressed VBI	Captioning	Comments
MPEG-2 525 line (NTSC)	Supported as 16 lines per field. Range: 7–22	Supported for record. Not supported for playout.	CC supported and always on. Not selectable.	—
MPEG-2 625 line (PAL)	Supported as 16 lines per field. Range: 7–22	Supported for record. Not supported for playout.	TT supported only as compressed or uncompressed VBI.	—
MPEG-D10 525 line (NTSC)	Supported	Not supported by D10 format.	CC supported, as native to D10.	—
MPEG-D10 625 line (PAL)	Supported	Not supported by D10 format.	TT supported, as native to D10.	—

Data track support on K2 Summit/Solo SD channels

The following table applies to SD channels when in Configuration Manager the Data Track settings are configured as follows:

- Record ancillary data: Yes
- Record Uncompressed VBI and captioning data to track: Yes

Video format	Data	Supported as follows:
525 line (NTSC)	Closed Captioning	Stored in EIA-708 packets. On playback, modulate to VBI line 21.
625 line (PAL)	Teletext	Stored in OP-47 packets. On playback, modulate to VBI line specified in OP-47 packet.
All supported SD formats	Uncompressed VBI	Selectable per line. Limited to 5 lines. The 5 line limit does not include any lines used for CC or TT. Can select either Luma or Chroma for each line, but not both.
	Ancillary timecode	Ancillary timecode is preserved only. No timecode track is constructed from ancillary timecode data. The timecode track is not inserted as ancillary timecode on playout.

Data track support on K2 Summit/Solo HD channels

On channels with the XDP (HD) license, the data track can contain ancillary data and other types of data. Luma ancillary data packets are stored. Chroma ancillary data packets are not supported.

Data	Supported as follows:
Ancillary timecode	For record, selectable to use VITC or LTC ancillary timecode as timecode source. For playout, selectable to insert recorded timecode track as ancillary data VITC or LTC timecode packets. If the recorded timecode track is inserted as VITC ancillary timecode and VITC ancillary timecode packets are already stored on the data track, then the recorded timecode track overrides the stored VITC ancillary timecode packets. If the recorded timecode track is inserted as LTC ancillary timecode and LTC ancillary timecode packets are already stored on the data track, then the recorded timecode track overrides the stored LTC ancillary timecode packets.
Vertical interval ancillary data packets	Extracted at input and stored on an ancillary data track. Upon playout, the data packets are inserted into the video stream on specified lines. Maximum 8 packets per field. CC and TT supported as native to format.

Captioning system support

An API is provided for access to captioning data, allowing Closed Captioning and Teletext systems to produce timecode correlated captions for an existing K2 clip.

CEA 608 to CEA 708 DTV CC Transcoder and FCC requirements

Federal Communications Commission (FCC) rules incorporate sections of industry standards EIA-708 and EIA-608. The K2 Summit/Solo system fulfills the requirement for older materials that do not have DTV CC. If SD material has EIA-608 CC present, the K2 Summit/Solo system can be configured so that when it up-converts the material the EIA-708 packet contains the EIA-608 data plus the DTV CC transcoded from EIA-608.

DTV CC transcoding is enabled on a per channel basis in the Configuration Manager under **Channel Configuration**. By default, transcoding is disabled and the behavior is the same as prior software releases that did not support this transcoding. When enabled, transcoding is applied to any CEA 708 packets played out to either 1080i or 720p outputs (NTSC timing only). Transcoding happens for the following cases:

- SD clips are recorded with CC on the data track.
- SD MPEG clips with CC in the MPEG user data.
- DVCPRO25 clips with CC in the DV frame.
- HD clips with CEA 708 packets on the data track that have Line 21 data is present and DTV CC is absent.

CEA 608 commands from the above sources are converted to CEA 708 DTV CC commands that generate caption presentations that are similar to the original CEA 608 captions. The appearance is similar but not the same due to the differences in fonts, text positioning, etc.

This applies to up-conversion only. HD material should already have compliant EIA-708 packets.

About privately defined data packets

In ancillary data, the K2 Solo 3G system supports data defined by a private organization. This is data that is not defined and registered with SMPTE.

For example, if a facility puts privately defined data as special "triggers" in their stream for downstream devices, these triggers are preserved on record and transfer and played with field accuracy when needed. SMPTE standard data is supported as well as the privately defined data, for fully compliant, field accurate data track support.

Data bridging of VBI information on K2 Summit/Solo HD channels

On channels with the XDP (HD) license, data is bridged as follows:

Source format	Source data	Conversion ——>	Converted format	Converted data
SD 525 line	Closed-captioning (CC) on line 21 (EIA-608) can be stored as UserData[17] CC packets or UserData VBI Line21 (Uncompressed VBI Line21)	Up-convert	HD	Ancillary Closed Caption EIA-708-B packets
	EIA-708	Up-convert	HD	EIA-708
SD 625 line	Teletext (except as below)	No up-conversion to HD		
	5 lines of VBI Teletext in OP-47 packets	Up-convert	HD	OP-47 ancillary data packet in SD data track file. SD Teletext is in ancillary data location as specified in OP-47 packet.
SD 625 line 525 line	Ancillary data	Up-convert	HD	Moved to valid lines
HD	EIA-708 & 608 Ancillary data packets	Down-convert	SD	Closed-captioning on line 21 (EIA-608 standard).
HD	Teletext as OP-47 packets	Down-convert	SD	Output as VBI waveforms on lines specified in OP-47 packet or as specified by "Teletext Output Lines" data track settings in AppCenter Configuration Manager.
HD 1080i	Ancillary data	Cross-convert	HD 720p	Moved to valid lines.
HD 720p	Ancillary data	Cross-convert	HD 1080i	Moved to valid lines. Any data on lines 21-25 is moved to line 20 on 1080i output.

Line mapping of ancillary data packets on K2 Summit/Solo HD channels

On channels with the XDP (HD) license, you can use "Output OP-47 packet on line" data track settings in AppCenter Configuration Manager to specify that all OP-47 packets are output on the selected video line during playout.

[17] UserData CC packets always on. If CC exists, it is recorded and played back. MPEG UserData can be played out but not recorded.

Source format	Source data	Line mapping ——>	Playout format	Converted data
HD 1080i	OP-47 packets, as specified by DID and SID, on a line valid for 1080i	Maps to	HD 1080i (same as source)	OP-47 packets on a different line valid for 1080i.
HD 720p	OP-47 packets, as specified by DID and SDID, on a line valid for 720p	Maps to	HD 720p (same as source)	OP-47 packets on a different line valid for 720p.

PitchBlue/H.264 ancillary data and timecode

The K2 Summit/Solo system extracts captioning as defined by ATSC a/72 embedded in the video information of H.264 material during ingest. The system plays this information during H.264 playout.

Timecode for a PitchBlue import is striped timecode (continuous timecode) that starts at 00:00:00:00 as required for a PitchBlue workflow.

This functionality supports the PitchBlue workflow. However, the functionality applies to all H.264 material, not only PitchBlue material.

Internationalization

When you enable internationalization on a K2 Solo 3G system, you can name your media assets in a local language. The K2 Solo 3G system supports the local language name as specified in the following table.

System	Internationalization support
Keyboard input and display	• English • Chinese • Japanese • French • German • Spanish • Cyrillic (Russian) • Portuguese • Korean
Media database	• All external views of movie assets can be represented as wide-file names. • AppCenter runs in Unicode. • Only movie assets and searchable User Data keys are Unicode.
Media file system	• Support for Kanji and wide-character file and folder names. • File-folder representation of movie are internationalized, as well as the QuickTime reference file it contains. • Key names (V:\media) remain unchanged, but are Unicode.
K2 Summit/Solo applications	• Movie assets are described in Unicode. • Application user interfaces are Unicode compliant.
Protocols	Refer to "Remote control protocols" in the "Configuring the K2 System" section of this Topic Library.
FTP transfers	Refer to "FTP internationalization" in the "Configuring the K2 System" section of this Topic Library.

Names of media assets and bins must conform to the naming specifications for assets and bins.

Limitations for creating and naming assets and bins

Media assets and bins must conform to the following specifications.

Characters not allowed in asset and bin names

Position	Character	Description
Anywhere in name	\	backward slash
	/	forward slash
	:	colon
	*	asterisk
	?	question mark

Position	Character	Description
	<	less than
	>	greater than
	%	percent sign
	|	pipe
	"	double quote
At beginning of name	~	tilde
		space
At the end of name		space

Asset and bin name limitations

The maximum number of characters in an asset path name, including the bin name, is 259 characters. This includes separators such as "\" and parts of the path name that are not visible in AppCenter. The file system limits the number of bytes in a name as well as the number of characters. The values in this table apply to names in English and other languages referred to in ISO 8859-1. The full count of 259 characters might not be available with some other character sets.

	Asset name, bin name, and path			
Sections of an asset/path name	**The rest of the path name** (i.e. everything apart from the bin and asset names)	Bin name	Asset media directory and extension	Asset name and extension
Naming limitation	This part of the path name is not visible in AppCenter.	The bin name can be up to 227 characters (which would leave room for only a 1-character asset name)	This part of the path name is not visible in AppCenter. The directory name is the same as the asset name. 4 characters are reserved for the extension.	The extension is not visible in AppCenter. At least 25 characters are reserved for the asset name and extension, even if they are not all used.
Example	`\media`	`\mybin1\mybin2`	`\MyVideo.cmf`	`\MyVideo.xml`

The following examples show how a path name would appear in AppCenter and in the file system.

In AppCenter:

`V:\mybin1\mybin2\MyVideo`

In the file system:

`V:\media\mybin1\mybin2\MyVideo.cmf\MyVideo.xml`

Bin nesting limitations

The K2 media database supports nine levels of nested bins. This includes the top level (first) bin. Exceeding this specification results in a database error. When creating a bin do not create a bin at level ten or deeper.

For example:

- The following is supported:
  ```
  default\en\fr\es\de\it\be\dk\cn
  ```
- The following is not supported:
  ```
  default\en\fr\es\de\it\be\dk\cn\jp
  ```

Video network performance

K2 systems support streaming transfers to and from K2 Solo 3G system, K2 Media Clients, K2 SANs, Profile XP Media Platforms, or any device that supports General Exchange Format (GXF) as described in SMPTE 360M.

Parameter	Specification	Comments
Transfer bandwidth per internal storage K2 Solo 3G system	Up to 50 MBytes per second	—
Transfer bandwidth per K2-SVR-100	Up to 90Mbytes per second	Depending on system design
Transfer bandwidth per K2-SVR-NH10GE	Up to 600Mbytes per second	Depending on system design
Maximum concurrent transfers per transfer engine	4 to 10, configurable on SAN	Additional transfers are queued.
Minimum delay from start of record to start of transfer	20 seconds in actual time (not content duration)	This applies to both 60Hz timing and 50Hz timing.
Minimum delay between start of transfer into destination and start of play on destination	20 seconds in actual time (not content duration)	—

About file interchange mechanisms on K2 systems

K2 Summit, Solo, and SAN systems can send and receive files as follows:

- File based import/export — This is based on a file that is visible from the operating system. For example, AppCenter import/export features are file based.
- HotBin import/export — This is file based import/export, with automated features that are triggered when a clip is placed in a bin. Some HotBin functionality requires licensing.
- FTP stream — This is file interchange via File Transfer Protocol (FTP).

GXF interchange specification

This specification applies to GXF file transfer, import, and export on K2 Summit, Solo, and SAN systems.

Streaming between online K2 systems supports complex movies and agile playlists of mixed format.

Formats are supported are as follows:

Supported formats		Notes
Video	DVCPRO25	—
	DVCPRO50	—
	DVCPRO HD	Super Slo-Mo requires software version 7.1.x or higher
	DVCAM	—
	MPEG-2	Includes all MPEG-2 formats (IMX, XDCAM, etc.) that can be stored on a K2 system
	AVC-Intra	—
	H.264	Playable on K2 Summit 3G system only. Can transfer to systems with K2 software version 8.x and higher.
	Avid DNxHD	Playable on K2 Summit 3G system only. Can transfer to systems with K2 software version 8.x and higher.
Audio	48 kHz	—
	16 bit, 24 bit	—
	PCM, Dolby-E, AC-3	—
Data	VBI	—
	Ancillary	—

Interchange mechanisms are supported as follows:

Mechanism		Support
File based	Import	Yes
	Export	Yes
FTP stream	Import	Yes
	Export	Yes

Related Topics

Limitations with complex media types on page 292

MXF interchange specification

This specification applies to MXF file transfer, import, and export on K2 Summit, Solo, and SAN systems.

MXF supports simple clips with a single video track only.

Formats are supported are as follows:

Supported formats		Notes
Video	DVCPRO25	—
	DVCPRO50	—
	DVCPRO HD	Super Slo-Mo requires software version 7.1. x or higher
	DVCAM	—
	D10	See MXF export behavior for eVTR style D10AES3.
	MPEG-2	Includes all MPEG-2 formats (IMX, XDCAM, etc.) that can be stored on a K2 system
	AVC-Intra	—
	Avid DNxHD	Playable on K2 Summit 3G system only. Can transfer to systems with K2 software version 8.x and higher.
Audio	48 kHz	—
	16 bit, 24 bit	—
	PCM, Dolby-E, AC-3	—
Data	VBI	MXF supports either ancillary data packets or VBI lines in the data track but not both, so if ancillary data packets and VBI lines have been recorded into the K2 clip's data track, then the VBI lines will be dropped from the MXF data track on an MXF export.
	Ancillary	—

Interchange mechanisms are supported as follows:

Mechanism		Support
File based	Import	Yes
	Export	Yes
FTP stream	Import	Yes
	Export	Yes

With a special export option, you can export a completed continuous (loop) record clip as MXF or QuickTime, with the result being a flattened stream file. Recording must be complete before you export the clip, however you can make sub-clips while record is underway and export the sub-clips. For this feature, MPEG-2 long GoP is not supported.

Related Topics

Limitations with complex media types on page 292

MXF export behavior on K2 systems

Upon MXF export the K2 system checks clip structure for specifications as they apply to industry standard formats such as Sony XDCAM (SMPTE RDD-09) and Sony eVTR style (SMPTE ST 386). If specifications match, the media is exported as the appropriate format.

The K2 system allows you to override the MXF export behavior so that the exported MXF file no longer match the specifications for the industry-standard format. For example, you can export a clip containing more audio tracks than constrained by the specific MXF standard for the maximum number of audio tracks in a D10AES3 channel. If you export a clip with such an override, the K2 will generate a generic MXF op1a file (instead of the default D10 or XDCAM constrained MXF file).

About MXF with DIDs and SDIDs

You can import and export MXF containing ANC packets and VBI lines as specified in SMPTE ST 436. The K2 system extracts the ANC packets or VBI lines to the K2 clip's data track.

MXF Export Type

When importing and exporting MXF the K2 system behaves as follows, in relation to the MXF Export Type setting in K2Config or in K2 AppCenter:

- The MXF Export Type setting applies to all MXF exports on the K2 system. There is one setting for one K2 system. The K2 system can be a stand-alone K2 Summit/Solo system or a K2 SAN. If a K2 SAN, the one setting applies to the K2 Media Server with role of FTP server that handles exports for all SAN-attached K2 Summit systems.
- For export, the K2 system must be set to one of the following MXF Export Types:
  - **377M**: SMPTE ST 377:2004 compliant. Ensures compatibility with older products.
  - **377-1**: SMPTE ST 377-1:2009 compliant.
- By default the K2 system is set to SMPTE ST 377:2004. This setting is only applicable to the MXF op1a import and export.
- The SMPTE ST 377:2004 setting is recommended for compatibility with older systems which do not support SMPTE ST 377-1:2009.
- The following format does not support SMPTE ST 377-1:2009 export. Therefore the format is always exported as SMPTE ST 377:2004, regardless of the MXF Export Type setting:
  - D10 media
- For import, both SMPTE ST 377:2004 and SMPTE ST 377-1:2009 are supported, regardless of the MXF Export Type setting. The MXF Export Type setting affects export only.

AMWA AS-02 interchange

The K2 system behaves as follows in relation to the Advanced Media Workflow Association (AMWA) AS-02 version 1.0: 2011 MXF Versioning Specification:

- The K2 system supports the AS-02 specification with no customizations
- Supports import of AS-02 content
- Plays media imported with AS-02
- Exports media to AS-02 content
- Requires license K2-ExtendedFileServices.

Related Topics

Limitations with complex media types on page 292

QuickTime interchange specification

This specification applies to QuickTime file transfer, import, and export on K2 Summit, Solo, and SAN systems.

The following are not supported:

- Sequences and lists
- Lists of mixed formats or containing empty tracks, such as tracks that do not contain recorded media

Formats are supported are as follows:

Supported formats		Notes
Video	DVCPRO25	—
	DVCPRO50	—
	DVCPRO HD	Super Slo-Mo requires software version 7.1.x or higher
	DVCAM	—
	AVC-Intra	—
	D10/IMX	—
	XDCAM-HD	—
	XDCAM-EX	—
	XDCAM-HD422	—
	H.264	Playable on K2 Summit 3G system only. Can transfer to systems with K2 software version 8.x and higher.
	Avid DNxHD	—
Audio	48 kHz	
	16 bit, 24 bit PCM	
Data	None	—

Interchange mechanisms are supported as follows:

Mechanism		Support
File based	Import	Yes
	Export	Yes
FTP stream	Import	No
	Export	No

With a special export option, you can export a completed continuous (loop) record clip as MXF or QuickTime, with the result being a flattened stream file. Recording must be complete before you export the clip, however you can make sub-clips while record is underway and export the sub-clips. For this feature, MPEG-2 long GoP is not supported.

Related Topics

Limitations with complex media types on page 292

QuickTime video and key import specification

This specification applies to importing a QuickTime file with an alpha channel. This is a licensed feature.

The imported file must be QuickTime 32 with alpha RLE 32-bit raster encoding, as produced by the Apple Animation Codec.

Supported video formats for import are as follows:

Format		Scan	Frame Rate
SD video	720 x 480	Interlaced	29.97
	720 x 512	Interlaced	29.97
	720 x 576	Interlaced	25
	720 x 608	Progressive	25
HD video	1920 x 1080	Interlaced	29.97, 25
	1280 x 720	Progressive	59.94, 50

Supported audio formats for import are as follows:

Format		
Audio tracks (if present)	48 kHz	Mono or stereo
	16 bit, 24 bit	
	PCM	

Interchange mechanisms are supported as follows:

Mechanism		Support
File based	Import	Yes

Mechanism		Support
	Export	No
FTP stream	Import	No
	Export	No

When K2 software imports a file that meets the above requirements, it creates a K2 clip with two video tracks, in formats as follows:

Format			Frame Rate	Data Rate
SD video	D10/IMX	720 x 512	29.97	50 CBR
	D10/IMX	720 x 608	25	50 CBR
HD video	AVC-Intra 100	1920 x 1080	29.97, 25	100 Mbps
	AVC-Intra 100	1280 x 720	29.97, 25	100 Mbps

Audio tracks, if present are imported.

Timecode data is imported as K2 striped timecode. The first timecode value is the starting value and subsequent timecode is continuous.

The import process consumes system resource since this involves video transcoding. Be aware of this if running other resource intensive processes during import.

QuickTime reference files

The following formats are supported as QuickTime reference files:

- DV
- AVC-Intra
- XDCAM-EX
- XDCAM-HD
- XDCAM-HD 422
- IMX
- Avid DNxHD

MPEG interchange specification

This specification applies to MPEG import on K2 Summit, Solo, and SAN systems.

Formats are supported are as follows:

Supported formats		Notes
Video	MPEG-2	Supports import of MPEG-2 program and transport streams. If the transport stream contains multiple programs, the first detected program in the transport stream is imported as a K2 clip.

Supported formats		Notes
	H.264	AVCHD /H.264 is K2 Summit 3G system only. Import only supported.
Audio	48kHz	—
	MPEG-1 (layer 1 & 2)	—
	SMPTE 302M AES3 LPCM	—
	AC-3	—
	AVCHD DVD VOB LPCM	AVCHD /H.264 is K2 Summit 3G system only. Import only supported.
	DVD/VOB AC-3	—
Data	ATSC a/53 captions	For MPEG-2 imports.
	ATSC a/72 captions	For H.264 imports.
	SMPTE RDD-11 ancillary data	—

Interchange mechanisms are supported as follows:

Mechanism		Support
File based	Import	Yes
	Export	No
FTP stream	Import	Yes
	Export	No

Related Topics

Limitations with complex media types on page 292

P2 interchange specification

This specification applies to P2 file transfer, import, and export on K2 Summit, Solo, and SAN systems.

Formats are supported are as follows:

Supported formats		Notes
Video	AVC - LongG	
	AVC-Intra	
	DVCPRO25	

Supported formats		Notes
	DVCPRO50	
	DVCPRO HD	
	DVCAM	
Audio	48 kHz	All audio tracks on the clip being exported have to be of the same type to comply with the P2 file format. For instance, exporting a clip with some PCM 16 audio tracks and others PCM 24 is not supported.
	16 bit, 24 bit PCM	

Interchange mechanisms are supported as follows:

Mechanism		Support	
File based	Import	Yes	Directory structure as specified by P2
	Export	Yes	
FTP stream	Import	Yes	For AVC – LongG MXF file format only
	Export	No	

Related Topics

Limitations with complex media types on page 292

WAV audio interchange specification

This specification applies to WAV import on K2 Summit, Solo, and SAN systems.

Formats are supported are as follows:

Supported formats		Notes
Video	NA	—
Audio	48 kHz	—
	16 bit stereo PCM	
Data	NA	—

Interchange mechanisms are supported as follows:

Mechanism		Support
File based	Import	Yes
	Export	No
FTP stream	Import	No
	Export	No

Media file system performance on K2 systems

This section specifies media operations on K2 systems. On a K2 SAN, these specification are qualified at channel counts up to 48 channels. Performance on larger systems is not tested.

Record-to-play specifications

The following tables specify the minimum length of time supported between recording on one channel and cueing the same clip for playout on another channel. Live play mode is available only on a K2 Summit/Solo system with the AppCenter Pro license. On a K2 SAN, Live play mode is not supported with record-to-play on different K2 clients or on a K2 SAN with Live Production mode not enabled.

Standalone K2 Solo 3G system

Formats	Live play	Normal play
DV	0.5 seconds	6.0 seconds
MPEG-2 I-frame, AVC-Intra	0.75 seconds	6.25 seconds
MPEG-2 long GoP, XDCAM	1.0 seconds	6.50 seconds

Live Play on K2 SAN with Live Production mode enabled

Formats	Record-to play on same K2 Summit System
DV	0.5 seconds
MPEG-2 I-frame, AVC-Intra	0.75 seconds
MPEG-2 long GoP, XDCAM	1.0 seconds

Normal play on K2 SAN with Live Production mode enabled

Formats	Record-to play on same K2 Summit System	Record-to play on different K2 Summit Systems
DV	6.0 seconds	8.0 seconds
MPEG-2 I-frame, AVC-Intra	6.25 seconds	8.25 seconds
MPEG-2 long GoP, XDCAM	6.50 seconds	8.50 seconds

Normal play on K2 SAN with Live Production mode not enabled

Formats	Record-to play on same K2 Summit System	Record-to play on different K2 Summit Systems
All formats	10 seconds	20 seconds

Other media file system specifications

Parameter	Stand-alone K2 Solo 3G system	K2 SAN
Maximum number of clips[18]	20,000	50,000
Maximum length continuous record	24 hours	24 hours
Off-speed play range for audio scrub[19]	-2x to +2x	-1.5x to +1.5x
Off-speed play range for insertion of MPEG user data and/or ancillary data on playout	0 to +1.2	0 to +1.2
Minimum duration between recordings	10 seconds	10 seconds
Minimum duration between start of clip import and clip play	10 seconds	10 seconds

Transition effects formats and limitations

Transition (mix) effects are supported on K2 Solo 3G system as follows.

Transition effects on first generation K2 Solo 3G system

	DV	AVC-Intra	MPEG-2 I-frame	MPEG-2 long GoP
DV	Yes	No	No	No
AVC-Intra	No	Yes	No	No
MPEG-2 I-frame	No	No	Yes	No
MPEG-2 long GoP	No	No	No	No

When adding transitions to all events in a playlist for an on-the-fly (the **Go To** feature) pause or transition, limitations on the time for the length of the transition are as follows:

- 0.5 second or less on first generation K2 Solo 3G system

Transition effects on K2 Summit 3G system

	DV	AVC-Intra	AVCHD/H.264	MPEG-2 I-frame	MPEG-2 long GoP	Avid DNxHD	AVC - LongG
DV	Yes	No	No	No	No	No	No
AVC-Intra	No	Yes	Yes	No	No	No	No
AVCHD/H.264	No	Yes	Yes	No	No	No	No

[18] The maximum number of clips is based on clips with 16 or less audio tracks. Large quantities of clips with more than 16 audio tracks proportionally reduce the maximum number of clips.

[19] Dolby audio tracks muted during off-speed play

MPEG-2 I-frame	No	No	No	Yes	No	No	No
MPEG-2 long GoP	No	No	No	No	Yes	No	No
Avid DNxHD	No	No	No	No	No	Yes	No
AVC - LongG	No	No	No	No	No	No	Yes

When adding transitions to all events in a playlist for an on-the-fly (the **Go To** feature) pause or transition, limitations on the time for the length of the transition are as follows:

- 0.5 second or less on K2 Summit 3G systems

Protocols supported

AMP, VCDP, and BVW protocols are supported.

Transfer compatibility with K2 Summit/Solo

When transferring material between a K2 Summit/Solo and other Grass Valley products, you must consider the specifications of the different products. The following tables illustrate some of these considerations. In these tables, source material is assumed to have been recorded on the source device.

Transfer compatibility with K2 Media Client

Transfer	Material transferred	Compatibility
From K2 Summit/Solo to K2 Media Client	DVCPRO25, DVCPRO50	Playout supported.
	DVCPRO HD	Not supported
	MPEG	Supported
	AVC-intra	Not supported
	H.264	Not supported
	Avid DNxHD	Not supported
From K2 Media Client to K2 Summit/Solo	All types of material supported, according to the SD and/or HD capability.	

Transfer compatibility with Profile XP Media Platform

Transfer	Material transferred	Compatibility
From K2 Summit/Solo to Profile XP Media Platform	DVCPRO25, DVCPRO50	Playout supported.
	DVCPRO HD	Not supported

Transfer	Material transferred	Compatibility
	MPEG-2 HD 4:2:0 80 Mb or less MPEG-2 SD 4:2:2, XDCAM-HD422, XDCAM-EX	Supported. Can be played out.
	MPEG-2 720p MPEG-2 HD 4:2:2 XDCAM-HD HDV 1440x1080	Supported for storage only. Transfer is successful but playout not supported.
	AVC-intra	Not supported
	H.264	Not supported
	Avid DNxHD	Not supported
From Profile XP Media Platform to K2 Summit/Solo	All types of material supported, according to the SD and/or HD capability of the model.	

Data compatibility between K2 Summit/Solo and PVS models

When material is transferred between a PVS Profile XP Media Platform and a K2 Solo 3G system, data is supported as follows:

Transferring from PVS (source) to K2 Summit/Solo with HD license (destination)

Source format	Source data	SD playout data support on destination	HD playout data support on destination
DVCPRO25	Closed captioning	Yes	Yes
	Ancillary data	No	No
DVCPRO50	Closed captioning in compressed VBI	Yes	No
	Ancillary data	Yes	Yes
DVCPRO50	Compressed VBI	Yes	No
SD MPEG-2	Uncompressed VBI	Yes	Yes, with data bridging for CC only. Other VBI lines are discarded.
	Closed captioning	Yes	Yes. Ancillary data packets
	Compressed VBI	Yes	Yes, if enabled
	Ancillary data	Yes	Yes
HD MPEG-2	Ancillary data	Yes	Yes

Transferring from K2 Summit/Solo (source) to PVS (destination)

Source format	Source data	SD playout data support on destination	HD playout data support on destination
DVCPRO25, DVCPRO50	Any supported on K2 Summit/Solo	Yes	NA
DVCPRO HD	Any supported on K2 Summit/Solo	NA	NA
AVC-Intra	Any	NA — AVC-Intra not supported on PVS	
H.264	Any	NA — H.264 not supported on PVS	
Avid DNxHD	Any	NA — Avid DNxHD not supported on PVS	
SD MPEG-2	Any data recorded with Profile compatible setting[20].	All supported	Yes
	Uncompressed VBI and captioning on data track	Not supported. Do not attempt to transfer to PVS.	
	Compressed VBI	Yes	Yes, with data bridging for CC only. Other VBI lines are discarded.
	Uncompressed VBI	Yes	No, except for bridging of CC data, which requires Profile software v5.4.9.
HD MPEG-2	Ancillary data	Yes. CC bridging requires data-bridging SDI board.	Yes.

Control Point PC system requirements

If you are building your own Control Point PC, the machine you choose must meet the following requirements. These requirements assume that the PC is dedicated to its function as the host for Grass Valley product control and configuration applications. You should not run other applications on the PC that could interfere with system performance.

Control Point PC system requirements are as follows:

Requirements	Comments
Operating System	Microsoft Windows (Must be a U.S. version) 64-bit: • Windows 7 • Server 2008 R2
RAM	Minimum 512 MB, 1 GB recommended

[20] When Record ancillary data = No or when Record Uncompressed VBI and captioning data to track = No

Requirements	Comments
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 4.0
Sun Java 2 Runtime Environment	Version 1.5.0_11, Version 1.6.0 or higher. Required for the HP Ethernet Switch configuration interface, which is used for K2 SAN (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.
Quicktime	Version 7 or higher
Acrobat Reader	Version 8 or higher

Find software at Internet locations such as the following:

- http://msdn.microsoft.com/en-us/netframework/default.aspx
- http://java.sun.com/javase/downloads/index.jsp
- http://www.microsoft.com/downloads/details.aspx?FamilyId=3144B72B-B4F2-46DA-B4B6-C5D7485F2B42&displaylang=en
- http://www.apple.com/quicktime/download/
- http://get.adobe.com/reader/

Super Slo-Mo camera formats

Formats specified for output by Super Slo-Mo cameras are supported as follows:

Camera	Format	Frame Rate (Hz)	Speed support
Grass Valley LDK8000 SportElite HD Camera	• 720p • 1080i	• 50/59.94/100/119.88 • 50/59.94/100/119.88	2x;
Grass Valley LDK8300 Camera	• 720p • 1080i	• 50/59.94/100/119.88/150/179.82 • 50/59.94/100/119.88/150/179.82	2x; 3x
Grass Valley LDX HiSpeed Camera	• 720p • 1080i	• 50/59.94/150/179.82 • 50/59.94/150/179.82	3x
Grass Valley LDX XtremeSpeed Camera	• 720p • 1080i • 1080p	• 50/59.94/150/179.82/300/359.64 • 50/59.94/150/ 179.82/300/359.64 • 50/59.94/150/179.82	• 3x in 720p; 1080i; 1080p • 6x in 720p; 1080i
Sony 3300	• 720p • 1080i	• 50/59.94/150/179.82 • 50/59.94/150/179.82	3x

MIB specifications

This section specifies Management Information Base (MIB) information for monitoring K2 devices with the Simple Network Management Protocol (SNMP). The Grass Valley NetCentral product uses this protocol. This information is intended for SNMP developers. MIB files can be obtained from the Grass Valley Developers website.

In addition to the MIBs specified in this section, a K2 device might support other MIBs based on third party software/hardware. To determine whether other MIBs are supported by the operating system or independent hardware/software vendors, perform a “MIB walk” operation on the K2 device using conventional SNMP utilities and determine MIBs supported.

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

K2 client MIBs

Grass Valley MIBs

MIB	Description
gvg-reg.mi2 (GVG-REG)	Grass Valley SMI enterprise namespace

MIB	Description
gvg-element.mi2 (GVG-ELEMENT-MIB)	Common object definitions for a Grass Valley device. • Generic device tracking information • SNMP trap target configuration • Generic IO/signal status information
gvg-prod.mi2 (GVG-PROD-REG)	Product sysObjectOID registrations for the Grass Valley devices
gvg-drs.mi2 (GVG-DRS-MIB)	Video disk recorder/server status information
gvg-tcm.mi2 (GVG-TCM-MIB)	Media transfer (import/export) statistical information
gvg-manclient.mi2 (GVG-MANCLIENT-MIB)	SAN client status information. Available only when the K2 client is connected to a SAN.

Other MIBs

MIB	Description
RFC1213-MIB.mib (RFC1213-MIB)	MIB-2 support as implemented by Microsoft for the Windows operating system.
hostmib.mib (HOST-RESOURCES-MIB)	Generic system information as implemented by Microsoft for the Windows operating system
lmmib2.mib (LanMgr-Mib-II-MIB)	Generic Windows networking, user account and service information as implemented by Microsoft for the Windows operating system
SUPERMICRO-SMI.my (SUPERMICRO-SMI)	Motherboard electromechanical sensor information (motherboard temperature hotspots, CPU fan, voltages, etc.)
SUPERMICRO-HEALTH-MIB.my (SUPERMICRO-HEALTH-MIB)	
MEGARAID.mib (RAID-Adapter-MIB)	Internal RAID-1 SCSI drive and controller information

K2 Media Server MIBs

Grass Valley MIBs

MIB	Description
gvg-reg.mi2 (GVG-REG)	Grass Valley SMI enterprise namespace
gvg-element.mi2 (GVG-ELEMENT-MIB)	Common object definitions for a Grass Valley device. • Generic device tracking information • SNMP trap target configuration
gvg-prod.mi2 (GVG-PROD-REG)	Product sysObjectOID registrations for the Grass Valley devices
gvg-ssr.mi2 (GVG-SSR-MIB)	K2 Storage roles configured for the server by the K2 System Configuration application and their status information
gvg-sbs.mi2 (GVG-SBS-MIB)	K2 iSCSI Bridge and TOE (TCP Offload Engine) related status information. Available only if the K2 Media Server has the iSCSI Bridge role.
gvg-manfsm.mi2 (GVG-MANFSM-MIB)	Video File System and Clip Database (FSM) related status information. Available only if the K2 Media Server has role(s) of media file system server and/or database server.
gvg-tcm.mi2 (GVG-TCM-MIB)	Media transfer (import/export) statistical information. Available only if the K2 Media Server is configured to be a transfer/FTP/hotbins server.
gvg-manclient.mi2 (GVG-MANCLIENT-MIB)	SAN client status information. Available only when the K2 Media Server is a media system and/or database client. For example, if the K2 Media Server has the role of FTP server only, then it must be a media file system/database client to another K2 Media Server that is the media file system/database server.

Other MIBs

MIB	Description
RFC1213-MIB.mib (RFC1213-MIB)	MIB-2 support as implemented by Microsoft for the Windows operating system.
hostmib.mib (HOST-RESOURCES-MIB)	Generic system information as implemented by Microsoft for the Windows operating system

MIB	Description
lmmib2.mib (LanMgr-Mib-II-MIB)	Generic Windows networking, user account and service information as implemented by Microsoft for the Windows operating system
mssql.mib (MSSQLSERVER-MIB)	Microsoft SQL Server information
10892.mib (MIB-Dell-10892)	Dell PowerEdge chassis related electro-mechanical status information
arymgr.mib (ArrayManager-MIB)	Dell RAID1 system disk (PERC) and controller information

K2 Appliance (Generic Windows computer based) MIBs

For details on the hardware/chassis running the K2 Appliance, check the chassis vendor's MIBs.

Grass Valley MIBs

MIB	Description
gvg-reg.mi2 (GVG-REG)	Grass Valley SMI enterprise namespace
gvg-element.mi2 (GVG-ELEMENT-MIB)	Common object definitions for a Grass Valley device. • Generic device tracking information • SNMP trap target configuration
gvg-prod.mi2 (GVG-PROD-REG)	Product sysObjectOID registrations for the Grass Valley devices
gvg-ssr.mi2 (GVG-SSR-MIB)	K2 Storage roles configured for the server by the K2 System Configuration application and their status information
gvg-tcm.mi2 (GVG-TCM-MIB)	Media transfer (import/export) statistical information. Available only if the K2 Media Server is configured to be a transfer/FTP/hotbins server.
gvg-manclient.mi2 (GVG-MANCLIENT-MIB)	SAN client status information. Available only when the K2 appliance is a media system and/or database client.

Other MIBs

MIB	Description
RFC1213-MIB.mib (RFC1213-MIB)	MIB-2 support as implemented by Microsoft for the Windows operating system.
hostmib.mib (HOST-RESOURCES-MIB)	Generic system information as implemented by Microsoft for the Windows operating system
lmmib2.mib (LanMgr-Mib-II-MIB)	Generic Windows networking, user account and service information as implemented by Microsoft for the Windows operating system

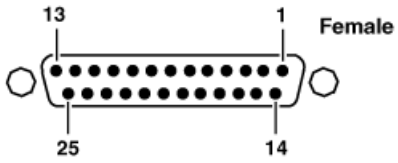
Connector pinouts

K2 Solo 3G system connector pinouts

The following sections describe K2 Solo 3G system rear panel connector pinouts.

AES Audio

Pinouts for each channel's AES Audio DB25 connector are as follows:



Pin #	Signal	Description
1	IN_P<0>	Channel Input 1&2 positive
2	IN_P<1>	Channel Input 3&4 positive
3	IN_P<2>	Channel Input 5&6 positive
4	IN_P<3>	Channel Input 7&8 positive
5	OUT_P<0>	Channel Output 1&2 positive
6	OUT_P<1>	Channel Output 3&4 positive
7	OUT_P<2>	Channel Output 5&6 positive
8	OUT_P<3>	Channel Output 7&8 positive
9	NO_C	NO_C
10	GND	GND

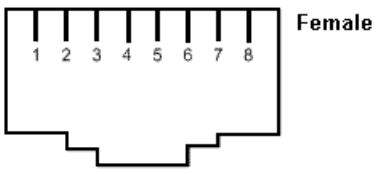
Pin #	Signal	Description
11	NO_C	NO_C
12	GND	GND
13	GND	GND
14	IN_N<0>	Channel Input 1&2 negative
15	IN_N<1>	Channel Input 3&4 negative
16	IN_N<2>	Channel Input 5&6 negative
17	IN_N<3>	Channel Input 7&8 negative
18	OUT_N<0>	Channel Output 1&2 negative
19	OUT_N<1>	Channel Output 3&4 negative
20	OUT_N<2>	Channel Output 5&6 negative
21	OUT_N<3>	Channel Output 7&8 negative
22-25	GND	GND

The optional audio cable has connections as follows:

RS-422 connector pinouts K2 Summit 3G

The K2 Summit 3G Production Client RS-422 interface conforms to ANSI/SMPTE 207M-1997 standard (SMPTE 422).

Pinouts for the individual RJ45 connectors are as follows:



Pin #	Signal	Description
1	+TXD	Differential Transmit Data (high) (out TXB)
2	-TXD	Differential Transmit Data (low) (out TXA)
3	+RXD	Differential Receive Data (high) (in RXB)

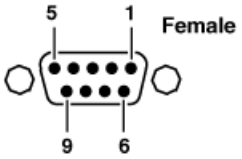
Pin #	Signal	Description
4	GND	Signal Ground
5	GND	Signal Ground
6	-RXD	Differential Receive Data (low) (in RXA)
7	GND	Signal Ground
8	GND	Signal Ground

Balanced signals are placed on twisted wire pairs within a standard CAT5 or CAT3 cable.

RS-422 connector pinouts first generation K2 Solo 3G system

The first generation K2 Solo 3G system RS-422 interface conforms to ANSI/SMPTE 207M-1997 standard (SMPTE 422).

Pinouts for the individual DB9 connectors are as follows:

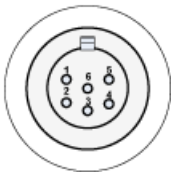


Pin #	Signal	Description
1	GND	Frame Ground
2	-TXD	Differential Transmit Data (low)
3	+RXD	Differential Receive Data (high)
4	GND	Transmit Signal Common
5	NC	Spare
6	GND	Receive Signal Common
7	+TXD	Differential Transmit Data (high)
8	-RXD	Differential Receive Data (low)
9	GND	Signal Ground

LTC connectors pinouts

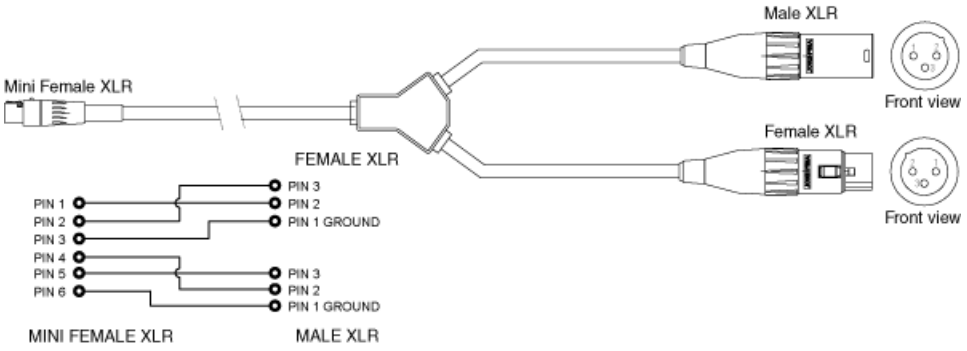
The K2 Solo 3G system LTC panel connector provides balanced linear timecode input and output connections. The interface conforms to SMTPE 12M Linear Timecode.

On the K2 Solo 3G system there is one 6 pin Switchcraft TRA6M Mini-XLR male connector for each channel. Pinouts are as follows:

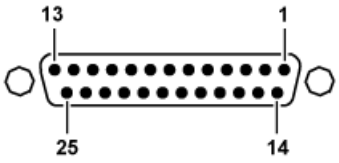


Pin #	Signal	Description
1	IN_P<0>	
2	IN_N<0>	
3	GND	Frame Ground
4	OUT_P<0>	
5	OUT_N<0>	
6	GND	Frame Ground

The mini-XLR to XLR LTC cable has connections as follows:



GPI I/O connector pinouts



Pin	Signal
1	Output 1
2	Output 2
3	Output 3

Pin	Signal
4	Output 4
5	Output 5
6	Output 6
7	Output 7
8	Output 8
9	Output 9
10	Output 10
11	Output 11
12	Output 12
13	Ground
14	Input 1
15	Input 2
16	Input 3
17	Input 4
18	Input 5
19	Input 6
20	Input 7
21	Input 8
22	Input 9
23	Input 10
24	Input 11
25	Input 12

K2 Media Server connector pinouts

The following sections describe K2 Media Server rear panel connector pinouts.

Redundant server heartbeat serial cable

Take care to use the proper serial cable to interconnect redundant K2 Media Servers that take the role of file system/database servers. This cable supports the heartbeat mechanism whereby the servers monitor each other's health. It is a 9 pin serial cable, but it is not a standard RS-232 null modem cable. The heartbeat cable is supplied with your system (Grass Valley part number 174-8137-00) and has a pin configuration as follows:

1 – 4

2 – 3

3 – 2

4 – 1&6

5 – 5

6 – 4

7 – 8

8 – 7

9 – No Connect

Rack mounting

Rack-mount considerations

When planning the placement of equipment in your equipment rack, bear in mind the following:

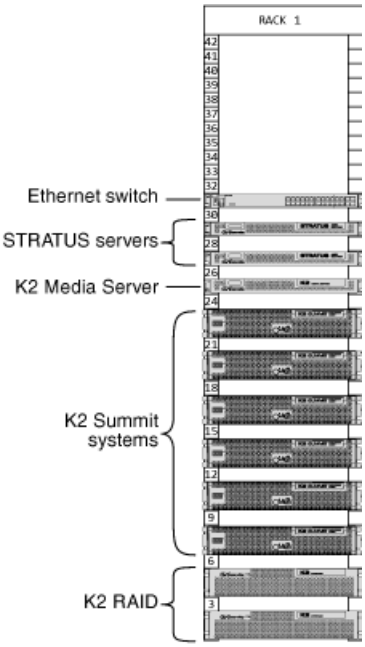
- Ensure adequate air flow around the chassis to provide sufficient cooling. Operating ambient temperature will affect the amount of air circulation required to keep the K2 system within its temperature limitations.
- Ensure that safety labels located on the top of the unit are visible after installation. This requires sufficient open space over the unit without cables or other devices impeding the view.
- If the system is installed with its ventilation intakes near another system's exhaust or in a closed or multi-unit rack assembly, the operating ambient temperature inside the chassis may be greater than the room's ambient temperature. Install the system in an environment compatible with this recommended maximum ambient temperature.
- Ensure that the power socket-outlet is installed near the equipment and is easily accessible.
- Ensure the rack is anchored to the floor so that it cannot tip over when the K2 system is extended out of the rack.
- Be sure to mount the K2 system in a way that ensures even weight distribution in the rack. Uneven mechanical loading can result in a hazardous condition. Secure all mounting bolts when installing the chassis to the rack.

The following sections describe installing the K2 Summit Production Client step-by-step. For the K2 Solo Media Server, refer to *K2 Solo Media Server Accessories Installation Instructions* that you received with the rack kit.

Rack-mount devices

All systems require this process.

Follow the instructions you received with the rack-mount hardware to install each component of the system. One rack-unit spacing is recommended between components for ventilation. The recommended arrangement of devices is as follows:



HP ProCurve Switch Rack specifications

Use the following specifications to determine load, spacing, power, and other factors when planning system racks.

Table 16: Mechanical specifications

Characteristic	Specification
Cabinet Type	Rack-mount
Rack units	1
External Dimensions	443 (w) x 44 (h) x 392 (d) mm
Weight	Maximum 7 kg

Table 17: Power specifications

Characteristic	Specification
Type	100-127 VAC/200-240 VAC; 50/60 Hz
Power Consumption	4.0/2.0 A, 200W

Dell R620 Rack specifications

Use the following specifications to determine load, spacing, power, and other factors when planning system racks.

Table 18: Mechanical specifications

Characteristic	Specification
Cabinet Type	Rack-mount
Rack units	1
External Dimensions	482.4 (w) x 42.8 (h) x 683.7 (d) mm
Weight	Maximum 18.6kg , 40.96 lbs

Table 19: Power specifications

Specification	1100W DC	1100W AC	750W AC	495W AC
Current consumption	32A	12A-6.5A	10A-5A	6.5A-3A
Supply voltage	-48V to -60V DC	100-240VAC	100-240VAC	100-240VAC
Frequency	N/A	50/60Hz	50/60Hz	50/60Hz
Heat dissipation (BTU/hr max)	4416	4100	2843	1908
Maximum inrush current	55A	55A	55A	55A

K2 Summit 3G Rack specifications

Use the following specifications to determine load, spacing, power, and other factors when planning system racks. These specifications apply to K2 Summit 3G chassis.

Table 20: Mechanical specifications

Characteristic	Specification
Cabinet Type	Rack-mount
Rack units	2
External Dimensions	447 x 617 x 89 mm
Weight	25.0 kg maximum

Table 21: Power specifications

Characteristic	Specification
Power conditions	Dual, redundant
Mains Input Voltage	90 to 260V auto-range, 47-63Hz

Characteristic	Specification
Maximum power consumption (when operating in a 25° C environment)	450W typical (standalone) 390W typical (SAN client) Maximum AC current 8A @ 115VAC, 4A @ 230VAC

K2 RAID Rack specifications

Use the following specifications to determine load, spacing, power, and other factors when planning system racks. These specifications apply to K2 10Gv2 RAID (M100) chassis.

Table 22: Mechanical specifications

Characteristic	Primary chassis	Expansion chassis
Cabinet Type	Rack-mount	Rack-mount
Rack units	2	2
External Dimensions	482 x 513.2 x 87.8 mm (no front bezel)	482 x 513.2 x 87.8 mm (no front bezel)
Weight	31 kg maximum	29 kg maximum

Table 23: Power specifications

Characteristic	Primary chassis	Primary chassis
Power conditions	100 to 240 VAC, single-phase 50/60 Hz	100 to 240 VAC, single-phase 50/60 Hz
Maximum power consumption (when operating in a 25° C environment)	400 W	290 W

FT Server Rack specifications

Use the following specifications to determine load, spacing, power, and other factors when planning system racks.

Table 24: Mechanical specifications

Characteristic	Type I and Type II Specification
Cabinet Type	Rack-mount
Rack units	4
External Dimensions	483 (w) x 178 (h) x 736 (d) mm, 19.0 in. (w) x 7.0 in. (h) x 28.9 in. (d)

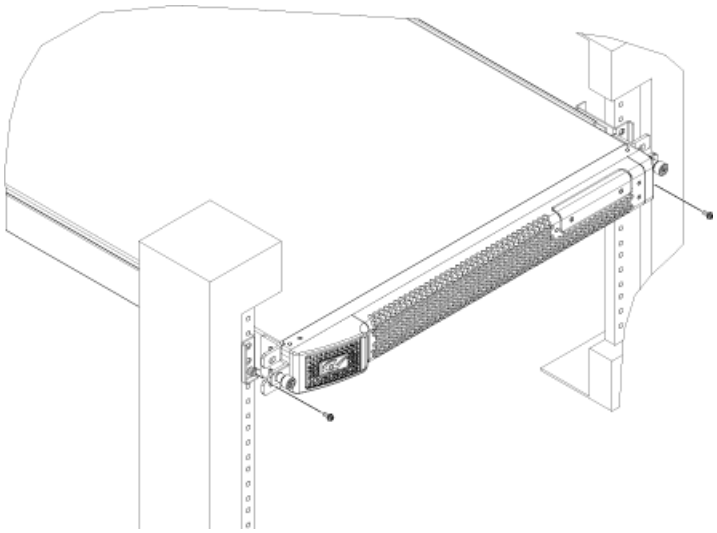
Characteristic	Type I and Type II Specification
Rack clearance	40 cm or more on top, 1 m or more on the front and rear, 60 cm or more on the right and left.
Weight	Maximum 51.5kg , 113.3 lbs

Table 25: Power specifications

Power Supply	Type I Specifications	Type II Specifications
Type	AC 100V-240V +/- 10%, 50/60Hz +/- 3Hz	AC 100V-240V +/- 10%, 50/60Hz +/- 3Hz
Power Consumption	1400VA, 1390W	1300VA, 1290W

Securing a server to a rack

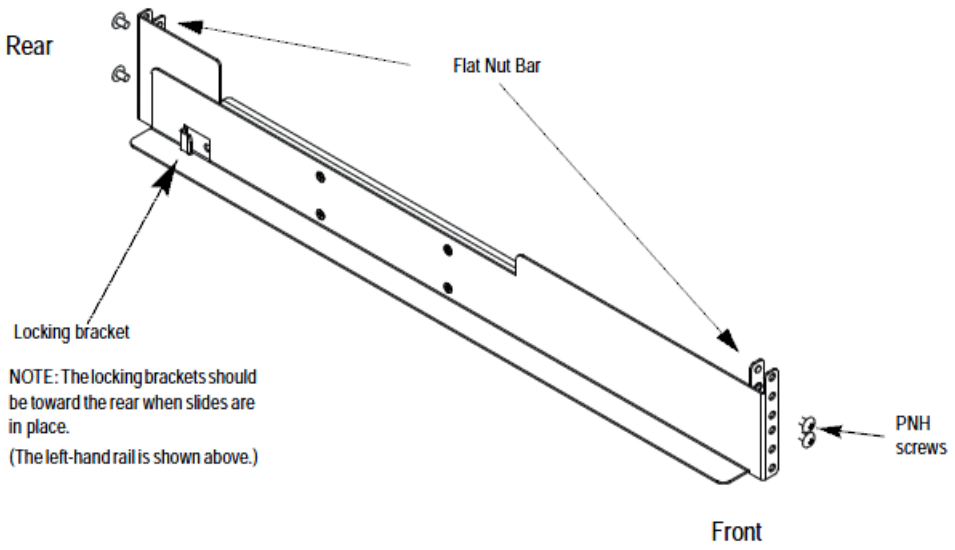
If the server is a Dell server, follow the instructions provided in the shipping box to install the rack rails and position the server in the rack. For the Dell 1RU PowerEdge Server, follow the illustration below to secure the system to the rack.



Install a screw in the bottom hole of the bracket on each side. Do not attempt to install a screw in the top hole of the bracket.

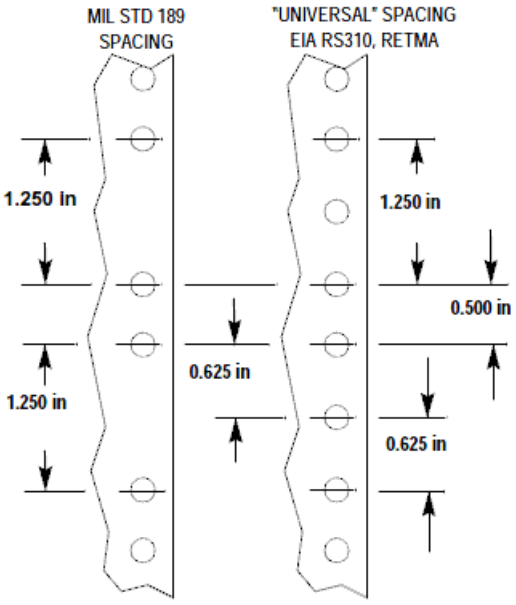
Rack mount hardware shipped with the K2 system

Your K2 system rack mount kit comes with rack mounting hardware as shown.

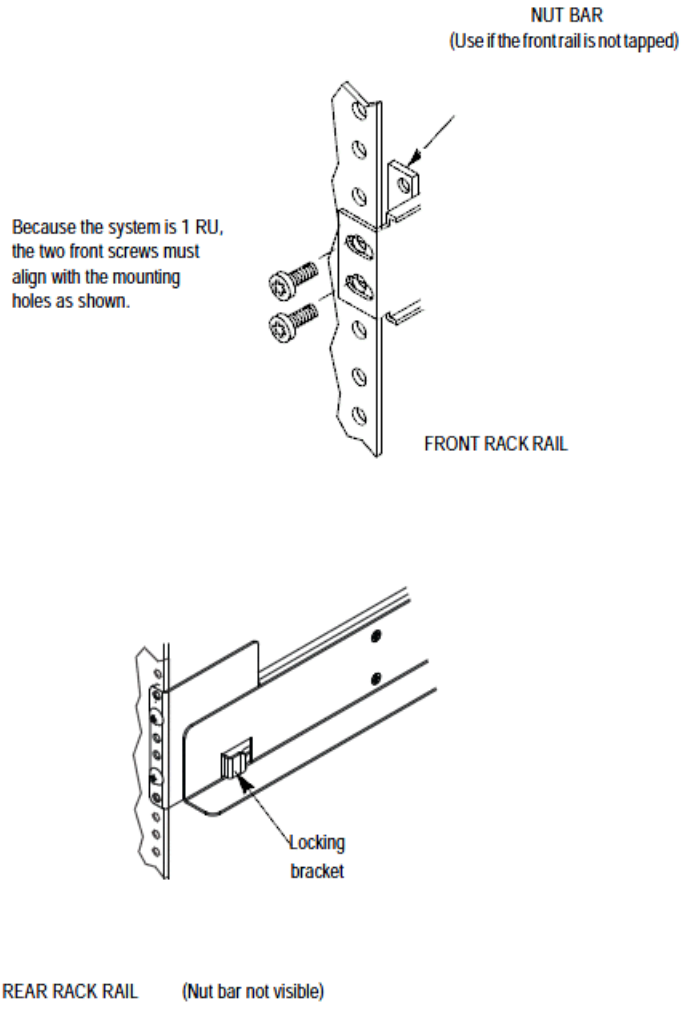


Mounting the Rack Slides

Choose the proper set of rail mounting holes on the rack. Notice that the hole spacing can vary with the rack type. When mounting the slides in racks with EIA spacing, make sure that the slides are attached to the 0.5-inch spaced holes.



Front and rear rack rail mounting hardware is provided with the rack mount kit. Mount the rails using the enclosed hardware. Make sure the stationary sections are horizontally aligned and are level, as well as parallel to each other.



Installing the K2 system on the rack mount rails

1. Pull the slide-out track section to the fully extended position.

   ⚠ ***WARNING: To prevent injury, two people are required to lift the K2 system. It is too heavy for one person to install in the rack.***

   ⚠ ***WARNING: To prevent serious injury, ensure that the rack is anchored to the floor so that it cannot tip over when the K2 system is extended out of the rack.***

2. Push the chassis toward the rack until the chassis sections meet the locking bracket.
3. Verify the cabinet is pushed fully into the rack.
4. Insert and tighten the front panel retaining screws as shown in the previous diagram.

Making Rack Slide Adjustments

After installation, binding may occur if the slide tracks are not properly adjusted. To adjust the tracks:

1. Slide the chassis out approximately 10 inches.
2. Slightly loosen the mounting screws holding the tracks to the front of the rails and allow the tracks to seek an unbound position.
3. Tighten the mounting screws and check the tracks for smooth operation by sliding the chassis in and out of the rack several times.
4. Tighten the front panel retaining screws once the cabinet is in place within the rack to complete the installation.

Cabling K2 Storage

Start with the K2 storage system diagram

To follow cabling instructions

The K2 10Gv2 SAN, and its K2 10Gv2 RAID storage, is documented in this manual. The K2 10Gv2 SAN is defined as follows: The K2 SAN with 8 Gig Fibre Channel and 10 Gig iSCSI connections. Includes support for 2.5 inch drives and large capacity drives. Introduced in late 2012. The K2 10Gv2 SAN requires K2 software version 9.0 and higher. Some devices and/or systems used with older K2 SANs are not compatible with the K2 10Gv2 SAN. Consult the "About This Release" section of the K2 Topic Library for compatibility information.

To follow cabling instructions for your K2™ Storage Area Network (SAN) or direct-connect storage K2 Solo 3G system, do the following:

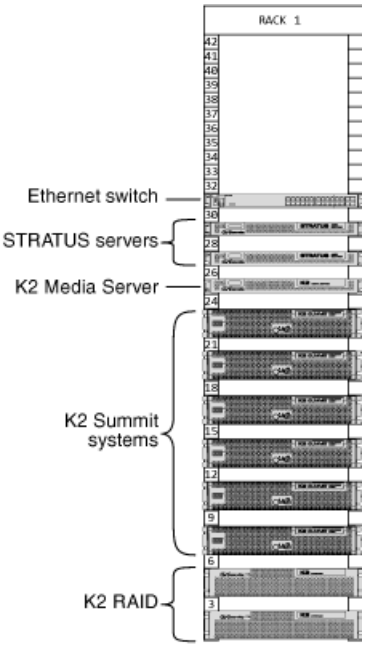
1. Find the system cabling diagram that matches your K2 system.
2. Follow the references below the system diagram to locate cabling instructions for the individual devices of your K2 system.

Refer to the the "Installing and Servicing the K2 SAN" section of the K2 Topic Library for more information on K2 SANs and devices. Refer to the the "Configuring the K2 System" section of this Topic Library for more information on direct-connect K2 client storage.

Rack-mount devices

All systems require this process.

Follow the instructions you received with the rack-mount hardware to install each component of the system. One rack-unit spacing is recommended between components for ventilation. The recommended arrangement of devices is as follows:



HP ProCurve Switch Rack specifications

Use the following specifications to determine load, spacing, power, and other factors when planning system racks.

Table 26: Mechanical specifications

Characteristic	Specification
Cabinet Type	Rack-mount
Rack units	1
External Dimensions	443 (w) x 44 (h) x 392 (d) mm
Weight	Maximum 7 kg

Table 27: Power specifications

Characteristic	Specification
Type	100-127 VAC/200-240 VAC; 50/60 Hz
Power Consumption	4.0/2.0 A, 200W

Dell R620 Rack specifications

Use the following specifications to determine load, spacing, power, and other factors when planning system racks.

Table 28: Mechanical specifications

Characteristic	Specification
Cabinet Type	Rack-mount
Rack units	1
External Dimensions	482.4 (w) x 42.8 (h) x 683.7 (d) mm
Weight	Maximum 18.6kg , 40.96 lbs

Table 29: Power specifications

Specification	1100W DC	1100W AC	750W AC	495W AC
Current consumption	32A	12A-6.5A	10A-5A	6.5A-3A
Supply voltage	-48V to -60V DC	100-240VAC	100-240VAC	100-240VAC
Frequency	N/A	50/60Hz	50/60Hz	50/60Hz
Heat dissipation (BTU/hr max)	4416	4100	2843	1908
Maximum inrush current	55A	55A	55A	55A

K2 Summit 3G Rack specifications

Use the following specifications to determine load, spacing, power, and other factors when planning system racks. These specifications apply to K2 Summit 3G chassis.

Table 30: Mechanical specifications

Characteristic	Specification
Cabinet Type	Rack-mount
Rack units	2
External Dimensions	447 x 617 x 89 mm
Weight	25.0 kg maximum

Table 31: Power specifications

Characteristic	Specification
Power conditions	Dual, redundant
Mains Input Voltage	90 to 260V auto-range, 47-63Hz

Characteristic	Specification
Maximum power consumption (when operating in a 25° C environment)	450W typical (standalone) 390W typical (SAN client) Maximum AC current 8A @ 115VAC, 4A @ 230VAC

K2 RAID Rack specifications

Use the following specifications to determine load, spacing, power, and other factors when planning system racks. These specifications apply to K2 10Gv2 RAID (M100) chassis.

Table 32: Mechanical specifications

Characteristic	Primary chassis	Expansion chassis
Cabinet Type	Rack-mount	Rack-mount
Rack units	2	2
External Dimensions	482 x 513.2 x 87.8 mm (no front bezel)	482 x 513.2 x 87.8 mm (no front bezel)
Weight	31 kg maximum	29 kg maximum

Table 33: Power specifications

Characteristic	Primary chassis	Primary chassis
Power conditions	100 to 240 VAC, single-phase 50/60 Hz	100 to 240 VAC, single-phase 50/60 Hz
Maximum power consumption (when operating in a 25° C environment)	400 W	290 W

FT Server Rack specifications

Use the following specifications to determine load, spacing, power, and other factors when planning system racks.

Table 34: Mechanical specifications

Characteristic	Type I and Type II Specification
Cabinet Type	Rack-mount
Rack units	4
External Dimensions	483 (w) x 178 (h) x 736 (d) mm, 19.0 in. (w) x 7.0 in. (h) x 28.9 in. (d)

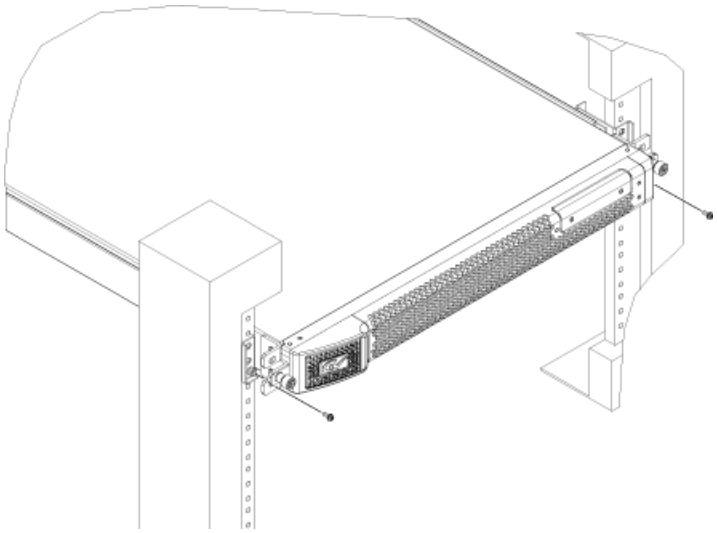
Characteristic	Type I and Type II Specification
Rack clearance	40 cm or more on top, 1 m or more on the front and rear, 60 cm or more on the right and left.
Weight	Maximum 51.5kg , 113.3 lbs

Table 35: Power specifications

Power Supply	Type I Specifications	Type II Specifications
Type	AC 100V-240V +/- 10%, 50/60Hz +/- 3Hz	AC 100V-240V +/- 10%, 50/60Hz +/- 3Hz
Power Consumption	1400VA, 1390W	1300VA, 1290W

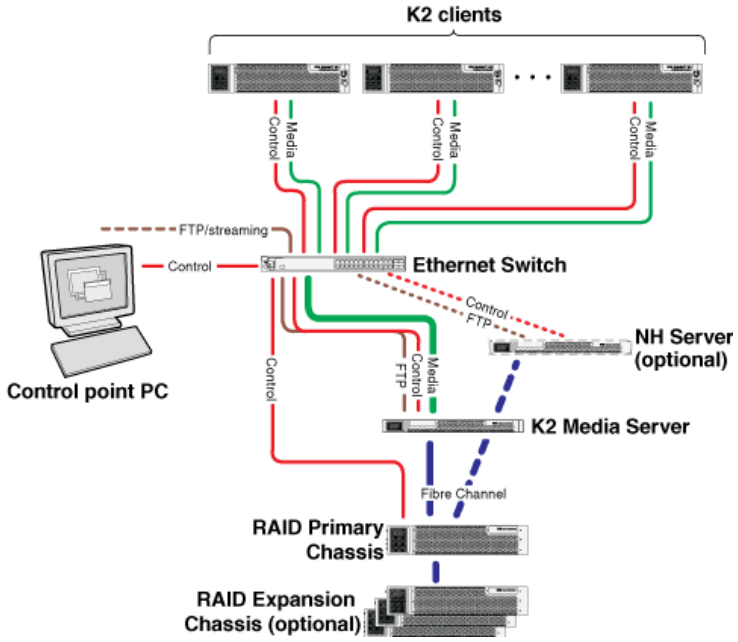
Securing a server to a rack

If the server is a Dell server, follow the instructions provided in the shipping box to install the rack rails and position the server in the rack. For the Dell 1RU PowerEdge Server, follow the illustration below to secure the system to the rack.



Install a screw in the bottom hole of the bracket on each side. Do not attempt to install a screw in the top hole of the bracket.

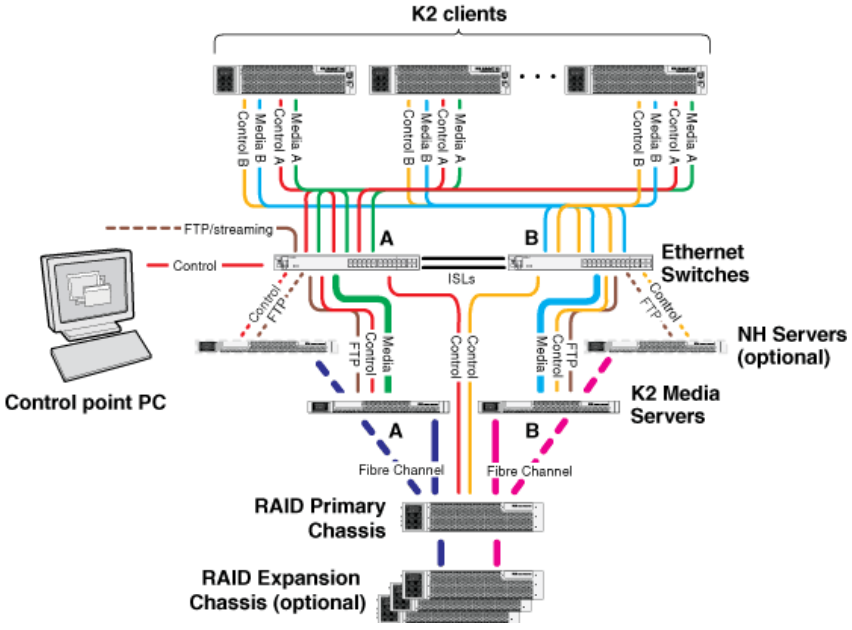
Basic K2 SAN - Online or Production



To cable this K2 SAN device…	Of this model or platform…	Turn to these instructions:
K2 Solo 3G system	K2 Summit 3G system or first generation K2 Summit system	*K2-XDP basic* on page 477
Gigabit Ethernet Switch	HP 29xx	*K2-SWE basic online/production* on page 479
K2 Media Server	Dell R620	*K2-SVR basic Dell R620* on page 483
NH10GE K2 Media Server (optional)	Dell R620	*K2-SVR-NH10GE online/production Dell R620* on page 484
K2 RAID	K2 RAID	*K2 RAID basic online/production* on page 486

This manual documents the default GigE switch configuration. Other configurations are available, depending on your port count and FTP bandwidth requirements.

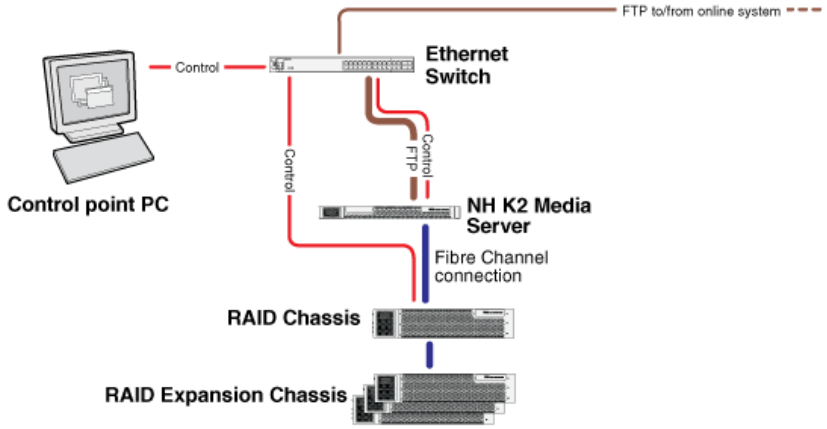
Redundant K2 SAN - Online or Production



To cable this K2 SAN device…	Of this model or platform…	Turn to these instructions:
K2 Solo 3G system	K2 Summit 3G system or first generation K2 Summit system	*K2-XDP redundant* on page 478
Gigabit Ethernet Switch	HP 29xx	*K2-SWE redundant online/production* on page 480
K2 Media Server	Dell R620	*K2-SVR redundant Dell R620* on page 483
NH10GE K2 Media Server (optional)	Dell R620	*K2-SVR-NH10GE online/production Dell R620* on page 484
K2 RAID	K2 RAID	*K2 RAID redundant online/production* on page 486

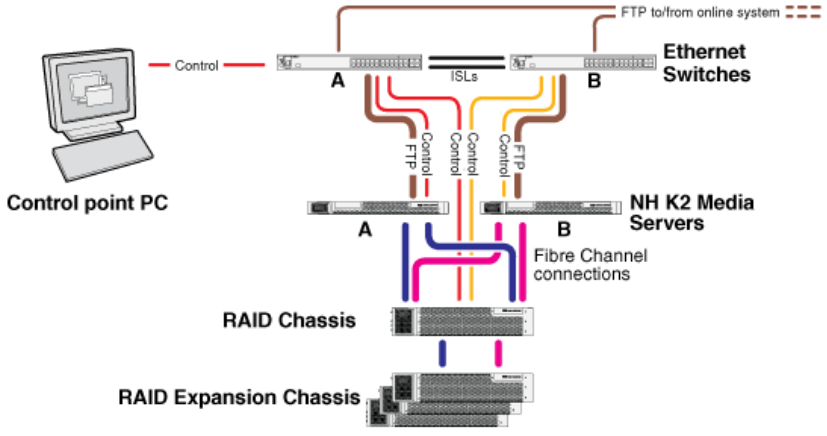
This manual documents the default GigE switch configuration. Other configurations are available, depending on your port count and FTP bandwidth requirements.

Basic Nearline K2 SAN



To cable this K2 SAN device…	Of this model or platform…	Turn to these instructions:
Gigabit Ethernet Switch	HP 29xx	*K2-SWE basic nearline* on page 481
NH10GE K2 Media Server	Dell R620	*K2-SVR-NH10GE basic nearline Dell R620* on page 485
K2 RAID	K2 RAID	*K2 RAID basic nearline* on page 487

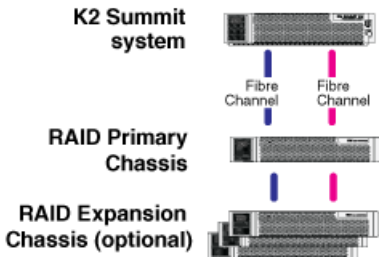
Redundant Nearline K2 SAN



To cable this K2 SAN device…	Of this model or platform…	Turn to these instructions:
Gigabit Ethernet Switch	HP 29xx	*K2-SWE redundant nearline* on page 481
NH10GE K2 Media Server	Dell R620	*K2-SVR-NH10GE redundant nearline Dell R620* on page 485

To cable this K2 SAN device…	Of this model or platform…	Turn to these instructions:
K2 RAID	K2 RAID	*K2 RAID redundant nearline* on page 488

K2 client with direct-connect storage



To cable this K2 device…	Of this model or platform…	Turn to these instructions:
K2 Solo 3G system	K2 Summit 3G system or first generation K2 Summit system	*XDP/XDT direct-connect storage* on page 478
K2 RAID	K2 RAID	*K2 RAID direct-connect* on page 488

Cable K2 devices

Cable K2 Summit system

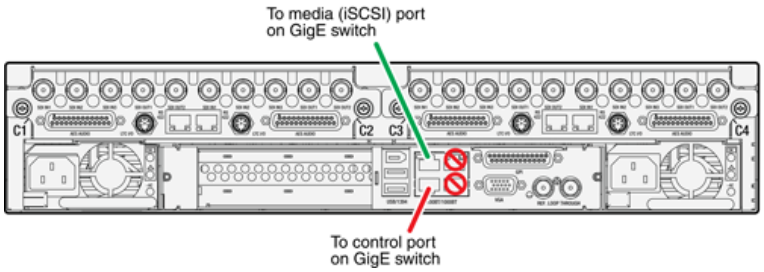
As directed by the system diagram for your K2 storage, cable the K2 Summit system using the instructions in this section.

K2-XDP basic

These cabling instructions apply to the following:

- K2 Summit 3G system or first generation K2 Summit system on a basic (non-redundant) online or production K2 SAN

Refer to "K2 Summit Production Client Quick Start Guide" for additional cabling details.

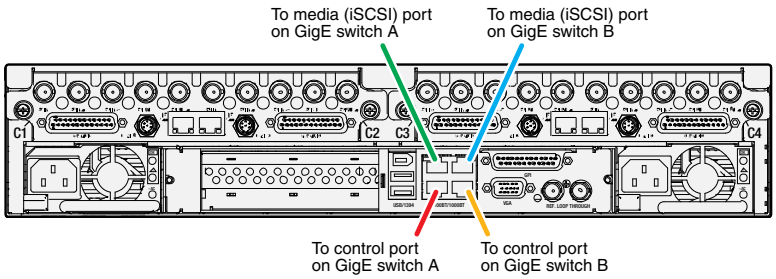


K2-XDP redundant

These cabling instructions apply to the following:

- K2 Summit 3G system or first generation K2 Summit system on a redundant online or production K2 SAN

Refer to "K2 Summit Production Client Quick Start Guide" for additional cabling details.



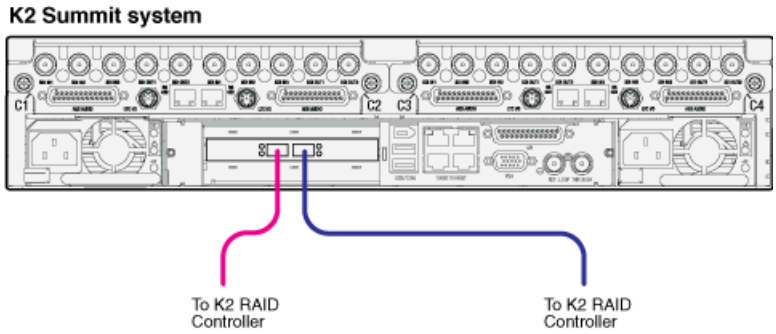
XDP/XDT direct-connect storage

These cabling instructions apply to the following:

- K2 Summit 3G system, first generation K2 Summit system, or K2 Summit Transmission Client with direct-connect K2 RAID storage.

Refer to related topics in the "Configuring the K2 System" section of this Topic Library for additional information about direct-connect storage.

Refer to "K2 Summit Production Client Quick Start Guide" for additional cabling details.



Cable Ethernet switch

As directed by the system diagram for your storage system, cable the switch or switches for your system using the instructions in this section.

These instructions are for the HP ProCurve switch 29xx series.

If a different brand of switch, such as a Cisco Catalyst switch, is required by your site, apply the information in the following procedures accordingly. Refer to the documentation you received with the switch as necessary.

Install the switch in its permanent location. When installing in a video equipment rack, use 10-32 screws. Do not use HP's 12-24 screws, as they can cause thread damage.

Provide power to the switch.

Ethernet cable requirements

For making Ethernet connections, cabling must meet the following requirements:

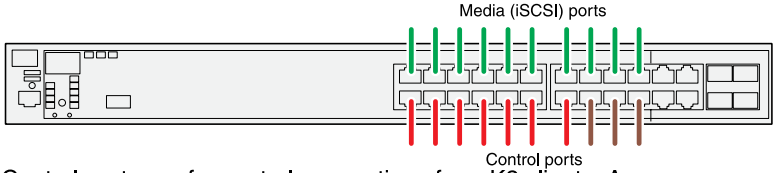
- Use CAT5e or CAT6 cables. The maximum cable length is 50 meters for CAT5e and 100 meters for CAT6.

K2-SWE basic online/production

These cabling instructions apply to the following:

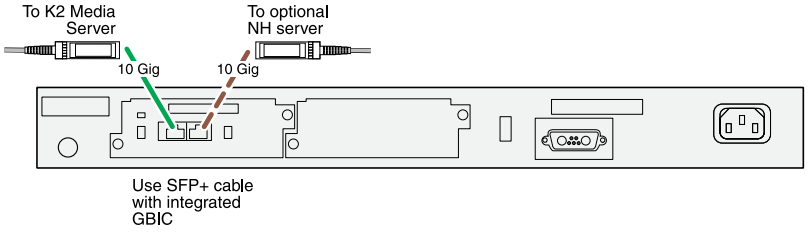
- HP 29xx series Gigabit Ethernet switch on a basic (non-redundant) online or production K2 SAN.

Front view



Control ports are for control connections from K2 clients, Aurora products, automation, etc., as well as FTP connections from Grass Valley and 3rd party systems.

Rear view

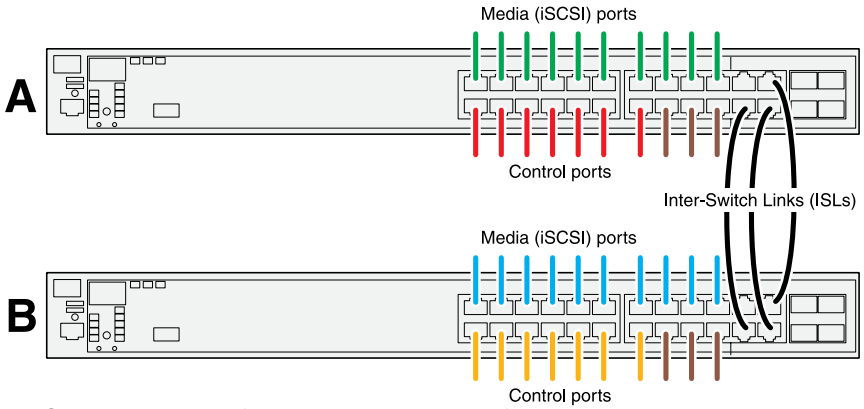


K2-SWE redundant online/production

These cabling instructions apply to the following:

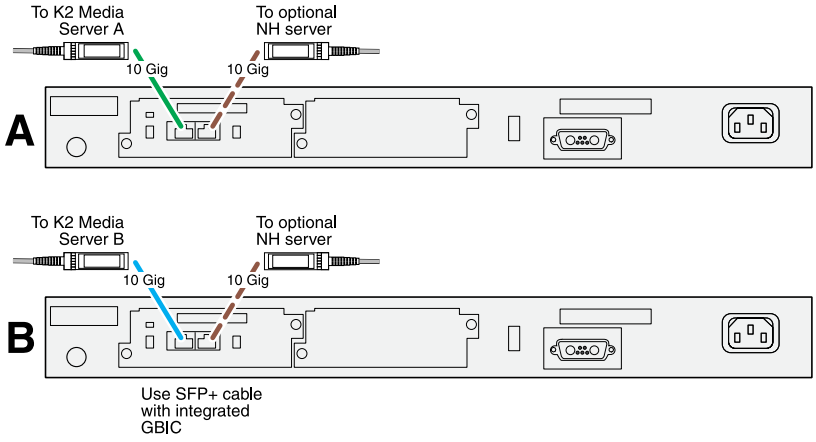
- HP 29xx series Gigabit Ethernet switch on a redundant online or production K2 SAN.

Front view



Control ports are for control connections from K2 clients, Aurora products, automation, etc., as well as FTP connections from Grass Valley and 3rd party systems.

Rear view



If you have other iSCSI clients, such as GV STRATUS high-resolution clients, that have just one iSCSI connection and one control connection, approximately half of the clients should be connected to switch A and half of the clients should be connected to switch B. In a failover event, only the clients connected to one of the switches will remain operational, so make connections accordingly. Connect the client's iSCSI connection to one of the media ports on a switch and the client's control connection to one of the control ports on the same switch.

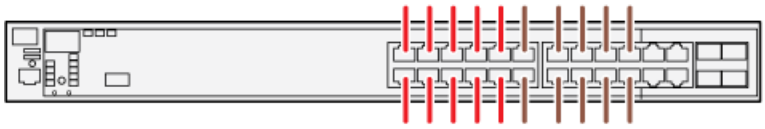
If you have more than one optional NH10GE K2 Media Servers, balance servers between switch A and switch B.

K2-SWE basic nearline

These cabling instructions apply to the following:

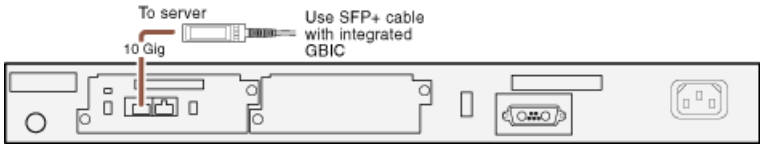
- HP 29xx series Gigabit Ethernet switch on a nearline K2 SAN with one NH K2 Media Server.

Front view



Ports are for control connections as well as FTP connections from Grass Valley and 3rd party systems.

Rear view

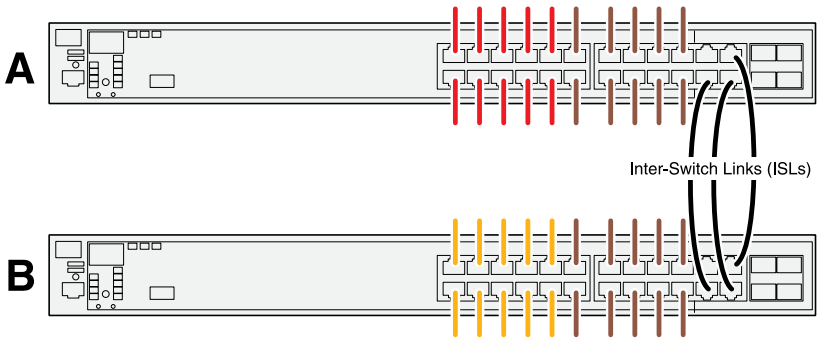


K2-SWE redundant nearline

These cabling instructions apply to the following:

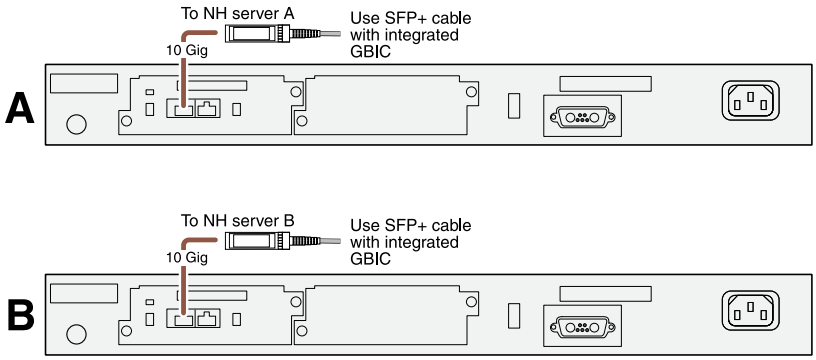
- HP 29xx series Gigabit Ethernet switch on a nearline K2 SAN.

Front view



Ports are for control connections as well as FTP connections from Grass Valley and 3rd party systems.

Rear view

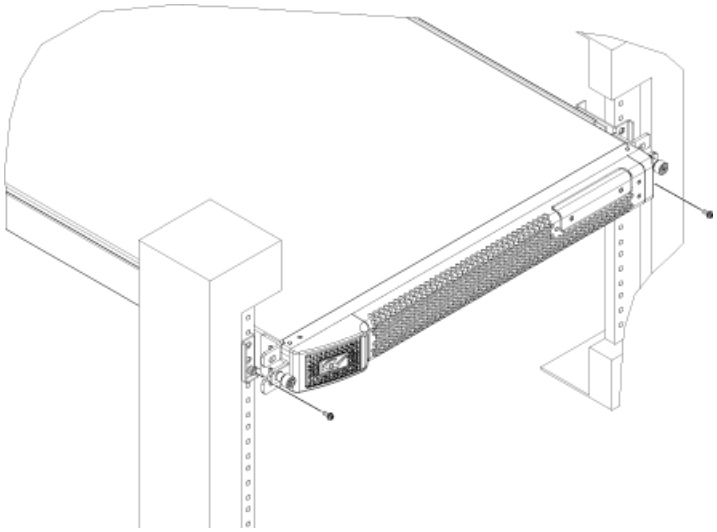


Cable K2 Media Server

As directed by the system diagram for your K2 SAN, cable the K2 Media Server or Servers for your K2 SAN using the instructions in this section.

Securing a server to a rack

If the server is a Dell server, follow the instructions provided in the shipping box to install the rack rails and position the server in the rack. For the Dell 1RU PowerEdge Server, follow the illustration below to secure the system to the rack.

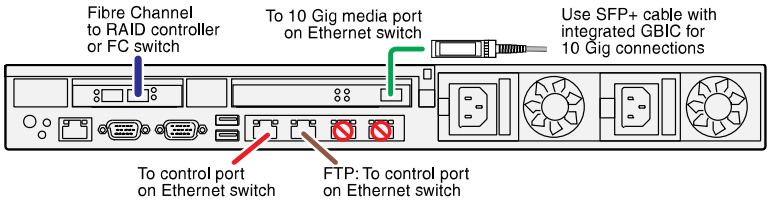


Install a screw in the bottom hole of the bracket on each side. Do not attempt to install a screw in the top hole of the bracket.

K2-SVR basic Dell R620

These cabling instructions apply to the following:

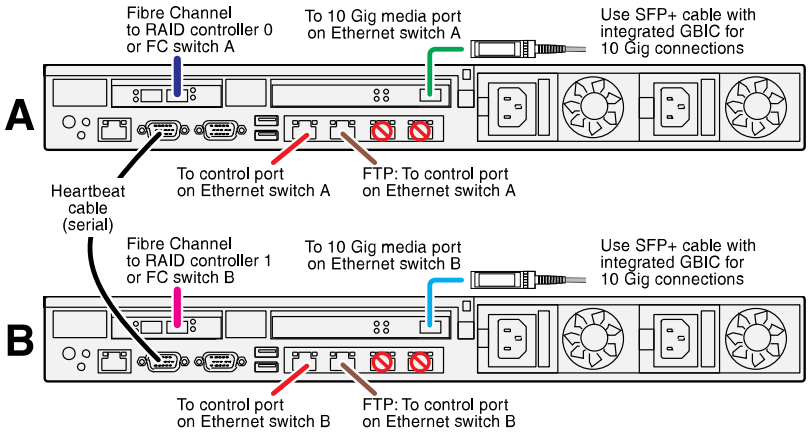
- Dell R620 PowerEdge Server on a basic (non-redundant) online or production K2 SAN.



K2-SVR redundant Dell R620

These cabling instructions apply to the following:

- Dell R620 PowerEdge Server on a redundant online or production K2 SAN.



Redundant server heartbeat serial cable

Take care to use the proper serial cable to interconnect redundant K2 Media Servers that take the role of file system/database servers. This cable supports the heartbeat mechanism whereby the servers monitor each other's health. It is a 9 pin serial cable, but it is not a standard RS-232 null modem cable. The heartbeat cable is supplied with your system (Grass Valley part number 174-8137-00) and has a pin configuration as follows:

1 – 4

2 – 3

3 – 2

4 – 1&6

5 – 5

6 – 4

7 – 8

8 – 7

9 – No Connect

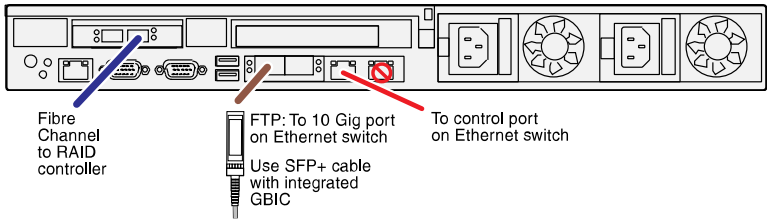
Cable NH10GE K2 Media Server

As directed by the system diagram for your K2 SAN, cable the NH10GE K2 Media Server or Servers for your K2 SAN using the instructions in this section

K2-SVR-NH10GE online/production Dell R620

These cabling instructions apply to the following:

- Dell R620 PowerEdge Server NH10GE on an online or production K2 SAN.

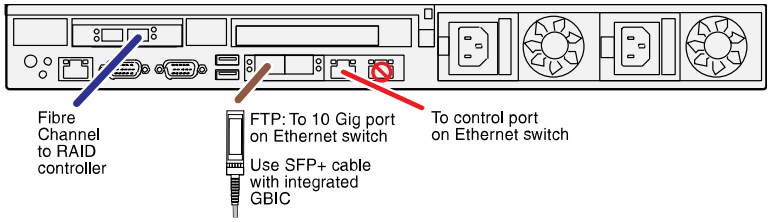


If you have more than one NH1 server, balance servers between controller 0 and controller 1.

K2-SVR-NH10GE basic nearline Dell R620

These cabling instructions apply to the following:

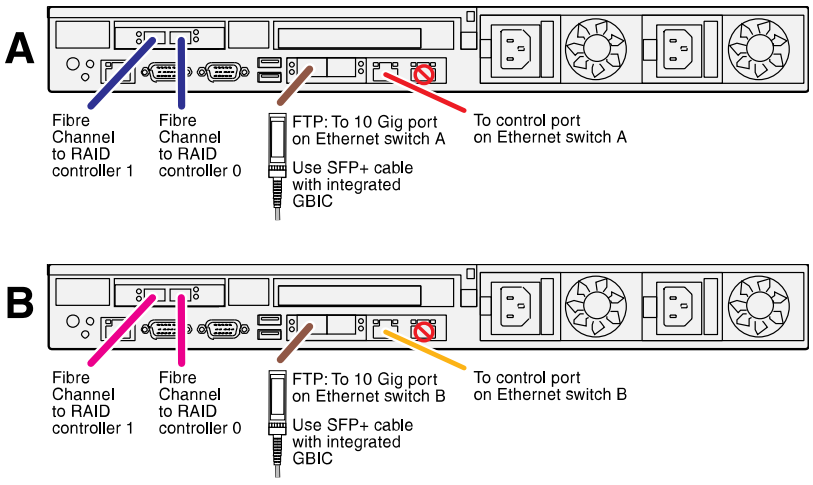
- Dell R620 PowerEdge Server NH10GE on a basic nearline K2 SAN.



K2-SVR-NH10GE redundant nearline Dell R620

These cabling instructions apply to the following:

- Dell R620 PowerEdge Server NH10GE on a nearline K2 SAN.



Cable K2 RAID

Before cabling, install the K2 RAID chassis in its permanent location. After mounting the chassis in the rack, you must secure brackets to the front rail to support the Grass Valley bezel. Refer to related topics in this document for rack mount instructions.

You do not need to manually set a Fibre Channel address ID on controllers or a chassis address on Expansion chassis.

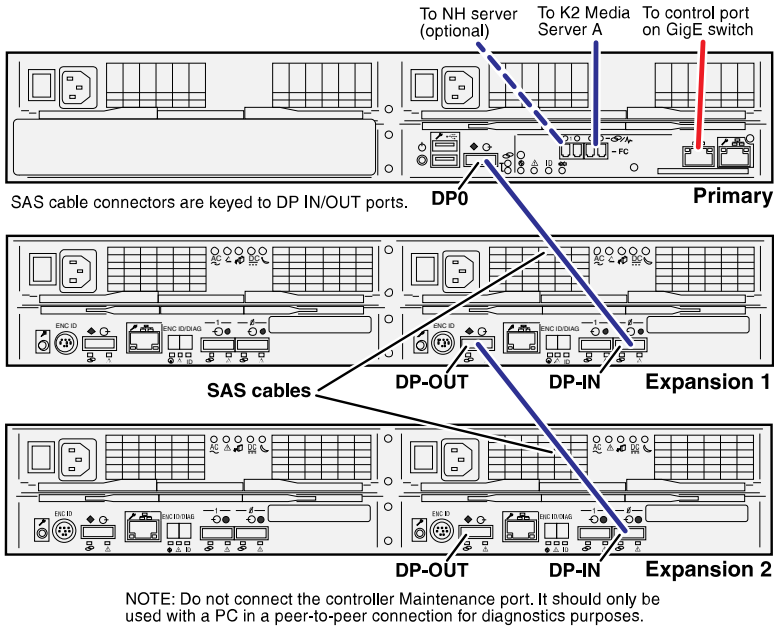
As directed by the system diagram for your storage system, cable the K2 RAID devices using the instructions in this section.

Once the RAID storage is connected and configured, do not swap Expansion chassis or otherwise reconfigure storage. If you connect an Expansion chassis in a different order or to the wrong controller, the controller will see a configuration mismatch and fault.

K2 RAID basic online/production

These cabling instructions apply to the following:

- K2 10Gv2 RAID on a basic (non-redundant) online or production K2 SAN.

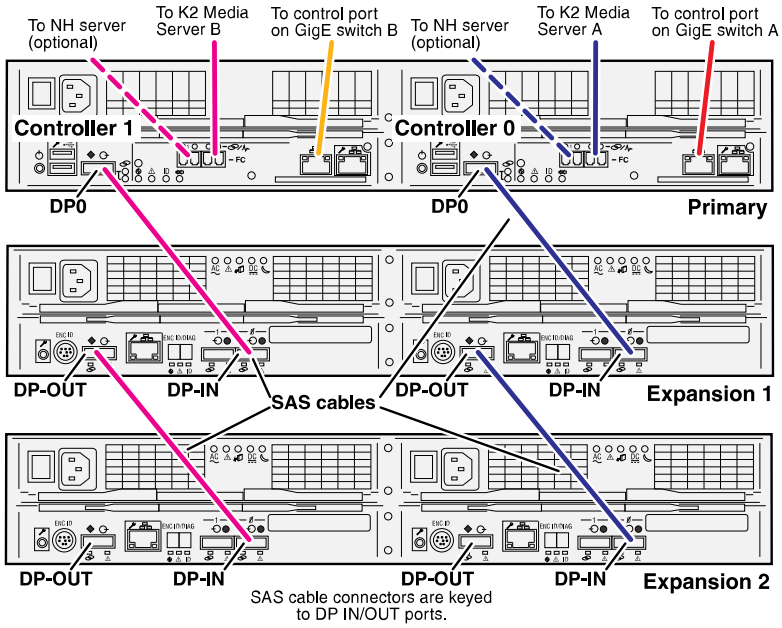


Continue this cable pattern for additional Expansion Chassis.

K2 RAID redundant online/production

These cabling instructions apply to the following:

- K2 10Gv2 RAID on a redundant online or production K2 SAN.



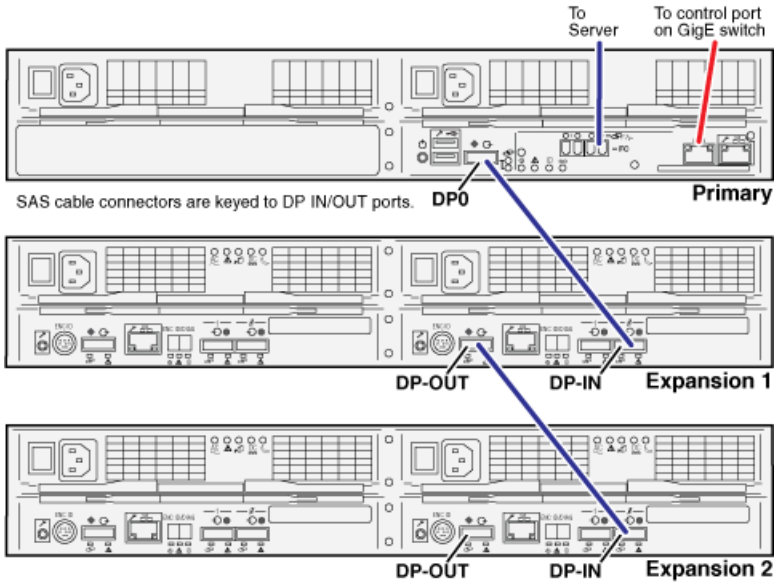
NOTE: Do not connect the controller MNT port. It should only be used with a PC in a peer-to-peer connection for diagnostics purposes.

Continue this cable pattern for additional Expansion Chassis.

K2 RAID basic nearline

These cabling instructions apply to the following:

- K2 10Gv2 RAID on a basic nearline K2 SAN.



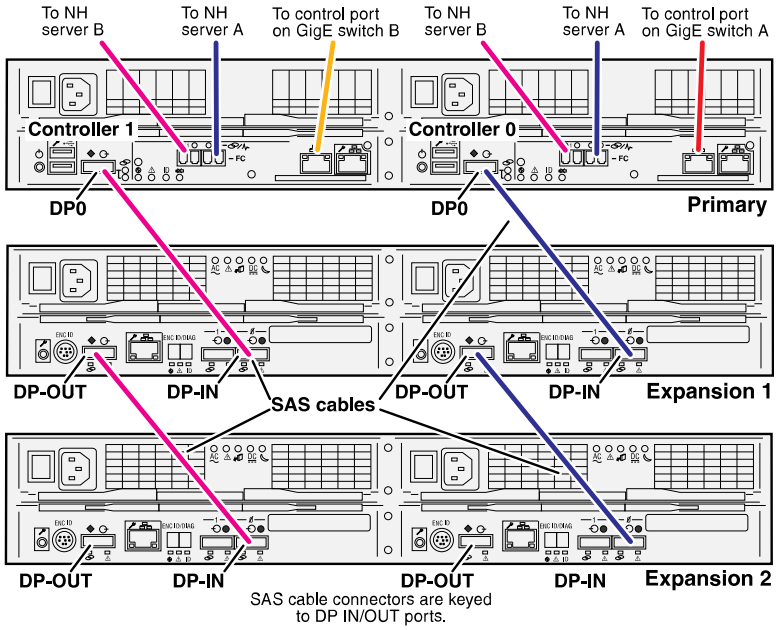
NOTE: Do not connect the controller MNT port. It should only be used with a PC in a peer-to-peer connection for diagnostics purposes.

Continue this cable pattern for additional Expansion Chassis.

K2 RAID redundant nearline

These cabling instructions apply to the following:

- K2 10Gv2 RAID on a Nearline K2 SAN.



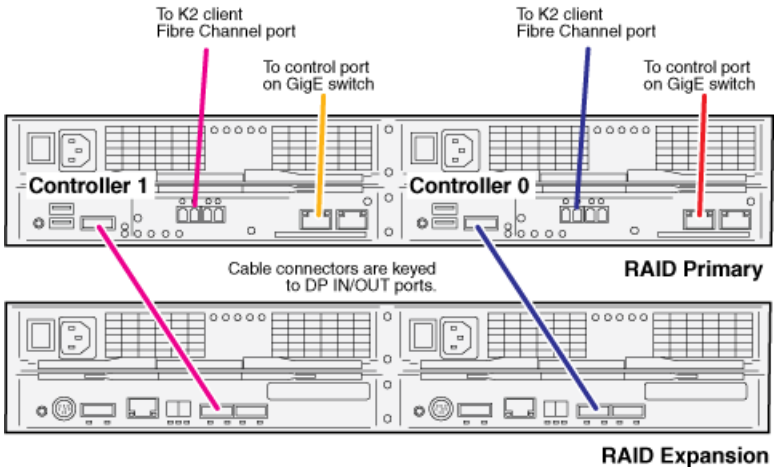
NOTE: Do not connect the controller MNT port. It should only be used with a PC in a peer-to-peer connection for diagnostics purposes.

Continue this cable pattern for additional Expansion Chassis.

K2 RAID direct-connect

These cabling instructions apply to the following:

- K2 10Gv2 RAID providing direct-connect storage for a K2 Solo 3G system. Make Fibre Channel connections to K2 Solo 3G system and between RAID chassis.



For more information

For the installer of a standalone K2 product with internal storage

If you are installing a K2 system, such as a K2 Summit/Solo system, with standalone internal storage, refer to documentation in the following sequence:

	Find this document…	In these locations…	In these formats:
1	K2 Release Notes	Grass Valley Website	PDF file
2	Quick Start Guide for the K2 product	K2 product shipping box	Printed
		K2 Documentation Set	PDF file
		Grass Valley Website	PDF file
3	K2 System Guide	K2 Documentation Set	PDF file
		Grass Valley Website	PDF file

For the installer of a K2 product with direct connect storage

If you are installing a standalone K2 system, such as a K2 Summit system, with direct connect external RAID storage, refer to documentation in the following sequence:

	Find this document…	In these locations…	In these formats:
1	K2 Release Notes	Grass Valley Website	PDF file
2	K2 Storage Cabling Guide	K2 RAID shipping box	Printed
		K2 Documentation Set	PDF file
		Grass Valley Website	PDF file

	Find this document…	In these locations…	In these formats:
3	Quick Start Guide for the K2 product	K2 product shipping box	Printed
		K2 Documentation Set	PDF file
		Grass Valley Website	PDF file
4	K2 System Guide	K2 Documentation Set	PDF file
		Grass Valley Website	PDF file

For the installer of K2 Summit systems with K2 SAN shared storage

If you are installing a K2 SAN with connected K2 Summit systems, refer to documentation in the following sequence:

	Find this document…	In these locations…	In these formats:
1	K2 Release Notes	Grass Valley Website	PDF file
2	K2 Storage Cabling Guide	K2 RAID shipping box	Printed
		K2 Documentation Set	PDF file
		Grass Valley Website	PDF file
3	Quick Start Guide for the K2 product	K2 product shipping box	Printed
		K2 Documentation Set	PDF file
		Grass Valley Website	PDF file
4	K2 SAN Installation and Service Manual	K2 Documentation Set	PDF file
		Grass Valley Website	PDF file
5	K2 System Guide	K2 Documentation Set	PDF file
		Grass Valley Website	PDF file

K2 Release Notes

Contains the latest information about the software shipped on your system, including software upgrade instructions, software specifications and requirements, feature changes from the previous releases, and any known problems. You should always check the Grass Valley Website to determine if there is an updated version of release notes available.

Quick Start Guides

The Quick Start Guide is a printed document, shipped in the product packaging with K2 Summit/Solo systems and K2 Dyno Replay Controllers. The Quick Start Guide provides step-by-step installation instructions for basic installation and operation of the product.

K2 Storage Cabling Guide

The K2 Storage Cabling Guide is a printed document, shipped in the product packaging with the primary RAID storage chassis. The cabling guide provides instructions for K2 Storage Area Network (SAN) cabling and external configuration. The cabling guide provides instructions for each level of K2 SAN and covers both redundant and basic (non-redundant) systems. It also provides instructions for connecting direct-connect external RAID storage to K2 Summit systems.

K2 Documentation Set

Except for the release notes, the full set of support documentation, including this manual, is available in the K2 or K2/STRATUS Documentation Set. You can find the Documentation Set on the Grass Valley website. The following URL allows you to browse by K2 software version:

http://www.grassvalley.com/dl/k2_summit

You can also find the Documentation Set on the USB Recovery Flash drive that ships with your K2 Summit/Solo system.

The Documentation Set includes the following K2 product documents:

K2 AppCenter User Manual	Provides instructions for configuring and operating the media channels of product.
Quick Start Guides	The Quick Start Guide provides step-by-step installation instructions for basic installation and operation of the product.
K2 System Guide	Contains the product specifications and instructions for modifying system settings.
K2 Service Manuals	Contains information on servicing and maintaining the K2 product.
K2 SAN Installation and Service Manual	Contains installation, configuration, and maintenance procedures for shared storage options.
K2 Storage Cabling Guide	The cabling guide provides instructions for K2 Storage Area Network (SAN) cabling and external configuration. The cabling guide provides instructions for each level of K2 SAN and covers both redundant and basic (non-redundant) systems. It also provides instructions for connecting direct-connect external RAID storage to K2 Summit systems.
Fibre Channel Switch Installation Manual	Contains information on configuring and servicing the Fibre Channel switch.

On-line Help Systems

You can find documentation online with products as follows:

K2 AppCenter Help	Contains information on using K2 AppCenter. In the AppCenter user interface menu bar select **Help**, then choose **AppCenter Help Topics** from the drop-down menu.

SiteConfig Help	Contains information on using SiteConfig. In the SiteConfig user interface menu bar select **Help**, then choose **SiteConfig Help Topics** from the drop-down menu.

K2 FCP Connect documentation

The K2 FCP Connect product has its own documentation set, described as follows:

GV Connect User Manual	Provides instructions for using GV Connect, which is a Final Cut Pro plugin, to access and work with K2 assets. GV Connect is part of the K2 FCP Connect product.
K2 FCP Connect Installation Manual	Provides detailed instructions to install and configure the K2 FCP Connect product.
K2 FCP Connect Release Notes	Contains the latest information about the K2 FCP Connect product, including software upgrade instructions, software specifications and requirements, feature changes from the previous releases, and any known problems. You should always check the Grass Valley Website to determine if there is an updated version of release notes available.

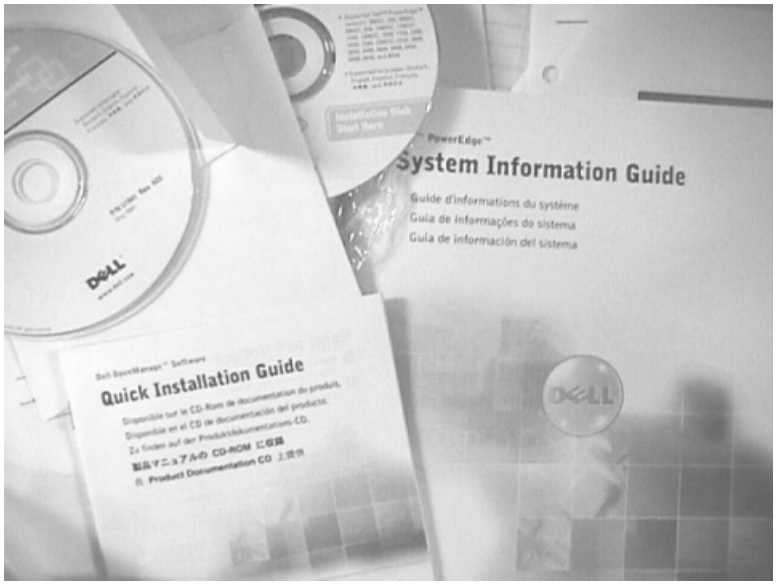
Grass Valley Website

This public Web site contains all the latest manuals and documentation, and additional support information. Use the following URL.

http://www.grassvalley.com

Dell Server Documentation

If your system includes a Grass Valley product on a Dell server platform, refer to the applicable Grass Valley product manual for installation and configuration information. However, a full set of Dell server documentation has been provided on the *Dell Product Documentation* CD-ROM. Refer to the documents on this CD-ROM only as required by procedures in Grass Valley product manual.



Information referenced on the *Dell Product Documentation* CD-ROM includes, but is not limited to:

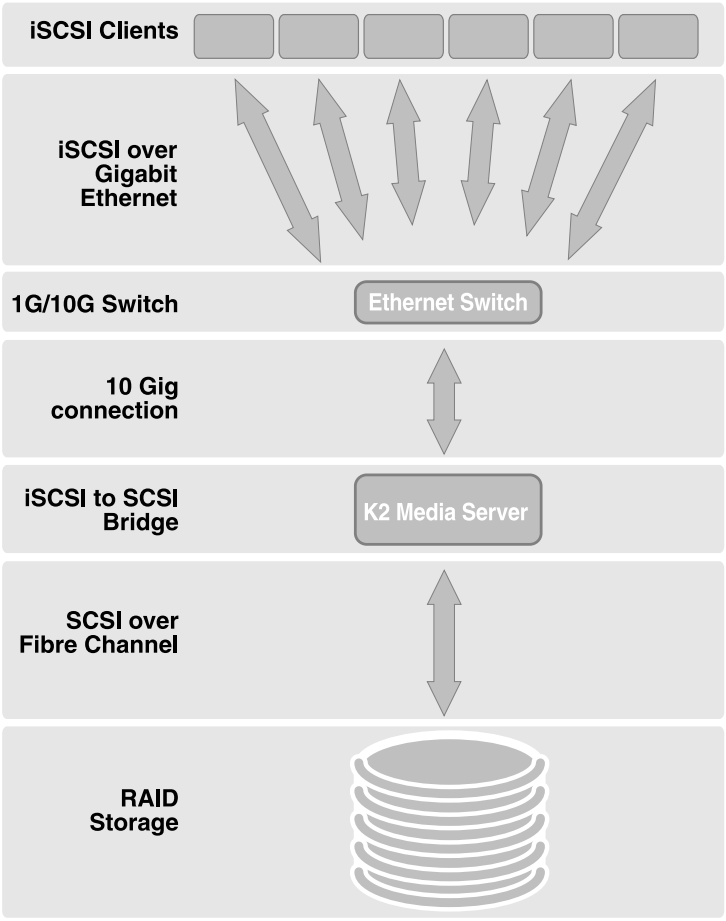
- Unpacking and rack-mounting
- Important safety and regulatory information
- Status indicators, messages, and error codes
- Troubleshooting help

⚠ ***CAUTION: Do not use the Dell Quick Installation Guide provided with the Dell CD-ROM package. This guide includes instructions for using the OpenManage software CD-ROM to install an operating system, which is not necessary on the Grass Valley product.***

Product description

K2 SAN overview description

The K2 Storage Area Network (SAN) is Grass Valley's shared storage solution that gives multiple clients access to a common pool of media. In the iSCSI SAN, clients access the shared media storage via a Gigabit Ethernet network and a Fibre Channel connection. Data is communicated using the Small Computer System Interface (SCSI) data transfer interface and the Internet SCSI (iSCSI) protocol.



A custom-designed Fibre Channel SAN is also available in which clients access RAID storage via a Fibre Channel network, and the K2 Media Server connects via Ethernet for control functions only.

Refer to related topics in the "Configuring the K2 System" section of this Topic Library for diagrams and explanations of the media file system and the media database.

K2 SAN key features

The key features of the iSCSI K2 SAN are as follows:

- iSCSI storage access protocol
- Gigabit Ethernet connectivity
- RAID 5 and RAID 6 storage
- FTP transfers
- Enhanced IT networked storage configurations to fit a wide variety of size and performance requirements.
- Scaling from 100 to < 5000 MB/s
- Redundancy and fault recovery with no single point of failure
- Tuned and optimized file system for reliable and robust transaction of media files
- Best in class storage management for high throughput, deterministic performance with load balancing, priority of service, and quality of service
- Best in class support for 3rd party editors

What's new in the K2 10Gv2 SAN

The primary differences between K2 10Gv2 SAN and previous K2 SANs are as follows:

- 2.5 inch drives — A chassis is available that holds 2.5 inch drives with a capacity of 24 drives. A chassis is also available that holds 3.5 inch drives, similar to previous K2 SANs.
- Larger capacity drives — Both 2.5 inch and 3.5 inch drives have increased capacity.

If you are familiar with previous K2 SANs, keep these differences in mind as you read about the K2 10Gv2 SAN in this manual. If you need information about previous K2 SANs, refer to previous versions of this manual.

K2 Storage types and terms

Grass Valley configures K2 storage to meet their customer's workflow needs. This topic describes some typical configurations and terminology.

Online – Online storage is considered "Tier 1" K2 storage in that it is suitable for both record and play. The purpose of an online SAN is to record and play media for broadcast or other on-air applications. Performance requirements are critical for online applications, so this type of SAN features high performance, low latency storage. Online storage can be iSCSI or Fibre Channel.

Production – Production storage is considered "Tier 2" K2 storage in that it is suitable for record (ingest) but not recommended for on-air playout. The purpose of production storage is to provide cost effective storage for production and editing applications. These applications require high performance but internal buffering in editing software puts less stress on the storage system, so performance requirements are lower than for online storage. Therefore, production storage can use low cost, high capacity drives, such as 7.2K SAS drives. In a typical workflow, production is finished on the production storage and then the content is pushed to an online K2 system for playout. Production storage is configured similar to Online storage, but with the 7.2K SAS RAID devices and drives. Production storage can be iSCSI or Fibre Channel.

Nearline – Nearline storage is considered "Tier 3" K2 storage in that it is suitable for media file transfer but does not support either record or play. The purpose of a nearline SAN is to provide a large pool of storage to which files can be saved. The nearline system is considered an "offline" system, which means the system stores files only, such GXF files or MXF files, with no ability to record or play those files directly on the system. The files on a nearline system can be readily available to an online K2 system via FTP or CIFS connections over Ethernet. Nearline storage has Fibre Channel connections between the K2 Media Server and the RAID storage devices.

Workgroup – Workgroup storage is a Fibre-Channel-only type of production storage intended for small workgroups. This type of storage is no longer recommended, as technology advances provide better value with standard iSCSI Production storage.

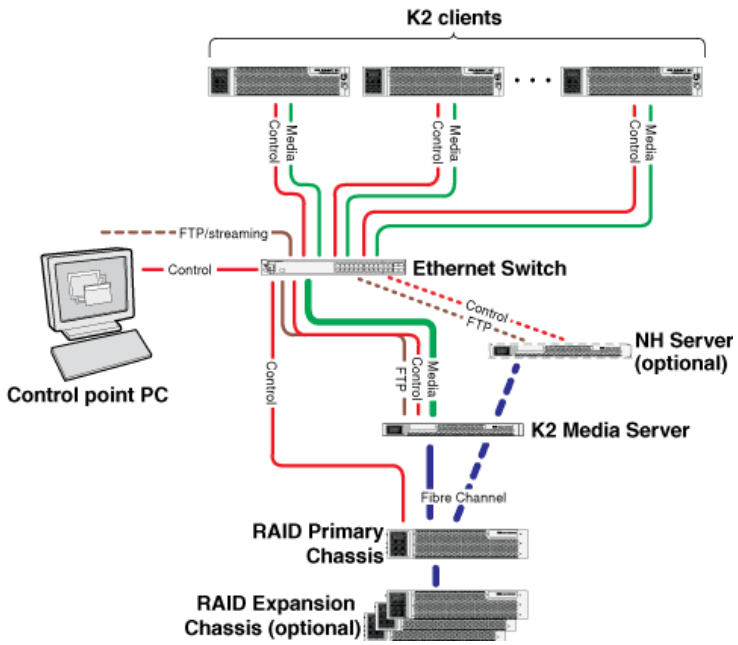
Live Production – In K2Config you can create a Live Production K2 SAN. This mode can be applied to online and production SANs. A K2 SAN with Live Production mode has a shorter minimum delay between start record and start playout and is ideal for use with K2 Dyno. To support this mode, Grass Valley must design your K2 SAN for increased bandwidth.

Stand-alone – This is not shared storage. It is the local storage for a K2 Media Client, K2 Summit Production Client, or K2 Solo Media Server. Stand-alone storage can be internal media drives or direct-connect K2 RAID devices. Refer to the *K2 System Guide*.

K2 SAN descriptions

The following sections describe the standard, pre-defined structures of the K2 SAN. Refer to related topics in this document for more information on custom K2 SAN systems.

Basic K2 SAN description



The basic (non-redundant) K2 SAN can be an online SAN or a production SAN. The SAN has one Ethernet switch, one K2 Media Server, and one basic K2 RAID chassis. RAID Expansion chassis are optional for increased storage capacity.

K2 clients and other iSCSI clients, such as high resolution GV STRATUS clients, are connected to the Ethernet switch. Each K2 client has one GigE connection for media and one GigE connection for control. The GigE switch is configured with V-LANs to keep the control/FTP traffic and the media (iSCSI) traffic separate.

The K2 Media Server has one 10 Gig connection for media (iSCSI), one GigE connection for control, one GigE connection for FTP, and one Fibre Channel connection to the RAID storage. The server hosts an iSCSI interface card for the 10 Gig media connection and a Fibre Channel card for the RAID storage connection. The iSCSI interface card provides a bridge between iSCSI and Fibre Channel SCSI. The server also hosts software components that allow it to function in various roles, including media file system manager, media database server, and FTP server.

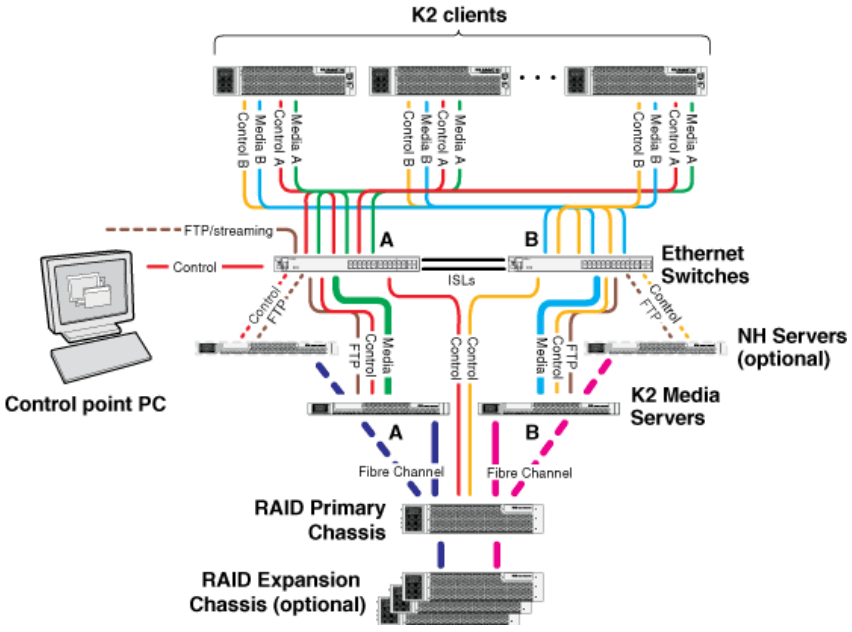
The basic K2 RAID chassis is connected via a single Fibre Channel connection to the K2 Media Server. It also must be connected to the GigE control network. An online SAN has 2.5 inch 10K drives, with 24 drives per chassis. A production SAN has 3.5 inch 7.2K drives with 12 drives per chassis.

Optional 10 Gig NH K2 Media Servers are available to provide additional FTP bandwidth. If the optional NH server is used, all FTP traffic goes to this server, so the K2 Media Server is not cabled or configured for FTP.

The K2Config control point PC is connected to the GigE control network. The K2Config application runs on this PC for configuring the SAN. The SiteConfig application also runs on this PC.

FTP/streaming traffic accesses the K2 SAN via the FTP GigE port on K2 Media Servers. FTP/streaming traffic does not go to K2 clients.

Redundant K2 SAN description



The redundant K2 SAN can be an online SAN or a production SAN. The SAN has two Ethernet switches connected by Inter-Switch Links (ISLs) to support a redundant Ethernet fabric. The SAN also has redundant K2 Media Servers. The servers are configured to have identical roles. This provides redundancy for database, file system, iSCSI bridge, and FTP roles. One K2 RAID supports redundant Fibre Channel connections. Expansion chassis are optional for increased storage capacity.

K2 clients have a pair of redundant (teamed) Gigabit Ethernet ports for control and two Gigabit Ethernet ports (A and B) for media (iSCSI). Each port of the control team is connected to a different switch. The A media port goes to the A switch and the B media port goes to the B switch. The switches are configured with V-LANs to keep the control/FTP and media (iSCSI) traffic separate.

Each K2 Media Server has one 10 Gig connection for media (iSCSI), one GigE connection for control, one GigE connection for FTP, and one Fibre Channel connection to the RAID storage. All GigE connections and the 10 Gig connection on a server go to the same GigE switch. The server hosts a 10 Gig iSCSI interface card for the 10 Gig media connections and a Fibre Channel card for the RAID storage connection. The iSCSI interface card provides a bridge between iSCSI and Fibre Channel SCSI. The server also hosts software components that allow it to function in its roles, including media file system manager, media database server, and FTP server. Redundant K2 Media Servers are connected by a serial cable which supports the heartbeat signal required for automatic system recovery (failover) features.

The redundant K2 RAID chassis has redundant RAID controllers to support the Fibre Channel connections from the K2 Media Servers. The redundant K2 RAID chassis is also connected to the GigE control network. It also must be connected to the GigE control network.

On the redundant K2 RAID chassis there is one RAID 1 RANK (also know as LUN) for media file system metadata file and journal file that comes with one hot spare drive. The first set of drives

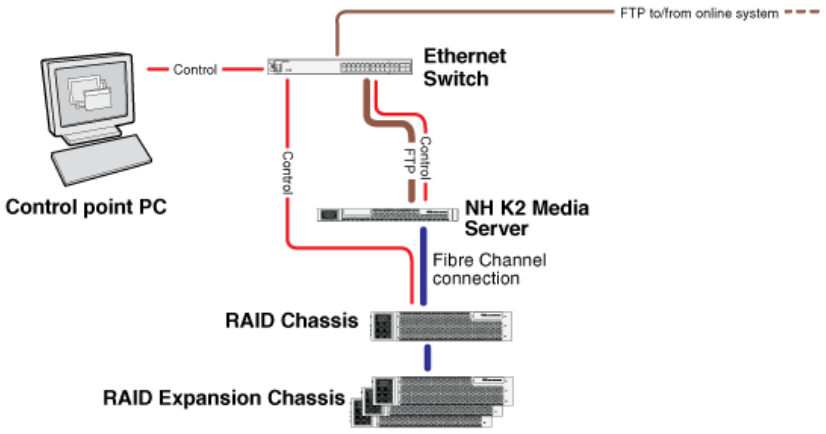
consists of 3 blank slots. The remainder of the RAID storage is RAID 5 or RAID 6 for media. An online SAN has 2.5 inch 10K drives, with 24 drives per chassis. A production SAN has 3.5 inch 7.2K drives with 12 drives per chassis.

Optional 10 Gig NH K2 Media Servers are available to provide additional FTP bandwidth. If the optional NH server is used, all FTP traffic goes to this server, so neither K2 Media Server is cabled or configured for FTP.

The K2Config control point PC is connected to the GigE control network. The K2Config application runs on this PC for configuring the SAN. The SiteConfig application also runs on this PC.

FTP/streaming traffic accesses the K2 SAN via the FTP GigE port on K2 Media Servers. FTP/streaming traffic does not go to K2 clients.

Basic Nearline K2 SAN description



The purpose of a Nearline SAN is to provide a large pool of storage to which files can be saved. The Nearline system is considered an “offline” system, which means the system stores files only, such GXF files or MXF files, with no ability to record or play those files directly on the system. This is because the Nearline system has no media database to support “movies” or “clips”, such as there is on an “online” K2 SAN. However, the files on a Nearline system can be readily available to an online K2 system via FTP transfer.

The basic Nearline SAN has one Ethernet switch.

The SAN also has one 10 Gig NH K2 Media Server. The NH server for a Nearline system has two ports for Fibre Channel connections. NH servers do not have media (iSCSI) ports.

A NH server on a Nearline system is configured with roles of FTP server and Media file system server.

In the Nearline system no K2 Media Servers take the role of iSCSI bridge or media database server.

No K2 clients or any other generic client are part of the Nearline system.

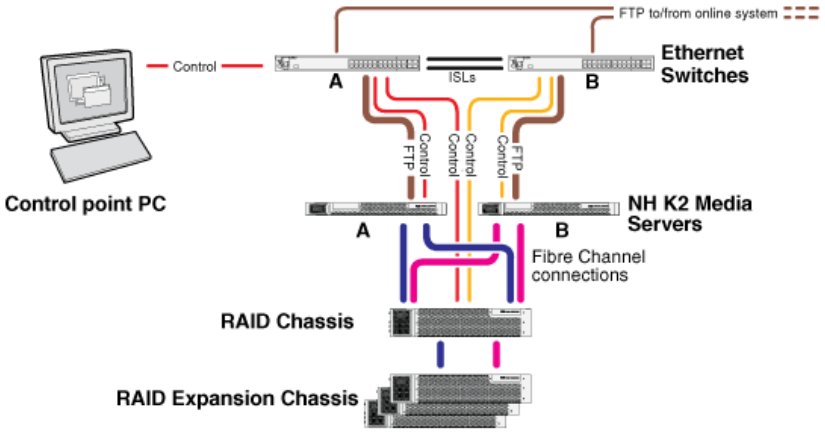
7.2K SAS drives provide the media file storage on a Nearline system. While these drives do not provide the high bandwidth of the drives required by an online K2 SAN, they offer larger capacity and lower cost. This makes these drives ideal for the Nearline SAN.

The primary RAID chassis has one controller. The primary RAID chassis is connected via Fibre Channel to the NH server. The controller in the RAID chassis also must be connected to the GigE control network.

There must be one primary RAID chassis and there may be optional Expansion chassis. Primary chassis and Expansion chassis contain twelve 3.5 inch drives. All disks in both primary and optional Expansion chassis are bound as RAID 6.

The K2Config control point PC is connected to the GigE control network. The K2Config application runs on this PC for configuring the SAN. The SiteConfig application also runs on this PC.

Redundant Nearline K2 SAN description



The purpose of a Nearline SAN is to provide a large pool of storage to which files can be saved. The Nearline system is considered an “offline” system, which means the system stores files only, such GXF files or MXF files, with no ability to record or play those files directly on the system. This is because the Nearline system has no media database to support “movies” or “clips”, such as there is on an “online” K2 SAN. However, the files on a Nearline system can be readily available to an online K2 system via FTP transfer.

The redundant Nearline SAN has two Ethernet switches, connected by Inter-Switch Links (ISLs) to support a redundant Ethernet fabric.

The SAN also has two 10 Gig NH K2 Media Servers. The NH server for a Nearline system has two ports for Fibre Channel connections. NH servers do not have media (iSCSI) ports.

A NH server on a Nearline system is configured with roles of FTP server and Media file system server. On a redundant system these roles are identical on both servers and provide redundancy as follows:

- FTP server — Both servers are active in this role simultaneously. To provide FTP redundancy in the event of a server failure, your facility’s FTP system must be able to access alternate FTP servers.
- Media file system server — Only one server is active at any one time in this role, and the media file system provides redundancy. If a fault occurs on the active server, one of the other servers automatically takes over as the active media file system server.

In the Nearline system no K2 Media Servers take the role of iSCSI bridge or media database server.

No K2 clients or any other generic client are part of the Nearline system.

7.2K SAS drives provide the media file storage on a Nearline system. While these drives do not provide the high bandwidth of the drives required by an online K2 SAN, they offer larger capacity and lower cost. This makes these drives ideal for the Nearline SAN.

The primary RAID chassis has two controllers. The primary RAID chassis is connected via Fibre Channel to the NH server. These Fibre Channel connections access the disks simultaneously for redundancy and increased bandwidth. Each controller in the RAID chassis must also be connected to the GigE control network.

There must be one primary RAID chassis and there may be optional Expansion chassis. Primary chassis and Expansion chassis contain twelve 3.5 inch drives. All disks in both primary and optional Expansion chassis are bound as RAID 6.

The K2Config control point PC is connected to the GigE control network. The K2Config application runs on this PC for configuring the SAN. The SiteConfig application also runs on this PC.

Preparing for installation

K2 SAN installation checklists

Use the following sequence of checklists to guide the overall task flow of installing and commissioning a K2 SAN.

Pre-installation planning checklist

	Task	Instructions	Comment
☐	Procure existing or create new SiteConfig system description	*About developing a system description* on page 533	You can do this before arriving at the customer site.
☐	Next: Infrastructure checklist		

Infrastructure checklist

	Task	Instructions	Comment
☐	Rack and cable	*Cabling K2 SAN devices* on page 508	—
☐	Configure Ethernet switch(es)	*Setting up the Ethernet switch* on page 525	—
☐	Install/update SiteConfig on control point PC	*Install SiteConfig on control point PC* on page 530	—
☐	Next: Network setup and implementation checklist		

Network setup and implementation checklist

	Task	Instructions	Comment
☐	Import or create the SiteConfig system description on the control point PC	*Importing a system description* on page 533	Select IP address range for each network and each device type.
☐	Modify names and networks in the SiteConfig system description.	*Modifying a device name* on page 534, *Modifying the control network* on page 534, *Modifying the FTP/streaming network* on page 536, *Modifying a media (iSCSI) network* on page 538	Set subnet mask and other settings.
☐	Verify/modify device interfaces	*Modifying K2 client unassigned (unmanaged) interface* on page 542, *Modifying K2 Media Server unassigned (unmanaged) interface* on page 544	Do not proceed until the system description accurately represents all aspects of the actual system. Refer to SiteConfig Help Topics . Use procedures as appropriate for your site.
☐	Discover devices	*Discovering devices with SiteConfig* on page 359	—
☐	Assign placeholder devices to discovered devices	*Assigning discovered devices* on page 360	—
☐	Configure IP settings of network interfaces on discovered devices	*Modifying K2 client managed network interfaces* on page 549, *Modifying K2 Media Server managed network interfaces* on page 553	—
☐	Configure names	*Making the host name the same as the device name* on page 368	—
☐	Validate networks	*Pinging devices from the PC that hosts SiteConfig* on page 369	—
☐	Distribute host table information	*Generating host tables using SiteConfig* on page 370	—
☐	Next: Software update checklist		

Software update checklist

	Task	Instructions	Comment
☐	Create deployment groups	*Configuring deployment groups* on page 371	—

	Task	Instructions	Comment
☐	Place software on control point PC	*Adding a software package to a deployment group* on page 562	—
☐	Check software on devices	*Checking all currently installed software on devices* on page 562	—
☐	Upgrade/install software to devices from control point PC	*About deploying software for the K2 SAN* on page 563	Refer to *K2 Release Notes*.
☐	Next: SAN configuration checklist		

SAN configuration checklist

	Task	Instructions	Comment
☐	Import SiteConfig system description into K2Config	*Importing a SiteConfig system description into K2Config* on page 581	—
☐	Configure SAN in K2Config	Configuring and licensing the K2 SAN Use the appropriate instructions for your K2 SAN.	—
☐	Verify SAN license	*Verify license on K2 Media Server* on page 681	The K2 Media Server with role of file system server must be licensed for your SAN's design and bandwidth requirements.
☐	Add K2 clients to SAN	*Configuring a K2 client for the K2 Storage System* on page 684	—
☐	K2 SAN installation complete		

Understanding system concepts

Make sure you understand the following system concepts before planning or implementing a K2 SAN.

Control network description

The control network is for communication between devices and components. It does not have real-time media traffic or streaming/FTP media traffic. The control network traffic must be separated from the streaming/FTP network traffic and the media (iSCSI) network traffic. This separation may be provided by different subnets, VLANs, or physical switch fabrics. The control network and the streaming/FTP network, if on different subnets, may be on the same VLAN. The control network

and the media (iSCSI) network must not be on the same VLAN. Static IP addresses with name resolution via host files are recommended for the control network.

The control network applies to both online, production, and nearline K2 SANs.

All the devices of the K2 SAN are on the control network. Stand-alone K2 clients can also be on the same control network.

Redundant K2 SANs have one control network with hardware separated into an A side and a B side. There is an A Ethernet switch and a B Ethernet switch. Switches are connected by InterSwitch Links (ISLs or trunks) to provide redundant paths for control network traffic. On a redundant K2 SAN, devices are on the control network as follows:

- Shared Storage K2 client - The two control GigE ports are configured as a team. The control team shares a single IP address. One port of the team is on the A side and the other port of the team is on the B side.
- K2 Media Server - Redundant K2 Media Servers with role of media file system/metadata server are balanced between the A and B sides. One server is on the A side and the other server is on the B side. K2 Media Servers with other roles, such as FTP server, are likewise balanced between A and B sides.
- K2 RAID - When a K2 RAID device has redundant controllers, controller 0 is on the A side and controller 1 is on the B side.
- Ethernet switch - For control and configuration, the A switch is on the A side and the B switch is on the B side

Streaming/FTP network description

The streaming/FTP network is for media transfers and FTP traffic. The streaming/FTP network network traffic must be separated from the control network traffic and the media (iSCSI) network traffic. This separation may be provided by different subnets, VLANs, or physical switch fabrics. The control network and the streaming/FTP network, if on different subnets, may be on the same VLAN. The control network and the media (iSCSI) network must not be on the same VLAN. Static IP addresses with name resolution via host files are recommended for the streaming/FTP network. Hostnames of network adapters that are dedicated to the streaming/FTP network must be aliased in the hosts file with the *_he0* suffix. This directs the streaming traffic to the correct port.

The streaming/FTP network applies to both online and nearline K2 SANs. For nearline systems, this is the primary network for moving media to and from the storage system.

Redundant K2 SANs have one streaming/FTP network with hardware separated into an A side and a B side. There is an A Ethernet switch and a B Ethernet switch. Switches are connected by InterSwitch Links (ISLs) to provide redundant paths for streaming/FTP traffic.

Only those K2 devices that host a K2 FTP interface are on the streaming/FTP network, as follows:

- K2 Media Servers - Those with the role of FTP server are connected via their dedicated FTP port. On a redundant K2 SAN, if you have multiple K2 Media Servers with role of FTP server, balance servers between the A and B sides.
- Stand-alone K2 clients - While not a part of a K2 SAN, stand-alone K2 clients can also be on the streaming/FTP network. Connect to the dedicated FTP port.

NOTE: Shared storage K2 clients are not on the streaming/FTP network. They do not have a FTP interface and they do not send or receive streaming/FTP traffic.

Automatic FTP server failover is not provided by the K2 SAN. If you require automatic failover to a redundant FTP server for your streaming/FTP traffic, you must provide it through your FTP application.

Media (iSCSI) network description

The media network is exclusively for real-time iSCSI traffic on a K2 SAN. It must be on a different subnet than the control network and the streaming/FTP network. Furthermore, its traffic is kept physically separate from that of other networks. This separation is provided by dedicated ports, cables, and by a dedicated VLAN on the Ethernet switch or by separate switches. Static IP addresses are required for the media network. Name resolution is not necessary, so media network IP addresses are not required in host files.

The media network applies to online K2 SANs. Nearline K2 SANs do not have a media network.

Redundant K2 SANs have redundant media networks: an A media network and a B media network. The two networks are on separate subnets and are also physically separated onto the A Ethernet switch and the B Ethernet switch. InterSwitch Links (ISLs) between switches do not carry media (iSCSI) traffic. ISLs provide redundant paths for control network traffic and streaming/FTP network traffic only.

Devices are on the media network as follows:

- Shared Storage K2 client - On a non-redundant K2 SAN, the A media port connects to the media network. On a redundant K2 SAN, the A media port connects to the A media network and the B media port connects to the B media network.
- K2 Media Server - A server has one port available for connection to a media network. This is a 10 Gig iSCSI interface adapter, which supports the functionality of a TCP/IP Offload Engine (TOE). On a redundant K2 SAN, one server is on the A media network and one server is on the B media network.

Networking tips

- Before configuring any devices for networks, determine the full scope of IP addresses and names needed for the all the machines in your system. Work with the network administrator at your facility to have IP addresses and names available for your use.
- It is recommended that you use the patterns offered in SiteConfig by default to establish a consistent convention for machine names and IP addresses. You can plan, organize, and enter this information in SiteConfig as you develop a system description. You can do this even before you have devices installed and/or cabled.
- On 64-bit devices, configure IPv4 addresses. Disable the IPv6 interface of the Control and FTP interfaces. SiteConfig always configures IPv4 addresses for 64-bit devices.

Network considerations and constraints

- If your GV STRATUS system is on a domain, all servers and client PCs on that system that have any interaction with Grass Valley components must be logged on to Windows with a domain user account. Do not use a local user account.
- Do not use any 10.1.0.n or 10.2.0.n IP addresses. These are used by the K2 RAID maintenance port and must be reserved for that purpose. If these addresses are otherwise used, maintenance port communication errors occur.

About host files

The hosts file is used by the control network and the streaming/FTP network for name resolution, which determines the IP address of a device on the network when only the device name (hostname) is given. The hosts file is located at *C:\Windows\system32\drivers\etc\hosts* on Windows XP and later operating systems. The hosts file must be the same on all network devices. It includes the names and addresses of all the devices on the network.

For FTP transfers on a K2 SAN, transfers go to/from K2 Media Servers that have the role of FTP server. No transfers go directly to/from the shared storage K2 clients that are on the K2 SAN. To support FTP transfers, in the hosts file the K2 Media Server hostname must have the *_he0* extension added at the end of the name and that hostname must be associated with the K2 Media Server's FTP/streaming network IP address.

Here is an example of IP addresses and names associated in a hosts file:

```
192.168.100.11   root_server_1
192.168.101.11   root_server_1_he0
192.168.100.21   root_server_2
192.168.101.21   root_server_2_he0
192.168.100.31   root_server_3
192.168.101.31   root_server_3_he0
192.168.100.41   root_server_4
192.168.101.41   root_server_4_he0
192.168.100.51   root_raid_1
192.168.100.61   root_gige_1
```

In this example 192.168.100.xx is the control network and 192.168.101.xx is the streaming/FTP network. Each K2 Media Server has its hostname associated with its control network IP address. In addition, each K2 Media Server (that has the role of FTP server) has its *_he0* hostname associated with its streaming/FTP network address.

Use SiteConfig to define your networks and devices. When you do so, SiteConfig creates the correct hosts file and copies the hosts file to each network device. This enforces consistent hosts files across networks and reduces errors introduced by editing and copying hosts files on individual devices. You can also view hosts files from SiteConfig for troubleshooting purposes.

Host Table tips

- If transferring to or from a Profile XP or Open SAN system via UIM, the hosts file must also follow UIM naming conventions for those systems. Refer to the *UIM Instruction Manual*.
- Do not enable name resolutions for media (iSCSI) network IP addresses in the hosts file, as hostname resolution is not required for the media network. If desired, you can enter media network information in the hosts file as commented text as an aid to managing your networks.

- Use the following tip with care. While it can solve a problem, it also introduces a name resolution "anomaly" that might be confusing if not considered in future troubleshooting activities.

  For each SAN (shared storage) K2 client, add the "_he0" suffix to the hostname but then associate that hostname with the K2 Media Server's FTP/streaming network IP address, not the K2 client's IP address. Aliasing K2 client hostnames in this way would not be required if the transfer source/destination was always correctly specified as the K2 Media Server. However, a common mistake is to attempt a transfer in which the source/destination is incorrectly specified as the K2 client. The host file aliasing corrects this mistake and redirects to the K2 Media Server, which is the correct transfer source/destination.

  An example of a hosts file entry with this type of aliasing is as follows:

  ```
  192.168.101.11 server_1_he0 client_1_he0 client_2_he0
  ```

Dell R620 Rack specifications

Use the following specifications to determine load, spacing, power, and other factors when planning system racks.

Table 36: Mechanical specifications

Characteristic	Specification
Cabinet Type	Rack-mount
Rack units	1
External Dimensions	482.4 (w) x 42.8 (h) x 683.7 (d) mm
Weight	Maximum 18.6kg , 40.96 lbs

Table 37: Power specifications

Specification	1100W DC	1100W AC	750W AC	495W AC
Current consumption	32A	12A-6.5A	10A-5A	6.5A-3A
Supply voltage	-48V to -60V DC	100-240VAC	100-240VAC	100-240VAC
Frequency	N/A	50/60Hz	50/60Hz	50/60Hz
Heat dissipation (BTU/hr max)	4416	4100	2843	1908
Maximum inrush current	55A	55A	55A	55A

K2 RAID Rack specifications

Use the following specifications to determine load, spacing, power, and other factors when planning system racks. These specifications apply to K2 10Gv2 RAID (M100) chassis.

Table 38: Mechanical specifications

Characteristic	Primary chassis	Expansion chassis
Cabinet Type	Rack-mount	Rack-mount
Rack units	2	2
External Dimensions	482 x 513.2 x 87.8 mm (no front bezel)	482 x 513.2 x 87.8 mm (no front bezel)
Weight	31 kg maximum	29 kg maximum

Table 39: Power specifications

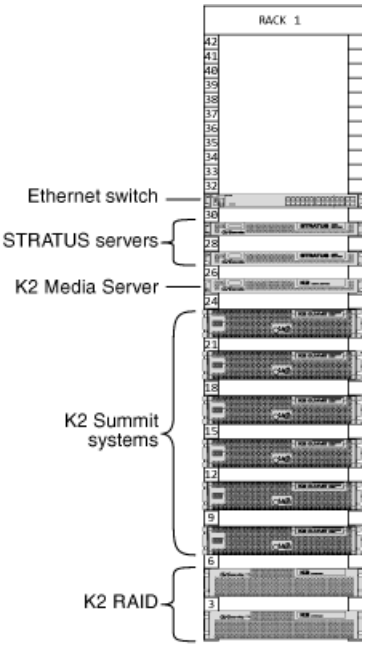
Characteristic	Primary chassis	Primary chassis
Power conditions	100 to 240 VAC, single-phase 50/60 Hz	100 to 240 VAC, single-phase 50/60 Hz
Maximum power consumption (when operating in a 25° C environment)	400 W	290 W

Cabling K2 SAN devices

Rack-mount devices

All systems require this process.

Follow the instructions you received with the rack-mount hardware to install each component of the system. One rack-unit spacing is recommended between components for ventilation. The recommended arrangement of devices is as follows:



HP ProCurve Switch Rack specifications

Use the following specifications to determine load, spacing, power, and other factors when planning system racks.

Table 40: Mechanical specifications

Characteristic	Specification
Cabinet Type	Rack-mount
Rack units	1
External Dimensions	443 (w) x 44 (h) x 392 (d) mm
Weight	Maximum 7 kg

Table 41: Power specifications

Characteristic	Specification
Type	100-127 VAC/200-240 VAC; 50/60 Hz
Power Consumption	4.0/2.0 A, 200W

Dell R620 Rack specifications

Use the following specifications to determine load, spacing, power, and other factors when planning system racks.

Table 42: Mechanical specifications

Characteristic	Specification
Cabinet Type	Rack-mount
Rack units	1
External Dimensions	482.4 (w) x 42.8 (h) x 683.7 (d) mm
Weight	Maximum 18.6kg , 40.96 lbs

Table 43: Power specifications

Specification	1100W DC	1100W AC	750W AC	495W AC
Current consumption	32A	12A-6.5A	10A-5A	6.5A-3A
Supply voltage	-48V to -60V DC	100-240VAC	100-240VAC	100-240VAC
Frequency	N/A	50/60Hz	50/60Hz	50/60Hz
Heat dissipation (BTU/hr max)	4416	4100	2843	1908
Maximum inrush current	55A	55A	55A	55A

K2 Summit 3G Rack specifications

Use the following specifications to determine load, spacing, power, and other factors when planning system racks. These specifications apply to K2 Summit 3G chassis.

Table 44: Mechanical specifications

Characteristic	Specification
Cabinet Type	Rack-mount
Rack units	2
External Dimensions	447 x 617 x 89 mm
Weight	25.0 kg maximum

Table 45: Power specifications

Characteristic	Specification
Power conditions	Dual, redundant
Mains Input Voltage	90 to 260V auto-range, 47-63Hz

Characteristic	Specification
Maximum power consumption (when operating in a 25° C environment)	450W typical (standalone) 390W typical (SAN client) Maximum AC current 8A @ 115VAC, 4A @ 230VAC

K2 RAID Rack specifications

Use the following specifications to determine load, spacing, power, and other factors when planning system racks. These specifications apply to K2 10Gv2 RAID (M100) chassis.

Table 46: Mechanical specifications

Characteristic	Primary chassis	Expansion chassis
Cabinet Type	Rack-mount	Rack-mount
Rack units	2	2
External Dimensions	482 x 513.2 x 87.8 mm (no front bezel)	482 x 513.2 x 87.8 mm (no front bezel)
Weight	31 kg maximum	29 kg maximum

Table 47: Power specifications

Characteristic	Primary chassis	Primary chassis
Power conditions	100 to 240 VAC, single-phase 50/60 Hz	100 to 240 VAC, single-phase 50/60 Hz
Maximum power consumption (when operating in a 25° C environment)	400 W	290 W

FT Server Rack specifications

Use the following specifications to determine load, spacing, power, and other factors when planning system racks.

Table 48: Mechanical specifications

Characteristic	Type I and Type II Specification
Cabinet Type	Rack-mount
Rack units	4
External Dimensions	483 (w) x 178 (h) x 736 (d) mm, 19.0 in. (w) x 7.0 in. (h) x 28.9 in. (d)

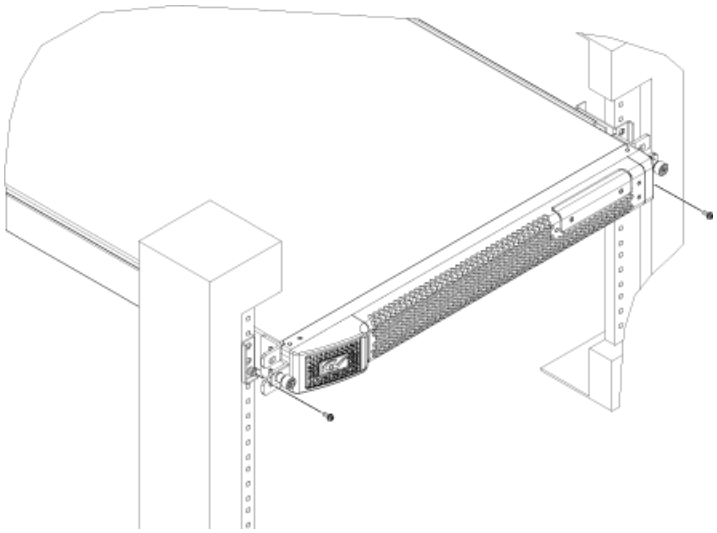
Characteristic	Type I and Type II Specification
Rack clearance	40 cm or more on top, 1 m or more on the front and rear, 60 cm or more on the right and left.
Weight	Maximum 51.5kg , 113.3 lbs

Table 49: Power specifications

Power Supply	Type I Specifications	Type II Specifications
Type	AC 100V-240V +/- 10%, 50/60Hz +/- 3Hz	AC 100V-240V +/- 10%, 50/60Hz +/- 3Hz
Power Consumption	1400VA, 1390W	1300VA, 1290W

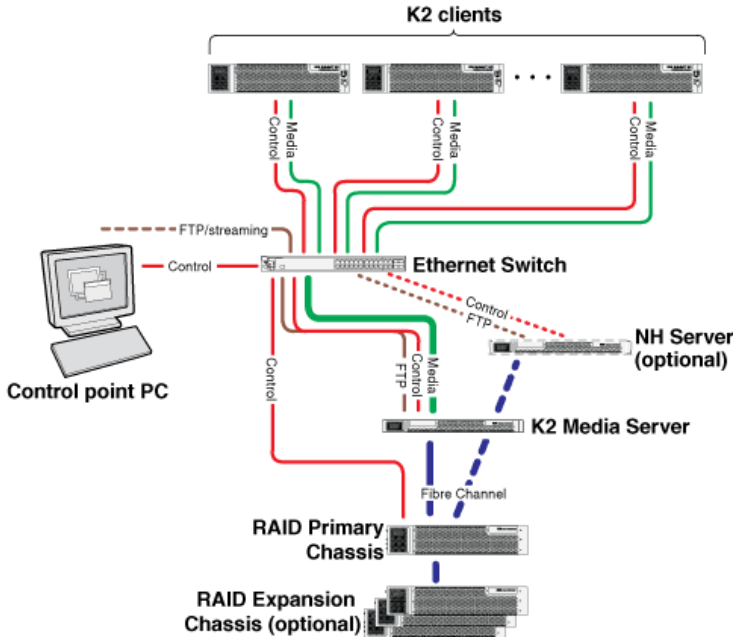
Securing a server to a rack

If the server is a Dell server, follow the instructions provided in the shipping box to install the rack rails and position the server in the rack. For the Dell 1RU PowerEdge Server, follow the illustration below to secure the system to the rack.



Install a screw in the bottom hole of the bracket on each side. Do not attempt to install a screw in the top hole of the bracket.

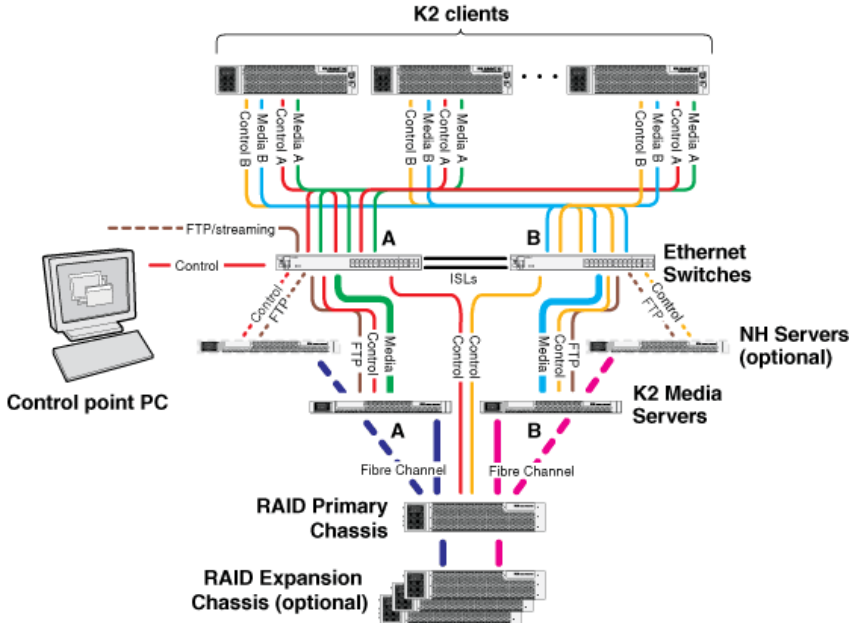
Basic K2 SAN - Online or Production



To cable this K2 SAN device…	Of this model or platform…	Turn to these instructions:
K2 Solo 3G system	K2 Summit 3G system or first generation K2 Summit system	*K2-XDP basic* on page 477
Gigabit Ethernet Switch	HP 29xx	*K2-SWE basic online/production* on page 479
K2 Media Server	Dell R620	*K2-SVR basic Dell R620* on page 483
NH10GE K2 Media Server (optional)	Dell R620	*K2-SVR-NH10GE online/production Dell R620* on page 484
K2 RAID	K2 RAID	*K2 RAID basic online/production* on page 486

This manual documents the default GigE switch configuration. Other configurations are available, depending on your port count and FTP bandwidth requirements.

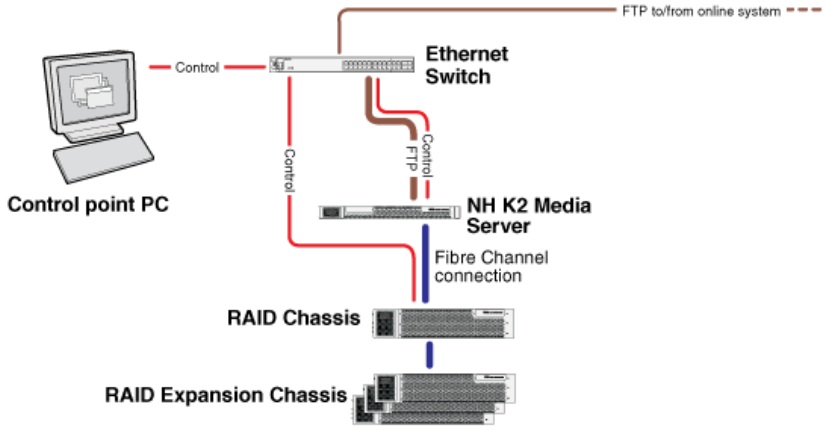
Redundant K2 SAN - Online or Production



To cable this K2 SAN device…	Of this model or platform…	Turn to these instructions:
K2 Solo 3G system	K2 Summit 3G system or first generation K2 Summit system	*K2-XDP redundant* on page 478
Gigabit Ethernet Switch	HP 29xx	*K2-SWE redundant online/production* on page 480
K2 Media Server	Dell R620	*K2-SVR redundant Dell R620* on page 483
NH10GE K2 Media Server (optional)	Dell R620	*K2-SVR-NH10GE online/production Dell R620* on page 484
K2 RAID	K2 RAID	*K2 RAID redundant online/production* on page 486

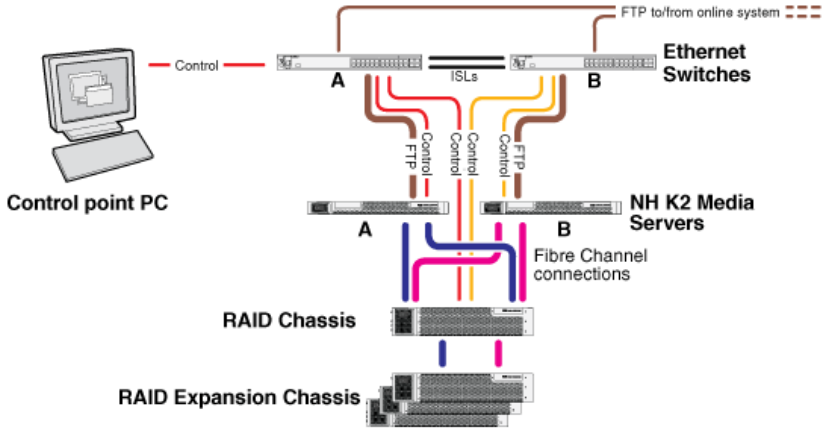
This manual documents the default GigE switch configuration. Other configurations are available, depending on your port count and FTP bandwidth requirements.

Basic Nearline K2 SAN



To cable this K2 SAN device…	Of this model or platform…	Turn to these instructions:
Gigabit Ethernet Switch	HP 29xx	*K2-SWE basic nearline* on page 481
NH10GE K2 Media Server	Dell R620	*K2-SVR-NH10GE basic nearline Dell R620* on page 485
K2 RAID	K2 RAID	*K2 RAID basic nearline* on page 487

Redundant Nearline K2 SAN



To cable this K2 SAN device…	Of this model or platform…	Turn to these instructions:
Gigabit Ethernet Switch	HP 29xx	*K2-SWE redundant nearline* on page 481
NH10GE K2 Media Server	Dell R620	*K2-SVR-NH10GE redundant nearline Dell R620* on page 485

To cable this K2 SAN device…	Of this model or platform…	Turn to these instructions:
K2 RAID	K2 RAID	*K2 RAID redundant nearline* on page 488

Cable K2 Summit system

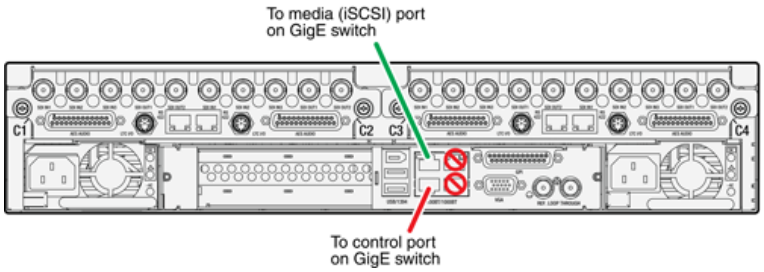
As directed by the system diagram for your K2 storage, cable the K2 Summit system using the instructions in this section.

K2-XDP basic

These cabling instructions apply to the following:

- K2 Summit 3G system or first generation K2 Summit system on a basic (non-redundant) online or production K2 SAN

Refer to "K2 Summit Production Client Quick Start Guide" for additional cabling details.

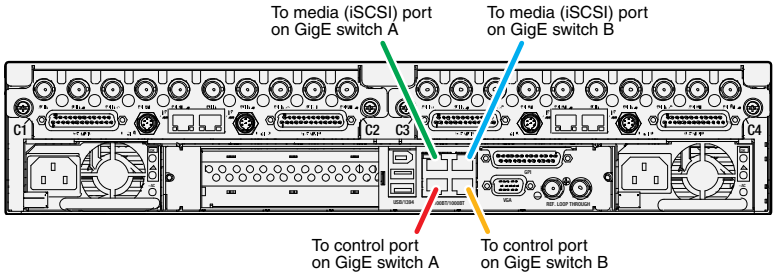


K2-XDP redundant

These cabling instructions apply to the following:

- K2 Summit 3G system or first generation K2 Summit system on a redundant online or production K2 SAN

Refer to "K2 Summit Production Client Quick Start Guide" for additional cabling details.



Cable Ethernet switch

As directed by the system diagram for your storage system, cable the switch or switches for your system using the instructions in this section.

These instructions are for the HP ProCurve switch 29xx series.

If a different brand of switch, such as a Cisco Catalyst switch, is required by your site, apply the information in the following procedures accordingly. Refer to the documentation you received with the switch as necessary.

Install the switch in its permanent location. When installing in a video equipment rack, use 10-32 screws. Do not use HP's 12-24 screws, as they can cause thread damage.

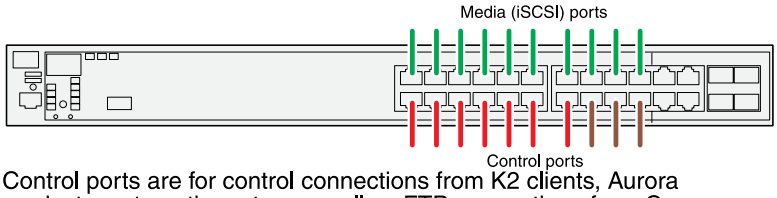
Provide power to the switch.

K2-SWE basic online/production

These cabling instructions apply to the following:

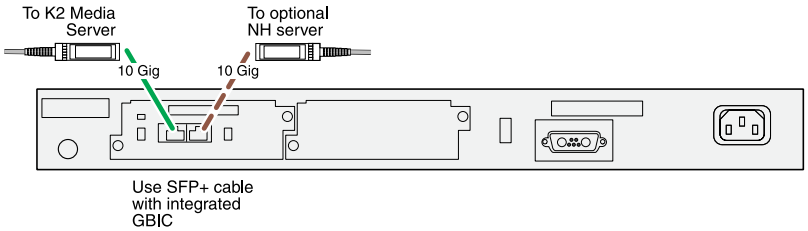
- HP 29xx series Gigabit Ethernet switch on a basic (non-redundant) online or production K2 SAN.

Front view



Control ports are for control connections from K2 clients, Aurora products, automation, etc., as well as FTP connections from Grass Valley and 3rd party systems.

Rear view

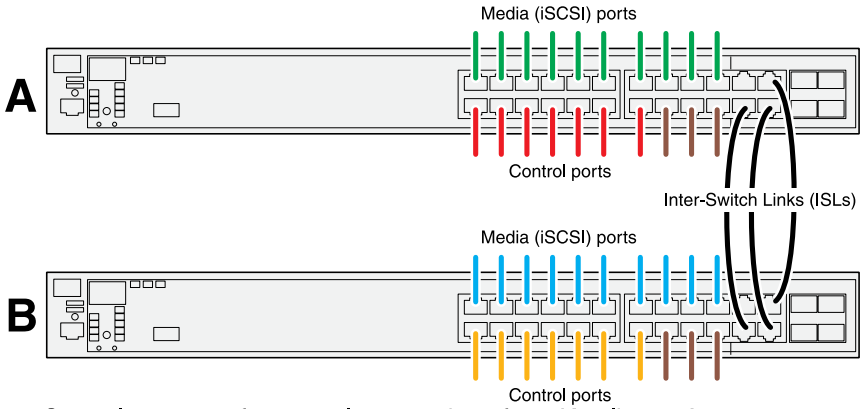


K2-SWE redundant online/production

These cabling instructions apply to the following:

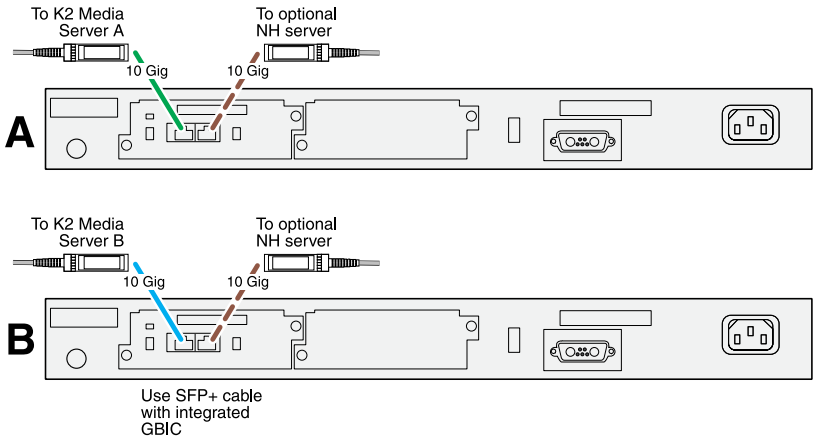
- HP 29xx series Gigabit Ethernet switch on a redundant online or production K2 SAN.

Front view



Control ports are for control connections from K2 clients, Aurora products, automation, etc., as well as FTP connections from Grass Valley and 3rd party systems.

Rear view



If you have other iSCSI clients, such as GV STRATUS high-resolution clients, that have just one iSCSI connection and one control connection, approximately half of the clients should be connected to switch A and half of the clients should be connected to switch B. In a failover event, only the clients connected to one of the switches will remain operational, so make connections accordingly. Connect the client's iSCSI connection to one of the media ports on a switch and the client's control connection to one of the control ports on the same switch.

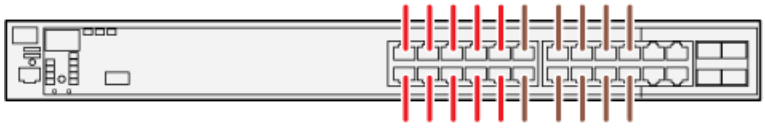
If you have more than one optional NH10GE K2 Media Servers, balance servers between switch A and switch B.

K2-SWE basic nearline

These cabling instructions apply to the following:

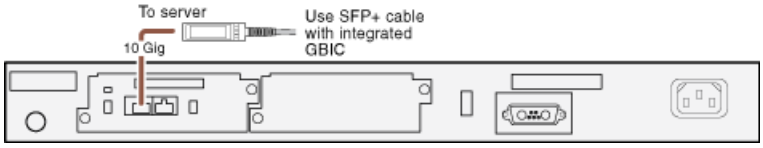
- HP 29xx series Gigabit Ethernet switch on a nearline K2 SAN with one NH K2 Media Server.

Front view



Ports are for control connections as well as FTP connections from Grass Valley and 3rd party systems.

Rear view

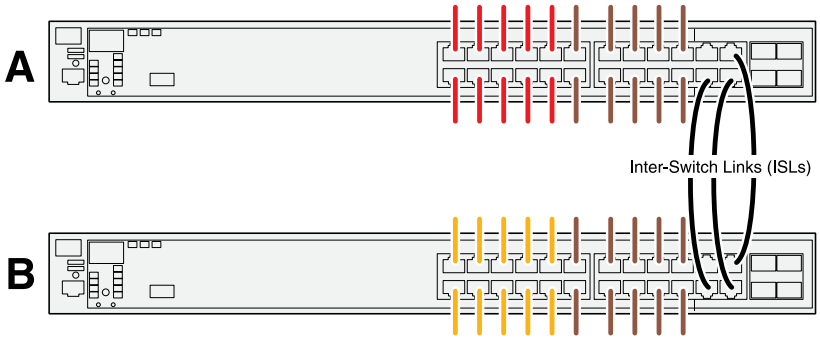


K2-SWE redundant nearline

These cabling instructions apply to the following:

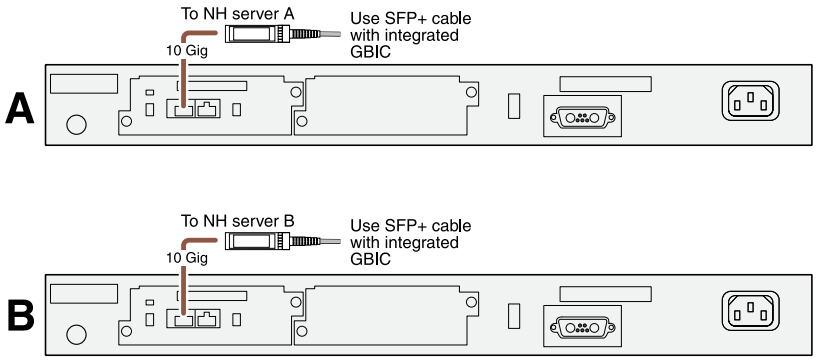
- HP 29xx series Gigabit Ethernet switch on a nearline K2 SAN.

Front view



Ports are for control connections as well as FTP connections from Grass Valley and 3rd party systems.

Rear view



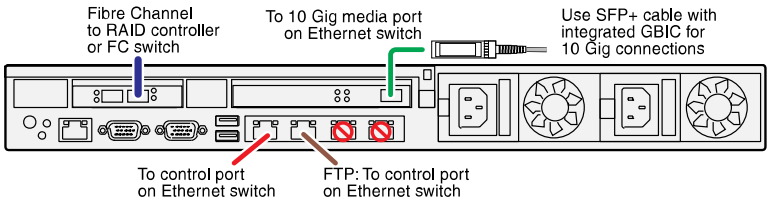
Cable K2 Media Server

As directed by the system diagram for your K2 SAN, cable the K2 Media Server or Servers for your K2 SAN using the instructions in this section.

K2-SVR basic Dell R620

These cabling instructions apply to the following:

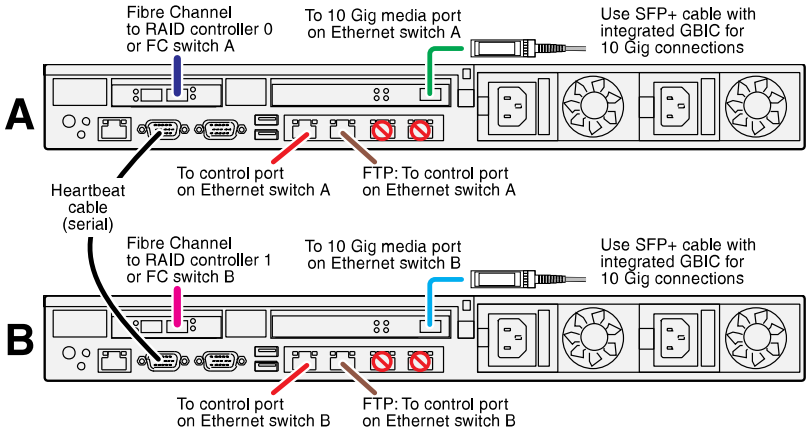
- Dell R620 PowerEdge Server on a basic (non-redundant) online or production K2 SAN.



K2-SVR redundant Dell R620

These cabling instructions apply to the following:

- Dell R620 PowerEdge Server on a redundant online or production K2 SAN.



Redundant server heartbeat serial cable

Take care to use the proper serial cable to interconnect redundant K2 Media Servers that take the role of file system/database servers. This cable supports the heartbeat mechanism whereby the servers monitor each other's health. It is a 9 pin serial cable, but it is not a standard RS-232 null modem cable. The heartbeat cable is supplied with your system (Grass Valley part number 174-8137-00) and has a pin configuration as follows:

1 – 4

2 – 3

3 – 2

4 – 1&6

5 – 5

6 – 4

7 – 8

8 – 7

9 – No Connect

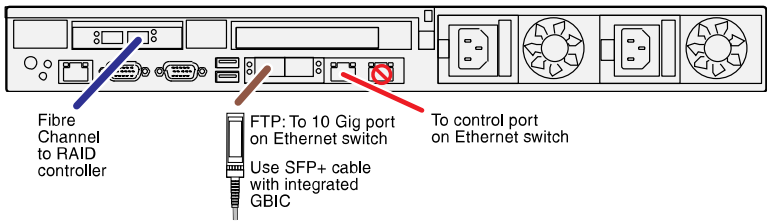
Cable NH10GE K2 Media Server

As directed by the system diagram for your K2 SAN, cable the NH10GE K2 Media Server or Servers for your K2 SAN using the instructions in this section

K2-SVR-NH10GE online/production Dell R620

These cabling instructions apply to the following:

- Dell R620 PowerEdge Server NH10GE on an online or production K2 SAN.

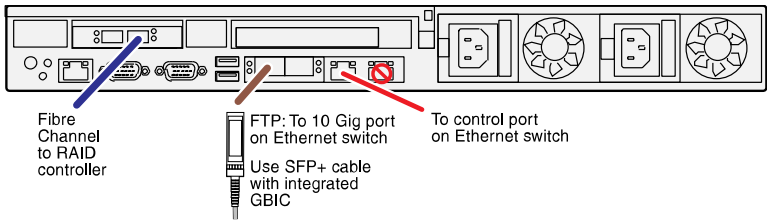


If you have more than one NH1 server, balance servers between controller 0 and controller 1.

K2-SVR-NH10GE basic nearline Dell R620

These cabling instructions apply to the following:

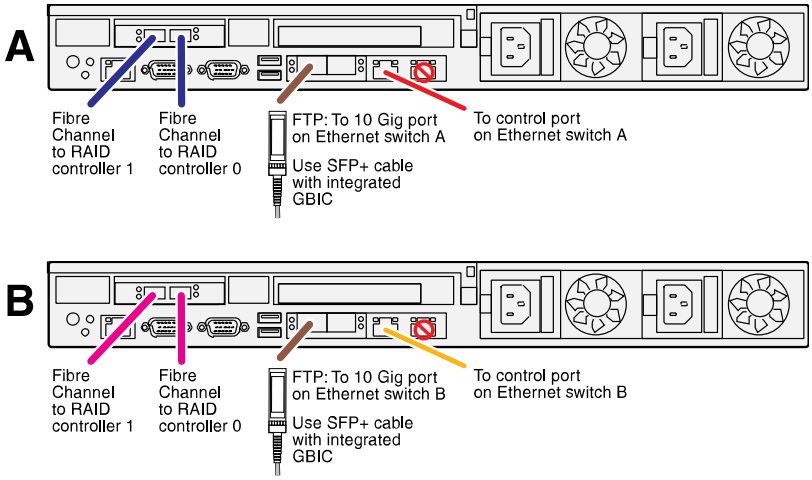
- Dell R620 PowerEdge Server NH10GE on a basic nearline K2 SAN.



K2-SVR-NH10GE redundant nearline Dell R620

These cabling instructions apply to the following:

- Dell R620 PowerEdge Server NH10GE on a nearline K2 SAN.



Cable K2 RAID

Before cabling, install the K2 RAID chassis in its permanent location. After mounting the chassis in the rack, you must secure brackets to the front rail to support the Grass Valley bezel. Refer to related topics in this document for rack mount instructions.

You do not need to manually set a Fibre Channel address ID on controllers or a chassis address on Expansion chassis.

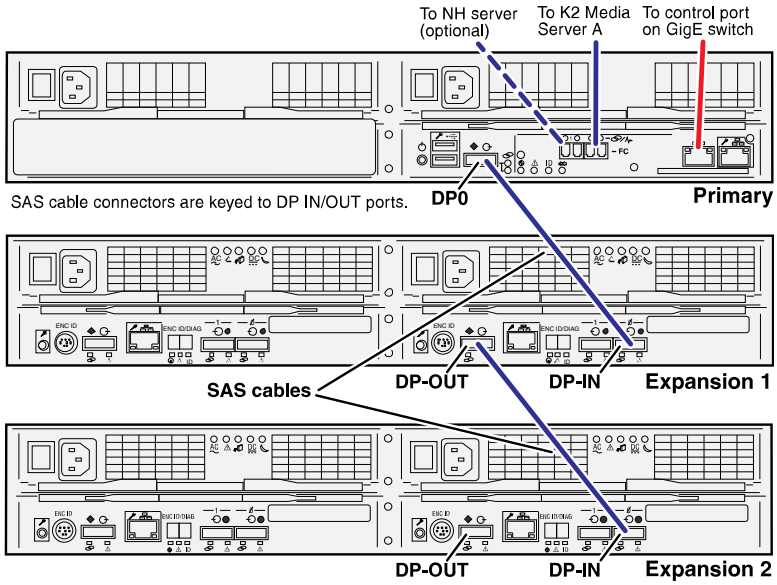
As directed by the system diagram for your storage system, cable the K2 RAID devices using the instructions in this section.

Once the RAID storage is connected and configured, do not swap Expansion chassis or otherwise reconfigure storage. If you connect an Expansion chassis in a different order or to the wrong controller, the controller will see a configuration mismatch and fault.

K2 RAID basic online/production

These cabling instructions apply to the following:

- K2 10Gv2 RAID on a basic (non-redundant) online or production K2 SAN.



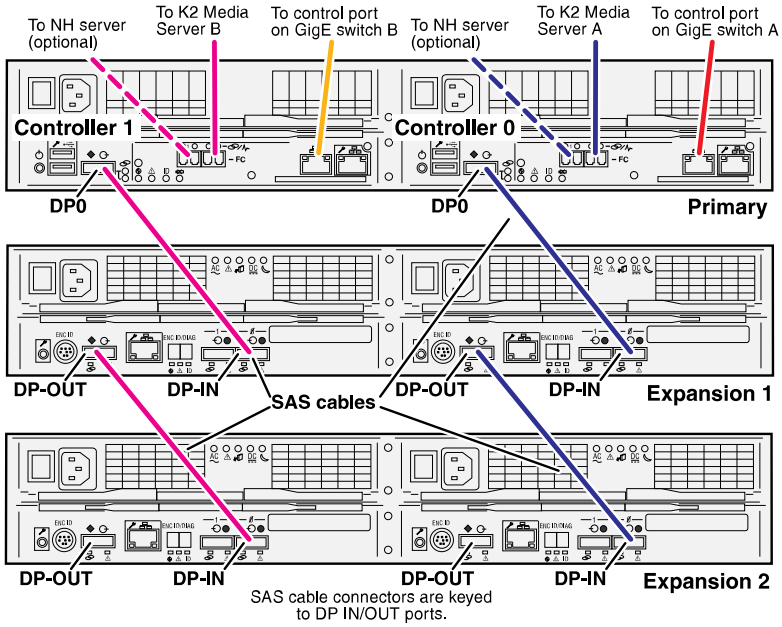
NOTE: Do not connect the controller Maintenance port. It should only be used with a PC in a peer-to-peer connection for diagnostics purposes.

Continue this cable pattern for additional Expansion Chassis.

K2 RAID redundant online/production

These cabling instructions apply to the following:

- K2 10Gv2 RAID on a redundant online or production K2 SAN.



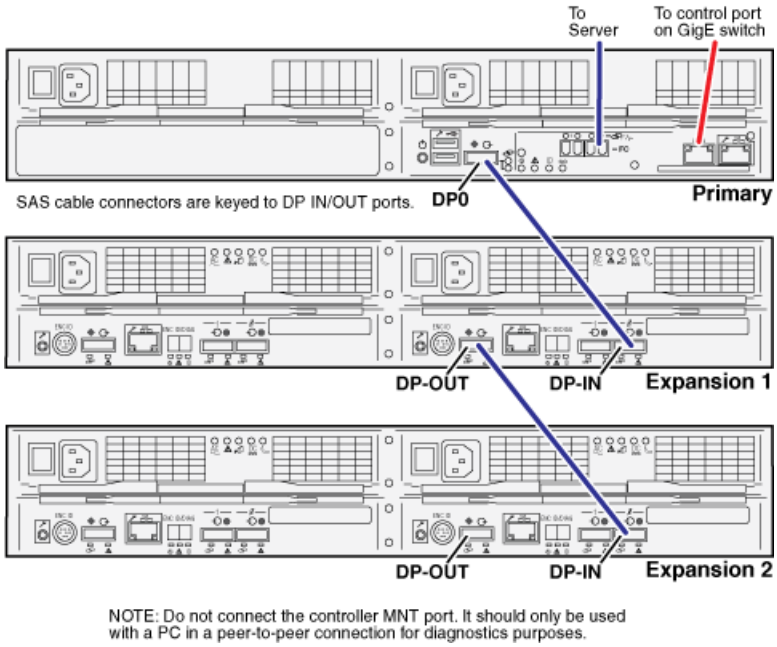
NOTE: Do not connect the controller MNT port. It should only be used with a PC in a peer-to-peer connection for diagnostics purposes.

Continue this cable pattern for additional Expansion Chassis.

K2 RAID basic nearline

These cabling instructions apply to the following:

- K2 10Gv2 RAID on a basic nearline K2 SAN.

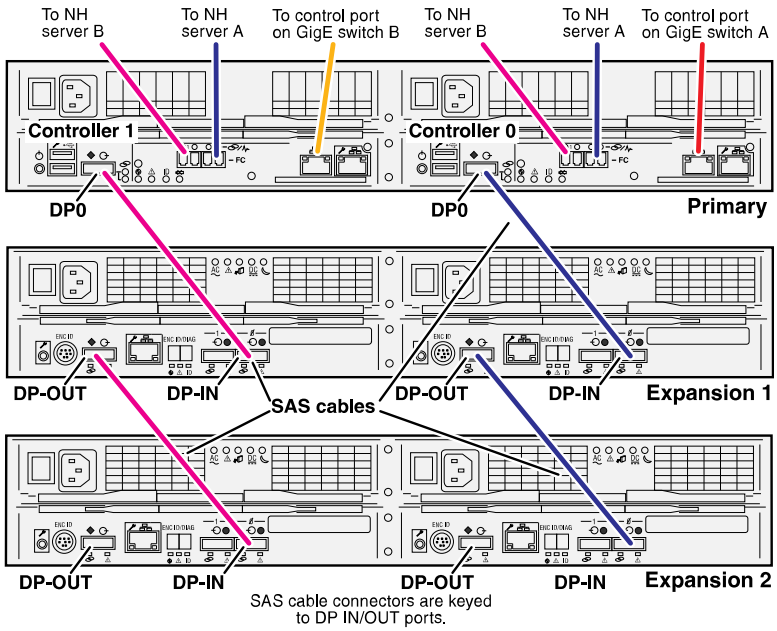


Continue this cable pattern for additional Expansion Chassis.

K2 RAID redundant nearline

These cabling instructions apply to the following:

- K2 10Gv2 RAID on a Nearline K2 SAN.



NOTE: Do not connect the controller MNT port. It should only be used with a PC in a peer-to-peer connection for diagnostics purposes.

Continue this cable pattern for additional Expansion Chassis.

Setting up the K2 SAN infrastructure

Setting up the Ethernet switch

Consult with Grass Valley and use the following topics to determine the network and switch configuration required for your site.

K2 SAN Ethernet switch requirements

K2 SAN Ethernet switch requirements are as follows:

- Redundancy — A redundant K2 SAN must have an “A” media network and a “B” media network and requires at least two switches, so that the A network and the B network never share the same switch. Media traffic does not cross between an “A” switch and a “B” switch.
- Separation of iSCSI traffic — Media (iSCSI) traffic must be kept separate from control traffic, FTP/streaming traffic, and any other type of traffic. This separation may be provided by VLANs or by using separate switches/fabrics.
- Inter Switch Links — Only control traffic and FTP traffic use ISLs. Media (iSCSI) traffic does not use ISLs.
- VLAN — When building VLANs on connected switches, common VLANs must have the same VLAN number. Never use VLAN 1 for anything other than the native VLAN.
- Trunks — Trunks must use LACP and must be tagged.
- Protocols — When integrating multiple switches, the spanning tree protocol must be MSTP. The routing protocol must be RIP.
- Port security — Do not use port security.

- IGMP — Enable IGMP snooping on the control network and on the corporate LAN, to support the low-resolution live streaming traffic generated by K2 Summit systems.

Default Ethernet switch design

A K2 SAN system that ships from Grass Valley with self-contained networks is described as follows. This network and switch configuration meets the K2 SAN Ethernet switch requirements:

- Switches are HP ProCurve.
- A non-redundant K2 SAN has a single switch. Redundant K2 SANs have at least two switches to support an "A" media network and a "B" media network.
- There are three 1 Gig Inter-Switch Links (ISLs) between redundant switches. This is the default configuration for all K2 SANs and provides sufficient bandwidth for most FTP traffic loads.
- The ISLs are configured as a trunk using LACP. Trunk ports are labeled Trk1.
- Each switch has two VLANs, with half the switch's ports on each VLAN. The media (iSCSI) traffic uses one VLAN and all other traffic uses the other VLAN. This "other" traffic can include both FTP and control traffic, as it is allowed that they be on the same VLAN.
- The control/FTP VLAN ID is 10. The media VLAN ID is 60.
- IGMP Snooping is enabled on the control/FTP VLAN, to support low-resolution live streaming.
- Even numbered ports are control/FTP VLAN. Odd numbered ports are media VLAN.
- The SNMP community name is public and RW permissions are unrestricted. SNMP trap authentication is enabled.
- Spanning Tree is enabled.
- If a 10 Gig SFP+ port on the back of the switch connects to a K2 Media Server (FSM) for media (iSCSI) traffic, the port is in the media VLAN. If a 10 Gig SFP+ port connects to a NH10GE K2 Media Server for FTP traffic, the port is in the control/FTP VLAN.
- If enough "control" ports (non-iSCSI ports) are available on a switch or switches configured for an online K2 SAN, the Nearline system can be connected to those control ports. It is not required that a GigE switch be dedicated to the Nearline system.

Design considerations for Ethernet switches

Extended network and switch configurations are available upon consultation with Grass Valley. Guidelines are as follows:

- Port count — The number of client connections, FTP/streaming connections, and other connections determine how many ports are required. As the port count increases, you must use switches with more ports and/or multiple switches. When multiple switches are used, the port count assigned to each VLAN and the ports used for ISLs must be considered.
- Switch/fabric design — On large multiple switch systems, designers with sufficient knowledge have options for the separation of iSCSI traffic. For example, you can use one switch/fabric for media traffic, one switch/fabric for control traffic, and one switch/fabric for FTP traffic.
- You can trunk up to ten Cisco ports and four HP ports together, as necessary for your switch design.

- FTP bandwidth — This is a consideration if using multiple switches that share the FTP traffic. In this case you must use sufficient ISLs to provide the bandwidth needed to support your FTP traffic load between switches. FTP traffic is variable and has potentially higher bandwidth needs, it is the primary consideration when designing ISLs. When using 1 Gig connections for ISLs, connect and configure as follows, taking your FTP bandwidth into consideration:

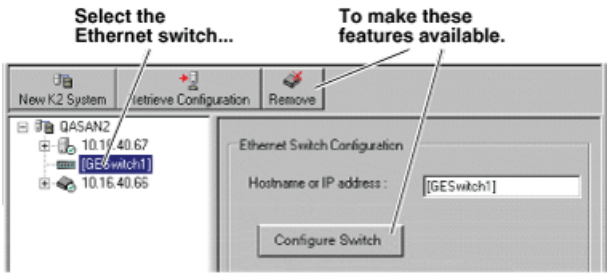
Maximum FTP bandwidth	Trunk/ISLs required
Less than 100 MB/sec	A trunk with three 1 Gb/s ISLs
100 - 300 MB/sec	A trunk with five 1 Gb/s ISLs
More than 300 MB/sec	A trunk with two 10 Gb/s ISLs

NOTE: One Gig ISLs must be an odd number (3 or 5).

If a switch's 10 Gig connections are not used for other purposes, such as connection to a K2 Media Server, you can use the 10 Gig connections for ISLs.

Configuring a switch through the K2Config application

In the K2 System Configuration (K2Config) application , features for working on a Ethernet switch are as follows:



From the K2Config application, you can click the **Configure Switch** button to open the switch's web configuration application. Refer to the installation procedures elsewhere in this document for switch configuration information.

Configuring QOS on the GigE switch

- The switch must be a HP ProCurve switch 29xx series.
- Trunks, VLANs and all other configuration must be complete.
- The switch must have an IP address

- You must have network access to the switch

Use this procedure to make the Quality of Service (QOS) setting on the HP ProCurve switch 29xx series.

1. If you have not already done so, from a network connected PC open the MS-DOS command prompt and login to the switch as administrator, as follows:
   a) Telnet to the switch. For example, if the switch's IP address is 192.168.40.12, you type the following, then press **Enter**.

      ```
      telnet 192.168.40.12
      ```

   b) Press **Enter** one or more times until the switch's username prompt appears.
   c) Type the switch's administrator username and press **Enter**, then type the switch's administrator password and press **Enter**. The switch console command (CLI) prompt appears.
2. Type `config` then press **Enter**.

   You are now in configuration mode.
3. Type `qos queue-config 2-queues` then press **Enter**.

   This limits the number of active queues within the switch giving the most buffering to VLANs 10 and 60.
4. Type `show qos vlan` then press **Enter**.

   The screen displays VLAN information. Note the ID number of the Media (iSCSI) VLAN. It should be 60, as follows:

   ```
   VLAN priorities

     VLAN ID Apply rule  | DSCP   Priority
     ------- ----------- + ------ -----------
     10      No-override |        No-override
     60      No-override |        No-override
   ```

5. a) Assign the Media VLAN the QOS priority of 3. For example, if the VLAN ID is 60, you type the following, then press **Enter**.

      ```
      vlan 60 qos priority 3
      ```

   b) Type `show qos vlan` then press **Enter**.

      The screen displays VLAN information. Make sure that the Priority column reports that the Media VLAN has a value of 3.

Next, verify flow control settings.

Upgrading firmware on HP switch

1. If you have not already done so, install a TFTP Server.

   For example, to install *`tftpd32.exe`*, go to *`http://tftpd32.jounin.net/`*.
2. Open the TFTP Server.
3. Make sure your current working directory includes the *`*.swi`* file that you are using for the upgrade.

4. Execute the copy command with the following syntax:

   ```
   copy tftp flash <ip-address> <remote-os-file> [ < primary | secondary
   > ]
   ```

   Note that if you do not specify the flash destination, the TFTP download defaults to the primary flash.

   For example, to download a software file named T_13_23.swi from a TFTP server with the IP address of 10.16.34.3 1, use the following:

   ```
   ProCurve # copy tftp flash 10.16.34.3 T_13_23.swi
   ```

5. When prompted `The primary OS image will be deleted. continue [y/n]?`, press **Y**.

   When the switch finishes downloading the software file from the server, it displays the progress message `Validating and Writing System Software to FLASH...`

6. Wait until the CLI prompt re-appears, then continue with the next step in this procedure.
7. Check the version of firmware on the switch. To do this, type the following, then press **Enter**:

   ```
   show flash
   ```

   Information is displayed similar to the following example:

   ```
   HP_iSCSI_switch1# show flash
   Image           Size(Bytes)   Date    Version
   -----           ----------  --------  -------
   Primary Image   : 6737518   07/25/08  T.13.23
   Secondary Image : 5886358   10/26/06  T.11.12
   Boot Rom Version: K.12.12
   Current Boot    : Primary
   ```

8. Verify that the new software version is in the expected flash area (primary or secondary).
9. Restart the switch from the flash area that holds the new software (primary or secondary).

Setting up the control point PC

To set up the Control Point PC, you have the following options:

- Use the Grass Valley Control Point PC that comes from the factory with software pre-installed.
- Use a PC that you own and install the required software.

1. For either option, you must do the following for the Control Point PC that runs the K2 System Configuration application:
   a) Assign a control network IP address to the PC.
   b) Connect the PC to the GigE control network.

2. To use your own PC, you must additionally do the following:
   a) Verify that the PC meets system requirements.
   b) Install the K2 Control Point software.
   c) Install SiteConfig software.
   d) Install other supporting software.
   e) Install and license SNMP Manager software. This can be on the K2 SAN control point PC or on a separate SNMP Manager PC that monitors the K2 SAN.

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

Install SiteConfig on control point PC

Work through the following topics to install the SiteConfig application on the control point PC.

About installing SiteConfig

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

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

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

For a given system, there should be just one instance of SiteConfig managing the system.

System requirements for SiteConfig host 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 3 • Server 2003 • Vista Enterprise Service Pack 1 • Windows 7 • Server 2008 R2
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

Requirements	Comments
Hard disk space	400 MB
Microsoft .NET Framework	Version 4.0
Java JRE	1.3.1_12 and 1.4.2_05 or higher. Required for the HP Ethernet Switch configuration interface, which is used for K2 SANs.
XML	Microsoft XML 4 Service Pack 2 is required.

Installing/upgrading SiteConfig

- The PC on which you are installing SiteConfg must meet system requirements.
- The PC must be connected to the LAN on which all the devices to be managed are connected.
- There must be no routed paths to the devices to be managed.

1. Procure SiteConfig installation files from the Grass Valley website or via other distribution mechanisms.

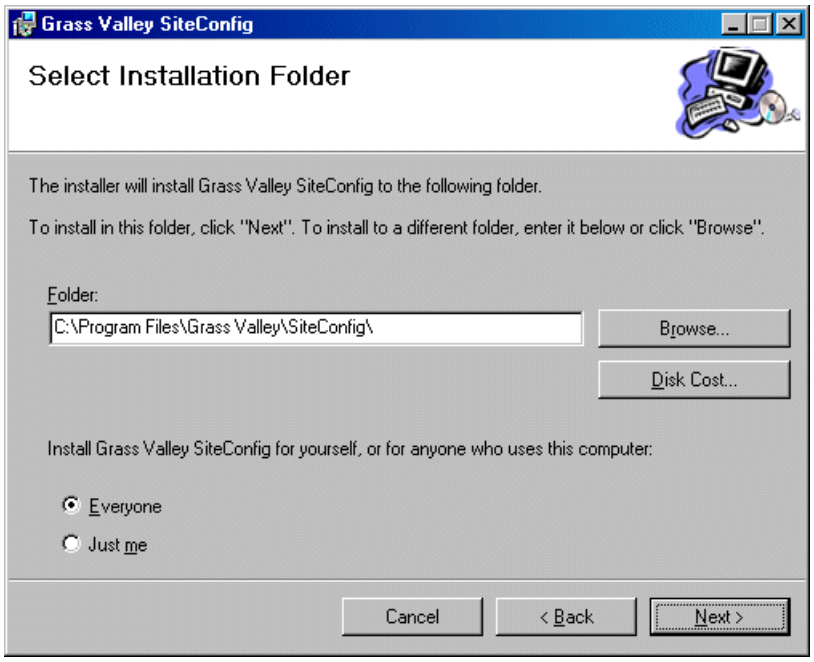
   The following directory and files are required to install SiteConfig:

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

2. If you already have a version of SiteConfig installed, go to Windows **Add/Remove Programs** and uninstall it.
3. Double-click *setup.exe*.

   The installation wizard opens.

4. Work through the wizard pages, clicking **Next** and **Finish**.



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

5. Open the Windows operating system Services control panel on the PC and look for an entry called " ProductFrame Discovery Agent".

   The Discovery Agent must be installed on the SiteConfig PC so that the PC can be discovered by SiteConfig and added to the system description as a managed device. This is necessary to ensure name resolution in SiteConfig's hosts file.

   The Discovery Agent is also known as the Network Configuration Connect Kit. For example, in Windows Add/Remove Programs, it can be displayed as either Network Configuration Connect Kit or SiteConfig Discovery Agent.

6. Proceed as follows:

   - If the Discovery Agent is not installed, navigate to the SiteConfig install location's Discovery Agent Setup subdirectory and double-click the `DiscoveryAgentServiceSetup.msi` file. This launches the setup program and installs the Discovery Agent. Follow the setup wizard to complete installation. A restart is required after installation. Then continue with the next step in this procedure.
   - If the Discovery Agent is already installed, continue with the next step in this procedure.

7. If not already configured, configure the SiteConfig PC with a valid Ethernet IP address for the LAN using Windows Network Connections.
8. If you are not going to be using SiteConfig to manage system hosts files, put the system hosts file on the SiteConfig PC.

Planning and implementing a K2 SAN with SiteConfig

About developing a system description

You use SiteConfig to create or modify a system description for the K2 SAN. You can do this in your planning phase, even before you have devices installed or cabled. Your goal is to have the SiteConfig system description accurately represent all aspects of your devices and networks before you begin actually implementing any networking or other configuration tasks.

There are several task flows you can take to develop a system description, as follows:

- Obtain the sales tool system description. This is the system description that was developed for your specific K2 SAN as part of the sales process. It should be a very accurate representation of the K2 SAN that is to be installed at the customer site. Import the system description into SiteConfig and then make final modifications.
- Obtain a similar K2 SAN's system description, import it into SiteConfig, and then modify it until it matches your K2 SAN.
- In SiteConfig, use the New Site Wizard to create a new system description. The wizard has models based on the pre-defined K2 SAN levels. You can enter much of your site-specific information as you work through the wizard, and then do final modifications using other SiteConfig features.

The topics in this manual follow the task flow for the sales tool system description. If you are using a different taskflow, use the topics in this manual as appropriate and refer to the *SiteConfig User Manual* or *SiteConfig Help Topics* for additional information.

Importing a system description

- The SiteConfig PC must have access to the system description file you are importing.
- Windows Explorer Folder Options must be set to Show hidden files and folders in order to see all the folders containing SiteConfig files.

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 **Import**.
   - If the SiteConfig main window opens, click **File | Import**.

   The Import System Description dialog box opens.

2. Browse to and select a system description file (`*.scsd`) and click **Open**.

The current system description is closed and the system description you are importing is displayed in SiteConfig.

About device and host names

In SiteConfig, a device can have different names, as follows:

- Device name — This is a name for display in SiteConfig only. It is stored in the SiteConfig system description, but not written to the actual device. It is displayed in the device tree view and in the device list view. It can be a different name than the device's host name.
- Host name — This is the network name of the device. SiteConfig has a default naming convention for host names which you can use or override with your own host names.

In most cases it is recommended that the Device name and Host name be the same. This avoids confusion and aids troubleshooting.

The Device name can serve as a placeholder as a system is planned and implemented. During the install/commission process, when you reconcile a device's current and planned network interface settings, the Host name as configured in the system description can be overwritten by the host name on the actual device. However, the Device name configured in the system description is not affected. Therefore it is recommended that in the early planned stages, you configure the Device name to be the desired name for the device, but do not yet configure the Host name. Then, after you have applied network interface settings, you can change the Host name to be the same as the Device name. This changes the host name on the actual device so that then all names are in sync.

SiteConfig does not allow duplicate device names or host names.

Items in the tree view are automatically sorted alphabetically, so if you change a name the item might sort to a different position.

Modifying a device name

1. In the **Network Configuration | Devices** tree view, right-click a device and select **Rename**.
2. Type in the new name.

   Note that this does not change the hostname on the physical device. If you want the hostname to match the device name, you must also modify the hostname.

Modifying the control network

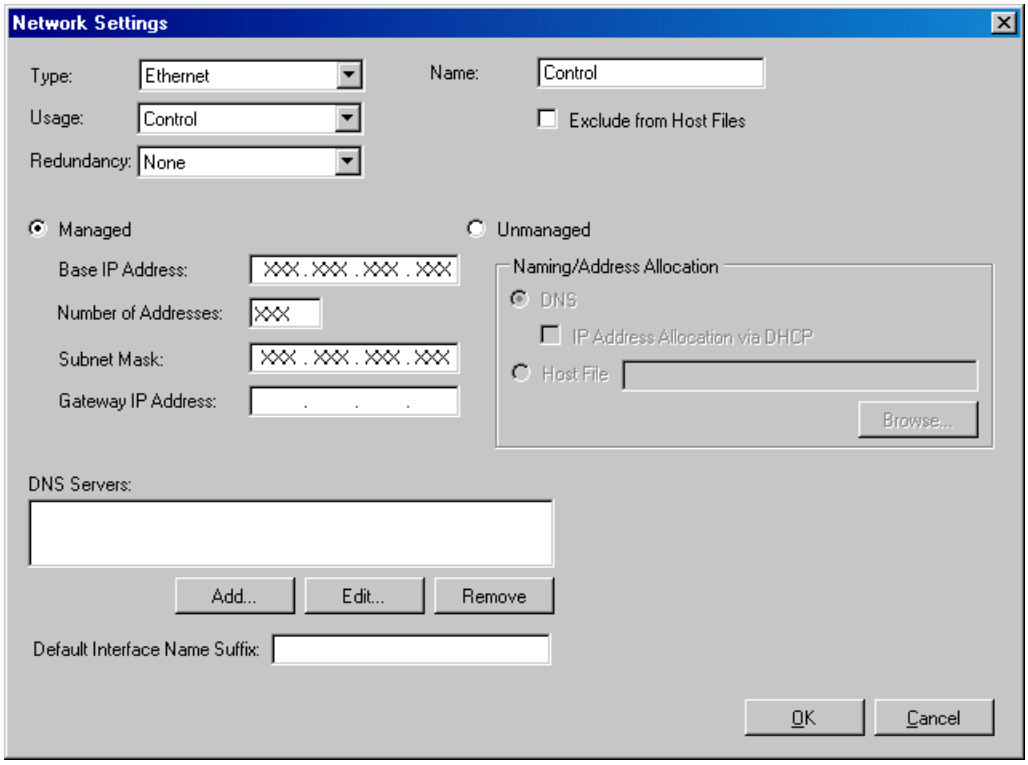
1. In the **Network Configuration | Networks** tree view, select the K2 SAN's Site node.

   The networks under that node are displayed in the list view.

2. Proceed as follows:

   - In the list view, right-click the Control network and select **Details**.

   The Network Settings dialog box opens.



3. Configure the settings for the network as follows:

Setting...	For control network
Type	*Ethernet* is required
Usage	*Control* is required
Redundancy	*None* is required. This is true even on a redundant K2 SAN. (Only the iSCSI network is redundant on a redundant K2 SAN.)
Name	*Control* is recommended
Exclude from Host Files	*Unselected* is required
Managed	*Selected* 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	*Unselected* 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.

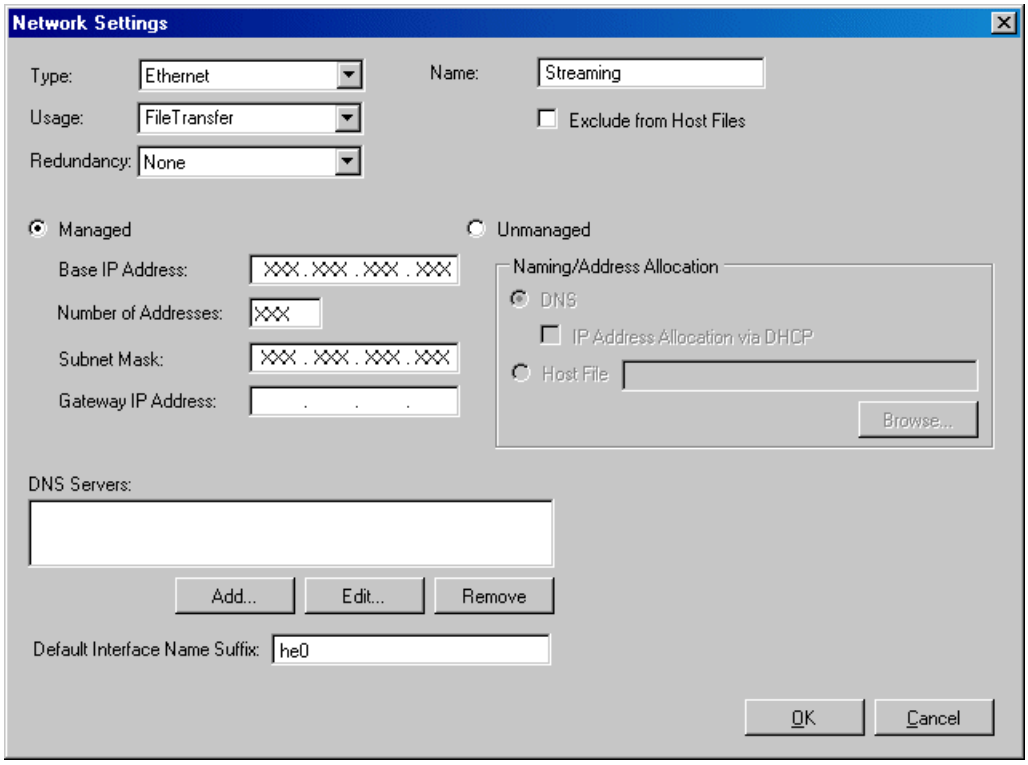
Modifying the FTP/streaming network

1. In the **Network Configuration | Networks** tree view, select the K2 SAN's Site node.
   The networks under that node are displayed in the list view.

2. Proceed as follows:

   - In the list view, right-click the Streaming network and select **Details**.

   The Network Settings dialog box opens.



3. Configure the settings for the network as follows:

Setting...	For FTP/streaming network
Type	*Ethernet* is required
Usage	*FileTransfer* is required
Redundancy	*None* is required. This is true even on a redundant K2 SAN. (Only the iSCSI network is redundant on a redundant K2 SAN.)
Name	*Streaming* is recommended
Exclude from Host Files	*Unselected* is required
Managed	*Selected* 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	*Unselected* is required. Related settings are disabled.
DNS Servers	Servers providing DNS for name resolution. Allowed.
Default Interface Name Suffix	*_he0* is required

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

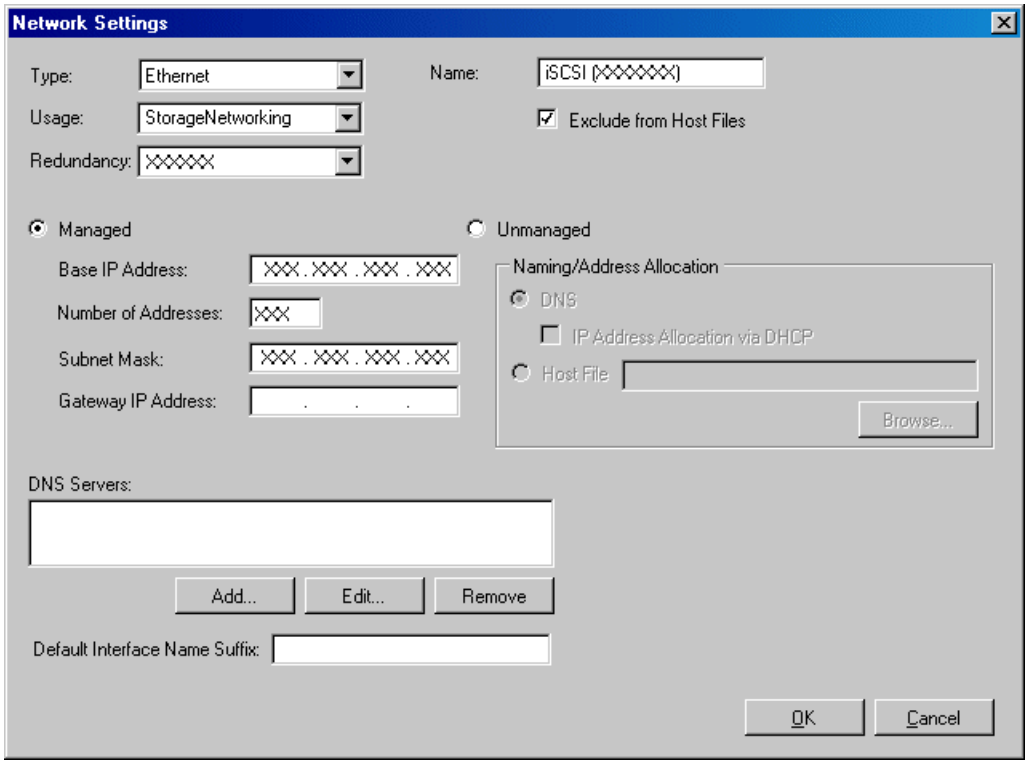
Modifying a media (iSCSI) network

1. In the **Network Configuration | Networks** tree view, select the K2 SAN's Site node.
   The networks under that node are displayed in the list view.

2. Proceed as follows:

   - If the K2 SAN is basic (non-redundant), in the list view, right-click the iSCSI network and select **Details**.
   - If the K2 SAN is redundant, in the list view, first right-click the primary iSCSI network and select **Details**. Then proceed to modify the primary iSCSI network. After the primary iSCSI network is modified, repeat these steps and modify the secondary iSCSI network.

   The Network Settings dialog box opens.



3. Configure the settings for the network as follows:

Setting...	For media (iSCSI) network
Type	*Ethernet* is required
Usage	*StorageNetworking* is required
Redundancy	*None* is required for a basic (non-redundant) K2 SAN
	Primary is required for a redundant K2 SAN media network A
	Secondary is required for a redundant K2 SAN media network B
Name	*iSCSI (non-Redundant)* is recommended for a basic (non-redundant) K2 SAN
	iSCSI (Primary Redundant) is recommended for a redundant K2 SAN media network A
	iSCSI (Secondary Redundant) is recommended for a redundant K2 SAN media network B
Exclude from Host Files	*Selected* is required
Managed	*Selected* 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	Not allowed
Unmanaged	*Unselected* is required. Related settings are disabled.
DNS Servers	Not allowed
Default Interface Name Suffix	Not allowed

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

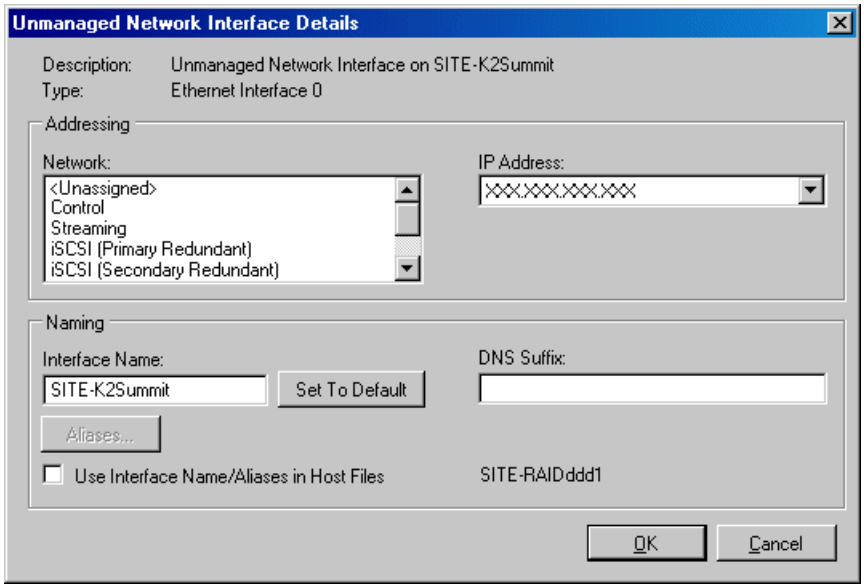
About IP configuration of network interfaces on devices

You can perform IP configuration of network interfaces when working with a placeholder device prior to discovery. When you add a device and choose a particular model, the model defines the number, type and usage characteristics of network interfaces to expect on such a device.

You can view and edit each network interface and set up IP configuration selecting an appropriate IP from the network to which each interface connects. The process for editing IP configuration varies, depending on the device's phase.

Placeholder device IP configuration

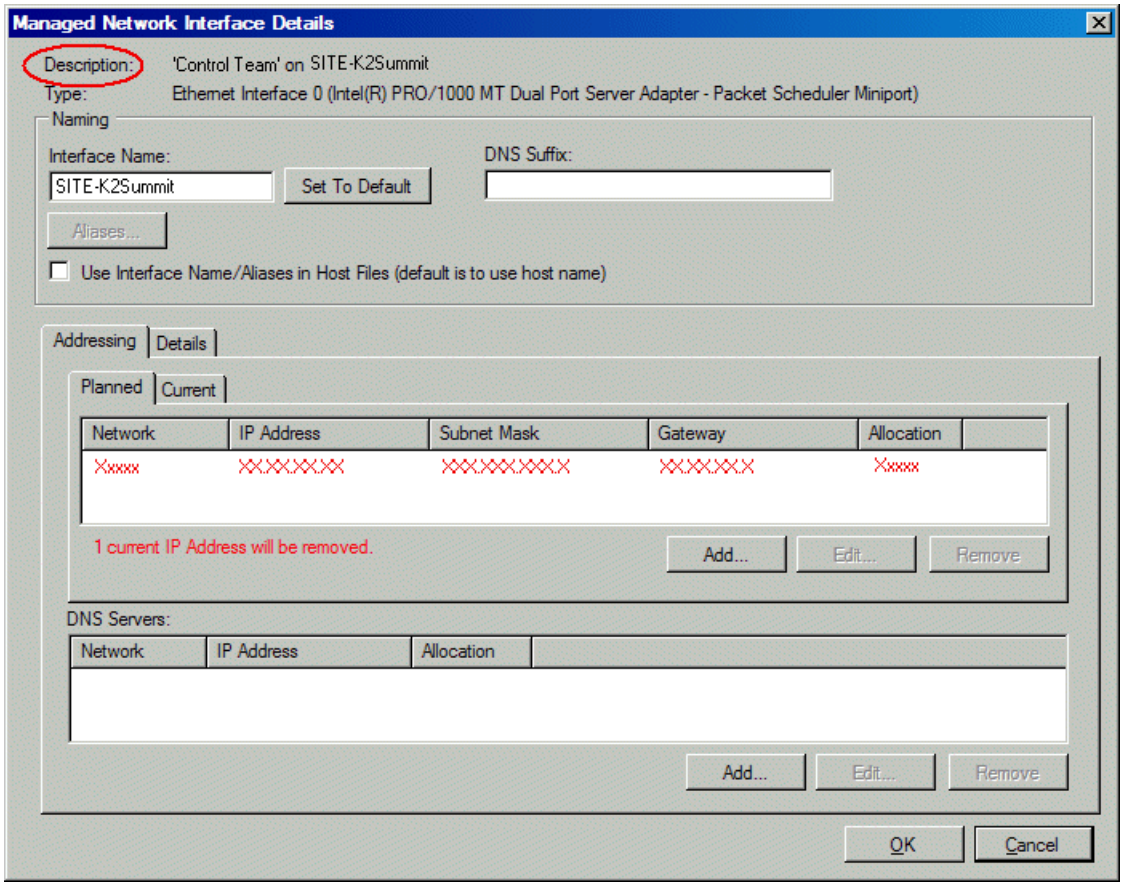
On a placeholder device, you edit network interfaces using the Unmanaged Network Interfaces dialog box.



The Unmanaged Network Interfaces dialog box allows you only to save changes to the system description.

Discovered device IP configuration

On a discovered device, you edit network interfaces using the Managed Network Interfaces dialog box.



The Managed Network Interfaces dialog box allows you to edit and save changes to the device.

Modifying K2 client unassigned (unmanaged) interface

- The system description has a SAN K2 client that is a placeholder device.
- The placeholder device must have one or more unmanaged network interfaces.

Use this task to modify unmanaged network interfaces on a K2 SAN device as follows:

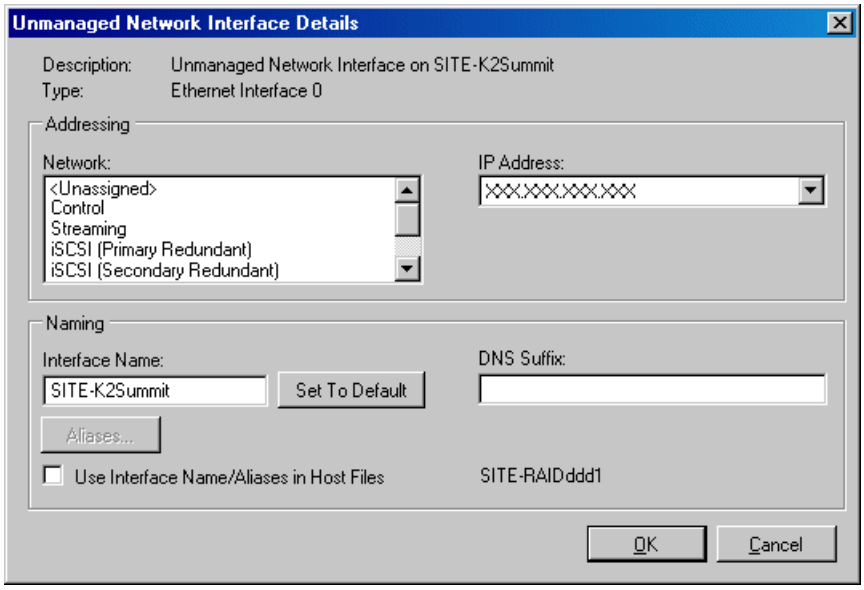
- K2 Summit Production Client

1. In the **Network Configuration | Devices** tree view, select a SAN K2 client placeholder device.

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

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	*Control* is required
IP Address	The IP address for this interface on the network. Required.
Interface Name	The device host name. Required.
Set to Default	Not recommended. Sets the interface name to SiteConfig default convention, based on the root Site name and device-type.
...use Interface Name/Aliases in Host Files...	*Unselected* is required. Since not selected, the default behavior occurs, which is to use the device host name in the hosts file.
Aliases	Not allowed
DNS Suffix	Allowed, if applicable to the network. The DNS suffix is added to the interface name.

Setting...	For media (iSCSI) network interface
Network	*iSCSI (non-Redundant)* is required for one iSCSI interface on a K2 client on a basic K2 SAN. The other iSCSI interface is unused.
	iSCSI (Primary Redundant) is required for one iSCSI interface on a K2 client on a redundant K2 SAN.
	iSCSI (Secondary Redundant) is required for the other iSCSI interface on a K2 client on a redundant K2 SAN
IP Address	The IP address for this interface on the network. Required.
Interface Name	Disabled, since names are excluded from the hosts file. Disregard.
Set to Default	Disabled, since names are excluded from the hosts file. Disregard.
...use Interface Name/Aliases in Host Files...	Disabled, since names are excluded from the hosts file. Disregard.
Aliases	Disabled, since names are excluded from the hosts file. Disregard.
DNS Suffix	Disabled, since names are excluded from the hosts file. Disregard.

NOTE: There is no FTP/streaming network for a SAN K2 client. On the K2 SAN, FTP/streaming goes to the K2 Media Server.

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

Modifying K2 Media Server unassigned (unmanaged) interface

- The system description has a K2 Media Server that is a placeholder device.

- The placeholder device must have one or more unmanaged network interfaces.

Use this task to modify managed network interfaces on a K2 SAN device as follows:

- K2 Media Server
- NH K2 Media Server

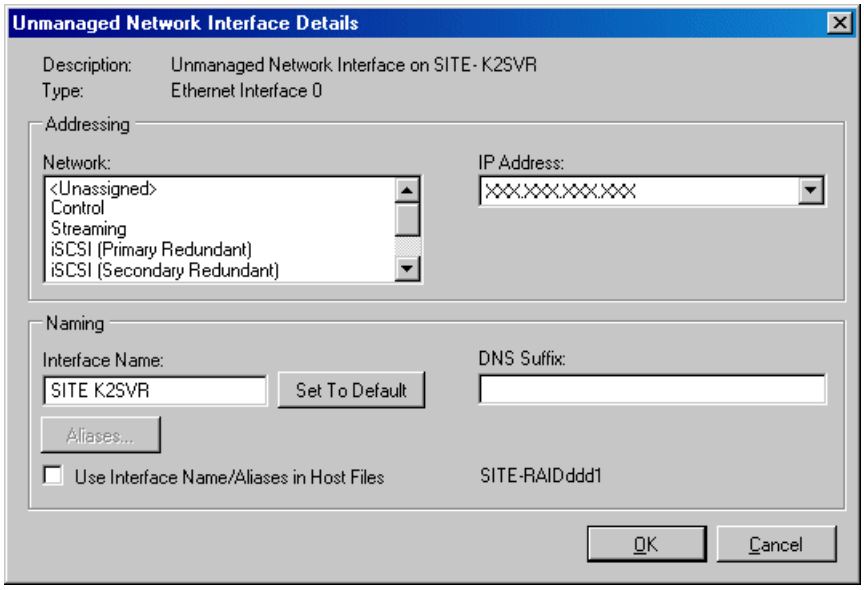
For the K2 Media Server, do not configure the Fibre Channel interface. SiteConfig does not manage this interface. It is represented in SiteConfig only to complete the description of the K2 Media Server.

1. In the **Network Configuration | Devices** tree view, select a K2 Media Server placeholder device.

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

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	*Control* is required
IP Address	The IP address for this interface on the network. Required.
Interface Name	The device host name. Required.
Set to Default	Not recommended. Sets the interface name to SiteConfig default convention, based on the root Site name and device-type.
...use Interface Name/Aliases in Host Files...	*Unselected* is required. Since not selected, the default behavior occurs, which is to use the device host name in the hosts file.
Aliases	Not allowed
DNS Suffix	Allowed, if applicable to the network. The DNS suffix is added to the interface name.

Setting...	For FTP/streaming network interface
Network	*Streaming* 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 *K2prod01*, then *K2prod01_he0* 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...	*Selected* is required
Aliases	Not allowed
DNS Suffix	Allowed, if applicable to the network. The DNS suffix is added to the interface name.

Setting...	For media (iSCSI) network interface
Network	*iSCSI (non-Redundant)* is required on K2 Media Server for all interfaces of type iSCSI on basic K2 SAN.
	iSCSI (Primary Redundant) is required on K2 Media Server A for all interfaces of type iSCSI on redundant K2 SAN
	iSCSI (Secondary Redundant) is required on K2 Media Server B for interfaces of type iSCSI on redundant K2 SAN
IP Address	The IP address for this interface on the network. Required.
Interface Name	Disabled, since names are excluded from the hosts file. Disregard.

Setting...	For media (iSCSI) network interface
Set to Default	Disabled, since names are excluded from the hosts file. Disregard.
...use Interface Name/Aliases in Host Files...	Disabled, since names are excluded from the hosts file. Disregard.
Aliases	Disabled, since names are excluded from the hosts file. Disregard.
DNS Suffix	Disabled, since names are excluded from the hosts file. Disregard.

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

About SiteConfig support on K2 devices

Before SiteConfig can be used to discover or manage a device, the device must meet the following requirements:

- The device must be a Microsoft Windows operating system device.
- The device must have Microsoft .NET version 3.5 installed, as reported in the Windows Add/Remove Programs control panel.
- The SiteConfig Discovery Agent service must be running on the device, as reported in the Windows Services control panel.

For K2 clients and K2 Media Servers shipped new from Grass Valley with K2 software version 7.0 or higher, these requirements are pre-installed. These requirements are pre-installed on recovery images for these K2 systems as well. Therefore, if you suspect a problem with these requirements, do not attempt to install SiteConfig support requirements. If you must restore SiteConfig support requirements, re-image the K2 system.

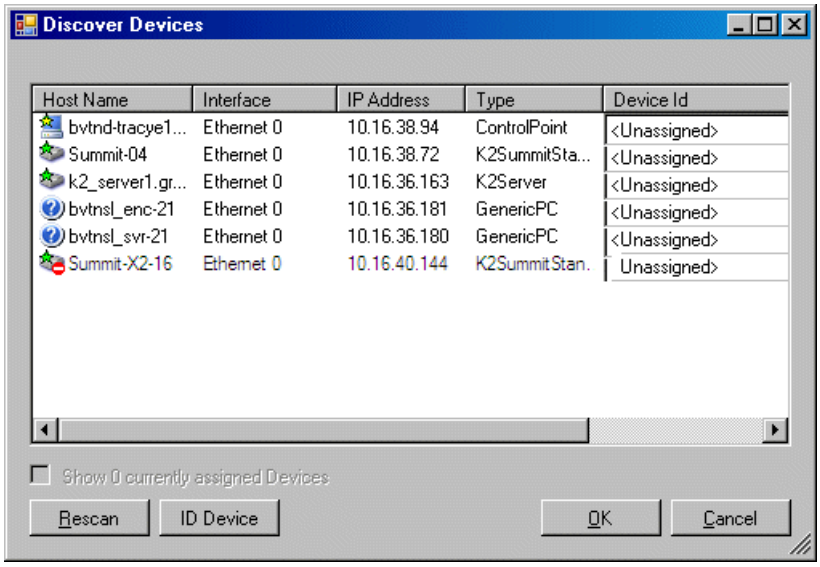
Discovering devices with SiteConfig

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

1. Open SiteConfig.

2. In the toolbar, click the discover devices button.

   The Discover Devices dialog box opens.



   A list of discovered devices is displayed.

3. Click **Rescan** to re-run the discovery mechanism. You can do this if a device that you want to discover has its network connection restored or otherwise becomes available. Additional devices discovered are added to the list.

Assigning discovered devices

- Devices must be discovered by SiteConfig
- Discovered devices must not yet be assigned to a device in the system description
- The system description must have placeholder devices to which to assign the discovered devices.

1. If the Discovered Devices Dialog box is not already open, click the discover devices button.

   The Discover Devices dialog box opens.

2. Identify discovered devices.

   - If a single device is discovered in multiple rows, it means the device has multiple network interfaces. Choose the interface that represents the device's currently connected control connection. This is typically Ethernet ... 0.
   - If necessary, select a device in the list and click **ID Device**. This triggers an action on the device, such as flashing an LED or ejecting a CD drive, to identify the device.

3. To also view previously discovered devices that have already been assigned to a device in the system description, select **Show ... currently assigned devices**.

   The currently assigned devices are added to the list. Viewing both assigned and unassigned devices in this way can be helpful to verify the match between discovered devices and placeholder devices.

4. In the row for each discovered device, view items on the Device Id drop-down list to determine the match with placeholder devices, as follows:
   - If SiteConfig finds a match between the device-type discovered and the device-type of one or more placeholder devices, it displays those placeholder devices in the list.
   - If SiteConfig does not find a match between the device-type discovered and the device-type of a placeholder device, no placeholder device is displayed in the list.
5. In the row for a discovered device, click the Device Id drop-down list and select the placeholder device that corresponds to the discovered device.

   If there is no corresponding placeholder device currently in the system description, you can select **Add** to create a new placeholder device and then assign the discovered device to it.
6. When discovered devices have been assigned, click **OK** to save settings and close.
7. In the **Network Configuration | Devices** tree view, select each of the devices to which you assigned a discovered device.

Modifying K2 client managed network interfaces

- The physical device you are configuring must be discovered and must be assigned to a device in the SiteConfig system description.
- SiteConfig must have communication with the device.
- The device must be defined in the system description with an appropriate network interface.

Use this task to modify managed network interfaces on a K2 SAN device as follows:

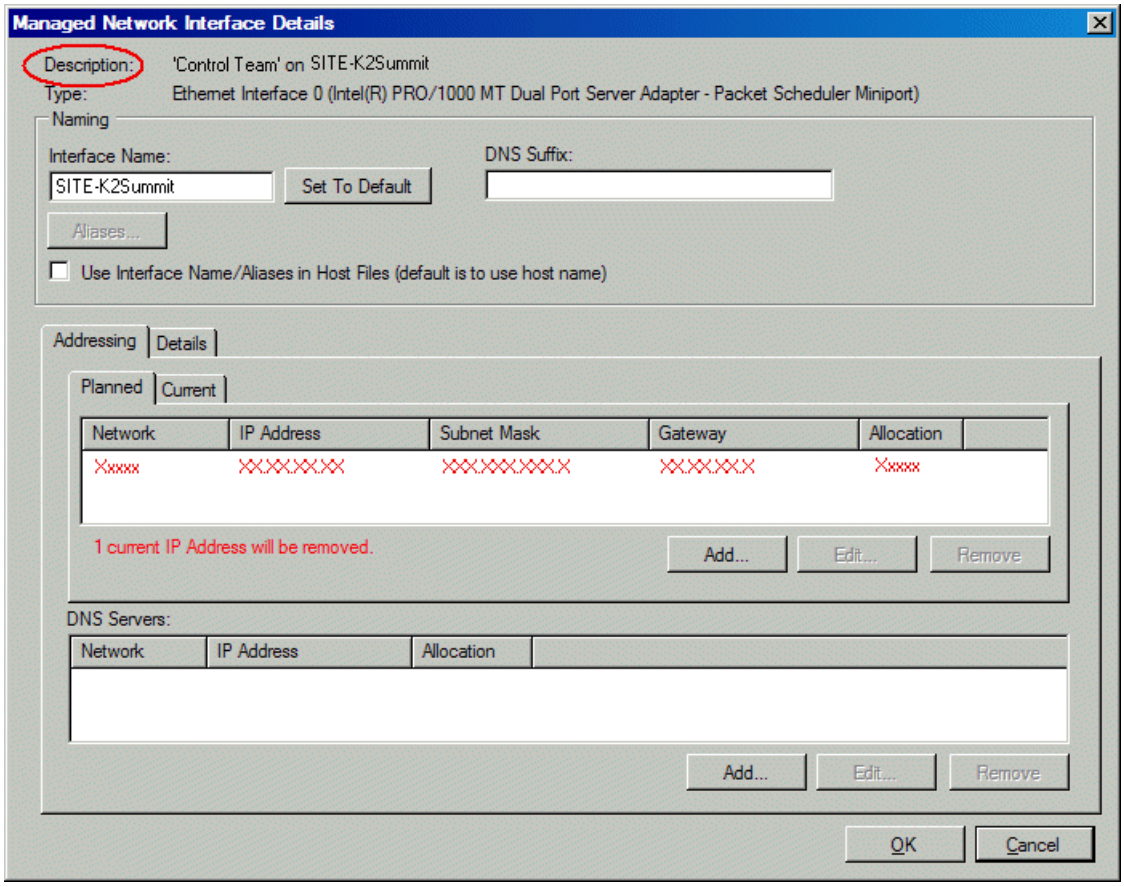
- K2 Summit Production Client

1. In the tree view select a K2 client, then in the Interfaces list view, identify interfaces as follows:
   - The SAN K2 client's control 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. Do not modify these two individual interfaces.
   - For a SAN K2 client on a basic (non-redundant) K2 SAN, identify the iSCSI (non-Redundant) interface. After the control team, modify this interface as instructed in this procedure. Do not configure any other iSCSI interface, as only one iSCSI interface is used for a basic K2 SAN.
   - For a SAN K2 client on a redundant K2 SAN, identify the iSCSI (Primary Redundant) interface and the iSCSI (Primary Secondary) interface. After the control team, modify these interfaces as instructed in this procedure.
   - The SAN K2 client has no interface for FTP/streaming. All FTP/streaming goes to the K2 Media Server.

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. The control connection should always be the first port on the motherboard, except when you have a loopback connection.
   - Configure the control network interface first before configuring any of the other interfaces.
   - 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.
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.
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
Use Interface Name/Aliases in Host Files	*Unselected* is required. Since not selected, the default behavior occurs, which is to use the device host name in the hosts file.

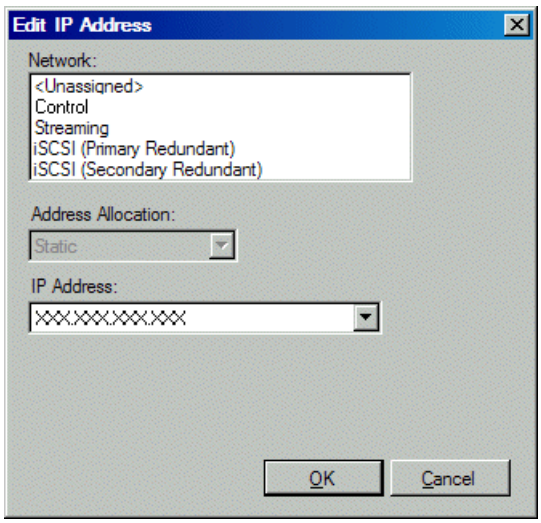
Setting...	For any network interface of type iSCSI
Interface Name	"Unused" is recommended. Displaying this text here serves as an aid in understanding SAN networks.The iSCSI network has no name resolution via the hosts file or otherwise, so the text you enter here is not actually use for name resolution.
Set To Default	Not recommended
DNS Suffix	Not allowed
Aliases	Not allowed
Use Interface Name/Aliases in Host Files	*Selected* is recommended. Since this interface's network has its names excluded from the hosts file, this setting has no affect. The interface name is excluded from the hosts file, regardless of settings here.

NOTE: There is no FTP/streaming network for a SAN K2 client. On the K2 SAN, FTP/streaming goes to the K2 Media Server.

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.

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	*Control* is required
Address Allocation	*Static* is recommended.
IP Address	The IP address for this interface on the network. Required.

Setting...	**For basic SAN network interface Media Connection #1**
Network	*iSCSI (non-Redundant)* is required
Address Allocation	*Static* is required.
IP Address	The IP address for this interface on the network. Required.

Setting...	**For redundant SAN network interface Media Connection #1**
Network	*iSCSI (Primary Redundant)* is required
Address Allocation	*Static* is required.
IP Address	The IP address for this interface on the network. Required.

Setting...	**For redundant SAN network interface Media Connection #2**
Network	*iSCSI (Secondary Redundant)* is required
Address Allocation	*Static* is required.
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.

Modifying K2 Media Server managed network interfaces

- The physical device you are configuring must be discovered and must be assigned to a device in the SiteConfig system description.
- SiteConfig must have communication with the device.
- The device must be defined in the system description with an appropriate network interface.

Use this task to modify managed network interfaces on a K2 SAN device as follows:

- K2 Media Server

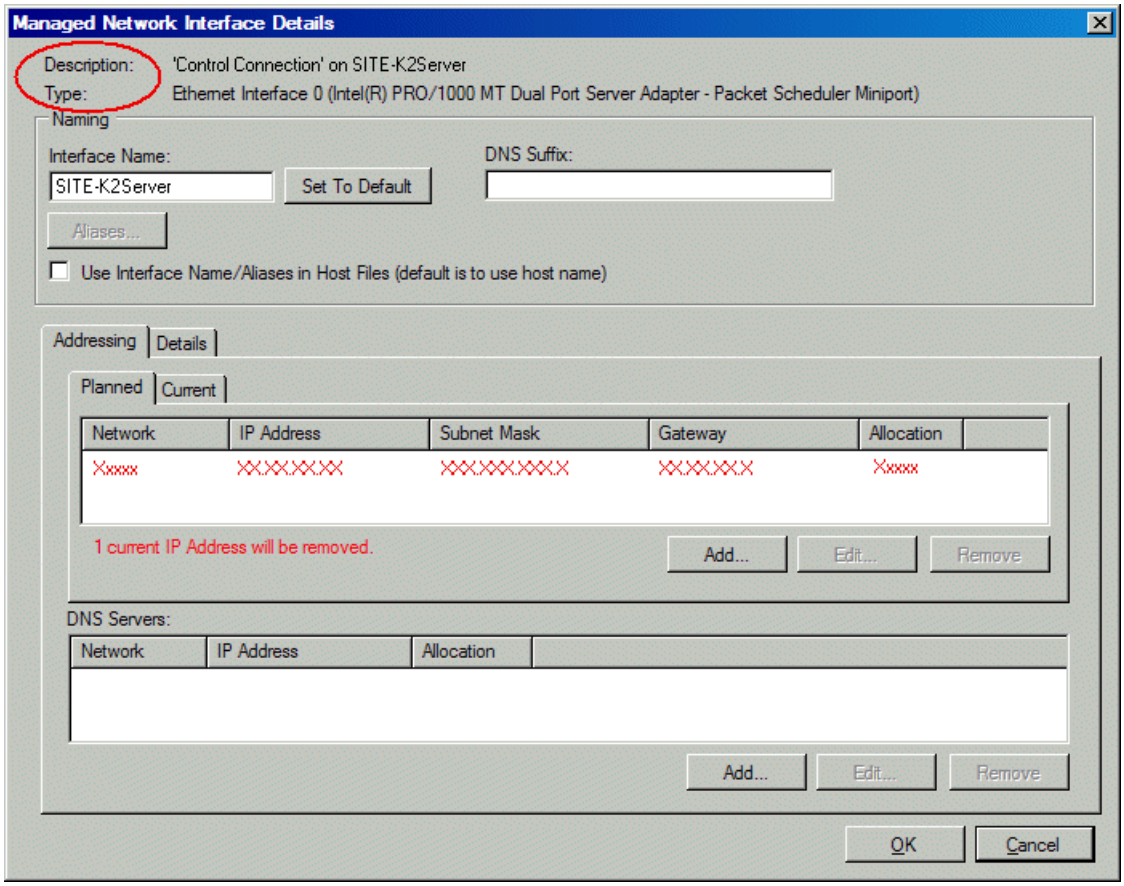
- NH K2 Media Server

1. In the Interfaces list view determine the interface to configure, as follows:
   - Identify the interface with which SiteConfig is currently communicating, indicated by the green star overlay icon. This should be the control network interface.
   - Verify that the interface over which SiteConfig is currently communicating is in fact the interface defined for the control network in the system description. If this is not the case, you might have the control network cable connected to the wrong interface port. The control connection should always be the first port on the motherboard, except when you have a loopback connection.
   - Configure the control network interface 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.
   - For the K2 Media Server, do not configure the Fibre Channel interface, which is a non-IP interface. SiteConfig does not manage this interface. It is represented in SiteConfig only to complete the description of the K2 Media Server.
2. In the Interfaces list view, check the icon for the interface you are configuring.

   If the icon has a red stop sign overlay, it indicates that current settings and planned settings do not match or that there is some other problem. Hover over the icon to read a tooltip with information about the problem.

3. In the Interfaces list view, right-click the interface you are configuring and select **Edit**.

   The Managed Network Interface Details dialog box opens.



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

   - Identify Ethernet LAN adapters by their "Description" name. This is the Windows connection name. SiteConfig reads this name from the device and displays it at the top of this dialog box. This is the most accurate way to identify the network adapter on the discovered device that you are configuring.
   - Identify iSCSI adapters by their "Type".

5. Configure naming settings as follows:

Setting...	For network interface Control Connection
Interface Name	The device host name. Required.
Set To Default	Not recommended
DNS Suffix	Allowed, if applicable to the network. The DNS suffix is added to the interface name.
Aliases	Not allowed
Use Interface Name/Aliases in Host Files	*Unselected* is required. Since not selected, the default behavior occurs, which is to use the device host name in the hosts file.

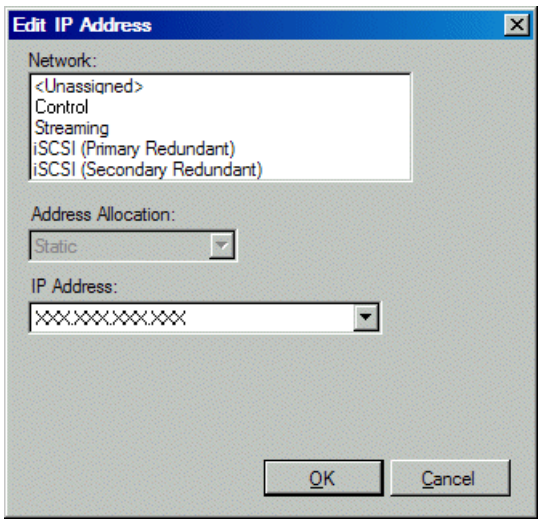
Setting...	For network interface FTP Connection
Interface Name	The device host name with the "_he0" suffix added is required.
Set To Default	Not recommended
DNS Suffix	Allowed, if applicable to the network. The DNS suffix is added to the interface name.
Aliases	Not allowed
Use Interface Name/Aliases in Host Files	*Selected* is required

Setting...	For any network interface of type iSCSI
Interface Name	The text "Unused" is recommended. Displaying this text here serves as an aid in understanding SAN networks.The iSCSI network has no name resolution via the hosts file or otherwise, so the text you enter here is not actually use for name resolution.
Set To Default	Not allowed
DNS Suffix	Not allowed
Aliases	Not allowed
Use Interface Name/Aliases in Host Files	*Selected* is recommended. Since this interface's network has its names excluded from the hosts file, this setting has no affect. The interface name is excluded from the hosts file, regardless of settings here.

6. Evaluate settings on the Planned tab and change if necessary.
   - Compare settings on the Planned tab with settings on the Current tab.
   - If you want to keep the current settings as reported in the Current tab, click **Remove** to remove the planned settings.
   - Do not specify multiple IP addresses for the same interface. Do not use the Add button.

7. To modify planned settings, do the following:
   a) Select the network settings and click **Edit**.

      The Edit IP Address dialog box opens.



   b) Edit IP address settings as follows:

Setting...	**For network interface Control Connection**
Network	*Control* is required
Address Allocation	*Static* is recommended.
IP Address	The IP address for this interface on the network. Required.

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

Setting...	**For basic SAN K2 Media Server any network interface of type iSCSI**
Network	*iSCSI (non-Redundant)* is required
Address Allocation	*Static* is required.
IP Address	The IP address for this interface on the network. Required.

Setting...	**For redundant SAN K2 Media Server A any network interface of type iSCSI**
Network	*iSCSI (Primary Redundant)* is required
Address Allocation	*Static* is required.

Setting...	For redundant SAN K2 Media Server A any network interface of type iSCSI
IP Address	The IP address for this interface on the network. Required.

Setting...	For redundant SAN K2 Media Server B any network interface of type iSCSI
Network	*iSCSI (Secondary Redundant)* is required
Address Allocation	*Static* is required.
IP Address	The IP address for this interface on the network. Required.

The networks listed in the Edit IP Address dialog box are those currently defined in the system description, with available settings restricted according to the network definition. If you require settings that are not available, you can close dialog boxes and go to the **Network Configuration | Networks** tab to modify network settings, then return to the Edit IP Address dialog box to continue.

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

   A Contacting Device message box reports progress.

9. After configuring control network settings, do the following
   a) If a message informs you of a possible loss of communication, click **OK**.

      This message is normal, since this is the network over which you are currently communicating.

   b) In the Device list view, observe the device icon and wait until the icon displays the green star overlay before proceeding.

      The icon might not display the green star overlay for several seconds as settings are reconfigured and communication is re-established.

   c) In the Interface list view, right-click the interface and select **Ping**.

      The Ping Host dialog box opens.

      If ping status reports success, the interface is communicating on the control network.

Making the host name the same as the device name

1. Verify that the current device name, as displayed in the SiteConfig tree view, is the same as your desired host name.
2. In the **Network Configuration | Devices | Device** list view, right-click the device and select **Edit**.

   The Edit Device dialog box opens.

3. Identify the state of buttons as follows:

   - If the host name is different than the device name, the **Set to Device Name** button is enabled.
   - If the host name is the same as the device name, the **Set to Device Name** button is disabled.

4. If enabled, click **Set to Device Name**.

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

5. Click **OK**.
6. When prompted, restart the device.

Pinging devices from the PC that hosts SiteConfig

- The devices you are pinging must be in the SiteConfig system description.

You can send the ping command to one or more devices in the system description over the network to which the SiteConfig host PC is connected. Typically this is the control network.

1. In the **Network Configuration** | **Networks** tree view, select a network, site, or system node.
2. In the Devices list view, select one or more devices. Use Ctrl + Click or Shift + Click to select multiple devices.
3. Right-click the selected device or devices and select **Ping**.

   The Ping Devices dialog box opens and lists the selected device or devices.

The Ping Devices dialog box reports the progress and results of the ping command per device.

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 using SiteConfig

- Planned control network settings must be applied to control network interfaces and devices must be communicating on the control network as defined in the system description.
- Interfaces for networks that require name resolution via the hosts file, such as the FTP/streaming network, must have settings applied and must be communicating.
- Host names defined in the system description must be correct.
- The SiteConfig PC must be added to the system description so that it is included in the host tables generated by SiteConfig.

When you add or modify devices or their IP addresses in the SiteConfig system description, you should update host tables on all devices that use them.

1. In the **Network Configuration | Networks** tree view, select a network, site, or system node.
2. Click **View Hosts file**.

   A Hosts File Contents window opens that displays the contents of the hosts file as currently defined in the system description.
3. Verify the information in the hosts file.
4. Do one of the following:

   - If you are managing host table information yourself, click **Save As** and save a copy of the hosts file to a location on the control point PC. Then open the copy of the hosts file, copy the desired host table information from it, and paste it into your facility hosts file as desired. Then you can use your own process to distribute the facility hosts file to devices. Remember to distribute to the control point PC so that SiteConfig and other management applications such as K2Config can resolve network host names.
   - If SiteConfig is managing hosts files, do the following:

   NOTE: Writing hosts files to multiple devices consumes system resource and network bandwidth. Therefore it is recommended that you wait and do this after the system is complete and fully implemented, rather than updating hosts files incrementally as you discover/assign devices.

   a) In the **Network Configuration | Devices | Devices** list view, right-click a device to which you intend to write the hosts file and select **View Current Host File**.

      A Host File Contents window opens that displays the contents of the hosts file that is currently on that actual device.

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

   c) In the **Network Configuration | Devices | Devices** list view, right-click a device or use Ctrl + Click to select multiple devices, and select **Update Host File**.

      The current hosts file is overwritten with the hosts file as defined in the system description.

Managing K2 Software

Configuring K2 software deployment

Take the following into consideration when using SiteConfig to deploy K2 SAN software.

- You typically configure one deployment group for K2 clients and one deployment group for K2 Media Servers. This allows you to target and sequence software deployment tasks to the different types of devices.
- You typically upgrade K2 Media Servers first, then K2 Media Clients.
- Always follow detailed steps in *K2 Release Notes* for the version of software to which you are upgrading.

Use the following topics to manage software deployment on a K2 SAN.

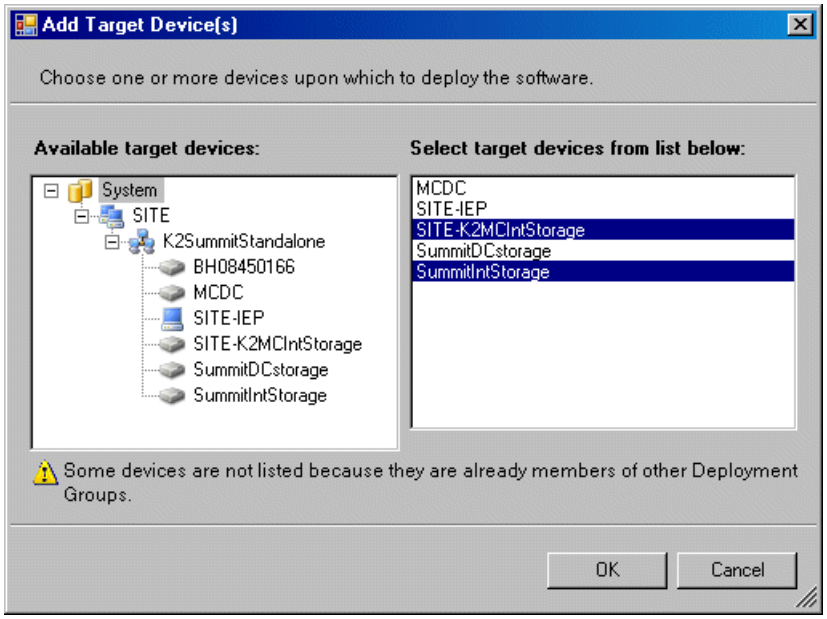
Configuring deployment groups

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

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

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

   The Add Target Device(s) wizard opens.



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

Adding a software package to a deployment group

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.

Checking all currently installed software on devices

- The device must be assigned in the SiteConfig system description and network connectivity must be present.
- SiteConfig must be able to log in to the device using the username/password credentials assigned to the device.
- The SiteConfig PC must not have a network drive mapped to an administrative share (such as C$) on a device on which you are checking software.

- If the SiteConfig Network Configuration Kit and/or Discovery Agent at version lower than 1.1.0.185 is currently installed, it must be manually uninstalled and updated. For more information refer to *SiteConfig Migration Instructions*.

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

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

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

   The Check Software dialog box appears. SiteConfig searches for software on the selected device or devices and gathers information. Progress is reported.

2. When the check is complete, close the Check Software dialog box.

An updated list of all currently installed software is displayed in the **Software Deployment | Devices | Installed Software** list view. If software is a SiteConfig managed software package, information is displayed in the Managed Package and Deployment Group columns.

About deploying software for the K2 SAN

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

Backup and Recovery Strategies

About the recovery disk image process

On the K2 Media Server, there are three partitions on the system drive to support backup and recovery strategies as follows:

- The C: drive is for the Windows operating system and applications.

- The D: drive is for the media file system (SNFS) and database. This allows you to restore the Windows operating system on the C: drive, yet keep the files on the D: drive intact. You can also restore the D: drive itself, however your backup and recovery strategy is different for non-redundant and redundant systems, as follows:
  - On non-redundant servers the media file system program, metadata, and journal files are on the D: drive. Also the media database program is on the D: drive. Therefore if you ever have a D: drive fault and you need to recover the data files (metadata, journal, and database), you can only restore them to the "snap-shot" contained in the most recent disk image you created. When you do this you restore the program files as well.
  - For redundant K2 SANs, the media file system program is on the D: drive, but the metadata and journal files are stored on the shared RAID storage. Also the media database program is on the D: drive, but the database data files are stored on the shared RAID storage. Therefore, if you ever have a D: drive fault, you can restore the media file system and database programs from a recovery disk image, and then access the data files (metadata, journal, database) from the shared RAID storage.
- The E: drive is for storing a system image of the other partitions. From the E: drive you can restore images to the C: and D: drives.

When you receive a K2 Media Server from the factory, the machine has a generic image on the E: drive. The generic image is not specific to the individual machine. It is generic for all machines of that type. Some K2 Media Servers also have a system-specific image on the E: drive.

You receive a recovery CD with your K2 Media Server. This recovery CD does not contain a disk image. Rather, the recovery CD is bootable and contains the Acronis True Image software necessary to create and restore a disk image. This recovery CD is specifically for the Windows server operating system which runs on the K2 Media Server. It is not for a desktop Windows operating system. Refer to the "About This Release" section of the K2 Topic Library for compatible versions of the recovery CD.

After your server is installed, configured, and running in your system environment, you should create new recovery disk images for the machine to capture settings changed from default. These "first birthday" images are the baseline recovery image for the machine in its life in your facility. You should likewise create new recovery disk images after completing any process that changes system software or data, such as a software upgrade. In this way you retain the ability to restore to a recent "last known good" state.

For the highest degree of safety, you should create a set of disk image recovery CDs, in addition to storing disk images on the E: partition. Since system drives are RAID protected, in most failure cases the disk images on the E: partition will still be accessible. But in the unlikely even of a catastrophic failure whereby you lose the entire RAID protected system drive, you can use your disk image recovery CDs to restore the system.

NOTE: Recovery disk images do not back up the media files themselves. You must implement other mechanisms, such as a redundant storage system or mirrored storage systems, to back up media files.

Recommended recovery process

The recommended recovery disk image process is summarized in the following steps.

At the K2 Media Server first birthday...

1. Boot from the Recovery CD.
2. Create a set of disk image recovery CDs. These CDs contain the C:, D:, and E: partitions.
3. Create a disk image, writing the disk image to the E: partition. This disk image contains the C: and D: partitions.
4. Copy the disk image from the E: partition to another location, such as a network drive.

At milestones, such as after software upgrades…

1. Boot from the Recovery CD.
2. Create a disk image, writing the disk image to the E: partition. This disk image contains the C: and D: partitions.
3. Copy the disk image from the E: partition to another location, such as a network drive.

If you need to restore the K2 Media Server…

1. Boot from the Recovery CD.
2. If the E: partition is accessible, read the image from the E: partition to restore the C: partition, restore the D: partition, or restore both partitions.
3. If the E: partition is not accessible, do the following:
   a. Read the disk image from your set of CDs and restore all three partitions
   b. Restart into Windows.
   c. Copy your most recent disk image to the E: partition.
   d. Boot from the Recovery CD.
   e. Read the image from the E: partition to restore the C: partition, restore the D: partition, or restore both partitions.

Plan a recovery strategy that is appropriate for your facility, then refer to procedures as necessary to implement your strategy.

Creating a recovery disk image for storing on E: Dell R610

Do the following at the local server to create a disk image of the C: partition and the D: partition and store the image file on the E: partition:

1. Make sure that media access is stopped and that the system on which you are working is not being used.
2. If you have not already done so, connect keyboard, monitor, and mouse.
3. Do the following:
   a) Insert the Recovery CD.
   b) Restart the machine.

      If there is a problem restarting, hold the standby button down for five seconds to force a hard shutdown. Then press the standby button again to startup.

   The system boots from the Recovery CD.

   The Acronis program loads.
4. At the startup screen, select **True Image Server OEM (Full Version)**.

   The Acronis main window appears.

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

   The Create Backup Wizard opens.

6. On the Welcome page, click **Next**.
7. On the Partitions Selection page, do the following:
   a) Select the **(C:)** and the **(D:)** partitions and then click **Next**.
8. On the Backup Archive Location page, do the following:
   a) In the tree view select the **Backup (E:)** partition and enter the name of the image file you are creating.

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

      For example, if the hostname is MySystem1, in the File name field you enter *E:\MySystem1_20121027.tib*.

   b) Click **Next**.
9. On the Backup Options page, do not change any settings. Click **Next**.
10. On the Archive Comment page, if desired, enter image comments such as the date, time, and software versions contained in the image you are creating. Click **Next**.
11. On the "…ready to proceed…" page, do the following:
   a) Verify that you are creating images from the C: and D: partitions and writing to the E: partition, then click **Proceed**.
12. On the Operation Progress page, observe the progress report.
13. When a message appears indicating a successful backup, click **OK**.
14. Click **Operations | Exit** to exit the Acronis True Image program.

    The machine restarts automatically.

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

Restoring from a system-specific recovery disk image on E: Dell R610

Use this task to restore a server using an image made from that particular server. If restoring from a generic factory default image, use the appropriate task.

1. Make sure that media access is stopped and that the system on which you are working is not being used.
2. If you have not already done so, connect keyboard, monitor, and mouse.
3. Do the following:
   a) Insert the Recovery CD.
   b) Restart the machine.

      If there is a problem restarting, hold the standby button down for five seconds to force a hard shutdown. Then press the standby button again to startup.

   The system boots from the Recovery CD.

   The Acronis program loads.

4. At the startup screen, select **True Image Server OEM (Full Version)**.

   The Acronis main window appears.

5. In the Acronis main window, click **Recovery**.

   The Restore Data Wizard opens.

6. On the Welcome page, click **Next**.
7. On the Backup Archive Selection page, in the tree view expand the node for the E: partition and select the image file, then click **Next**.
8. On the Restoration Type Selection page, select **Restore disks or partitions** and then click **Next**.
9. On the Partition or Disk to Restore page, select **(C:)** and then click **Next**.
10. On the Restored Partition Location page, select **(C:)** and then click **Next**.
11. On the Restored Partition Type page, leave the selection at **Active** and then click **Next**.
12. On the Restored Partition Size page, leave settings at their defaults. The size reported in the upper pane is the size detected of the actual C: partition. This should be the same as that reported in the Partition size field in the middle of the page. Free space before and Free space after should both be reported at 0 bytes. Click **Next**.
13. On the Next Selection page, depending on the partitions you are restoring, do one of the following:

    - If you are restoring only the C: partition, select **No, I do not** and then click **Next**.

      Skip ahead to the "…ready to proceed…" page in step 20.

    - If you are also restoring the D: partition, select **Yes, I want to restore another partition or hard disk drive** and then click **Next**.

      Continue with the next step in this procedure.

14. On the Partition or Disk to Restore page, select **(D:)** and then click **Next**.
15. On the Restored Partition Location page, select **(D:)** and then click **Next**.

    opens.

16. On the Restored Partition Type page, leave the selection at **Primary** and then click **Next**.
17. On the Restored Partition Size page, leave settings at their defaults. The size reported in the upper pane is the size detected of the actual D: partition. This should be the same as that reported in the Partition size field in the middle of the page. Free space before and Free space after should both be reported at 0 bytes. Click **Next**.
18. On the Next Selection page, select **No, I do not** and then click **Next**.
19. On the Restoration Options page, do not make any selections. Click **Next**.
20. On the "…ready to proceed…" page, verify that you are restoring the correct image to the correct location. Click **Proceed**.
21. On the Operation Progress page, observe the progress report.
22. When a message appears indicating a successful recovery, click **OK**.
23. Click **Operations | Exit** to exit the Acronis True Image program.

    The machine restarts automatically.

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

Restoring from the generic recovery disk image on E: Dell R610

There can be multiple versions of the generic recovery disk image on the server's E: partition. Refer to related topics in the server product's release notes to determine which version you should use.

This procedure can be used on a server that needs to be restored to its factory default state. For example, if you neglected to make a first birthday image, you might need to use this procedure. If the image from which you are restoring was made from the specific machine, refer to the appropriate procedure.

NOTE: This procedure restores the server (both C: and D: partitions) to its factory default condition. Passwords and other site-specific configurations are reset to factory defaults.

1. Make sure that media access is stopped and that the system on which you are working is not being used.
2. Connect all motherboard NICs to LAN connections.
3. If the server has a 10 Gig connection, make sure it is connected to the 10 Gig connection on the Ethernet switch.

   If not connected to a switch, 10 Gig network adapter detection and ordering are unpredictable on the restored image.
4. If you have not already done so, connect keyboard, monitor, and mouse.
5. Do the following:
   a) Insert the Recovery CD.
   b) Restart the machine.

      If there is a problem restarting, hold the standby button down for five seconds to force a hard shutdown. Then press the standby button again to startup.

   The system boots from the Recovery CD.

   The Acronis program loads.
6. At the startup screen, select **True Image Server OEM (Full Version)**.

   The Acronis main window appears.
7. In the Acronis main window, click **Recovery**.

   The Restore Data Wizard opens.
8. On the Welcome page, click **Next**.
9. On the Backup Archive Selection page, in the tree view expand the node for the E: partition and select the image file, then click **Next**.
10. On the Restoration Type Selection page, select **Restore disks or partitions** and then click **Next**.
11. On the Partition or Disk to Restore page, select **(C:)** and then click **Next**.
12. On the Restored Partition Location page, select **(C:)** and then click **Next**.
13. On the Restored Partition Type page, leave the selection at **Active** and then click **Next**.
14. On the Restored Partition Size page, leave settings at their defaults. The size reported in the upper pane is the size detected of the actual C: partition. This should be the same as that reported in the Partition size field in the middle of the page. Free space before and Free space after should both be reported at 0 bytes. Click **Next**.
15. On the Next Selection page, select **Yes, I want to restore another partition or hard disk drive** and then click **Next**.

16. On the Partition or Disk to Restore page, select **(D:)** and then click **Next**.
17. On the Restored Partition Location page, select **(D:)** and then click **Next**.

    opens.
18. On the Restored Partition Type page, leave the selection at **Primary** and then click **Next**.
19. On the Restored Partition Size page, leave settings at their defaults. The size reported in the upper pane is the size detected of the actual D: partition. This should be the same as that reported in the Partition size field in the middle of the page. Free space before and Free space after should both be reported at 0 bytes. Click **Next**.
20. On the Next Selection page, select **No, I do not** and then click **Next**.
21. On the Restoration Options page, do not make any selections. Click **Next**.
22. On the "…ready to proceed…" page, verify that you are restoring the correct image to the correct location. Click **Proceed**.
23. On the Operation Progress page, observe the progress report.
24. When a message appears indicating a successful recovery, click **OK**.
25. Click **Operations | Exit** to exit the Acronis True Image program.

    The machine restarts automatically.
26. Remove the recovery media while the machine is shutting down.
27. When prompted, enter the machine name.

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

    At first start up after reimage, the system is in Embedded Security Update mode by default.

Next, do the following to restore the K2 Media Server to its factory-default state. Refer to related topics in this document or as otherwise indicated.

1. Set up Windows.
2. Restore network configuration.
3. Install the SiteConfig Discovery Agent.
4. Install SNFS software manually. Do not use SiteConfig.
5. Restart.
6. Install K2 software manually. Do not use SiteConfig.

   While manually installing software, accept any hardware installation or driver/security prompts that appear. Also refer to related topics in the "About This Release" section of the K2 Topic Library.
7. Install Fibre Channel Card driver.
8. Activate Windows within 30 days.

Creating a recovery disk image for storing on E: Dell R620

Do the following at the local server to create a disk image of the C: partition and the D: partition and store the image file on the E: partition:

1. Make sure that media access is stopped and that the system on which you are working is not being used.
2. Connect all motherboard NICs to LAN connections.
3. If you have not already done so, connect keyboard, monitor, and mouse.

4. Do the following:
   a) Insert the Recovery CD.
   b) Restart the machine.

      If there is a problem restarting, hold the standby button down for five seconds to force a hard shutdown. Then press the standby button again to startup.

   The system boots from the Recovery CD.

   The Acronis program loads.
5. On the Acronis Rescue Media page, select **Acronis Backup and Recovery 11.5 (64-bit...)**

   The Acronis Backup and Recovery page opens.
6. On the Acronis Backup and Recovery page, select **Back up now**.

   The Back up now page opens.
7. On the Back up now page, under What to back up, select **Item to back up**.

   The Select item to back up dialog box opens.
8. On the Select item to back up dialog box, do the following:
   a) Under Disk 1 select **C** and **D**. Clear other check boxes.
   b) Click **OK**.

   The Select item to back up dialog box closes.
9. On the Back up now page, under Where to back up, select **Location**.

   The Select location back up dialog box opens.
10. On the Select location back up dialog box, do the following:.
    a) Expand the tree-view **Local folders** node and select **E:**.
    b) Enter a name for your backup.
    c) Click **OK**.

    The Select location back up dialog box closes.
11. On the Back up now page, under How to back up, do the following:
    a) Set Backup type to **Full**.
    b) This is recommended for your first backup. For subsequent backups, you can optionally set this to Incremental or Differential.
    c) Set Validation to **Validate a backup as soon as it is created**.
12. On the Back up now page, click **OK**.

    The backup begins and the Backup Details page opens.
13. On the Backup Details page, select the **Progress** tab to view the progress.
14. Verify when the data is successfully backed up.
15. Close all Acronis pages and the Acronis main window.

    The machine restarts automatically.
16. Remove the recovery media while the machine is shutting down.

The backup consists of a directory and multiple files. Keep all files and directories intact. Do not delete or separate.

Restoring from the system-specific recovery disk image on E: Dell R620

Use this task to restore a server using an image made from that particular server. If restoring from a generic factory default image, do not use this task.

1. Make sure that media access is stopped and that the system on which you are working is not being used.
2. Connect all motherboard NICs to LAN connections.
3. If you have not already done so, connect keyboard, monitor, and mouse.
4. Do the following:
   a) Insert the Recovery CD.
   b) Restart the machine.

      If there is a problem restarting, hold the standby button down for five seconds to force a hard shutdown. Then press the standby button again to startup.

   The system boots from the Recovery CD.

   The Acronis program loads.
5. On the Acronis Rescue Media page, select **Acronis Backup and Recovery 11.5 (64-bit...)**

   The Acronis Backup and Recovery page opens.
6. On the Acronis Backup and Recovery page, select **Recover**.

   The Recover Data page opens
7. On the Recover Data page, under What to Recover page, select **Select Data**.

   The Data to Recover Selection dialog box opens.
8. On the Data to Recover Selection dialog box, do the following:
   a) Select **Browse**.
   b) In the tree view, expand the **Local Folders** node.
   c) Select the **E** drive.

      Even though your backup is on the E drive, it is not yet visible.
   d) Click **OK**.

   On the Archive View tab, your backup name is listed.
9. On the Archive View tab, select your backup.
10. Under Backup contents, do the following:
    a) Select **C:** and **D:**.
    b) Click **OK**.

    The Data to Recover Selection dialog box closes.

11. On the Recover data page, under Where to recover, verify the following:

Recover to:	Physical machine
	Clear all
Recover 'NTFS (C:)' to...	Properties....Size:.....Letter: C
	Clear Disk 1/NTFS (C:)
Recover 'NTFS (D:)' to...	Properties....Size:.....Letter: D
	Clear Disk 1/NTFS (D:)

12. On the Recover Data page, click **OK**.

    The restore process begins.

13. On the My Recovery Details page, select the **Progress** tab to view the progress.

    The image loads in approximately 9 minutes.

14. When the data is successfully restored, click **OK**.
15. Close all Acronis pages and the Acronis main window.

    The machine restarts automatically.

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

Restoring from a generic recovery disk image Dell R620

This task restores a server to its factory default state. For example, if you neglected to make a first birthday image, you might need to use this procedure. If the image from which you are restoring was made from the same, specific machine to which it is being restored, do not use this task.

NOTE: This procedure restores the server (C:, D:, and E: partitions) to its factory default condition. Passwords and other site-specific configurations are reset to factory defaults.

1. Make sure that media access is stopped and that the system on which you are working is not being used.
2. Connect all motherboard NICs to LAN connections.
3. If you have not already done so, connect keyboard, monitor, and mouse.
4. Do the following:
   a) Insert the Recovery CD.
   b) Restart the machine.

      If there is a problem restarting, hold the standby button down for five seconds to force a hard shutdown. Then press the standby button again to startup.

   The system boots from the Recovery CD.

   The Acronis program loads.

5. On the Acronis Rescue Media page, select **Acronis Backup and Recovery 11.5 (64-bit...)**

   The Acronis Backup and Recovery page opens.

6. On the Acronis Backup and Recovery page, select **Recover**.

   The Recover Data page opens

7. On the Recover Data page, under What to Recover page, select **Select Data**.
   The Data to Recover Selection dialog box opens.
8. On the Data to Recover Selection dialog box, do the following:
   a) Select **Browse**.
   b) In the tree view, select the USB drive that contains the generic recovery disk image.
      Even though your backup is on the drive, it is not yet visible.
   c) Click **OK**.
   On the Archive View tab, your backup name is listed.
9. On the Archive View tab, select your backup.
10. Under Backup contents, do the following:
    a) Select **MBR**.
    b) Select **C:**, **D:**, and **E:**.
    c) Click **OK**.
    The Data to Recover Selection dialog box closes.
11. On the Recover data page, under Where to recover, select the correct destination partition for each source partition as follows:
    a) Select **Recover Disk 1 MBR**.
       The MBR Destination dialog box opens.
    b) In the MBR Destination dialog box, select **Disk 1: Dell PERC ...**, as appropriate for the particular Dell platform. The following are valid selections:
       - Disk 1: Dell PERC H710 SCSI
       - Disk 1 : Dell PERC H310 SCSI
    c) Click **OK**.
    d) Select **Recover NTFS (C:)**.
       The Volume Selection dialog box opens.
    e) In the Volume Selection dialog box, select **C**.
    f) Click **OK**.
    g) Select **Recover NTFS (D:)**.
       The Volume Selection dialog box opens.
    h) In the Volume Selection dialog box, select **D**.
    i) Click **OK**.
    j) Select **Recover NTFS (E:)**.
       The Volume Selection dialog box opens.
    k) In the Volume Selection dialog box, select **E**.
    l) Click **OK**.
12. On the Recover Data page, click **OK**.
    The restore process begins.
13. On the My Recovery Details page, select the **Progress** tab to view the progress.
    The image loads in approximately 9 minutes.

14. When the data is successfully restored, click **OK**.
15. Close all Acronis pages and the Acronis main window.

    The machine restarts automatically.
16. Remove the recovery media while the machine is shutting down.
17. When prompted, enter the machine name.

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

    After start up, one or more device discovery windows can open. Allow processes to complete without interference.

    At first start up after reimage, the system is in Embedded Security Update mode by default.

Next, do the following to restore the K2 Media Server to its factory-default state. Refer to related topics in this document or as otherwise indicated.

1. Set up Windows.
2. Restore network configuration.
3. Install the SiteConfig Discovery Agent.
4. Install SNFS software manually. Do not use SiteConfig.
5. Restart.
6. Install K2 software manually. Do not use SiteConfig.

   While manually installing software, accept any hardware installation or driver/security prompts that appear. Also refer to related topics in the "About This Release" section of the K2 Topic Library.
7. Install Fibre Channel Card driver.
8. Activate Windows within 30 days.

Installing the Discovery Agent on a K2 Media Server

If the device that you plan to manage with SiteConfig does not have a SiteConfig Discovery agent installed, use this topic to verify and, if necessary, manually install SiteConfig support software. Doing so allows SiteConfig to discover and manage the device. If the device has any version of the SiteConfig Discovery Agent currently installed, you should use SiteConfig to upgrade the Discovery Agent, rather than installing it manually.

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

   - ProductFrame Discovery Agent

2. Proceed as follows:

   - If you find the required items, no further steps are necessary. SiteConfig support software is installed.
   - If a required item is not present, navigate to your SiteConfig files. If you do not already have these files in convenient location, you can find them on the PC that hosts SiteConfig, in the SiteConfig install location. Then continue with next steps as appropriate.

3. To launch the program that installs the ProductFrame Discovery Agent Service do the following:
   a) Copy the `Discovery Agent Setup` directory to the device.
   b) In the directory, double-click the `DiscoveryAgentServiceSetup.msi` file.
      The setup program launches to install the SiteConfig Discovery Agent.
   c) Follow the setup wizard.
4. When presented with a list of device types, select the following:
   - K2Server
5. Complete the setup wizard and restart the device.
   The restart is required after the installation.

Setting up Windows

If a system is restored using the factory-default generic disk image or otherwise has the Windows operating system re-applied, a Windows set up process is required.

1. Upon first startup after reimage, a Windows Setup Wizard automatically opens. Work through the wizard as follows:
   a) Enter in the Windows Product Key and click **Next**.
      The Product Key is on a sticker on the top of the machine near the front right corner.
   b) Enter the name of the machine.
      To restore the factory-default name, enter the Serial Number (located at the right side and rear). The password is pre-set to the factory default. Leave the password as is.
   c) Click **Next**.
   d) Set Time and click **Next**.
   Windows loads components and restarts the K2 Media Server.
2. Upon restart, log in to Windows.
3. Rename the machine and set Windows clock as necessary.

Activating the Windows operating system

If a system is restored to its factory default state or otherwise has the Windows operating system re-applied, you might need to activate the operating system. This procedure provides instructions for doing this while the machine is connected to the Internet. The Activation wizard provides other options, which you can also choose if desired.

To active the Windows operating system, do the following:

1. Make sure the machine is connected to the Internet.
2. From the Windows desktop, in the system tray double-click on the key symbol icon. The Activate window opens.
3. Select **Yes, let's activate Windows over the Internet now** and click **Next**.
4. When prompted, “If you want to register with Microsoft right now.”, select **No**.

5. Wait for the connection. If the system times out, you are prompted for entering information in the Internet Protocol Connection dialog. Enter the proxy address and port number as appropriate for your facility's connections.
6. Ensure that "You have successfully activated your copy of Windows" message appears in Activate Windows.
7. Click **OK** to close the Activate Windows.

Embedded Security modes and policies

The Embedded Security solution protects against viruses and other unauthorized programs on the following Grass Valley systems:

- K2 Summit/Solo system
- All types/roles of K2 Media Server
- All types/roles of GV STRATUS server

Embedded Security prevents any unauthorized programs from running on the system. It contains a whitelist of programs that are authorized to run. Whenever a program attempts to run, it is checked against the whitelist. If the program is not on the whitelist, Embedded Security blocks the program from running. SiteConfig, and any software deployed by SiteConfig, is on the whitelist, so you do not need to manage Embedded Security in any way when using SiteConfig to deploy software. All versions of SiteConfig are compatible with Embedded Security.

When installing software manually (without SiteConfig) it might be necessary to manage Embedded Security. When necessary, you can put Embedded Security in Update mode. This mode allows you to manually install software that is not on the whitelist. Do not confuse Update mode with the idea that Embedded Security is "disabled". When in Update mode, Embedded Security is still active. While in Update mode, Embedded Security keeps track of any software you run or install and adds it to the whitelist. When you are done installing software and any required restarts, you must take Embedded Security out of Update mode so that it can protect the system. For software that requires a restart after installation, such as K2 system software and SNFS media file system software, Embedded Security must remain in Update mode until after the restart is complete.

No system restarts are required for entering or leaving Update mode, and a restart does not change the Update mode status. If in Update mode before a restart, the system remains in Update mode after a restart. You use the Embedded Security Manager to enter and leave Update mode.

The following policies apply to the Embedded Security:

- Use Update mode only as instructed by Grass Valley product documentation or as directed by Grass Valley Support. Do not do any other operations with Embedded Security Manager, unless under the direct supervision of Grass Valley Support.
- Do not keep Embedded Security in Update mode long-term, as Embedded Security does extra processing while in Update mode and eventually problems arise when attempting to run software.
- Make sure that Embedded Security is not in Update mode when using SiteConfig to install software. Update mode interferes with SiteConfig's automatic management of Embedded Security and causes problems running the software installed.
- Leave Embedded Security enabled for normal operation of your Grass Valley system. Do not disable Embedded Security except as instructed by Grass Valley product documentation or as directed by Grass Valley Support. Enabling and disabling Embedded Security requires a restart.

- Do not install any programs or modify any operating system settings unless approved by Grass Valley. By design, Embedded Security prevents any programs from being installed or from running that are not present when you receive the system new from Grass Valley. These Grass Valley systems are not general purpose Windows workstations. The applications and configuration have been specifically optimized on each system for its intended use as part of the Grass Valley system.
- While Embedded Security is the key anti-virus component on these systems, you should still follow the Grass Valley anti-virus scan policy and scan all the devices in your Grass Valley system to ensure viruses are not propagated between machines.

Embedded Security is part of the K2 Solo 3G system generic disk image and the K2 Media Server generic disk image compatible with K2 software version 9.0 or higher. Both K2 Media Servers and GV STRATUS servers use the same generic disk image, so GV STRATUS servers inherit the Embedded Security solution. On K2 Solo 3G systems, the Embedded Security solution introduced with K2 software version 9.0 replaces the write filter from previous versions.

Deploy Embedded Security solution - One-time process

You must have a system system-specific recovery disk image of the computer on which you are doing the Embedded Security one-time process.

NOTE: A re-image of the computer might be necessary if the Embedded Security one-time process is done incorrectly. Follow instructions carefully.

This is a two-phase task:

1. Run a script on the local system to which you are deploying software.
2. Deploy software with SiteConfig.

NOTE: You must carefully read and verify that you have completed each step in the task. Do not assume the task is the same as other software install tasks with which you are familiar.

On the computers in your system that are running the Grass Valley Embedded Security solution, you must do a one-time initial deployment process, as instructed by this task. This task isolates the steps required for the one-time process. If you have sufficient knowledge of systems and upgrades, you can modify your software upgrade steps as necessary to do the one-time process at the same time as your other software upgrades, rather than as isolated steps. After you have done this one-time process, you can do future upgrades using the normal upgrade process.

This applies to the following:

- K2 Summit/Solo system
- All types/roles of K2 Media Server

- All types/roles of GV STRATUS server

1. Determine the status of the Embedded Security solution on the computer. You can use SiteConfig check/view software to make this determination or on the local computer you can use the Programs and Features Control Panel to make this determination. Proceed as follows:
   - If the computer does not have **McAfee Solidifier**, which is a component of the Embedded Security solution, do not continue with these steps. The computer must already have the Embedded Security solution before the one-time process is applied.
   - If the computer has **McAfee Solidifier** at version 6.1.1.369, do not continue with these steps. That version indicates that the computer already has the one-time process applied, through either a software installation or a disk image process.
   - If the computer has **McAfee Solidifier** at a version lower than 6.1.1.369, continue with these steps.
2. Procure the McAfee script from the software download page on the Grass Valley website.

   The filename to download is *McAfee-6.1.1.zip*.
3. Unzip and copy the directory containing the McAfee script files to any location on the local computer.
4. Use Embedded Security Manager and put the local computer in Update Mode.
5. On the local computer, in the directory of McAfee script files that you downloaded from the Grass Valley website, run *UpdateMcAfee.cmd*.
6. Delete the directory of McAfee script files from the local computer.
7. In SiteConfig, do the following:
   a) Add the **GV Embedded Security Manager** role to the device.
   b) Add cab file as necessary to the device's deployment group so that the *GVEmbeddedSecurityManager* cab file is available for deployment.
   c) Do a **Check Software** operation on the device.
   d) Deploy software to the device.
8. Use Embedded Security Manager and leave the Update Mode.

   Embedded Security Manager now reports **Enabled**.
9. Do Windows updates on the local computer.

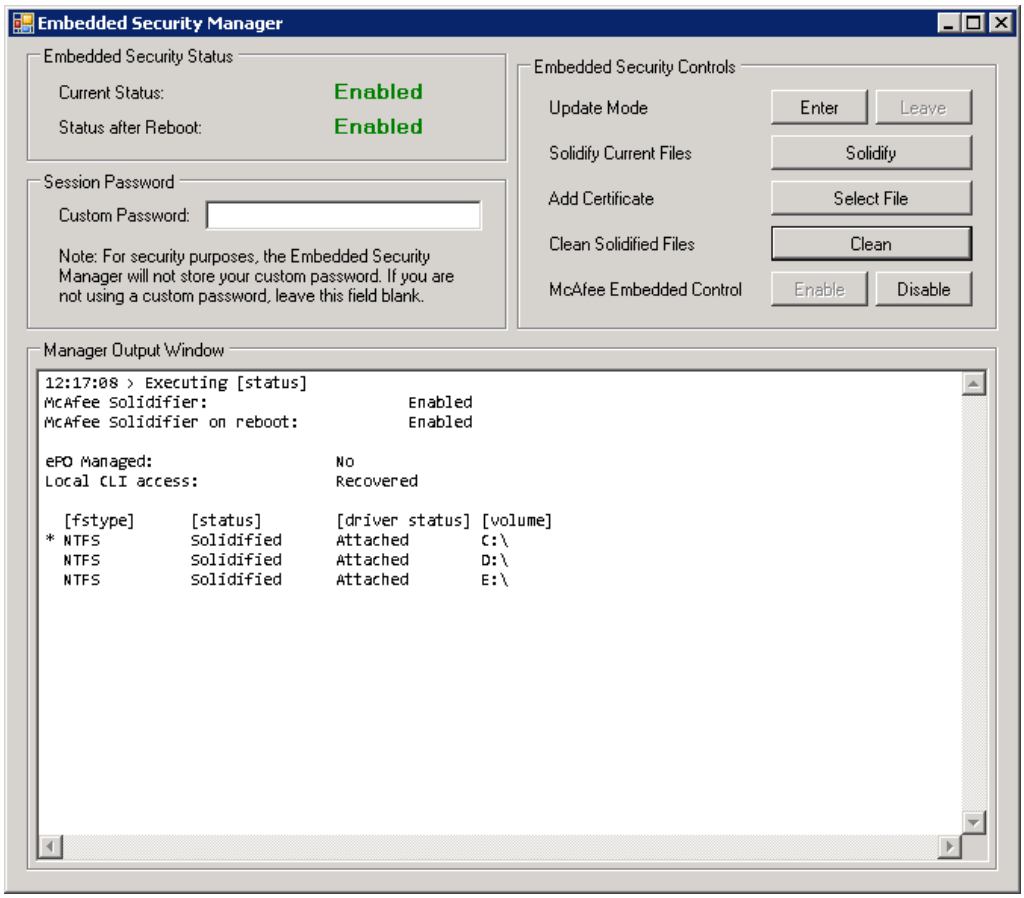
   You can now install Windows updates KB2859537 and KB2872339, which were previously not allowed on Grass Valley systems.

- For future Windows updates, it is no longer necessary to exclude KB2859537 and KB2872339.
- For future deployment of K2 and GV STRATUS software using SiteConfig, it is no longer necessary to put Embedded Security in Update Mode.

  NOTE: If not using SiteConfig, it can still be necessary to put Embedded Security in Update Mode. Refer to your product's software install/upgrade instructions.

Manage Embedded Security Update mode

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



   Interpret Current Status as follows:

   - **Enabled**: Embedded Security is enabled but is not in Update mode.
   - **Update**: Embedded Security is enabled and is in Update mode, ready for software installation.

2. Manage the Update mode as follows:

   - If Embedded Security is not in Update mode, click **Enter** to put it in Update mode.
   - If Embedded Security is already in Update mode, click **Leave** to take it out of Update mode.

   A restart is not required after you change the Update mode.

Configuring and licensing the K2 SAN

About K2 SAN licensing

When you purchase your K2 SAN, Grass Valley sizes the SAN according to your requirements for bandwidth and other considerations. Part of this sizing exercise is the application of the appropriate license for your SAN.

The K2 SAN license enables bandwidth in increments. A SAN with no license allows the lowest amount of bandwidth. With a license installed, additional bandwidth is allowed according to the bandwidth increment count embedded in the license.

The SAN license is a Sabretooth license. The license is installed on K2 Media Servers with role of iSCSI bridge. When you receive your SAN new from Grass Valley, the license is pre-installed. The K2Config application references the license on the K2 Media Server. When you add a client you specify its bandwidth and the K2Config application subtracts this bandwidth from the amount allowed by the license. The K2Config application reports when the total amount allowed is consumed and then does not allow you to add any more clients.

If you do not already have the highest bandwidth license on an existing system and you need more bandwidth and/or client connections, you can upgrade the license. You can replace your existing license with a license that has a higher bandwidth increment count embedded. You must consult with Grass Valley for a re-evaluation of your system design as part of the upgrade process. Some systems can require additional disks to support the increased bandwidth enabled by the license upgrade.

If you install K2 software version 7.3 or higher on K2 SAN with 1 GB iSCSI adapters (TOEs), no license is required. This is because the default amount of bandwidth allowed for a K2 SAN with no license is adequate for the maximum bandwidth needed for 1 GB iSCSI adapters.

About QOS on the K2 SAN

Grass Valley designs your system using Quality of Server (QOS) features for different categories of client Input/Output (I/O) traffic, as follows:

- Real Time Input Output (RTIO) — Clients supporting record/play operations are guaranteed I/Os with first priority.
- Non-Realtime Input Output — Clients that are not real-time, such as FTP servers, share an I/O pool that is separate from the real-time I/Os. The non-realtime clients can also temporarily use real-time I/Os when those I/Os are not being used by real-time clients.
- Reserved Input Output (RVIO) — Clients that have specific I/Os requirements are each assigned their own portion of the I/O pool. This guarantees the client has the I/Os it requires and also prevents the client from exceeding its designed amount. These I/Os are reserved only while the client is powered up. If the client is shutdown, the client's reserved I/Os become available in the I/O pool for use by other clients.

The exact QOS values for your K2 SAN are calculated by Grass Valley to meet your workflow requirements. When you operate your K2 SAN within the bounds of those requirements you should have no bandwidth problems, even during peak bandwidth events. If your workflow requirements

change, allow Grass Valley to re-calculate your QOS values. Some versions of K2 software have a RVIO calculator in the K2Config application. Do not use the RVIO calculator to change your RVIO value. The calculator is intended for use by qualified Grass Valley personnel only. Do not attempt to change any QOS values without guidance from Grass Valley. Doing so can result in unexpected performance problems.

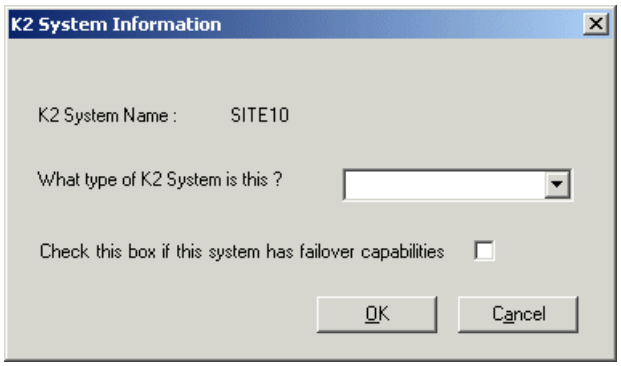
Importing a SiteConfig system description into K2Config

You can import a SiteConfig system description that contains a K2 SAN into the K2Config application. You should do this only after the K2 SAN is fully complete and implemented in SiteConfig, as changes are not automatically synchronized between SiteConfig and K2Config after the import.

When you import a SiteConfig system description, K2Config identifies your SAN devices, defines the SAN, and displays the unconfigured SAN in the tree view. Therefore you do not need to define the K2 SAN in K2Config. You can skip this task and instead begin your work in K2Config by configuring the first K2 Media Server.

1. In the K2Config application, click **File | Import SiteConfig**.
2. Browse to and select the system configuration file.

   A K2 System Information dialog box opens.



3. In the drop-down list, select the type of K2 SAN that you are importing.
4. If a redundant K2 SAN, select "…**failover capabilities**…"
5. Click **OK**.
6. The SAN appears in the K2Config application.

Configuring the basic K2 SAN - Online and Production

Work through the topics in this section sequentially to configure an Online (Tier 1) or Production (Tier 2) basic, non-redundant K2 SAN.

Prerequisites for initial configuration - Basic K2 SAN

Before beginning your initial configuration, make sure the devices of the K2 SAN meet the following prerequisites.

Control point PC

- Ethernet cable connected
- Control Point software must be installed
- Control network IP address must be assigned
- There must be network communication over the control network with all other K2 devices
- Power must be on

Ethernet switch

- Ethernet cables connected
- Control network IP address must be assigned
- VLANs must be set up
- Trunks must be set up
- Power must be on

K2 Media Server

- Ethernet cables connected
- Fibre Channel cable must be connected
- Softwaremust be installed, as from the factory, including QuickTime 7
- Control network IP address must be assigned
- Power must be on for all servers

K2 RAID chassis

- Fibre Channel cable(s) must be connected
- Ethernet cable(s) must be connected
- Power must be on

K2 RAID Expansion chassis (optional)

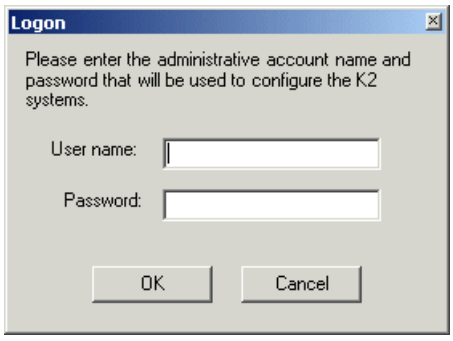
- Fibre channel cable(s) must be connected
- Power must be on

Defining a new K2 SAN

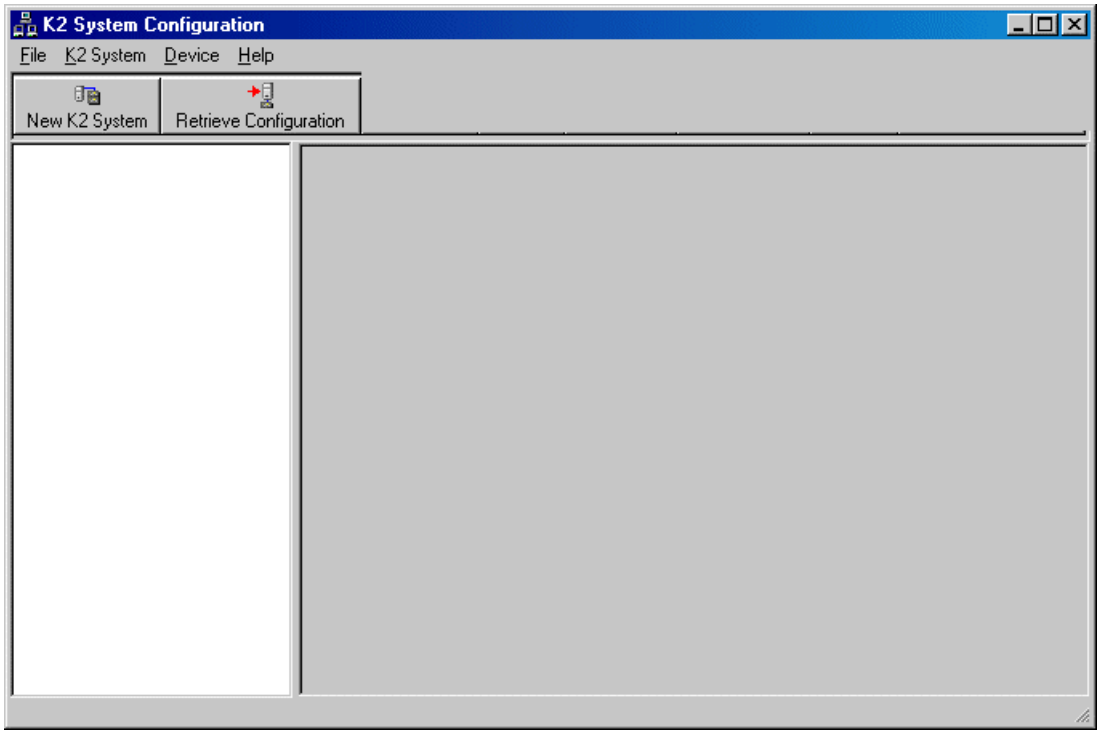
If you import a SiteConfig system description file in which the SAN is defined, you do not need to define a new SAN. You can skip this task and instead start by configuring the first K2 Media Server.

1. On the control point PC, open the K2Config application.

   A log on dialog box opens.



2. Log on to the K2Config application with the Windows administrator account.
   The K2Config application opens.



3. Click **New K2 System**.

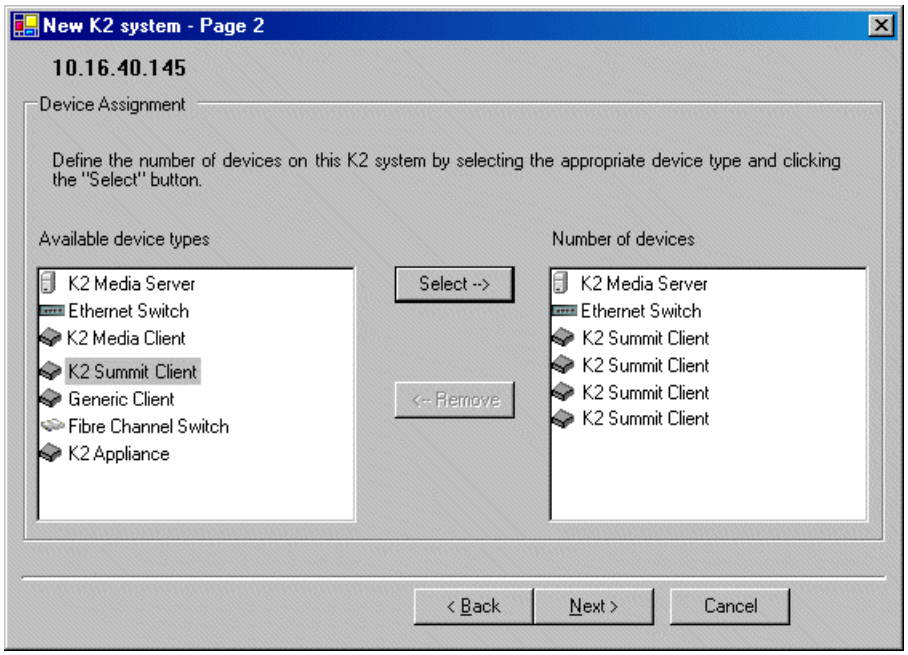
The New K2 System wizard opens to page 1.

Configure New K2 System page 1 - Basic K2 SAN

1. Create a name for your system and type it in the Name box.
2. Select **L30**.
3. If so designed, select **Enable Live Production mode**.
   Do not select the Server redundancy option.
4. Click **Next**.

Page 2 opens.

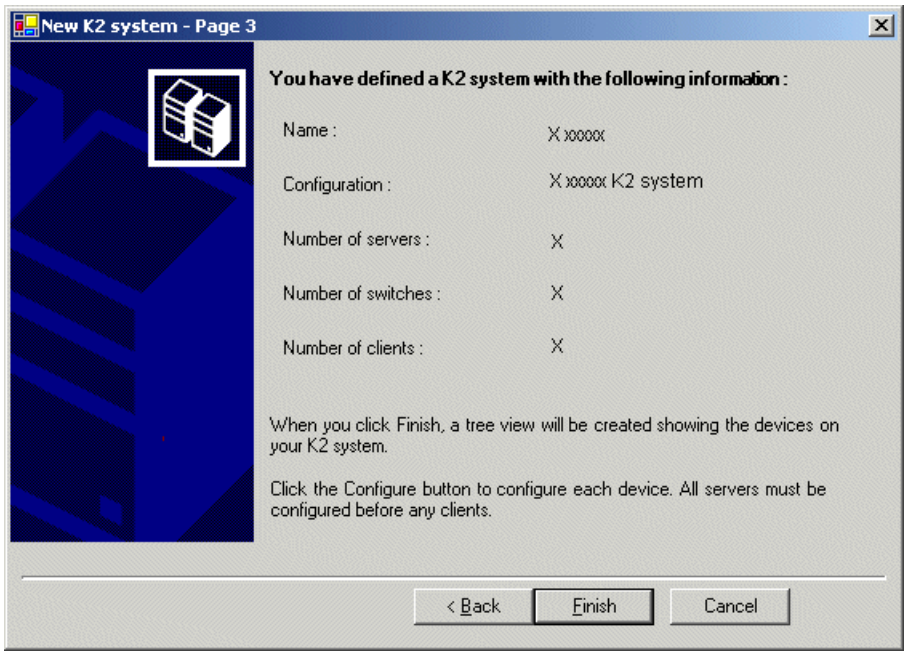
Configure New K2 System page 2 - Basic K2 SAN



1. Move the following into the Number of devices box:
   - One K2 Media Server
   - One Ethernet switch
   - K2 clients as appropriate for your system.
   - (Optional) One or more K2 Media Servers to represent each NH K2 Media Server on your system.
   - (Optional) Other devices as appropriate for your system.
2. Click **Next**.

Page 3 opens.

Configure New K2 System page 3 - Basic K2 SAN



1. Review the information on this page and verify that you have correctly defined your K2 SAN. For a basic K2 SAN you should have the following:
   - One Gigabit Ethernet switch
   - One K2 Media Server
   - Optionally, one or more NH K2 Media Servers
   - The number and type of clients appropriate for your system.
2. Click **Finish**.
   The Define New K2 Storage System wizard closes.

Your storage system appears in the tree view of the K2Config application.

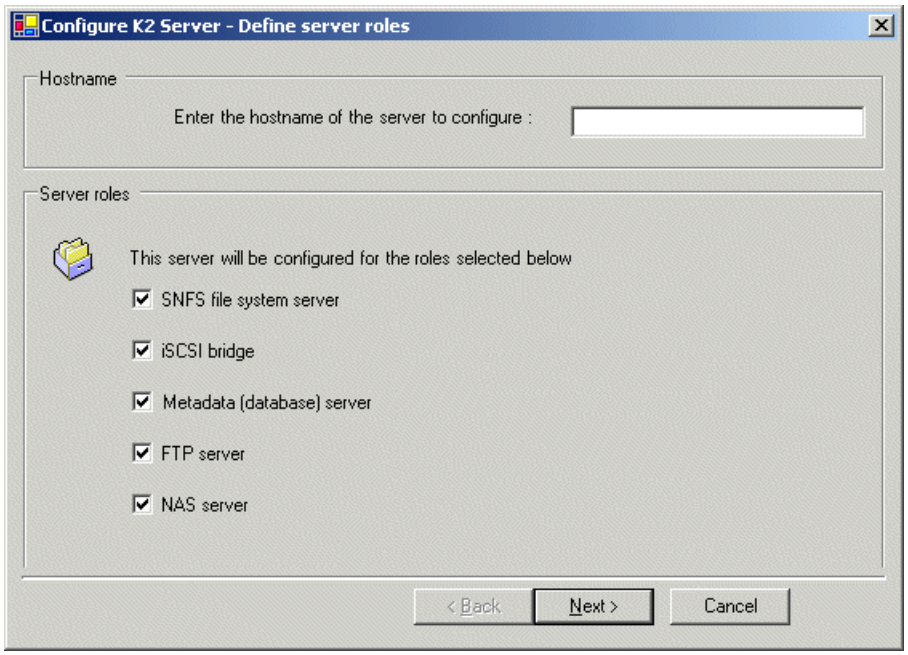
Next, configure the server.

Configuring the server - Part 1

1. In the K2Config application tree view, select **[K2Server1]**.
2. Click the **Configure** button.

The Configure K2 Server wizard opens to the Define server roles page.

Configure Define Server Roles page - Basic K2 SAN

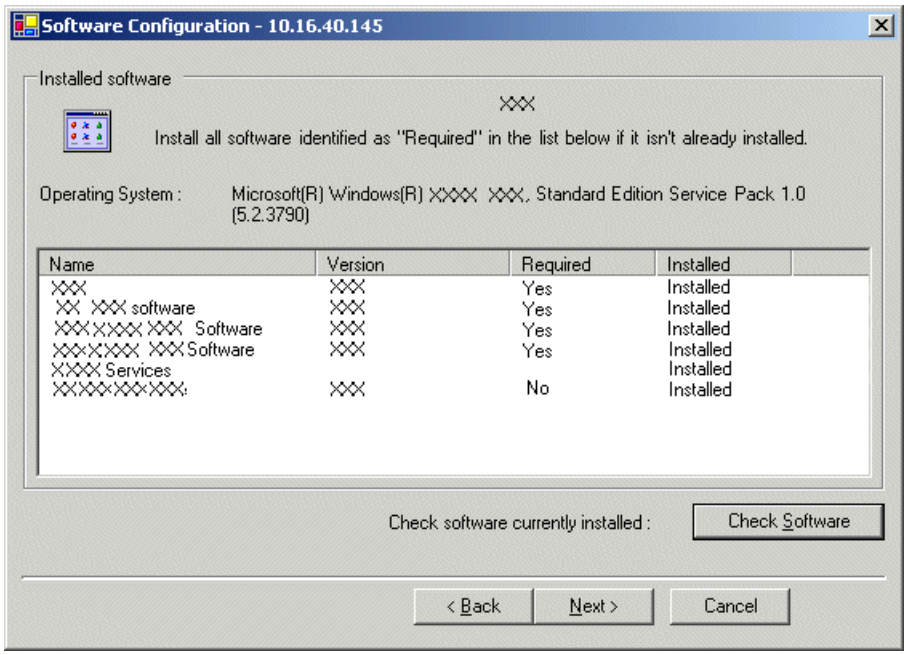


1. Enter the name for the K2 Media Server, as currently configured on the machine.
2. Select all roles, except as follows:

   If the K2 SAN has one or more optional NH servers, then FTP traffic should go to the NH server, not the K2 Media Server you are now configuring. In this case, do not select the FTP server role or the NAS server role
3. Click **Next**.

The Software Configuration page opens.

Configure Software Configuration page - Basic K2 SAN

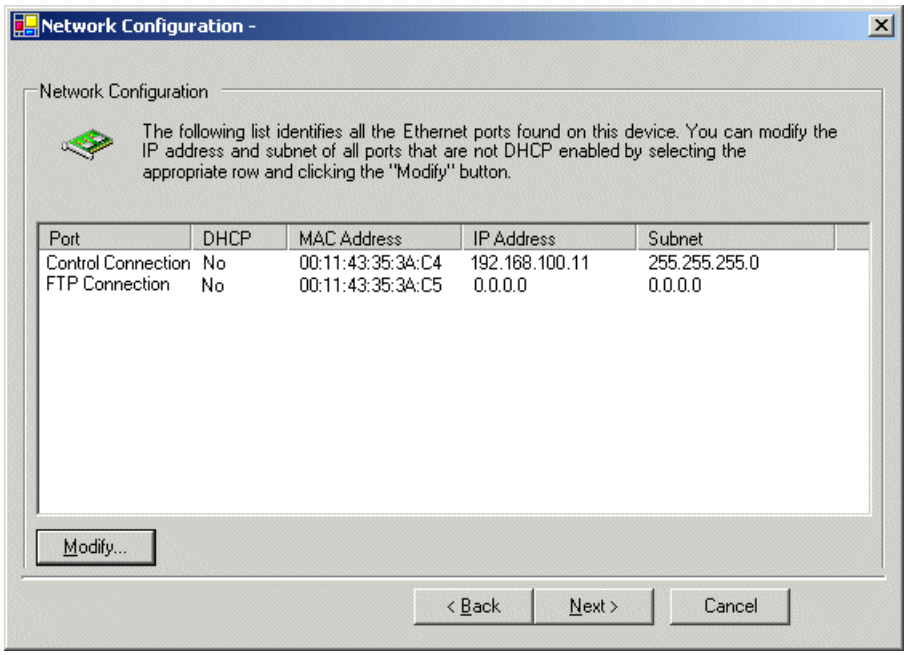


This page checks for the software required to support the roles you selected on the previous page.

1. If software with **Yes** in the Required column reports as **Not Installed**, install the software.
2. Click **Check Software**.
3. When all required software reports as **Installed**, click **Next**.

The Network Configuration page opens.

Configure Network Configuration page - Basic K2 SAN



This page displays the control network Ethernet port, and allows you to configure the FTP/Streaming network Ethernet port.

NOTE: This page does not configure the iSCSI interface (media network) ports.

1. Verify that the top port is configured correctly.

   The top port is the port over which the K2Config application is communicating. If correctly configured, it is already assigned the control network IP address, as displayed on this page.

2. If the server has the role of FTP server, verify that the other port is configured correctly. If not configured correctly, do the following:

   a) Select the other port and click **Modify**.

   A network configuration dialog box opens.

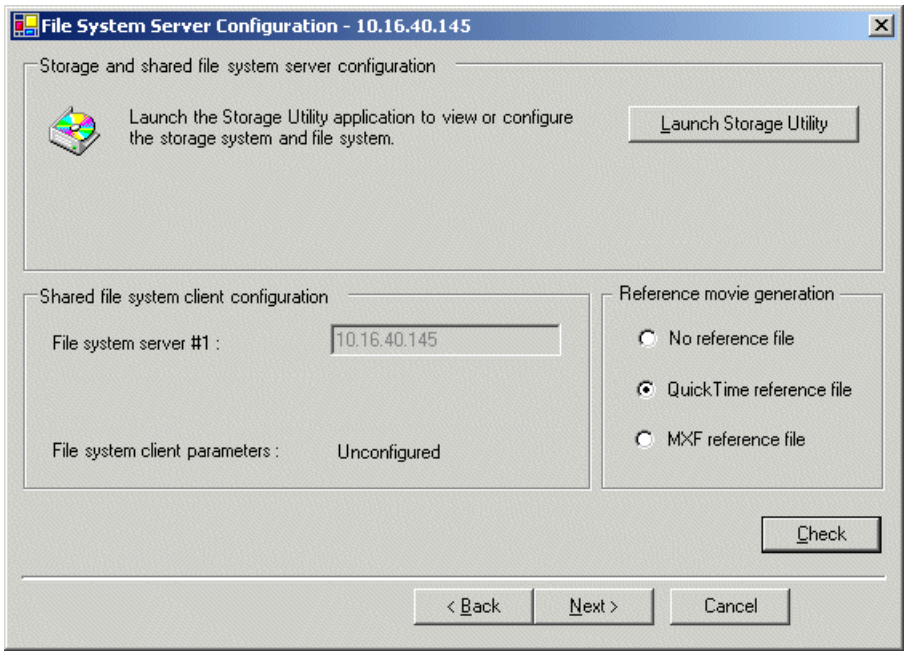
   b) Enter the FTP/Streaming IP address and the subnet mask and click **Apply**.

   For systems with an optional NH (FTP) server, the server you are now configuring does not take the role of FTP server, so configuring the second port here for the FTP/streaming network is not required.

3. Click **Next**.

The File System Server Configuration page opens.

Configure File System Server Configuration page - Basic K2 SAN



This page checks on the configuration of the K2 Media Server in one of its main roles as a file system server. The K2 Media Server also functions as a file system client, which is also checked from this page.

1. Click **Launch Storage Manager**.

   Storage Utility opens.

2. Leave the Configure K2 Server wizard open while you use Storage Utility.

   When you are done with Storage Utility, you continue with the wizard.

Next, use Storage Utility to configure the RAID storage and file system.

Configuring RAID

Use Storage Utility to complete the configuration of the K2 RAID storage devices, as explained in the following topics.

Configuring RAID network and SNMP settings - Basic

- Fibre Channel cable(s) must be connected
- Ethernet cable(s) must be connected
- Power must be on

- Fibre channel cable(s) must be connected
- Power must be on

Use the Storage Utility to configure the following settings for the K2 RAID controller:

- IP address
- Subnet mask

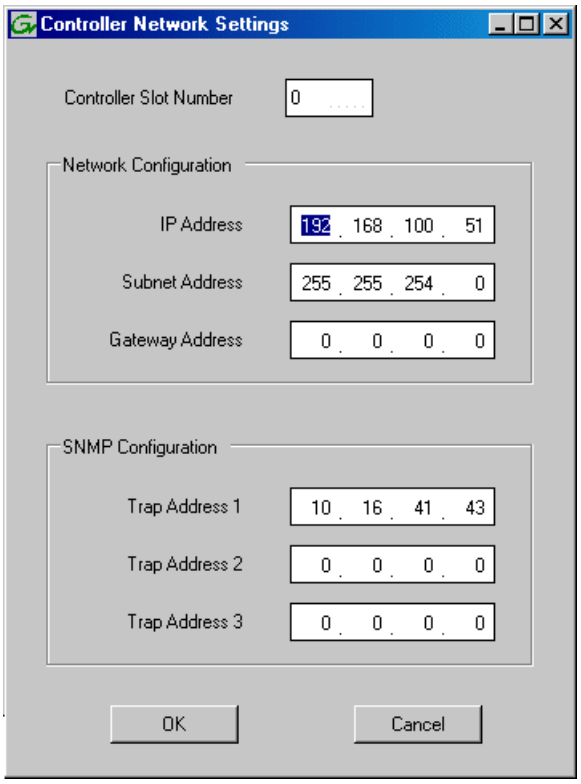
- Gateway Address
- SNMP trap destinations

For K2 RAID, network and SNMP settings are set and stored on the RAID controller module, so the combined RAID storage devices, including the optional Expansion chassis, exist as a single entity on the control network.

The RAID storage device is configured by default for the SNMP community name “public”. If your site’s policies require using a different SNMP community name, contact your Grass Valley representative.

1. Launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.
3. In Storage Utility tree view, expand the node for the K2 RAID, right-click the icon for a RAID controller, and select **Configuration | Network Properties**.

   The Controller Network Settings dialog box opens.



4. In the Controller Slot Number field enter **0** and then press **Enter**.

   The settings from controller 0 are loaded into the Controller Network Settings dialog box and are available for you to modify.
5. Enter the control network IP address and other network settings.

6. For SNMP Configuration, enter the IP address of the SNMP manager PC.

   You can also enter IP addresses for other SNMP managers to which you want to send SNMP trap messages.

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

7. Click **OK** to save settings and close.
8. In Storage Utility click **View | Refresh**.

Next, bind disk modules.

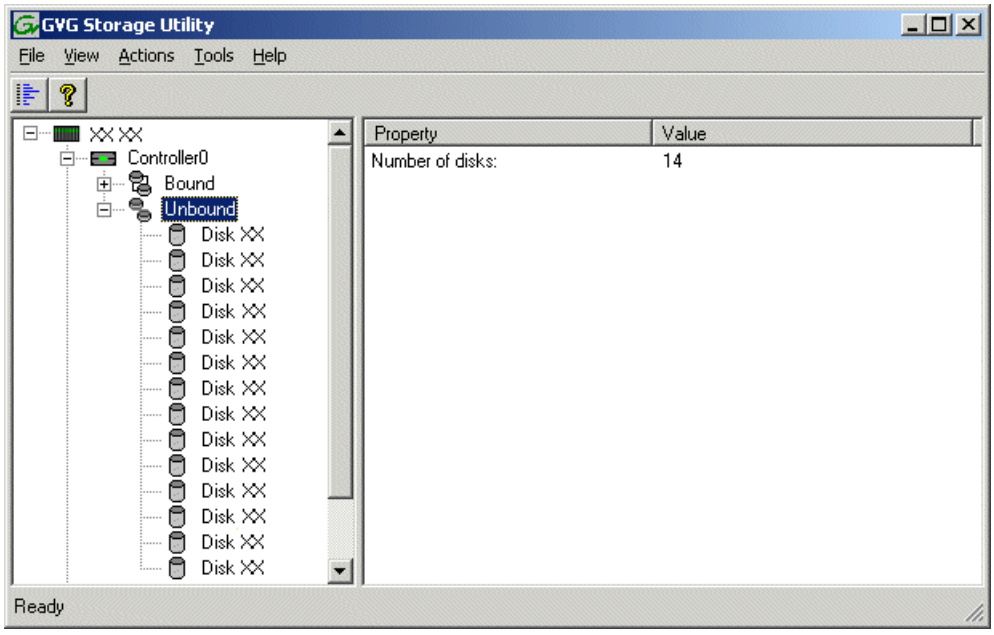
Binding disk modules - Basic K2 SAN

- Fibre Channel cable(s) must be connected
- Ethernet cable(s) must be connected
- Power must be on

- Fibre channel cable(s) must be connected
- Power must be on

NOTE: Binding destroys all user data on the disks.

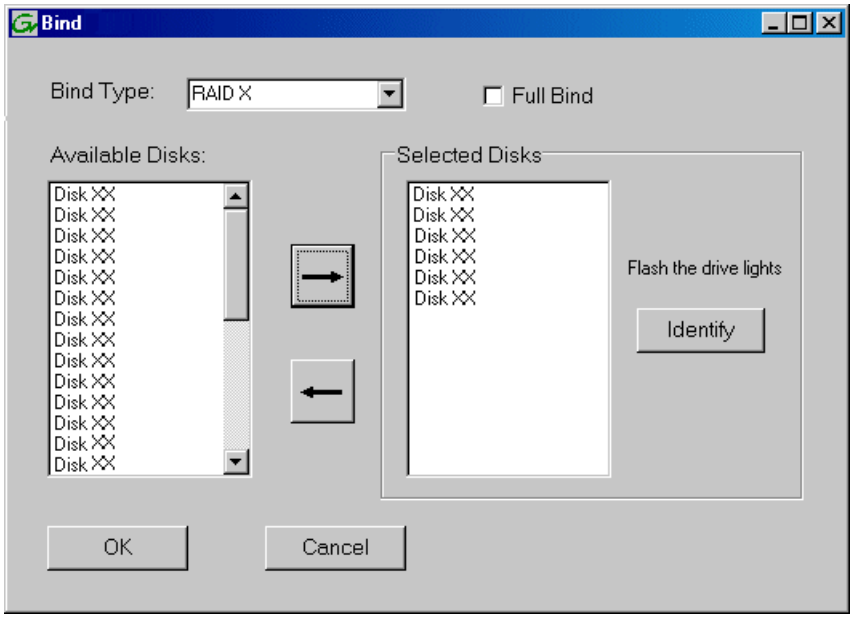
1. If you have not already done so, launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.
3. In the Storage Utility main window, identify bound RANKs and unbound disks by their placement in the hierarchy of the tree view. In the following illustration, disk numbers are represented by "XX".



4. Right-click the **Unbound** node for a controller, then select **Bind** in the context menu.

   If the RAID chassis has two controllers, both controllers are represented by the single “Controller” node.

   The Bind dialog box opens showing all unbound disks for the controller listed in the Available Disk list.



5. Leave **Full Bind** unchecked.
6. In the **Bind Type** drop down box, select **RAID 5** or **RAID 6**, as specified by your system design.
7. In the Available Disks box, select six contiguous disks at the top of the list.

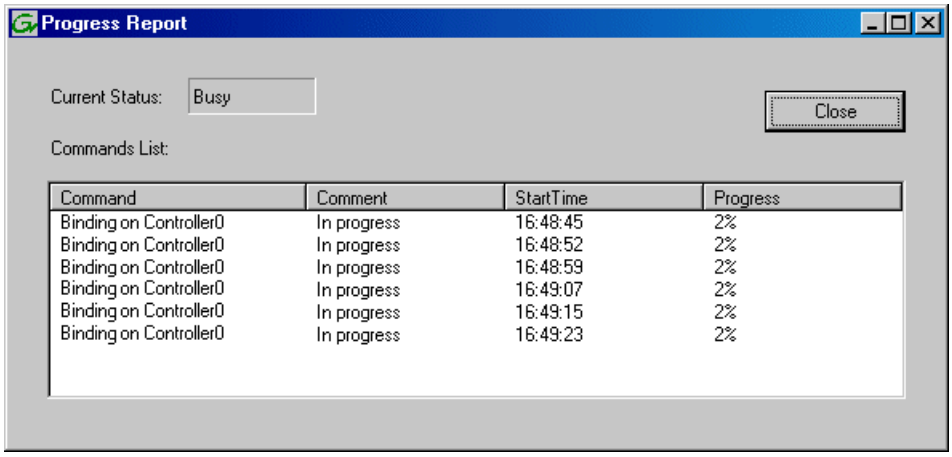
   Use ‘shift-click’ or ‘control-click’ to select disks.

8. Click the add (arrow) button to add disks to the Selected Disks list.

   NOTE: As an aid in identifying a disk module’s physical location, select it in the Selected Disks list, then click Identify Disks. This causes the disk drive light to flash.

9. Click **OK** to close the Bind dialog box and begin the binding process.

   The Progress Report dialog box opens, showing the status of the binding process.



10. Close the Progress Report and repeat these steps for other unbound disks.

    If specified by your system design, you can bind some disks as Hot Spares.

    When you are done, if you did not bind any extra Hot Spares, you should have the following results:

    For basic storage you should have multiple RAID 5 or RAID 6 RANKs, with each RANK having six disks, as necessary to fill the primary RAID chassis. For each optional Expansion chassis, RANKs are similar.

11. Click **Close** in Progress Report window.
12. Restart the K2 Media Server.

    NOTE: Make sure start up processes on the K2 Media Server are complete before proceeding.

Next, create a new file system.

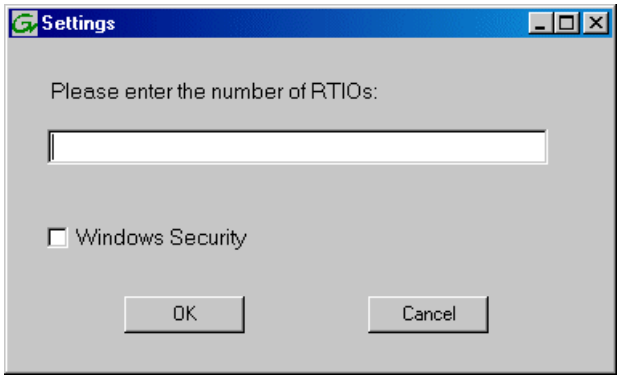
Creating a new file system - Basic K2 SAN

- Fibre Channel cable(s) must be connected
- Ethernet cable(s) must be connected
- Power must be on
- Disks must be bound

- Fibre channel cable(s) must be connected
- Power must be on
- Disks must be bound

1. If you have not already done so, launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.

3. In Storage Utility, click **Tools | Make New File System**.
   The Setting dialog box opens.

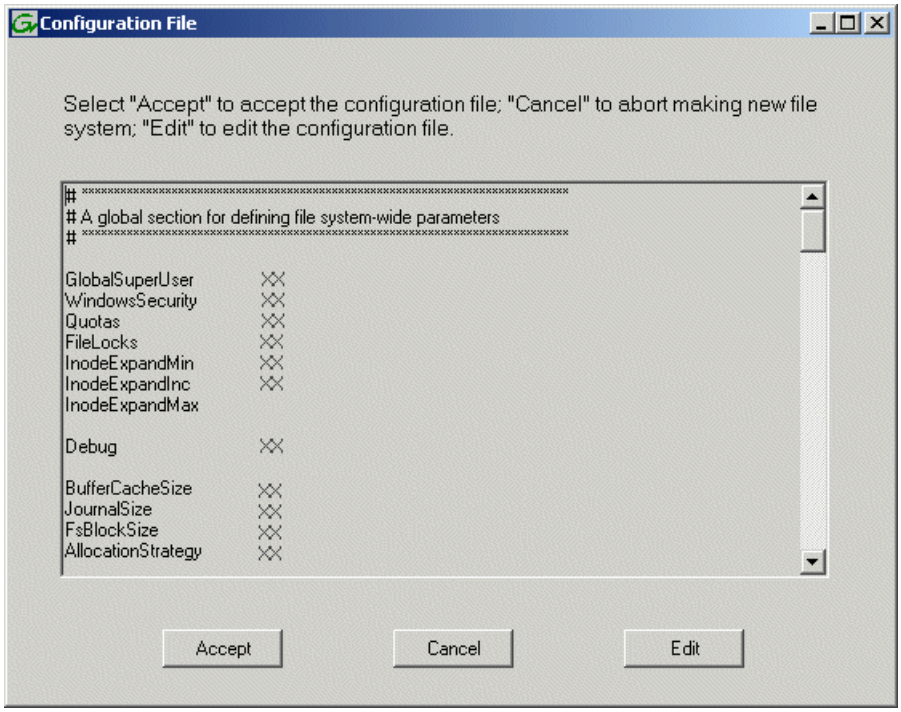


4. For the Real Time Input/Output (RTIO) rate, enter the value specified by your system design. If you do not know this value, contact your Grass Valley representative.
5. Configure Windows Security as follows:
   - If the K2 SAN is on a network Workgroup (not domain), do not select **Windows Security** .
   - If the K2 SAN is on a network domain, you may select **Windows Security**.

   NOTE: Only select Windows Security if the K2 SAN is on a domain. Never select Windows Security if the K2 SAN is on a workgroup.

6. Click **OK**.

   The Configuration File dialog box opens.



   The configuration file for the media file system is displayed.

7. Verify media file system parameters.

   Do not edit the configuration file for the media file system.

8. Click **Accept**.

   A "…Please wait…" message box displays progress and a "…succeeded…" message confirms the process is complete.

   A message informs you that you must restart the server, however the restart at the end of the Configure K2 Server wizard suffices, so you do not need to restart now.

9. Close the Storage Utility.

   NOTE: Do not attempt to start SAN-attached systems or otherwise bring the SAN online until instructed to do so by the documented procedure.

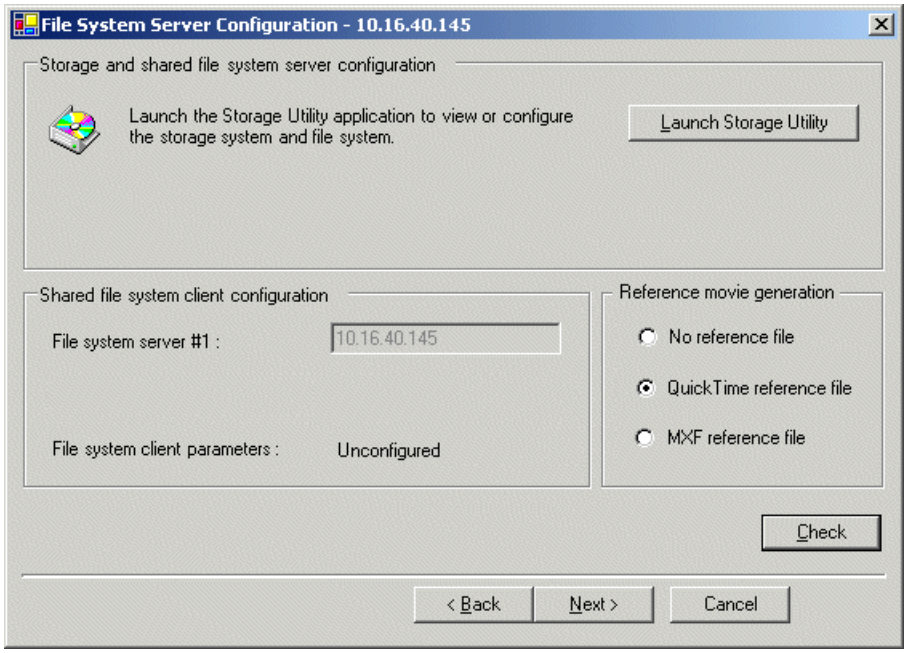
Next, continue with configuring the server using the K2Config application.

Configuring the server - Part 2

Configure File System Server Configuration page - Basic K2 SAN

- Network and SNMP must be settings configured
- Disks must be bound

- A new file system must be made



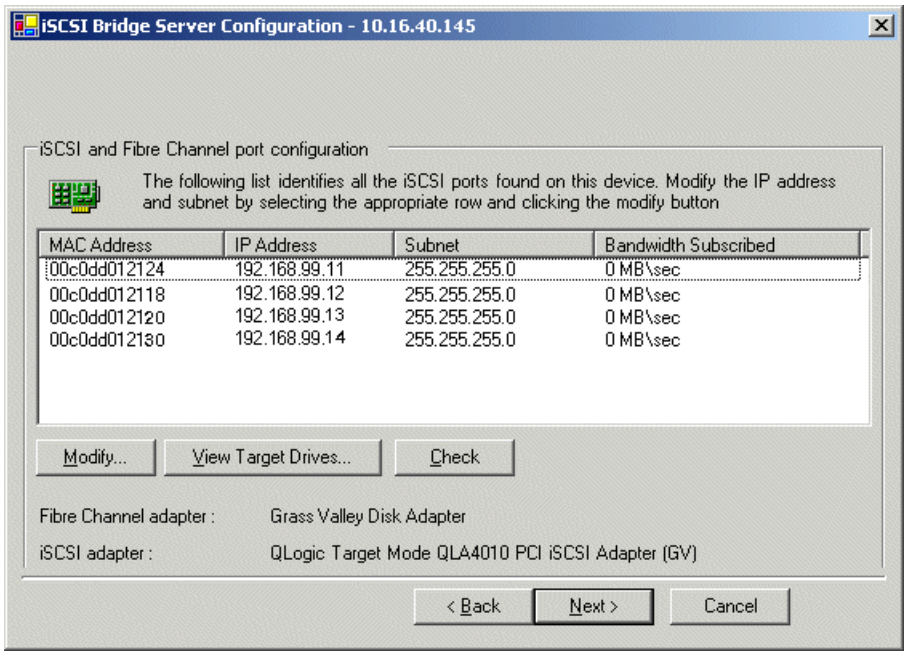
This page checks on the configuration of the K2 Media Server in one of its main roles as a file system server. The K2 Media Server also functions as a file system client, which is also checked from this page.

1. In K2Config open the server's File System Server Configuration page, if the page is not already open.
2. If desired, configure reference file generation.
3. Click **Check**.
4. When the wizard reports that the configuration is correct, click **Next**.

   If you get a "The V: will not be available until this device is rebooted…" message, you can safely continue now and reboot later when instructed to do so.

The iSCSI Bridge Server Configuration page opens.

Configure iSCSI Bridge Server Configuration page - Basic K2 SAN



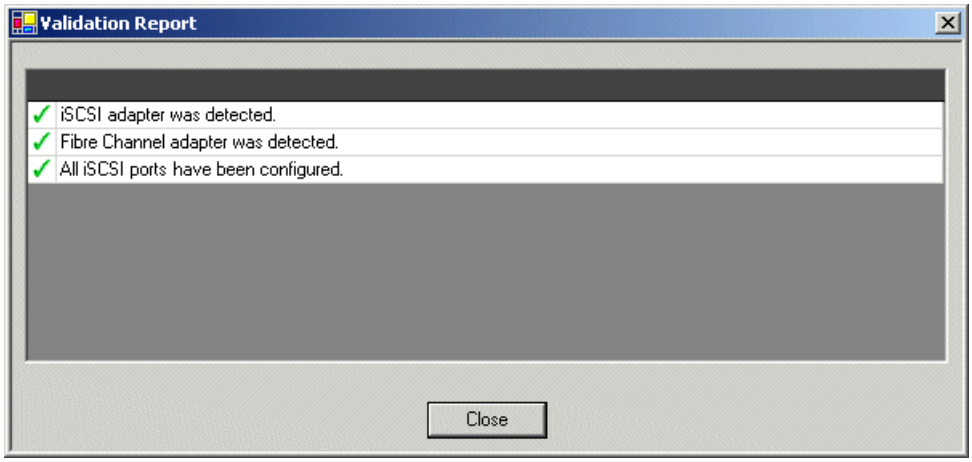
This page manages the components that bridge between iSCSI (the GigE media network) and the Fibre Channel connection to the RAID storage. You configure network settings on the iSCSI adapters and the page validates that the Fibre Channel adapter is in place and that the media RANKs are visible as iSCSI targets.

1. Select an iSCSI adapter and do the following:
   a) Click **Modify**.

      A network configuration dialog box opens.

   b) Verify or enter the media network IP address and the subnet mask.
   c) Click **Apply**.
   d) Click **View Target Drives**.
   e) Verify that all drives are shown in the **Drives exposed as iSCSI targets** field.
2. Repeat the previous step for the other iSCSI adapters.

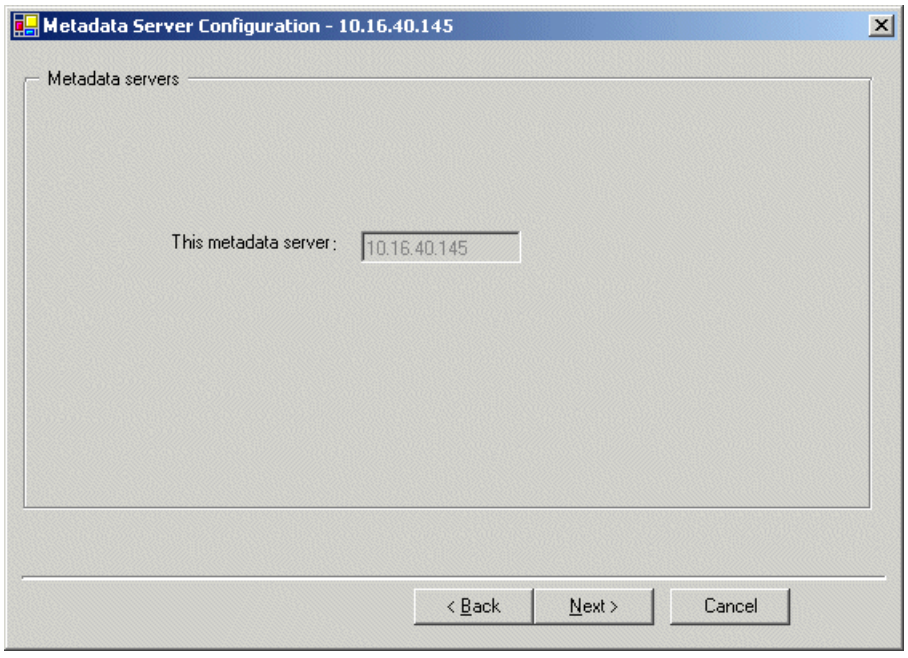
3. Click **Check**.
   The Validation Report opens.



4. Confirm that the iSCSI configuration is successful.
5. Close the Validation Report.
6. Click **Next**.

The Database Server Configuration page opens.

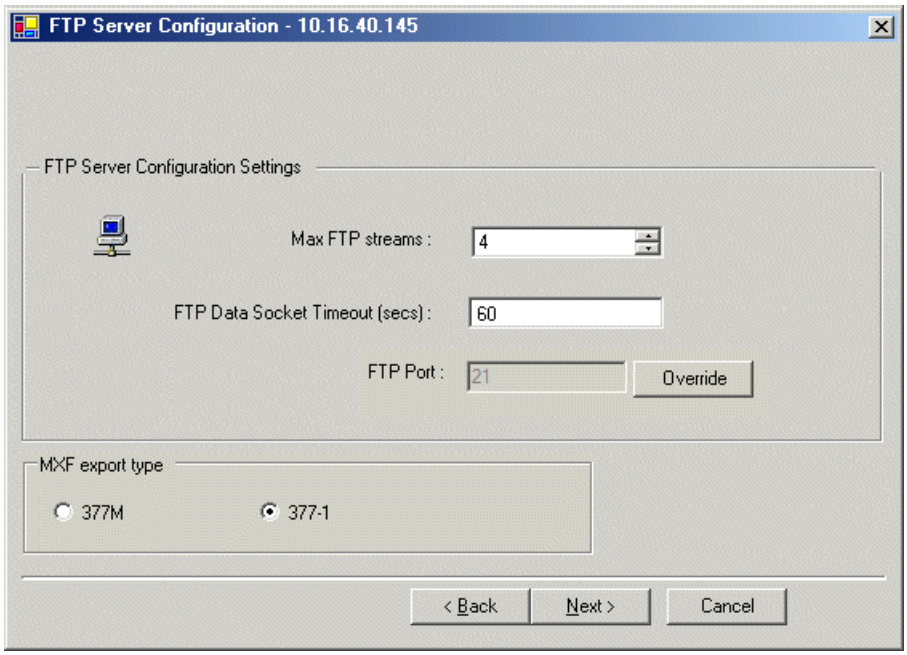
Configure Database Server Configuration page - Basic K2 SAN



Click **Next**.
You do not need to enter or configure anything on this page.

The FTP Server Configuration page opens.

Configure FTP Server Configuration page - Basic K2 SAN



This page appears only if the server has the role of FTP server.

Do not modify these settings. Leave at default values of Max FTP streams = 4, FTP Data Socket Timeout = 60, and FTP Port = 21. Only qualified Grass Valley personnel should specify other values, as these settings are intended for use only with custom systems designed by Grass Valley.

1. Select MXF export type as follows:

   - **377M**: Original SMPTE 377M style. Ensures compatibility with older products.
   - **377-1**: Newer SMPTE 377-1 style.

   Refer to related topics in the "Configuring the K2 System" section of this Topic Library for more information.

2. Click **Next**.

   The Completing the Configuration Wizard page opens.

3. Click **Finish**.

   The wizard closes. The server restarts.

Wait until all startup processes have completed before continuing.

Proceed as follows:

- If you have NH servers, configure them next.
- If you do not have NH servers, configure K2 clients and/or other iSCSI clients on the K2 SAN next.

Configuring optional NH servers

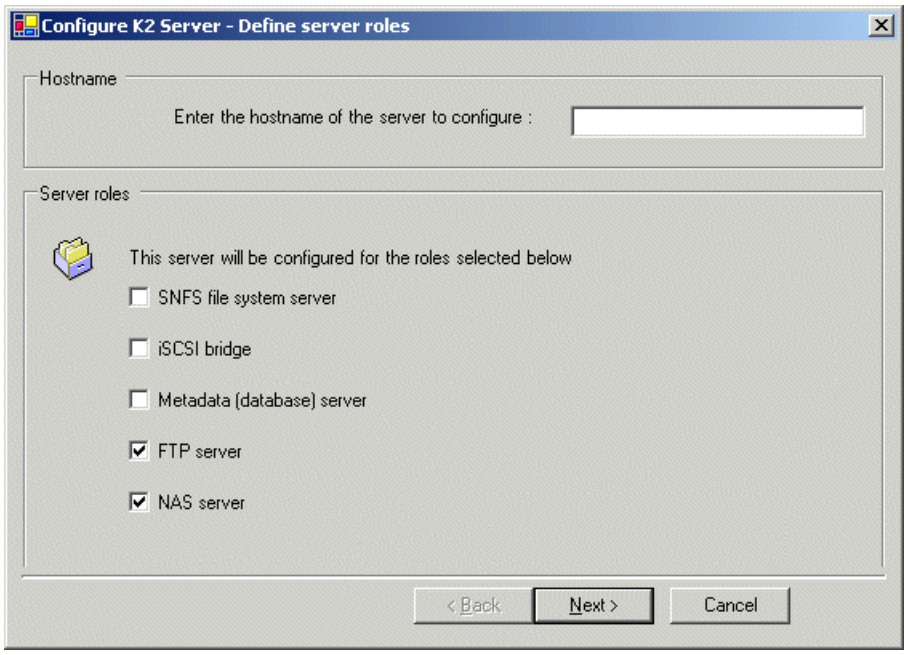
If you have one or more optional NH K2 Media Servers, you next configure those servers. This section applies to both NH1 (1 Gig FTP) servers and NH10GE (10 Gig FTP) servers.

NOTE: Multiple NH servers on a K2 SAN must be of the same type, either all NH1 or all NH10GE.

1. In the K2Config application tree view, select the K2 Media Server you are configuring.
2. Click the **Configure** button.

The Configure K2 Server wizard opens to the Define server roles page.

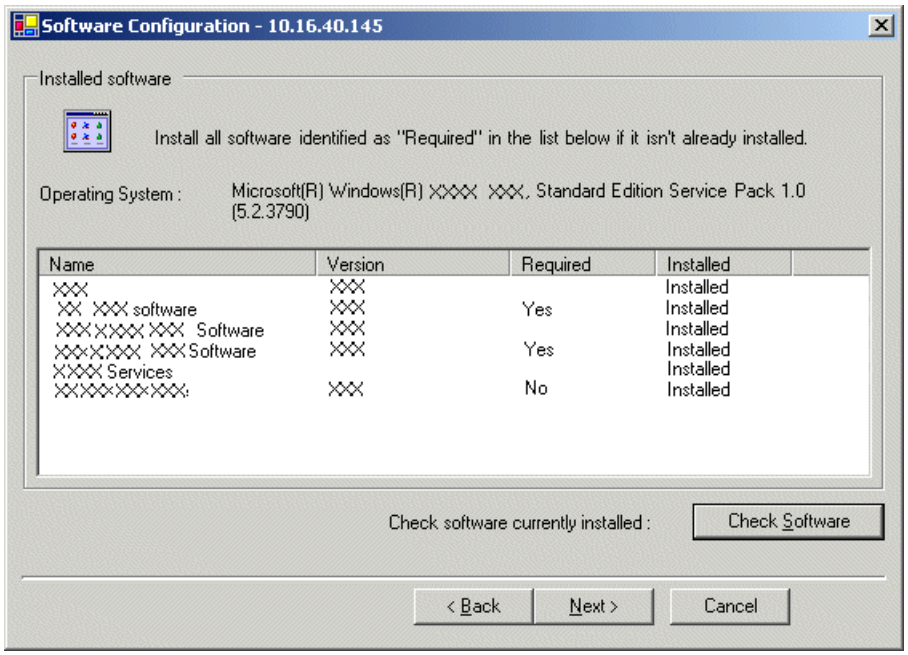
Configure Define Server Roles page - NH server



1. Enter the name for the K2 Media Server, as currently configured on the machine.
2. Select **FTP server** and **NAS server**.
3. Click **Next**.

The Software Configuration page opens.

Configure Software Configuration page - NH server

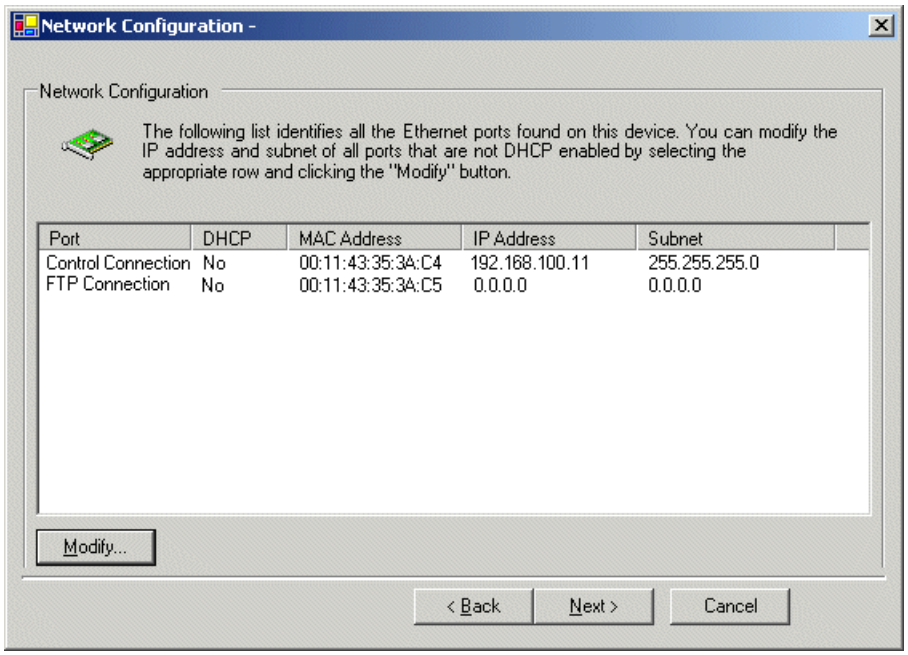


This page checks for the software required to support the roles you selected on the previous page.

1. If software with **Yes** in the Required column reports as **Not Installed**, install the software.
2. Click **Check Software**.
3. When all required software reports as **Installed**, click **Next**.

The Network Configuration page opens.

Configure Network Configuration page - NH server



This page displays the control network Ethernet port, and allows you to configure the FTP/Streaming network Ethernet port.

1. Verify that the top port is configured correctly.

   The top port is the port over which the K2Config application is communicating. If correctly configured, it is already assigned the control network IP address, as displayed on this page.

2. Verify that the FTP/Streaming port is configured correctly. If not configured correctly, do the following:

   a) Select the other port and click **Modify**.

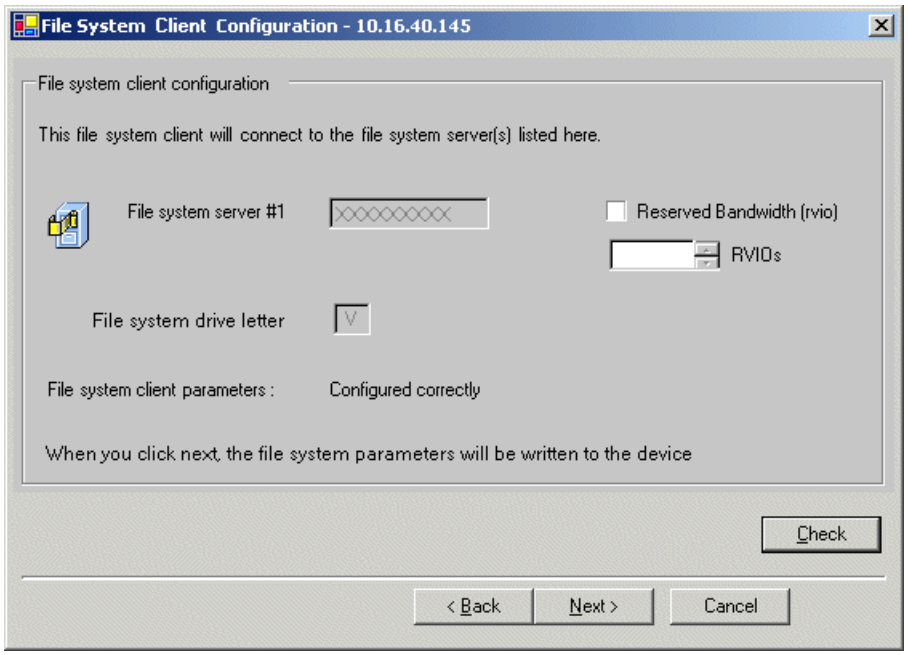
      A network configuration dialog box opens.

   b) Enter the FTP/Streaming IP address and the subnet mask and click **Apply**.

3. Click **Next**.

The File System Server Configuration page opens.

Configure File System Client Configuration page - NH server



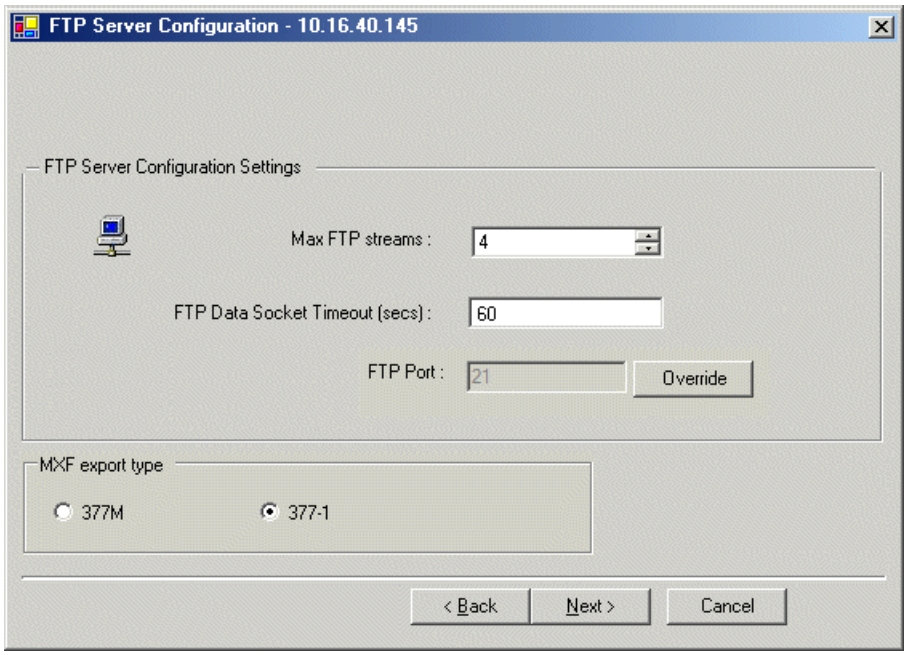
This system does not function as a file system server. It does function as a file system client, which is validated from this page.

1. Do not select **Reserved Bandwidth** unless instructed to do so by Grass Valley. This system is usually not configured for RVIO.
2. Click **Check**.
3. When the wizard reports that the configuration is correct, click **Next**.

   If you get a "The V: will not be available until this device is rebooted…" message, you can safely continue now and reboot later when instructed to do so.

The FTP Server Configuration page opens.

Configure FTP Server Configuration page - Basic SAN NH server



This page appears only if the server has the role of FTP server.

Do not modify these settings. Leave at default values of Max FTP streams = 4, FTP Data Socket Timeout = 60, and FTP Port = 21. Only qualified Grass Valley personnel should specify other values, as these settings are intended for use only with custom systems designed by Grass Valley.

1. Select MXF export type as follows:

   - **377M**: Original SMPTE 377M style. Ensures compatibility with older products.
   - **377-1**: Newer SMPTE 377-1 style.

   Refer to related topics in the "Configuring the K2 System" section of this Topic Library for more information.

2. Click **Next**.

   The Completing the Configuration Wizard page opens.

3. Click **Finish**.

   The wizard closes. The server restarts.

Wait until all startup processes have completed before continuing.

If you have other NH servers, configure them similarly, then configure K2 clients and/or other iSCSI clients on the K2 SAN next.

Configuring the redundant K2 SAN - Online and Production

Work through the topics in this section sequentially to configure an Online (Tier 1) or Production (Tier 2) redundant K2 SAN.

Prerequisites for initial configuration - Redundant K2 SAN

Before beginning your initial configuration, make sure the devices of the K2 SAN meet the following prerequisites.

Control point PC

- Ethernet cable connected
- Control Point software must be installed
- Control network IP address must be assigned
- There must be network communication over the control network with all other K2 devices
- Power must be on

Ethernet switch

- Ethernet cables connected
- Control network IP address must be assigned
- VLANs must be set up
- Trunks must be set up
- Power must be on

K2 Media Server

- Ethernet cables connected
- Fibre Channel cable must be connected
- Redundant servers must be connected by serial cable
- Software must be installed, as from the factory, including QuickTime 7
- Control network IP address must be assigned
- Power must be on for all servers

K2 RAID chassis

- Fibre Channel cable(s) must be connected
- Ethernet cable(s) must be connected
- Power must be on

K2 RAID Expansion chassis (optional)

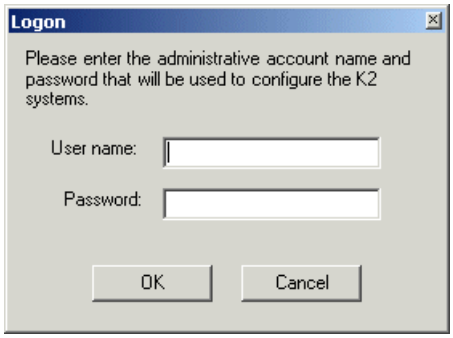
- Fibre channel cable(s) must be connected
- Power must be on

Defining a new K2 SAN

If you import a SiteConfig system description file in which the SAN is defined, you do not need to define a new SAN. You can skip this task and instead start by configuring the first K2 Media Server.

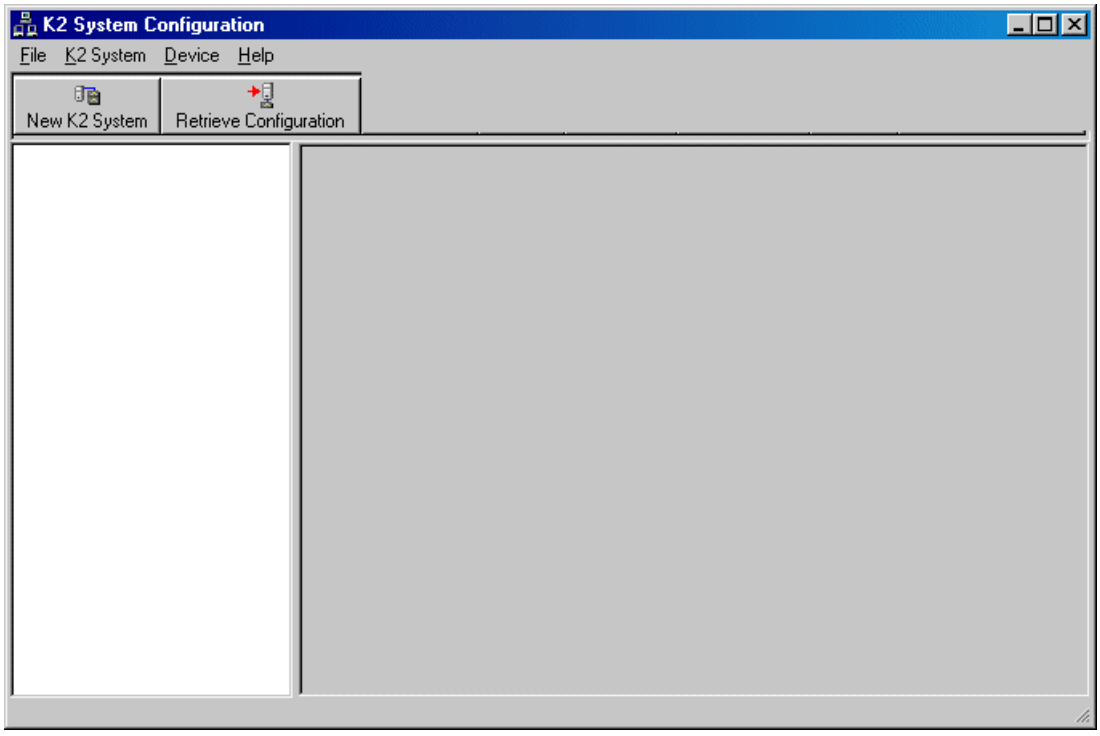
1. On the control point PC, open the K2Config application.

   A log on dialog box opens.



2. Log on to the K2Config application with the Windows administrator account.

   The K2Config application opens.



3. Click **New K2 System**.

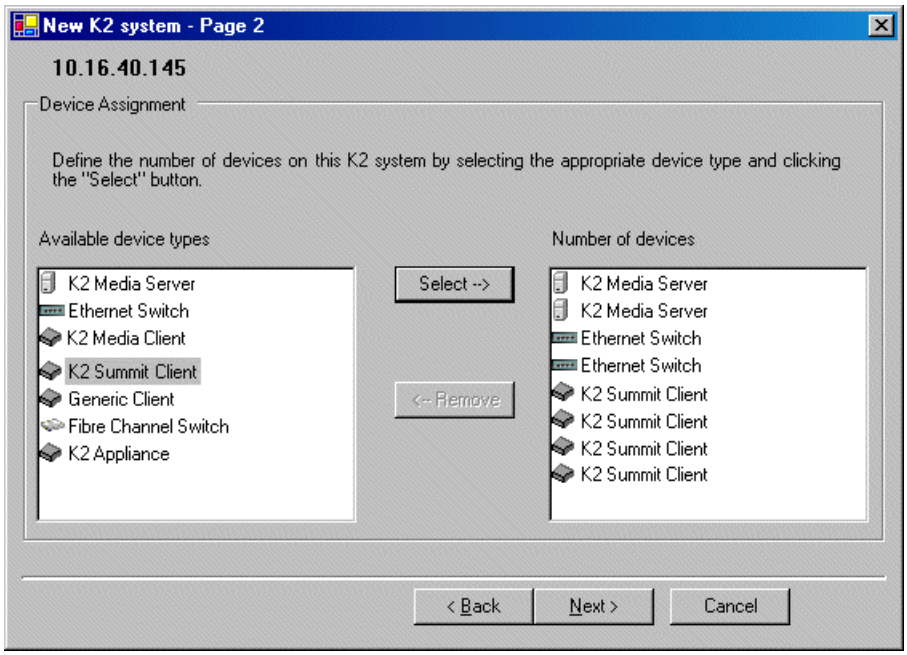
The New K2 System wizard opens to page 1.

Configure New K2 System page 1 - Redundant K2 SAN

1. Create a name for your system and type it in the Name box.
2. Select **L30**.
3. If so designed, select **Enable Live Production mode**.
4. Select the Server redundancy option.
5. Click **Next**.

Page 2 opens.

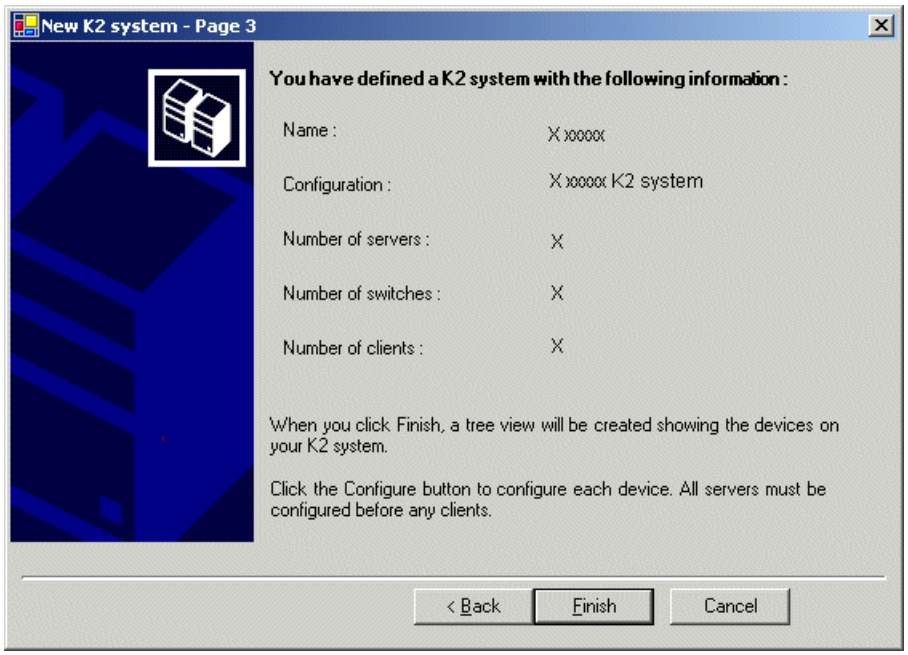
Configure New K2 System page 2 - Redundant K2 SAN



1. Move the following into the Number of devices box:
   - Two K2 Media Servers
   - Two Ethernet switches
   - K2 clients as appropriate for your system.
   - (Optional) One or more K2 Media Servers to represent each NH K2 Media Server on your system.
   - (Optional) Other devices as appropriate for your system.
2. Click **Next**.

Page 3 opens.

Configure New K2 System page 3 - Redundant K2 SAN



1. Review the information on this page and verify that you have correctly defined your K2 SAN. For a basic K2 SAN you should have the following:
   - One Gigabit Ethernet switch
   - One K2 Media Server
   - Optionally, one or more NH K2 Media Servers
   - The number and type of clients appropriate for your system.
2. Click **Finish**.
   The Define New K2 Storage System wizard closes.

Your storage system appears in the tree view of the K2Config application.

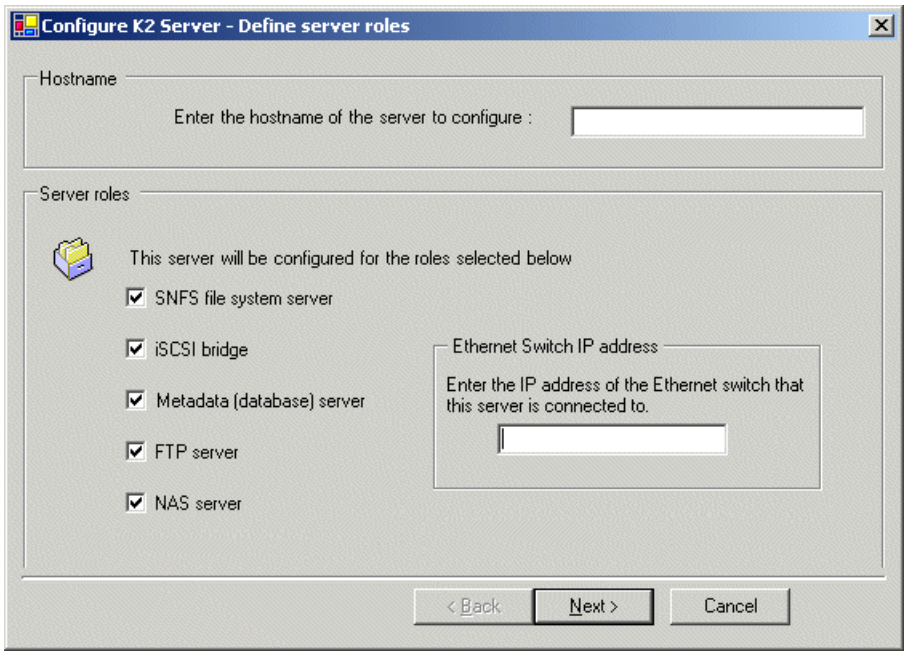
Next, configure the server.

Configuring server A - Part 1

1. In the K2Config application tree view, select **[K2Server1]**.
2. Click the **Configure** button.

The Configure K2 Server wizard opens to the Define server roles page.

Configure Define Server Roles page - Redundant K2 SAN server A and server B

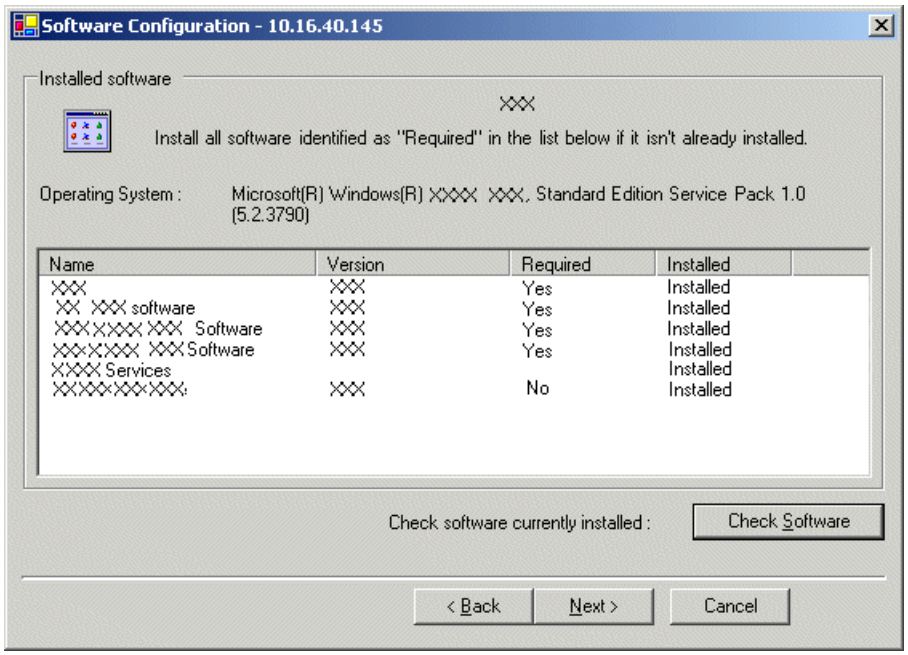


1. Enter the name for the K2 Media Server, as currently configured on the machine.
2. Enter the name or IP address of the Ethernet switch, as currently configured on the switch, to which the K2 Media Server is connected.
3. Select all roles, except as follows:

   If the K2 SAN has one or more optional NH servers, then FTP traffic should go to the NH server, not the K2 Media Server you are now configuring. In this case, do not select the FTP server role or the NAS server role
4. Click **Next**.

The Software Configuration page opens.

Configure Software Configuration page - Redundant K2 SAN server A and server B

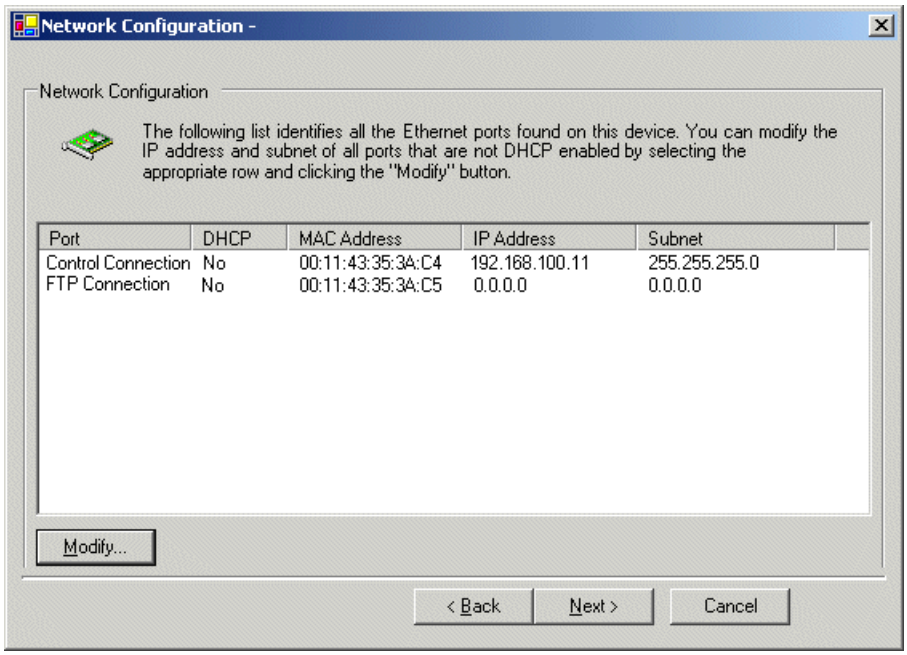


This page checks for the software required to support the roles you selected on the previous page.

1. If software with **Yes** in the Required column reports as **Not Installed**, install the software.
2. Click **Check Software**.
3. When all required software reports as **Installed**, click **Next**.

The Network Configuration page opens.

Configure Network Configuration page - Redundant K2 SAN server A and server B



This page displays the control network Ethernet port, and allows you to configure the FTP/Streaming network Ethernet port.

NOTE: This page does not configure the iSCSI interface (media network) ports.

1. Verify that the top port is configured correctly.

   The top port is the port over which the K2Config application is communicating. If correctly configured, it is already assigned the control network IP address, as displayed on this page.

2. If the server has the role of FTP server, verify that the other port is configured correctly. If not configured correctly, do the following:

   a) Select the other port and click **Modify**.

   A network configuration dialog box opens.

   b) Enter the FTP/Streaming IP address and the subnet mask and click **Apply**.

   For systems with an optional NH (FTP) server, the server you are now configuring does not take the role of FTP server, so configuring the second port here for the FTP/streaming network is not required.

3. Click **Next**.

The File System Server Configuration page opens.

Configure File System Server Configuration page - Redundant K2 SAN server A

1. Enter the name or IP address of the redundant K2 Media Server (server B).

   Do not yet enter anything in the File System Server #2 box.

2. Click **Launch Storage Manager**.

   Storage Utility opens.

3. Leave the Configure K2 Server wizard open while you use Storage Utility.

   When you are done with Storage Utility, you continue with the wizard.

Next, use Storage Utility to configure the RAID storage and file system.

Configuring RAID

Use Storage Utility to complete the configuration of the K2 RAID storage devices, as explained in the following topics.

Configuring RAID network and SNMP settings

- Fibre Channel cable(s) must be connected
- Ethernet cable(s) must be connected
- Power must be on

- Fibre channel cable(s) must be connected
- Power must be on

Use the Storage Utility to configure the following settings for the K2 RAID controller:

- IP address
- Subnet mask
- Gateway Address
- SNMP trap destinations

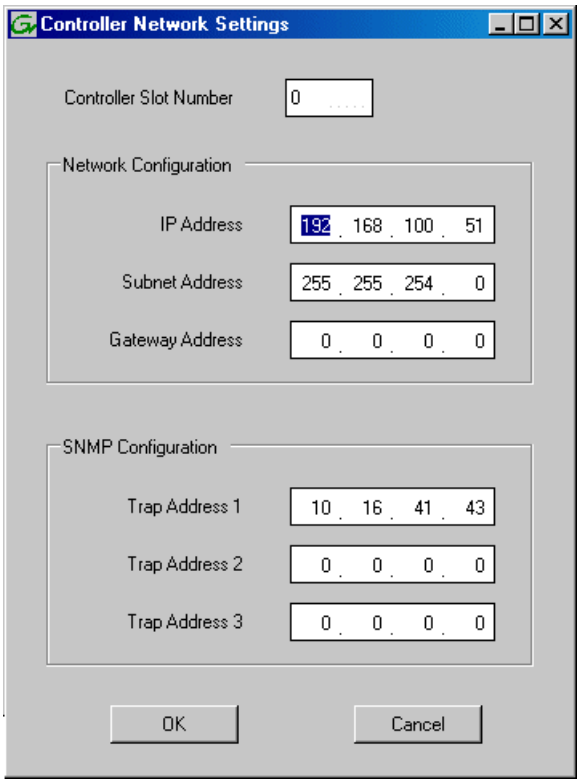
For K2 RAID, network and SNMP settings are set and stored on the RAID controller module. For the RAID chassis with two controllers, each controller has its own network settings and the RAID chassis exists as two entities on the control network.

The RAID storage device is configured by default for the SNMP community name “public”. If your site’s policies require using a different SNMP community name, contact your Grass Valley representative.

1. Launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.

3. In Storage Utility tree view, expand the node for the K2 RAID, right-click the icon for a RAID controller, and select **Configuration | Network Properties**.

   The Controller Network Settings dialog box opens.



4. In the Controller Slot Number field enter **0** and then press **Enter**.

   The settings from controller 0 are loaded into the Controller Network Settings dialog box and are available for you to modify.

5. Enter the control network IP address and other network settings.
6. For SNMP Configuration, enter the IP address of the SNMP manager PC.

   You can also enter IP addresses for other SNMP managers to which you want to send SNMP trap messages.

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

7. For the RAID chassis with two controllers, in the Controller Slot Number field enter **1** and then press **Enter**.

   The settings from controller 1 are loaded into the Controller Network Settings dialog box and are available for you to modify.

8. Repeat the previous steps to configure controller 1.
9. Click **OK** to save settings and close.
10. In Storage Utility click **View | Refresh**.

Next, bind disk modules.

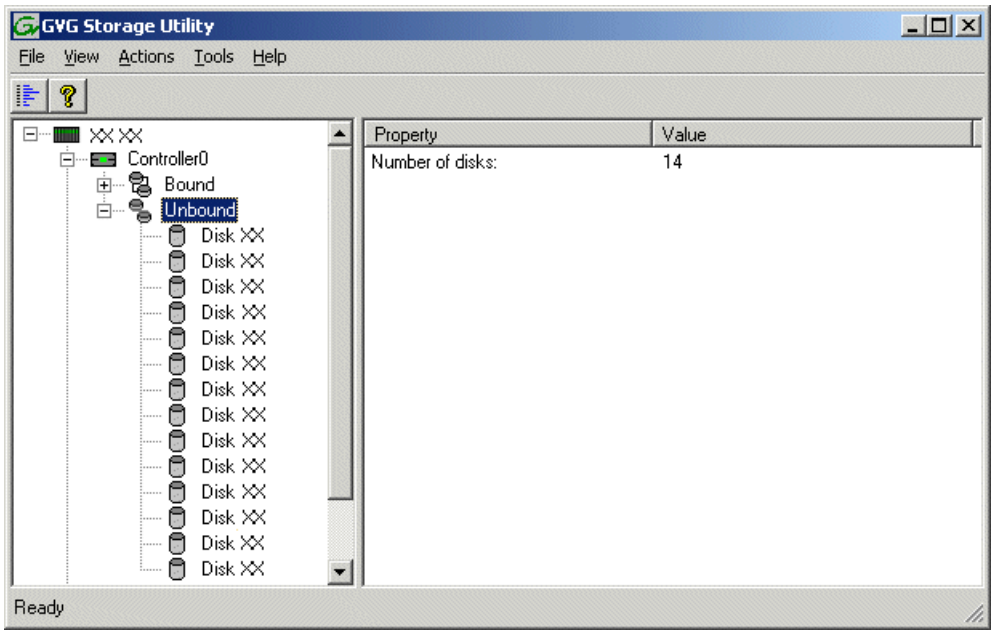
Binding disk modules - Redundant K2 SAN

- Fibre Channel cable(s) must be connected
- Ethernet cable(s) must be connected
- Power must be on

- Fibre channel cable(s) must be connected
- Power must be on

NOTE: Binding destroys all user data on the disks.

1. If you have not already done so, launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.
3. In the Storage Utility main window, identify bound RANKs and unbound disks by their placement in the hierarchy of the tree view. In the following illustration, disk numbers are represented by "XX".

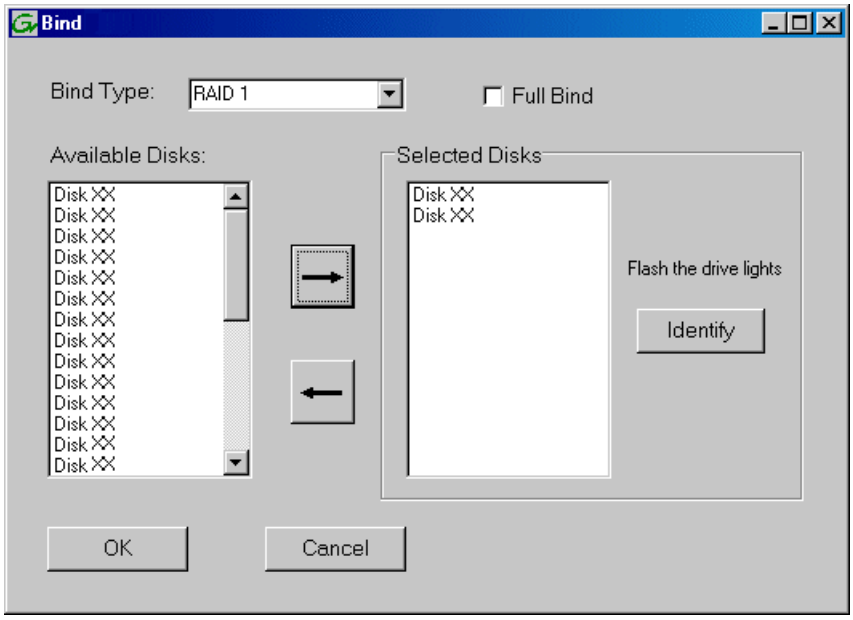


There is one RAID 1 pair with two disks.

View disk properties and identify the two disks you will use for the metadata/journal RAID 1 RANK. Make sure you select disks appropriately as you bind disks in the remainder of this procedure.

4. For systems that use RAID 1 RANKs, you must now create the separate RAID 1 storage for file system metadata files and journal files. To bind unbound disks for metadata and journal storage, do the following:
   a) Right-click the **Unbound** node for the controller, then select Bind in the context menu. (If the RAID chassis has two controllers, both controllers are represented by the single "Controller" node)

      The Bind dialog box opens showing all unbound disks for the controller listed in the Available Disk list.



   b) Leave **Full Bind** unchecked.
   c) In the **Bind Type** drop down box, select **RAID 1**.
   d) In the Available Disks box, select two contiguous disks at the top of the list. These should be the first two disks in the primary RAID chassis. (TIP: Use 'shift-click' or 'control-click' to select disks.) This creates a RAID 1 RANK for file system metadata and journal storage.
   e) Click the add (arrow) button to add disks to the Selected Disks list.

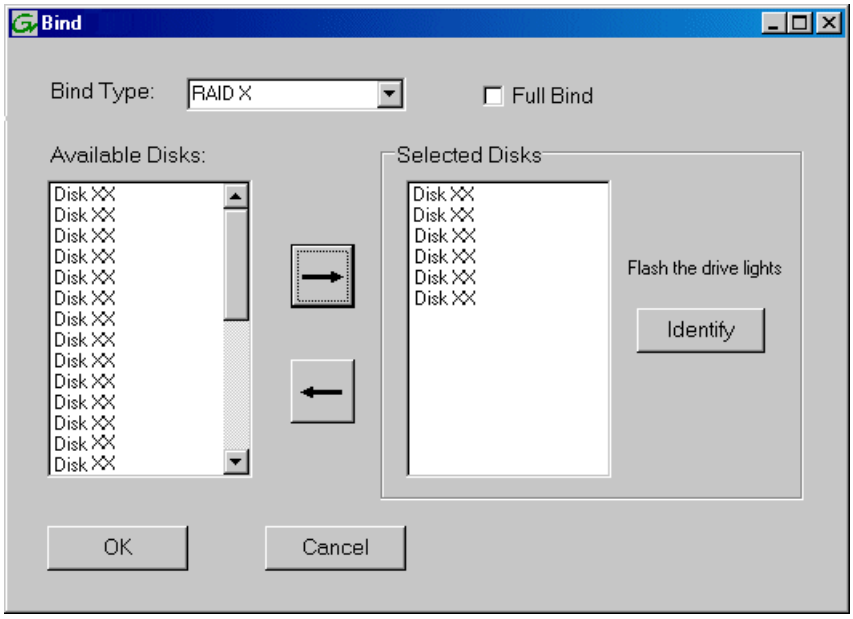
      NOTE: As an aid in identifying a disk module's physical location, select it in the Selected Disks list, then click Identify Disks. This causes the disk drive light to flash.

   f) Click **OK** to close the Bind dialog box and begin the binding process. The Progress Report dialog box opens, showing the status of the binding process.
   g) Close the Progress Report .
   h) Make the third disk in the primary RAID chassis a Hot Spare. In the **Bind Type** drop down box, select **Hot Spare**.

5. Right-click the **Unbound** node for a controller, then select **Bind** in the context menu.

   If the RAID chassis has two controllers, both controllers are represented by the single “Controller” node.

   The Bind dialog box opens showing all unbound disks for the controller listed in the Available Disk list.



6. Leave **Full Bind** unchecked.
7. In the **Bind Type** drop down box, select **RAID 5** or **RAID 6**, as specified by your system design.
8. In the Available Disks box, select six contiguous disks at the top of the list.

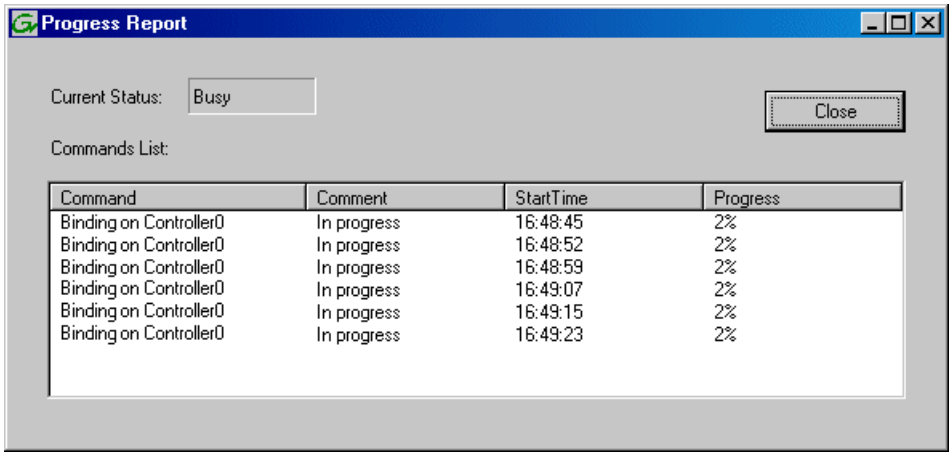
   Use ‘shift-click’ or ‘control-click’ to select disks.

9. Click the add (arrow) button to add disks to the Selected Disks list.

   NOTE: As an aid in identifying a disk module’s physical location, select it in the Selected Disks list, then click Identify Disks. This causes the disk drive light to flash.

10. Click **OK** to close the Bind dialog box and begin the binding process.

    The Progress Report dialog box opens, showing the status of the binding process.



11. Close the Progress Report and repeat these steps for other unbound disks.

    If specified by your system design, you can bind some disks as Hot Spares.

    When you are done, if you did not bind any extra Hot Spares, you should have the following results:

    For redundant storage, on the primary RAID chassis you should have one RAID 1 RANK disk, one Hot Spare Disk, and one or more RAID 5 or RAID 6 RANKs, with each RANK having six disks, as necessary to fill the primary RAID chassis. For each optional Expansion chassis, RANKs are similar.

12. Click **Close** in Progress Report window.
13. Restart the K2 Media Server.

    NOTE: Make sure start up processes on the K2 Media Server are complete before proceeding.

Next, create a new file system.

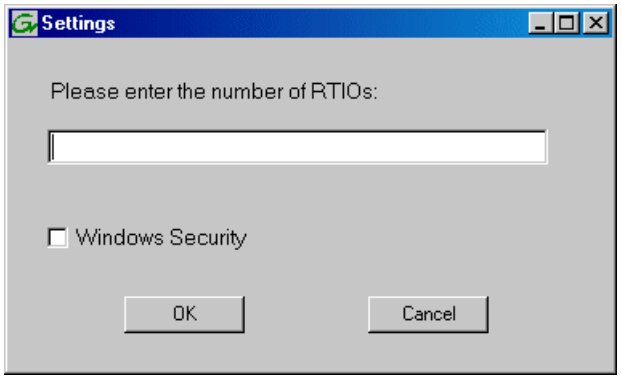
Creating a new file system - Redundant K2 SAN

- Fibre Channel cable(s) must be connected
- Ethernet cable(s) must be connected
- Power must be on
- Disks must be bound

- Fibre channel cable(s) must be connected
- Power must be on
- Disks must be bound

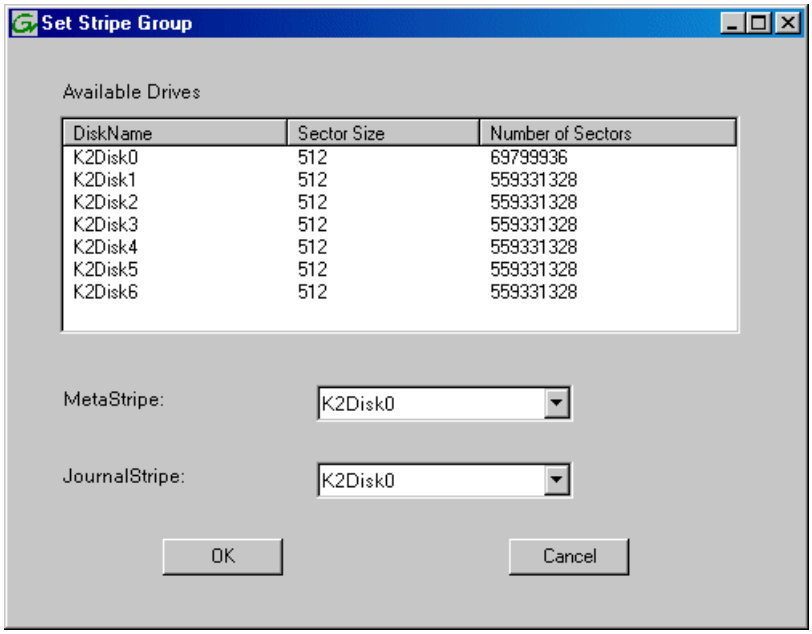
1. If you have not already done so, launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.

3. In Storage Utility, click **Tools | Make New File System**.
   The Setting dialog box opens.



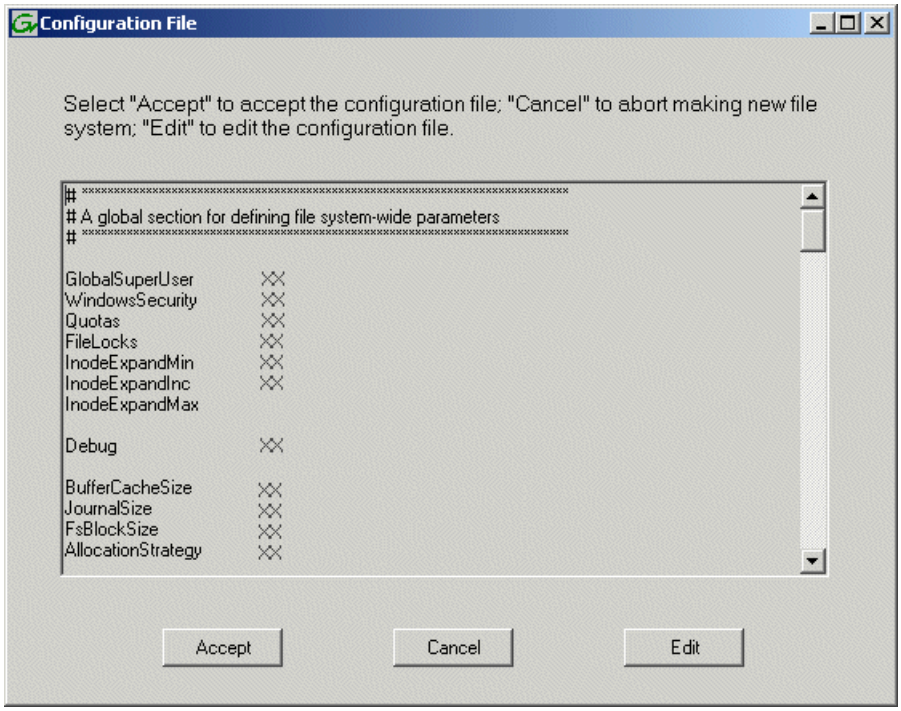
4. For the Real Time Input/Output (RTIO) rate, enter the value specified by your system design. If you do not know this value, contact your Grass Valley representative.
5. Configure Windows Security as follows:
   - If the K2 SAN is on a network Workgroup (not domain), do not select **Windows Security** .
   - If the K2 SAN is on a network domain, you may select **Windows Security**.

   NOTE: Only select Windows Security if the K2 SAN is on a domain. Never select Windows Security if the K2 SAN is on a workgroup.
6. Click **OK**.
   The Set Stripe Group dialog box opens.



7. If you have a RAID 1 RANK, assign the RAID 1 RANK for both MetaStripe and JournalStripe. You can distinguish a RAID 1 RANK from a media RANK by the value in the Number of Sectors column.
8. Click **OK**.

   The Configuration File dialog box opens.



   The configuration file for the media file system is displayed.

9. Verify media file system parameters.

   Do not edit the configuration file for the media file system.

10. Click **Accept**.

    A "…Please wait…" message box displays progress and a "…succeeded…" message confirms the process is complete.

    A message informs you that you must restart the server, however the restart at the end of the Configure K2 Server wizard suffices, so you do not need to restart now.

11. Close the Storage Utility.

    NOTE: Do not attempt to start SAN-attached systems or otherwise bring the SAN online until instructed to do so by the documented procedure.

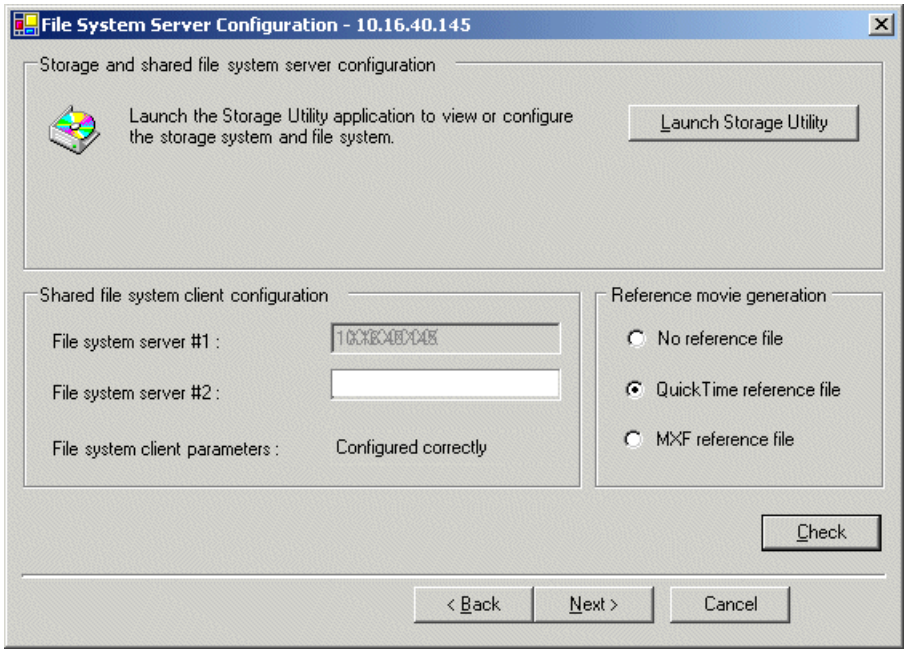
Next, continue with configuring the server using the K2Config application.

Configuring server A - Part 2

Configure File System Server Configuration page - Redundant K2 SAN server A

- Network and SNMP settings must be configured

- Disks must be bound
- There must be a new file system



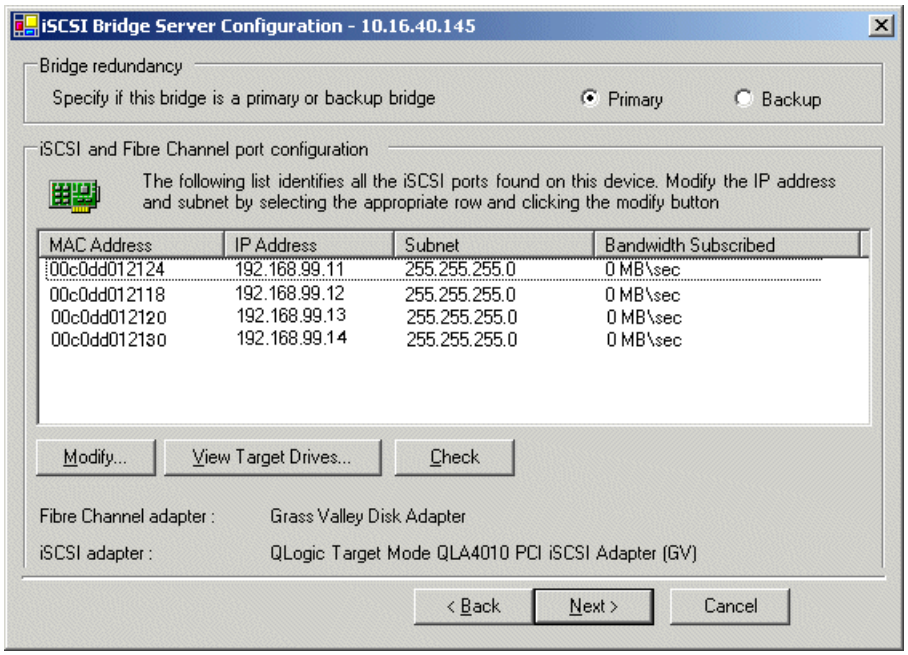
This page checks on the configuration of the K2 Media Server in one of its main roles as a file system server. The K2 Media Server also functions as a file system client, which is also checked from this page.

1. In Storage Utility open the server's File System Server Configuration page, if the page is not already open.
2. If you have not already done so, enter the name or IP address of the redundant K2 Media Server (server B).
3. If desired, configure reference file generation.
4. Click **Check**.
5. When the wizard reports that the configuration is correct, click **Next**.

   If you get a "The V: will not be available until this device is rebooted…" message, you can safely continue now and reboot later when instructed to do so.

The iSCSI Bridge Server Configuration page opens.

Configure iSCSI Bridge Server Configuration page - Redundant K2 SAN server A



This page manages the components that bridge between iSCSI (the GigE media network) and the Fibre Channel connection to the RAID storage. You configure network settings on the iSCSI adapters and the page validates that the Fibre Channel adapter is in place and that the media RANKs are visible as iSCSI targets.

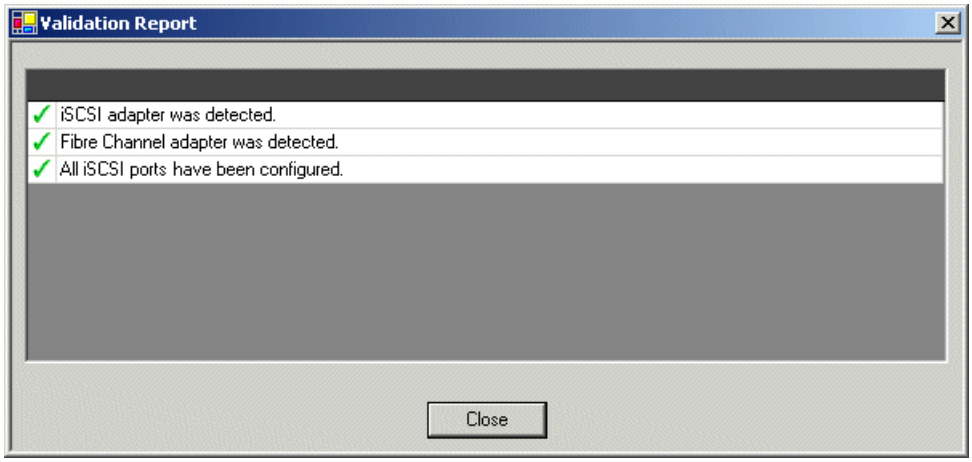
1. Select **Primary**.
2. Select an iSCSI adapter and do the following:
   a) Click **Modify**.

      A network configuration dialog box opens.

   b) Verify or enter the media network IP address and the subnet mask.
   c) Click **Apply**.
   d) Click **View Target Drives**.
   e) Verify that all drives are shown in the **Drives exposed as iSCSI targets** field.
3. Repeat the previous step for the other iSCSI adapters.

4. Click **Check**.

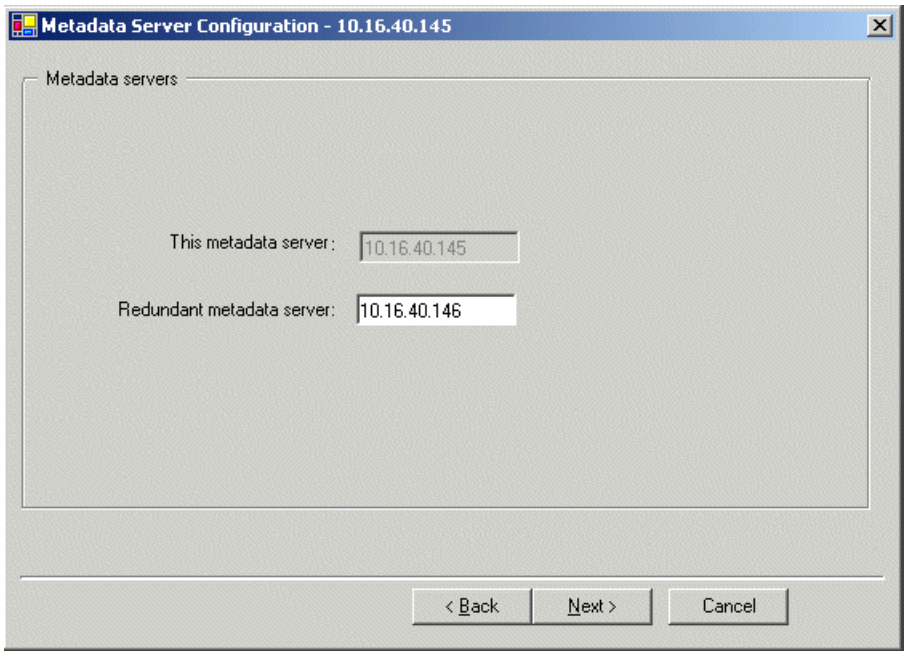
   The Validation Report opens.



5. Confirm that the iSCSI configuration is successful.
6. Close the Validation Report.
7. Click **Next**.

The Database Server Configuration page opens.

Configure Database Server Configuration page - Redundant K2 SAN server A

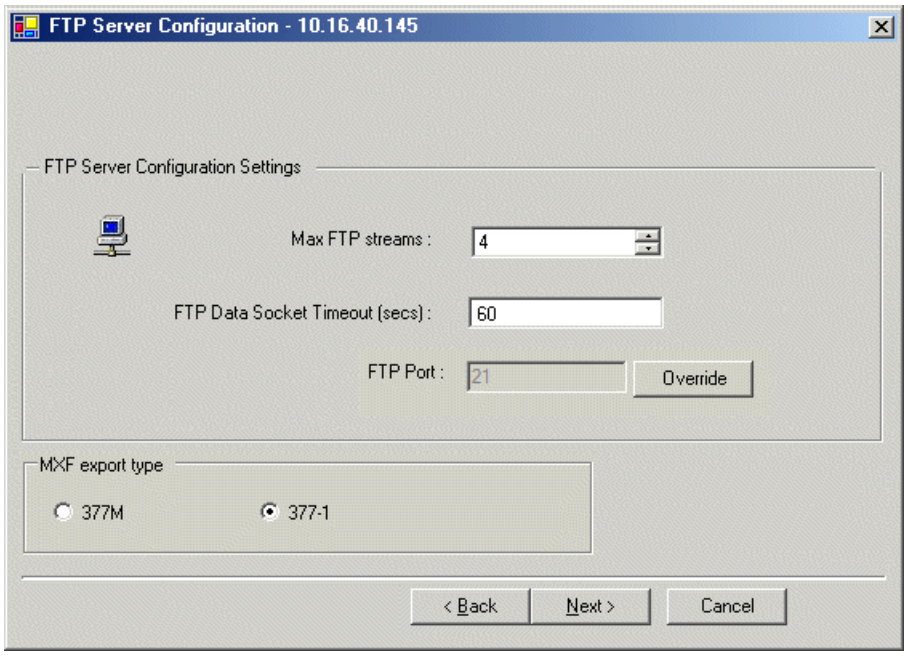


1. Enter the name or IP address of K2 Media server B. This is the redundant partner of the server you are now configuring.

2. Click **Next**.

The FTP Server Configuration page opens.

Configure FTP Server Configuration page - Redundant K2 SAN server A



This page appears only if the server has the role of FTP server.

Do not modify these settings. Leave at default values of Max FTP streams = 4, FTP Data Socket Timeout = 60, and FTP Port = 21. Only qualified Grass Valley personnel should specify other values, as these settings are intended for use only with custom systems designed by Grass Valley.

1. Select MXF export type as follows:
   - **377M**: Original SMPTE 377M style. Ensures compatibility with older products.
   - **377-1**: Newer SMPTE 377-1 style.

   Refer to related topics in the "Configuring the K2 System" section of this Topic Library for more information.
2. Click **Next**.

   The Completing the Configuration Wizard page opens.
3. Click **Finish**.

   The wizard closes. The server restarts.

Wait until all startup processes have completed before continuing.

Next, configure the redundant server.

Configuring server B

- Server A must be configured

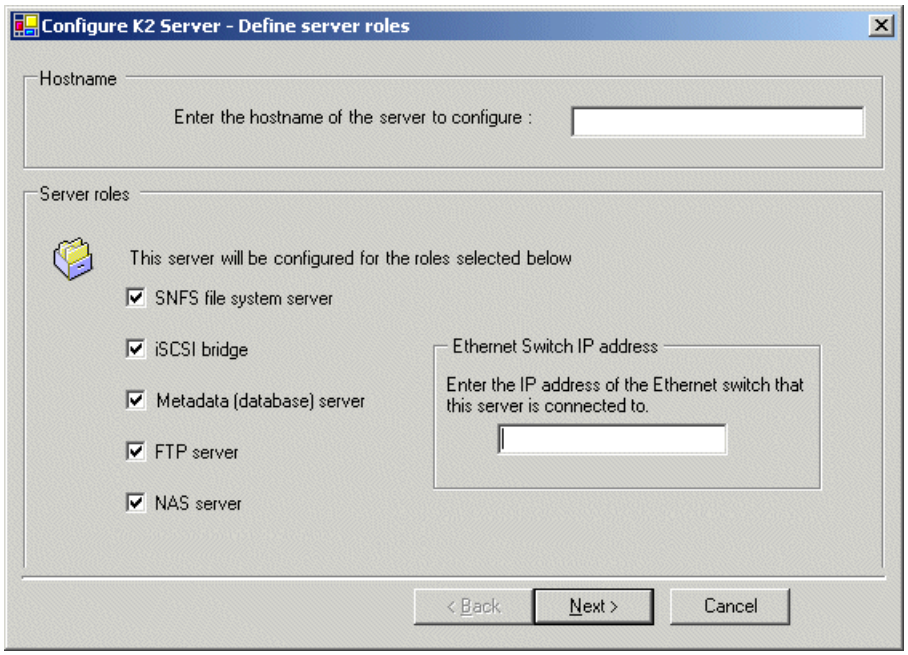
- The restart of server A after it is configured must be complete

After you have configured the first K2 Media Server (server A) you next configure the redundant K2 Media Serer (server B).

1. Verify that server A has restarted by opening the MS-DOS command prompt and use the “ping” command.
2. In the K2 System Configuration application tree view, select the K2 Media Server you are configuring as server B.
3. Click the **Configure** button.

The Configure K2 Server wizard opens to the Define server roles page.

Configure Define Server Roles page - Redundant K2 SAN server A and server B

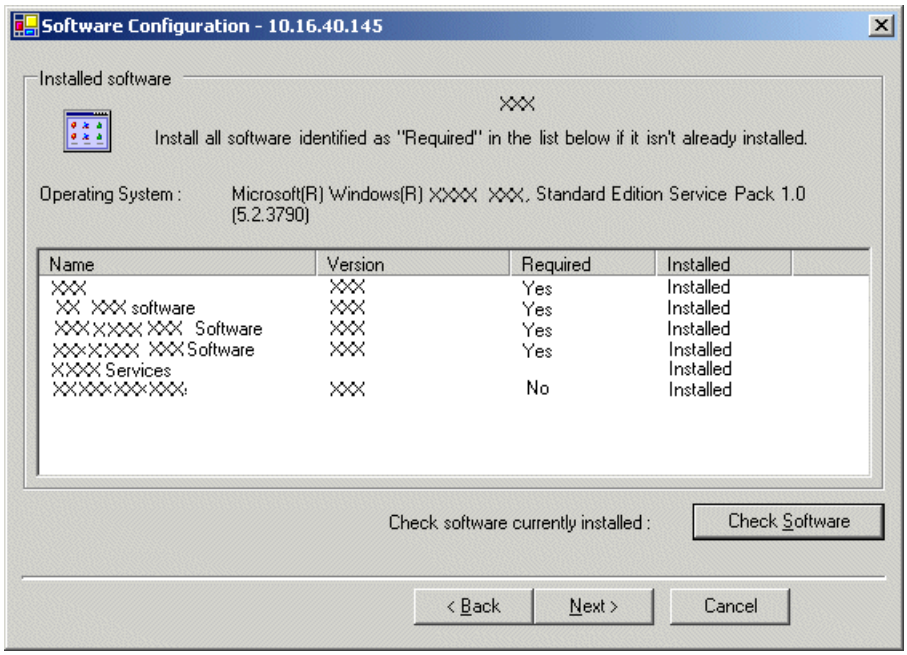


1. Enter the name for the K2 Media Server, as currently configured on the machine.
2. Enter the name or IP address of the Ethernet switch, as currently configured on the switch, to which the K2 Media Server is connected.
3. Select all roles, except as follows:

   If the K2 SAN has one or more optional NH servers, then FTP traffic should go to the NH server, not the K2 Media Server you are now configuring. In this case, do not select the FTP server role or the NAS server role
4. Click **Next**.

The Software Configuration page opens.

Configure Software Configuration page - Redundant K2 SAN server A and server B

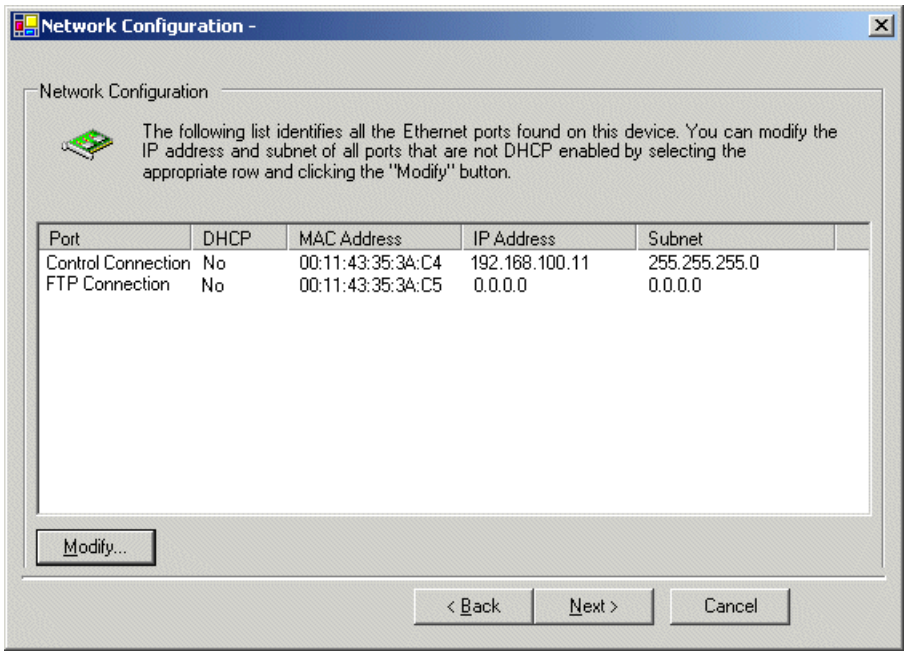


This page checks for the software required to support the roles you selected on the previous page.

1. If software with **Yes** in the Required column reports as **Not Installed**, install the software.
2. Click **Check Software**.
3. When all required software reports as **Installed**, click **Next**.

The Network Configuration page opens.

Configure Network Configuration page - Redundant K2 SAN server A and server B



This page displays the control network Ethernet port, and allows you to configure the FTP/Streaming network Ethernet port.

NOTE: This page does not configure the iSCSI interface (media network) ports.

1. Verify that the top port is configured correctly.

   The top port is the port over which the K2Config application is communicating. If correctly configured, it is already assigned the control network IP address, as displayed on this page.

2. If the server has the role of FTP server, verify that the other port is configured correctly. If not configured correctly, do the following:

   a) Select the other port and click **Modify**.

      A network configuration dialog box opens.

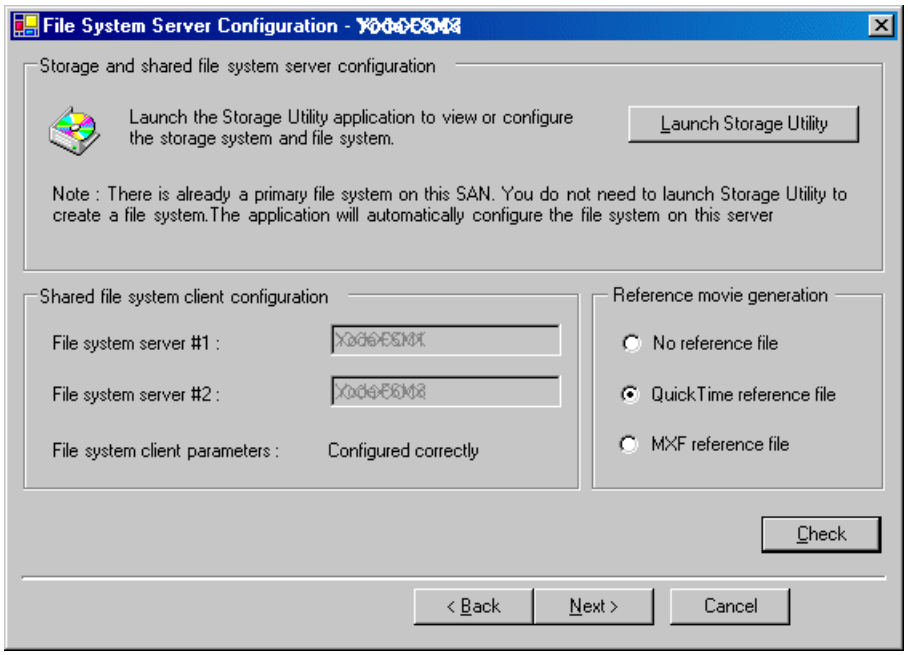
   b) Enter the FTP/Streaming IP address and the subnet mask and click **Apply**.

   For systems with an optional NH (FTP) server, the server you are now configuring does not take the role of FTP server, so configuring the second port here for the FTP/streaming network is not required.

3. Click **Next**.

The File System Server Configuration page opens.

Configure File System Server Configuration page - Redundant K2 SAN server B



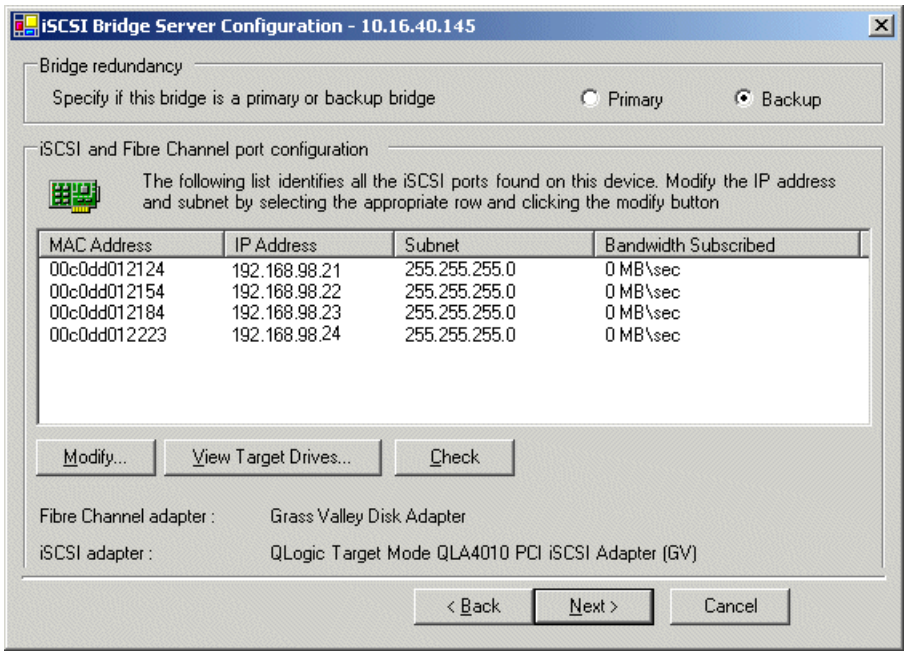
This page checks on the configuration of the K2 Media Server in one of its main roles as a file system server. The K2 Media Server also functions as a file system client, which is also checked from this page. It is not necessary to bind RANKs or create a file system, since this task was completed when you configured the previous K2 Media Server.

1. If desired, configure reference file generation.
2. Click **Check**.
3. Confirm a "… file copied…" message.
4. When the wizard reports that the configuration is correct, click **Next**.
5. Confirm messages about copying the file system configuration file to the other server.

   If you get a "The V: will not be available until this device is rebooted…" message, you can safely continue now and reboot later when instructed to do so.

The iSCSI Bridge Server Configuration page opens.

Configure iSCSI Bridge Server Configuration page - Redundant K2 SAN server B

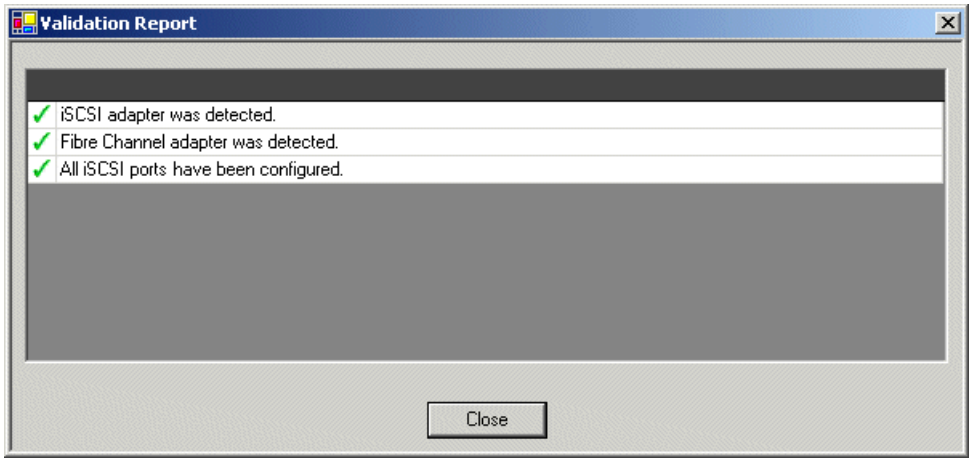


This page manages the components that bridge between iSCSI (the GigE media network) and the Fibre Channel connection to the RAID storage. You configure network settings on the iSCSI adapters and the page validates that the Fibre Channel adapter is in place and that the media RANKs are visible as iSCSI targets.

NOTE: The iSCSI adapters on this server must be on a different subnet than those on its redundant server partner.

1. Select **Backup**.
2. Select an iSCSI adapter and do the following:
   a) Click **Modify**.
      A network configuration dialog box opens.
   b) Verify or enter the media network IP address and the subnet mask.
   c) Click **Apply**.
   d) Click **View Target Drives**.
   e) Verify that all drives are shown in the **Drives exposed as iSCSI targets** field.
3. Repeat the previous step for the other iSCSI adapters.

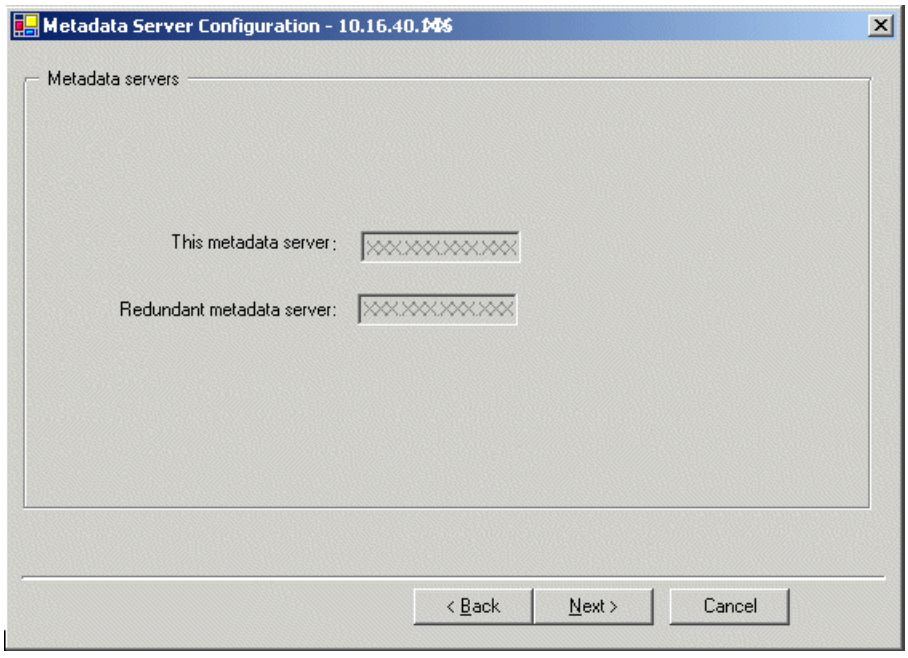
4. Click **Check**.
   The Validation Report opens.



5. Confirm that the iSCSI configuration is successful.
6. Close the Validation Report.
7. Click **Next**.

The Database Server Configuration page opens.

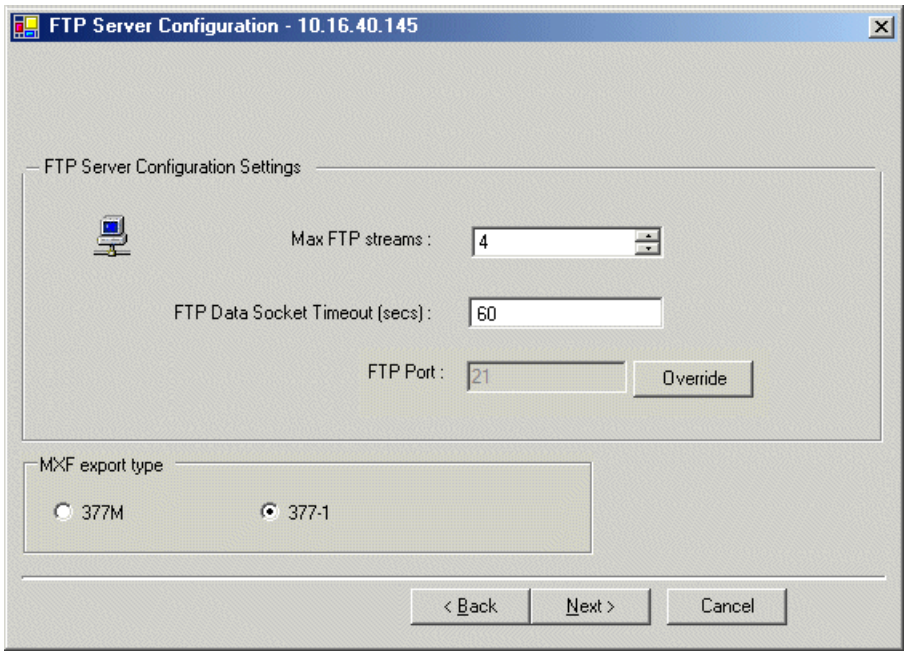
Configure Database Server Configuration page - Redundant K2 SAN server B



Click **Next**.
You do not need to enter or configure anything on this page.

The FTP Server Configuration page opens.

Configure FTP Server Configuration page - K2 SAN server B



This page appears only if the server has the role of FTP server.

Do not modify these settings. Leave at default values of Max FTP streams = 4, FTP Data Socket Timeout = 60, and FTP Port = 21. Only qualified Grass Valley personnel should specify other values, as these settings are intended for use only with custom systems designed by Grass Valley.

1. Select MXF export type as follows:
   - **377M**: Original SMPTE 377M style. Ensures compatibility with older products.
   - **377-1**: Newer SMPTE 377-1 style.

   Refer to related topics in the "Configuring the K2 System" section of this Topic Library for more information.
2. Click **Next**.

   The Completing the Configuration Wizard page opens.
3. Click **Finish**.

   The wizard closes. The server restarts.

Wait until all startup processes have completed before continuing.

Next, check the V: drive

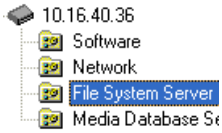
Check the V: drive

- The K2 Media Server must be configured

- The restart of the K2 Media Server after it is configured must be complete

This task is required for NAS server functionality.

1. Verify that the K2 Media Server has restarted by opening the MS-DOS command prompt and use the “ping” command.
2. In the K2Config application tree view, under the K2 Media Server select the File System Server node.



   The File System Server Configuration page appears.

3. Click **Check** and verify that the V: drive is shared.

Proceed as follows:

- If you have NH servers, configure them next.
- If you do not have NH servers, configure K2 clients and/or other iSCSI clients on the K2 SAN next.

Configuring optional NH servers

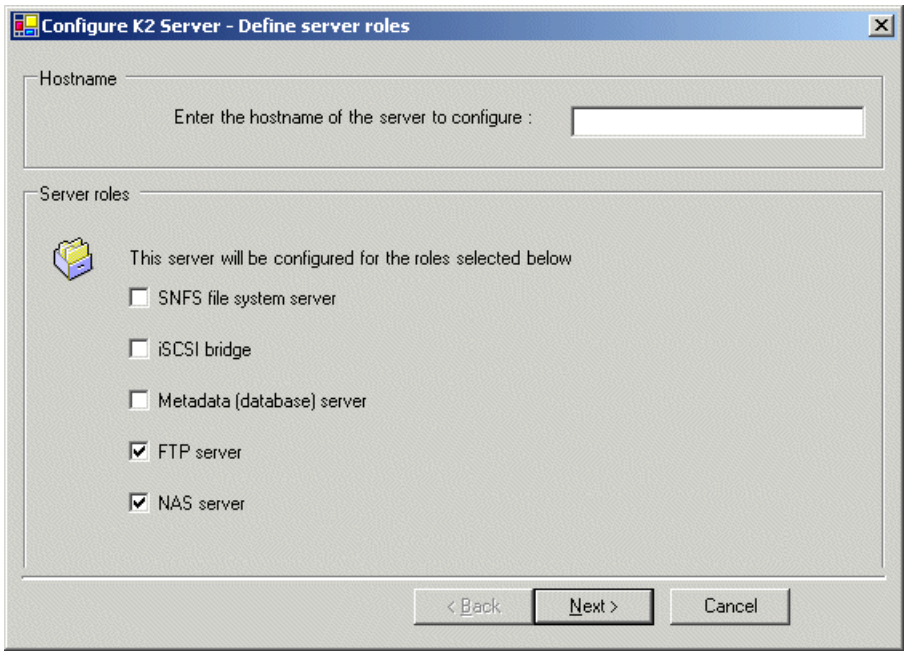
If you have one or more optional NH K2 Media Servers, you next configure those servers. This section applies to both NH1 (1 Gig FTP) servers and NH10GE (10 Gig FTP) servers.

NOTE: Multiple NH servers on a K2 SAN must be of the same type, either all NH1 or all NH10GE.

1. In the K2Config application tree view, select the K2 Media Server you are configuring.
2. Click the **Configure** button.

The Configure K2 Server wizard opens to the Define server roles page.

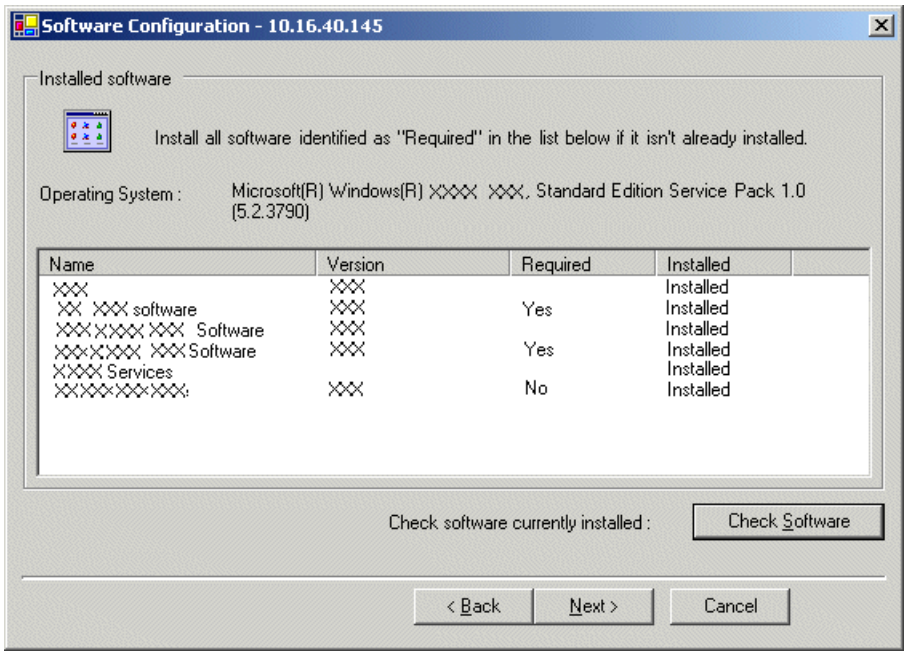
Configure Define Server Roles page - NH server



1. Enter the name for the K2 Media Server, as currently configured on the machine.
2. Select **FTP server** and **NAS server**.
3. Click **Next**.

The Software Configuration page opens.

Configure Software Configuration page - NH server

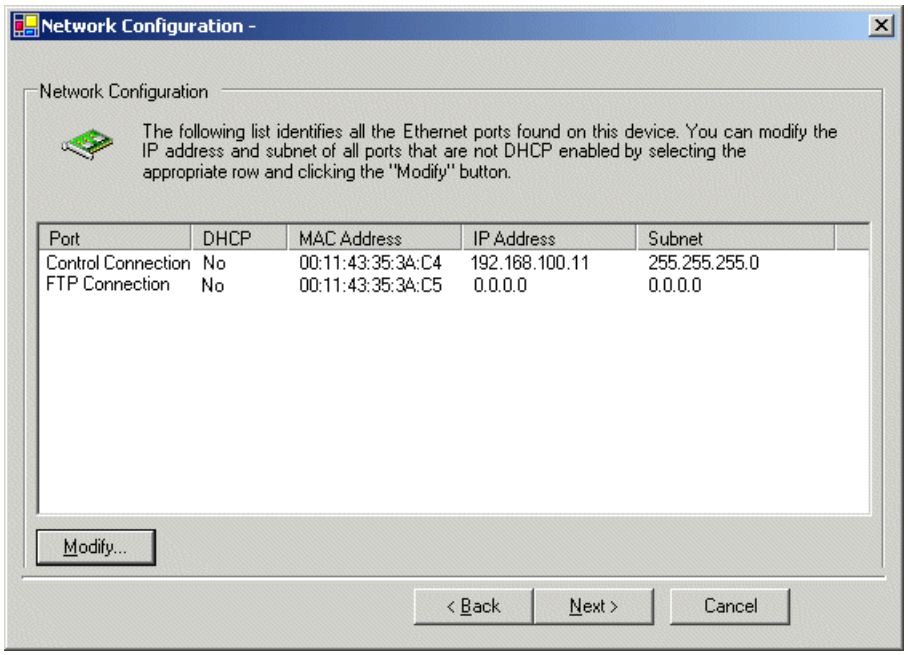


This page checks for the software required to support the roles you selected on the previous page.

1. If software with **Yes** in the Required column reports as **Not Installed**, install the software.
2. Click **Check Software**.
3. When all required software reports as **Installed**, click **Next**.

The Network Configuration page opens.

Configure Network Configuration page - NH server



This page displays the control network Ethernet port, and allows you to configure the FTP/Streaming network Ethernet port.

1. Verify that the top port is configured correctly.

   The top port is the port over which the K2Config application is communicating. If correctly configured, it is already assigned the control network IP address, as displayed on this page.

2. Verify that the FTP/Streaming port is configured correctly. If not configured correctly, do the following:

   a) Select the other port and click **Modify**.

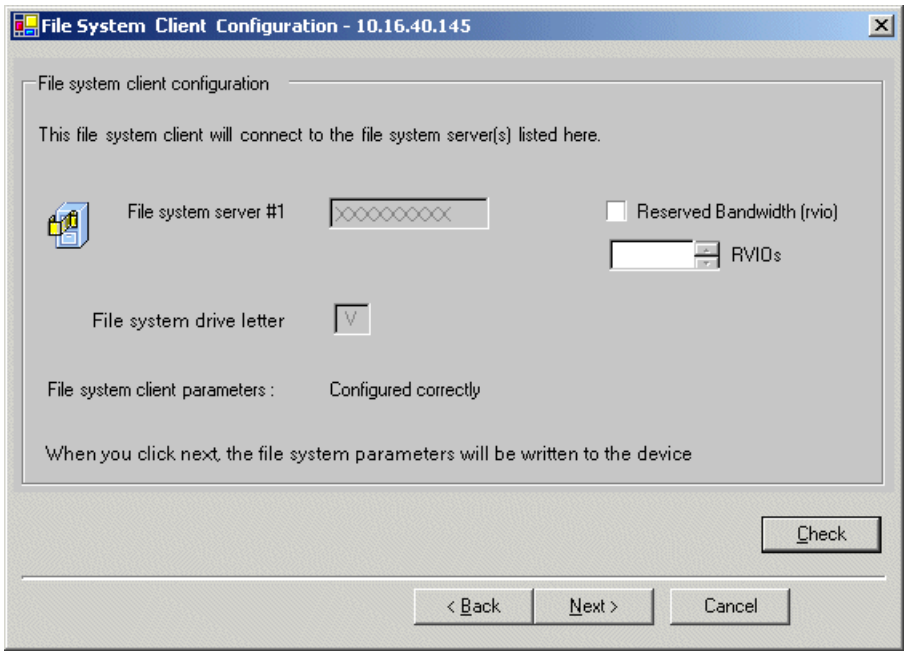
      A network configuration dialog box opens.

   b) Enter the FTP/Streaming IP address and the subnet mask and click **Apply**.

3. Click **Next**.

The File System Server Configuration page opens.

Configure File System Client Configuration page - NH server



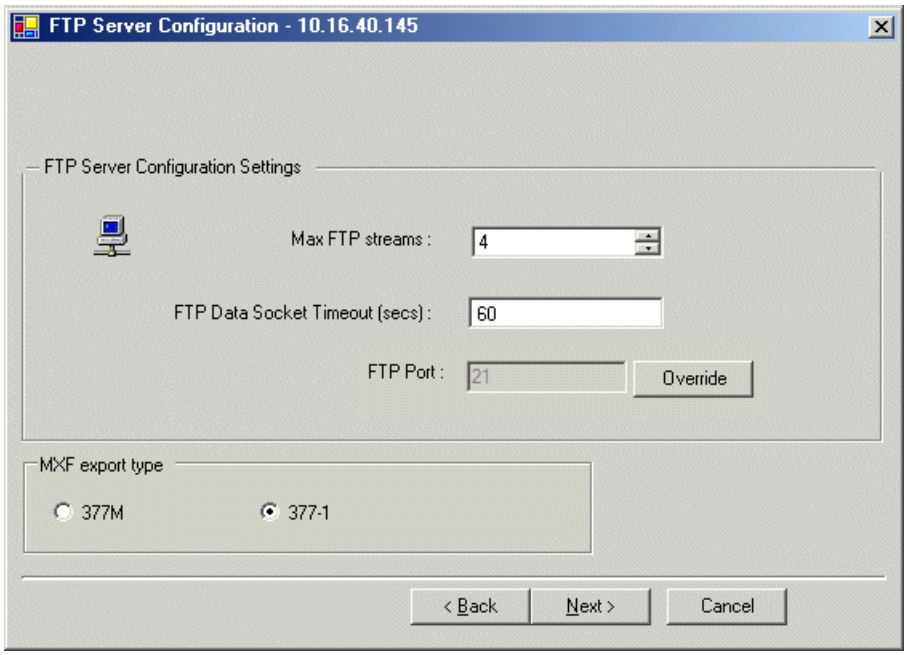
This system does not function as a file system server. It does function as a file system client, which is validated from this page.

1. Do not select **Reserved Bandwidth** unless instructed to do so by Grass Valley. This system is usually not configured for RVIO.
2. Click **Check**.
3. When the wizard reports that the configuration is correct, click **Next**.

   If you get a "The V: will not be available until this device is rebooted…" message, you can safely continue now and reboot later when instructed to do so.

The FTP Server Configuration page opens.

Configure FTP Server Configuration page - Redundant K2 SAN NH server



This page appears only if the server has the role of FTP server.

Do not modify these settings. Leave at default values of Max FTP streams = 4, FTP Data Socket Timeout = 60, and FTP Port = 21. Only qualified Grass Valley personnel should specify other values, as these settings are intended for use only with custom systems designed by Grass Valley.

1. Select MXF export type as follows:

   - **377M**: Original SMPTE 377M style. Ensures compatibility with older products.
   - **377-1**: Newer SMPTE 377-1 style.

   Refer to related topics in the "Configuring the K2 System" section of this Topic Library for more information.

2. Click **Next**.

   The Completing the Configuration Wizard page opens.

3. Click **Finish**.

   The wizard closes. The server restarts.

Wait until all startup processes have completed before continuing.

If you have other NH servers, configure them similarly. Then check the V: drive on each of your NH servers.

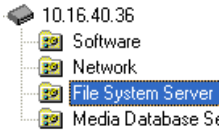
Check the V: drive

- The K2 Media Server must be configured

- The restart of the K2 Media Server after it is configured must be complete

This task is required for NAS server functionality.

1. Verify that the K2 Media Server has restarted by opening the MS-DOS command prompt and use the “ping” command.
2. In the K2Config application tree view, under the K2 Media Server select the File System Server node.



   The File System Server Configuration page appears.

3. Click **Check** and verify that the V: drive is shared.

Next, configure K2 clients and/or other iSCSI clients on the K2 SAN.

Configuring the basic nearline K2 SAN

Work through the topics in this section sequentially to configure a non-redundant nearline (Tier 3) K2 SAN.

Prerequisites for initial configuration - Basic nearline K2 SAN

Before beginning your initial configuration, make sure the devices of the K2 SAN meet the following prerequisites.

Control point PC

- Ethernet cable connected
- Control Point software must be installed
- Control network IP address must be assigned
- There must be network communication over the control network with all other K2 devices
- Power must be on

Ethernet switch

- Ethernet cables connected
- Control network IP address must be assigned
- VLANs must be set up
- Trunks must be set up
- Power must be on

K2 Media Server

- Ethernet cables connected
- Fibre Channel cable must be connected
- Softwaremust be installed, as from the factory, including QuickTime 7
- Control network IP address must be assigned
- Power must be on for all servers

K2 RAID chassis

- Fibre Channel cable(s) must be connected
- Ethernet cable(s) must be connected
- Power must be on

K2 RAID Expansion chassis (optional)

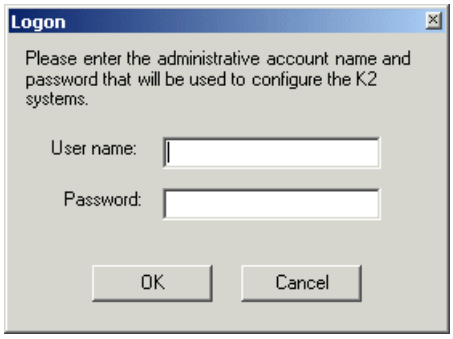
- Fibre channel cable(s) must be connected
- Power must be on

Defining a new K2 SAN

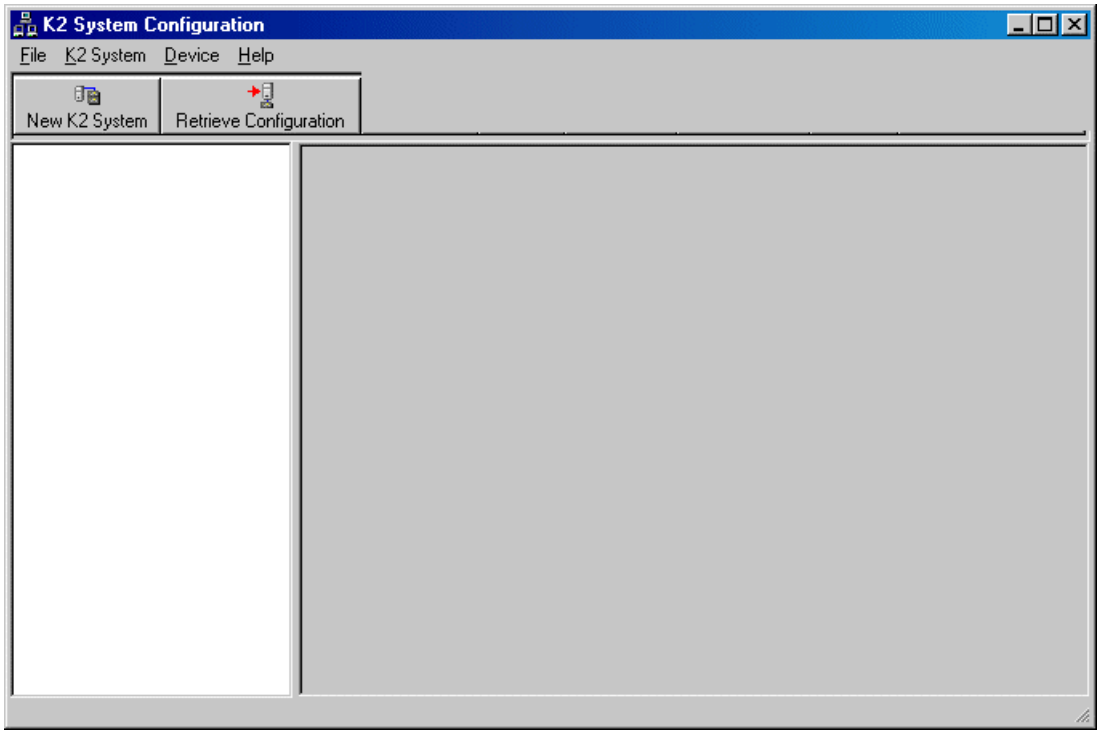
If you import a SiteConfig system description file in which the SAN is defined, you do not need to define a new SAN. You can skip this task and instead start by configuring the first K2 Media Server.

1. On the control point PC, open the K2Config application.

   A log on dialog box opens.



2. Log on to the K2Config application with the Windows administrator account.
   The K2Config application opens.



3. Click **New K2 System**.

The New K2 System wizard opens to page 1.

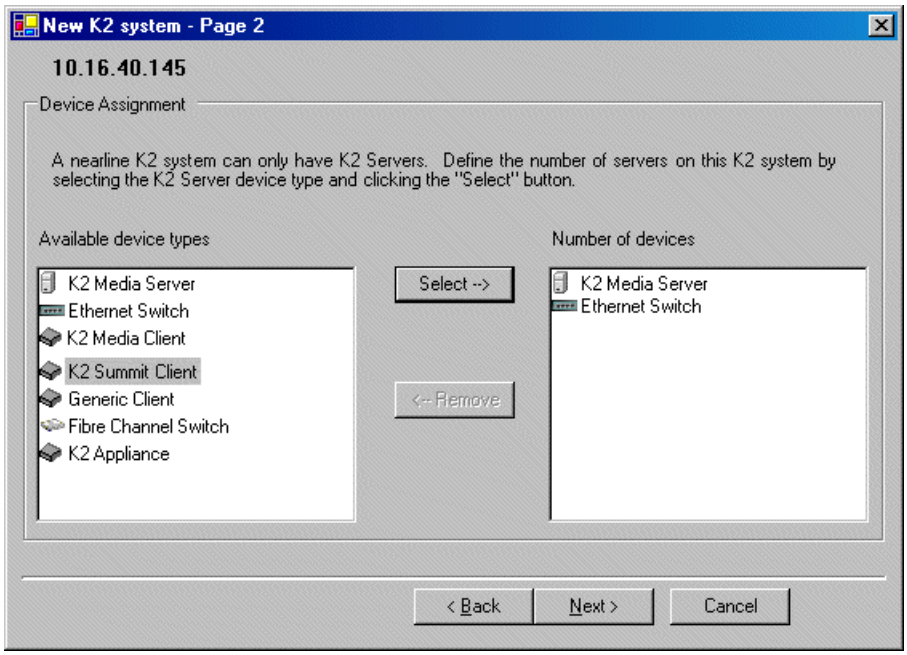
Configure New K2 System page 1 - Nearline K2 SAN

1. Create a name for your system and type it in the Name box.
2. Select **Nearline**.

   The Server redundancy option is not selected and is disabled. This option applies to media database redundancy. Since the Nearline system has no media database, this setting is correct for both redundant and non-redundant Nearline systems.
3. Click **Next**.

Page 2 opens.

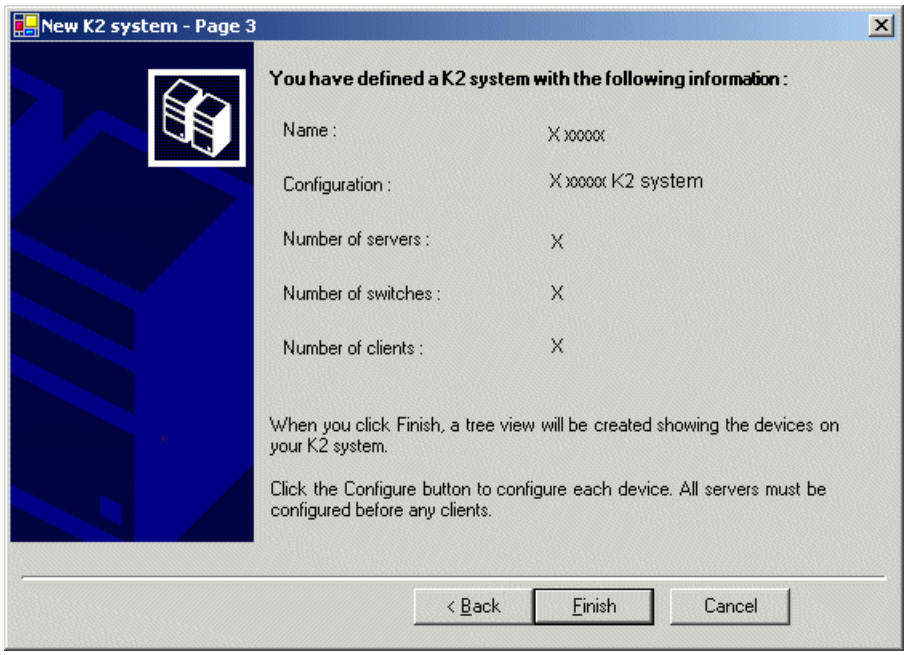
Configure New K2 System page 2 - Nearline K2 SAN



1. Move the following into the Number of devices box:
   - One K2 Media Server
   - One Ethernet switch
2. Click **Next**.

Page 3 opens.

Configure New K2 System page 3 - Nearline K2 SAN



1. Review the information on this page and verify that you have correctly defined your K2 SAN.
   For a redundant nearline K2 SAN you should have the following:
   - Two Gigabit Ethernet switches
   - Two K2 Media Servers
2. Click **Finish**.
   The Define New K2 Storage System wizard closes.

Your storage system appears in the tree view of the K2Config application.

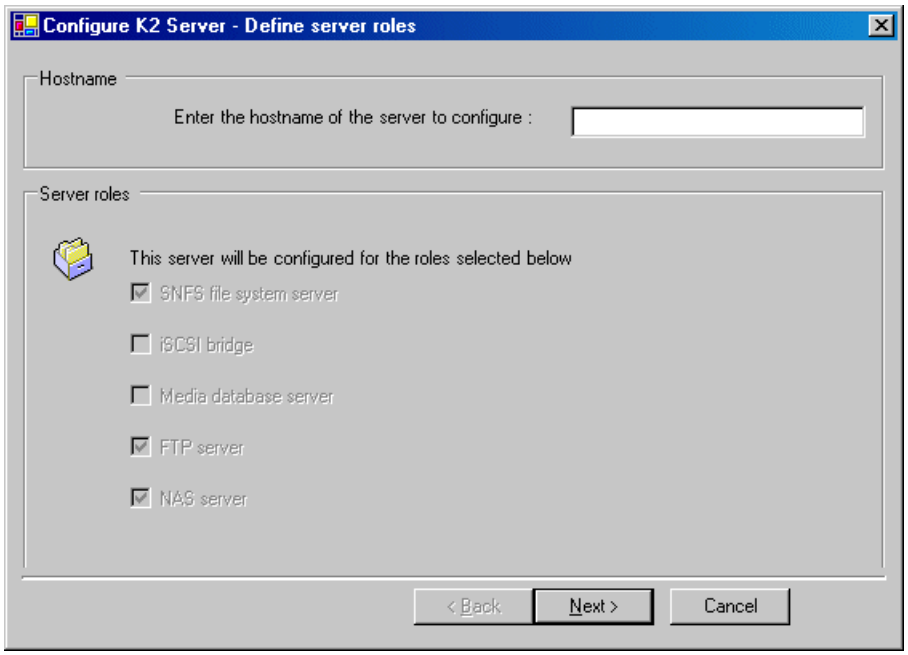
Next, configure the server.

Configuring NH server - Part 1

1. In the K2Config application tree view, select **[K2Server1]**.
   For the basic nearline K2 SAN, this is the only NH server.
2. Click the **Configure** button.

The Configure K2 Server wizard opens to the Define server roles page.

Configure Define Server Roles page - NH server



1. Enter the name for the K2 Media Server, as currently configured on the machine.

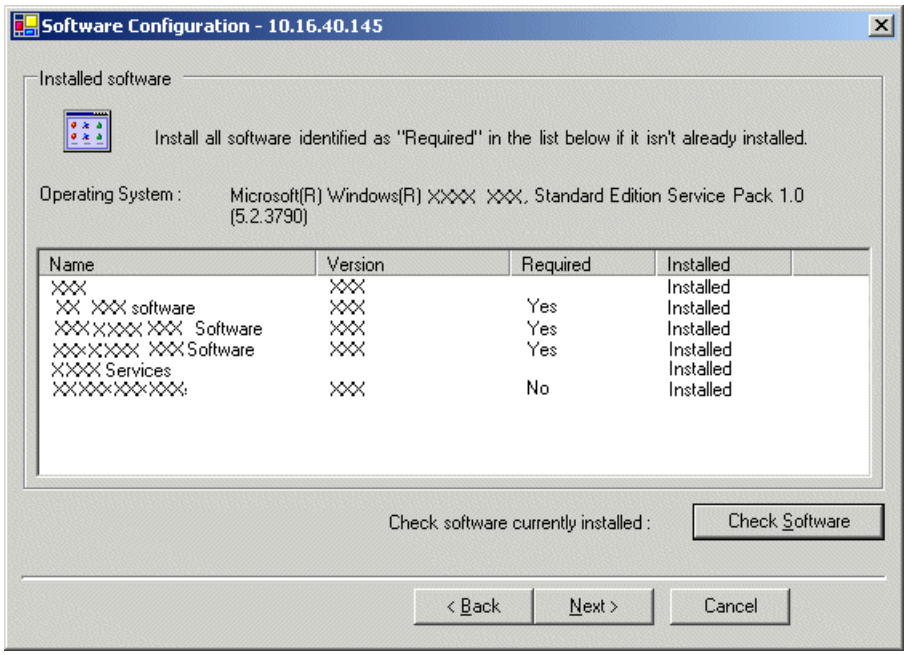
   For Nearline server roles, selections are disabled. Leave SNFS file system server, FTP server, and NAS server selected.

   The wizard does not allow you to select Media Database Server. There is no Media Database Server in a nearline system.

2. Click **Next**.

The Software Configuration page opens.

Configure Software Configuration page - NH server

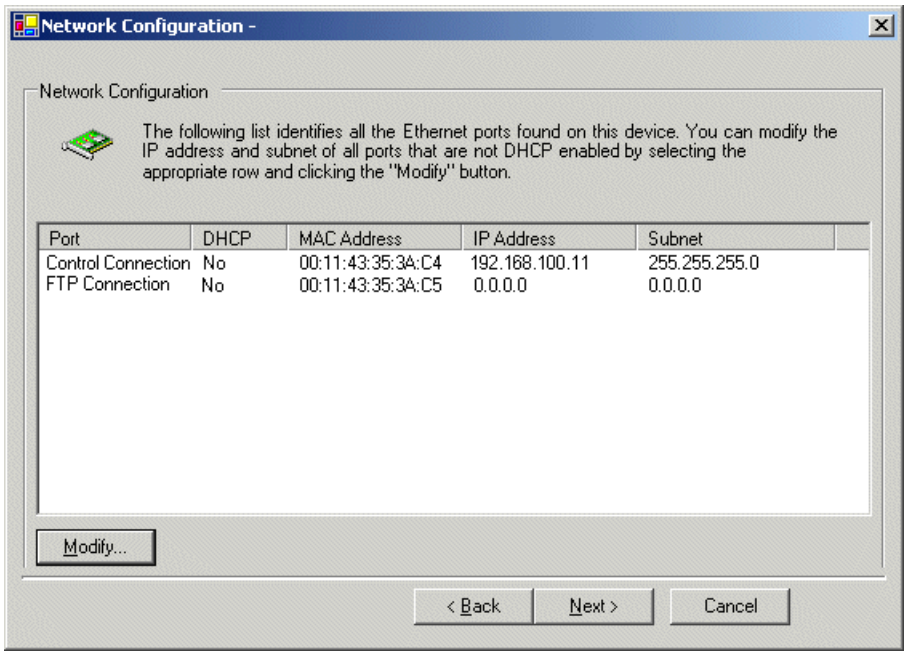


This page checks for the software required to support the roles you selected on the previous page.

1. If software with **Yes** in the Required column reports as **Not Installed**, install the software.
2. Click **Check Software**.
3. When all required software reports as **Installed**, click **Next**.

The Network Configuration page opens.

Configure Network Configuration page - NH server



This page displays the control network Ethernet port, and allows you to configure the FTP/Streaming network Ethernet port.

1. Verify that the top port is configured correctly.

   The top port is the port over which the K2Config application is communicating. If correctly configured, it is already assigned the control network IP address, as displayed on this page.

2. Verify that the FTP/Streaming port is configured correctly. If not configured correctly, do the following:

   a) Select the other port and click **Modify**.

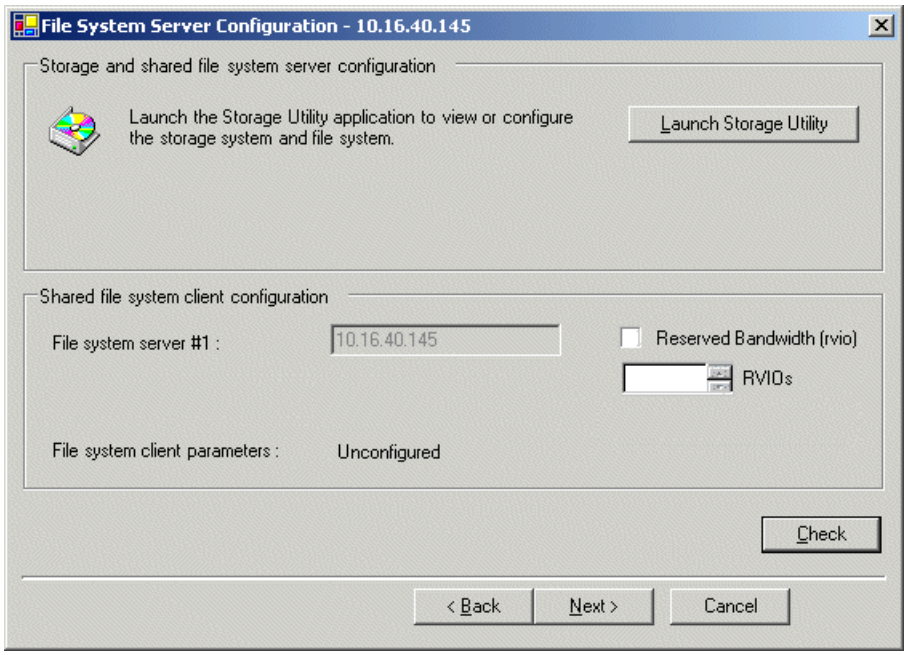
      A network configuration dialog box opens.

   b) Enter the FTP/Streaming IP address and the subnet mask and click **Apply**.

3. Click **Next**.

The File System Server Configuration page opens.

Configure File System Server Configuration page - NH server



This page checks on the file system server role. The server also functions as a file system client, which is also checked from this page.

1. Do not select **Reserved Bandwidth** unless instructed to do so by Grass Valley. This system is usually not configured for RVIO.
2. Click **Launch Storage Manager**.

   Storage Utility opens.
3. Leave the Configure K2 Server wizard open while you use Storage Utility.

   When you are done with Storage Utility, you continue with the wizard.

Next, use Storage Utility to configure the RAID storage and file system.

Configuring RAID

Use Storage Utility to complete the configuration of the K2 RAID storage devices, as explained in the following topics.

Configuring RAID network and SNMP settings - Basic

- Fibre Channel cable(s) must be connected
- Ethernet cable(s) must be connected
- Power must be on
- Fibre channel cable(s) must be connected
- Power must be on

Use the Storage Utility to configure the following settings for the K2 RAID controller:

- IP address

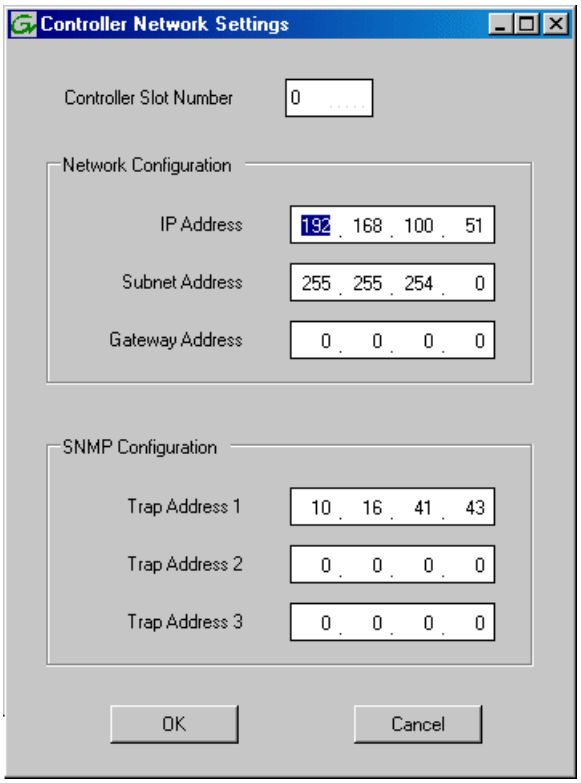
- Subnet mask
- Gateway Address
- SNMP trap destinations

For K2 RAID, network and SNMP settings are set and stored on the RAID controller module, so the combined RAID storage devices, including the optional Expansion chassis, exist as a single entity on the control network.

The RAID storage device is configured by default for the SNMP community name “public”. If your site’s policies require using a different SNMP community name, contact your Grass Valley representative.

1. Launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.
3. In Storage Utility tree view, expand the node for the K2 RAID, right-click the icon for a RAID controller, and select **Configuration I Network Properties**.

   The Controller Network Settings dialog box opens.



4. In the Controller Slot Number field enter **0** and then press **Enter**.

   The settings from controller 0 are loaded into the Controller Network Settings dialog box and are available for you to modify.
5. Enter the control network IP address and other network settings.

6. For SNMP Configuration, enter the IP address of the SNMP manager PC.

   You can also enter IP addresses for other SNMP managers to which you want to send SNMP trap messages.

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

7. Click **OK** to save settings and close.
8. In Storage Utility click **View | Refresh**.

Next, bind disk modules.

Binding disk modules - Nearline K2 SAN

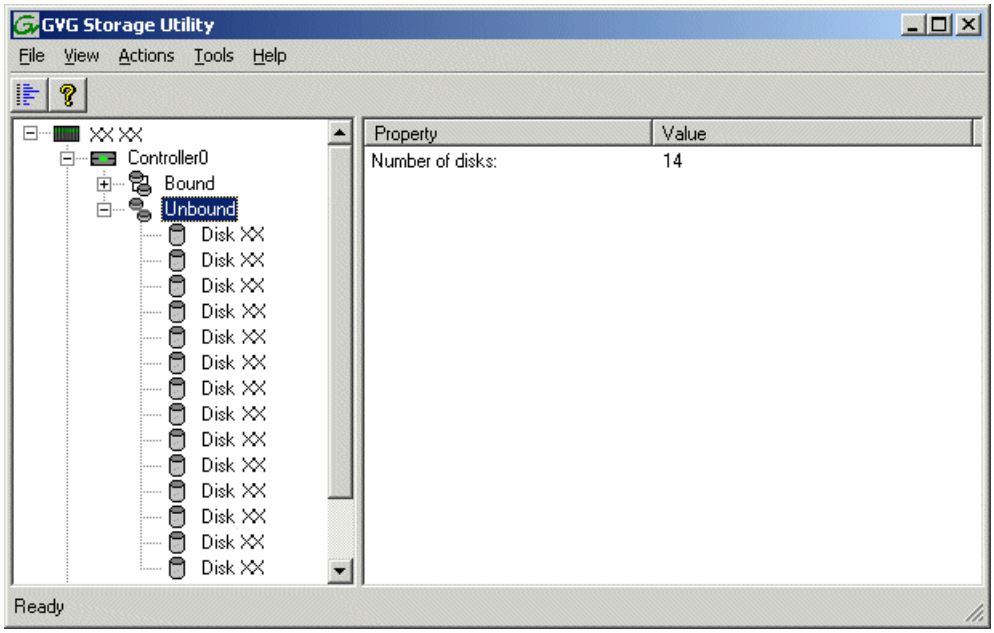
- Fibre Channel cable(s) must be connected
- Ethernet cable(s) must be connected
- Power must be on

- Fibre channel cable(s) must be connected
- Power must be on

NOTE: Binding destroys all user data on the disks.

1. If you have not already done so, launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.

3. In the Storage Utility main window, identify bound RANKs and unbound disks by their placement in the hierarchy of the tree view. In the following illustration, disk numbers are represented by "XX".



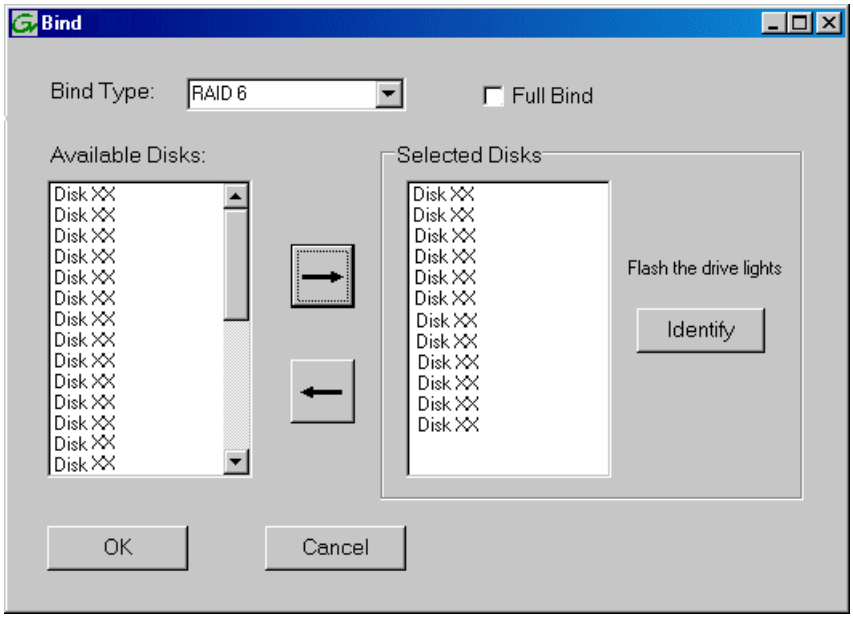
Nearline systems store media files across both the primary RAID chassis and the optional Expansion chassis. In addition, file system metadata files and journal files are mixed in with the media files.

The RAID configuration is the same on all chassis. Each chassis contains disks, which are bound as RAID 6 in a RANK of twelve disks. One twelve disk RANK fills one chassis.

4. Right-click the **Unbound** node for a controller, then select **Bind** in the context menu.

   If the RAID chassis has two controllers, both controllers are represented by the single “Controller” node.

   The Bind dialog box opens showing all unbound disks for the controller listed in the Available Disk list.



5. Leave **Full Bind** unchecked.
6. In the **Bind Type** drop down box, select **RAID 6**.
7. In the Available Disks box, select twelve contiguous disks at the top of the list.

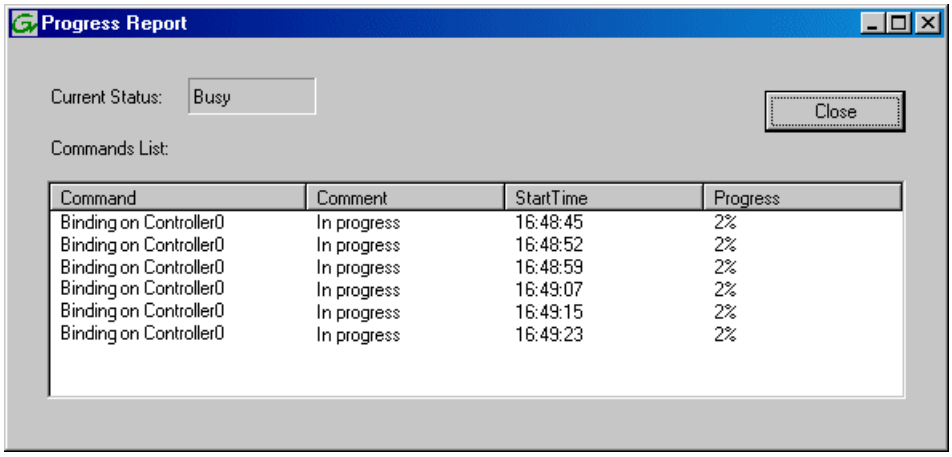
   Use ‘shift-click’ or ‘control-click’ to select disks.

8. Click the add (arrow) button to add disks to the Selected Disks list.

   NOTE: As an aid in identifying a disk module’s physical location, select it in the Selected Disks list, then click Identify Disks. This causes the disk drive light to flash.

9. Click **OK** to close the Bind dialog box and begin the binding process.

   The Progress Report dialog box opens, showing the status of the binding process.



10. Close the Progress Report and repeat these steps for other unbound disks.

    If specified by your system design, you can bind some disks as Hot Spares.

    When you are done, if you did not bind any extra Hot Spares, you should have the following results:

    The disks in the primary RAID chassis and in optional Expansion chassis should be bound as RAID 6 RANKs, with twelve disks to a RANK.

11. Click **Close** in Progress Report window.
12. Restart the K2 Media Server.

    NOTE: Make sure start up processes on the K2 Media Server are complete before proceeding.

Next, create a new file system.

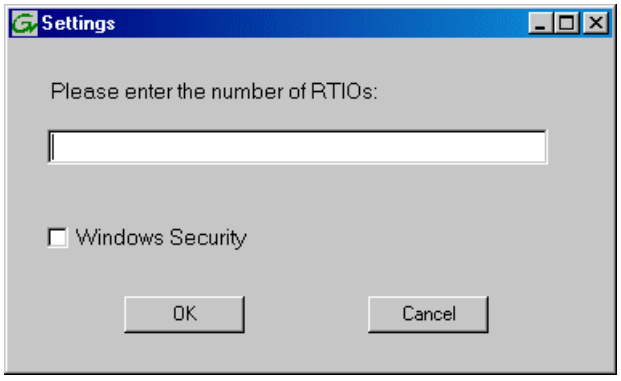
Creating a new file system - Nearline K2 SAN

- Fibre Channel cable(s) must be connected
- Ethernet cable(s) must be connected
- Power must be on
- Disks must be bound

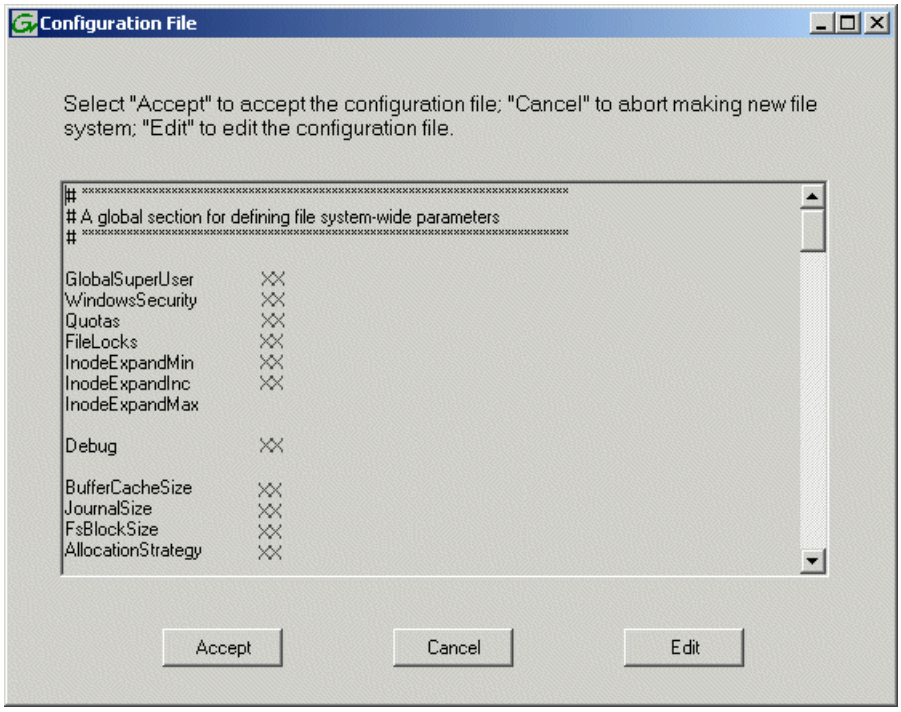
- Fibre channel cable(s) must be connected
- Power must be on
- Disks must be bound

1. If you have not already done so, launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.

3. In Storage Utility, click **Tools | Make New File System**.
   The Setting dialog box opens.



4. For a Nearline system, enter zero as the Real Time Input/Output (RTIO) rate.
5. Leave Windows Security unchecked.
6. Click **OK**.
   The Configuration File dialog box opens.



   The configuration file for the media file system is displayed.

7. Verify media file system parameters.
   Do not edit the configuration file for the media file system.

8. Click **Accept**.

   A "…Please wait…" message box displays progress and a "…succeeded…" message confirms the process is complete.

   A message informs you that you must restart the server, however the restart at the end of the Configure K2 Server wizard suffices, so you do not need to restart now.

9. Close the Storage Utility.

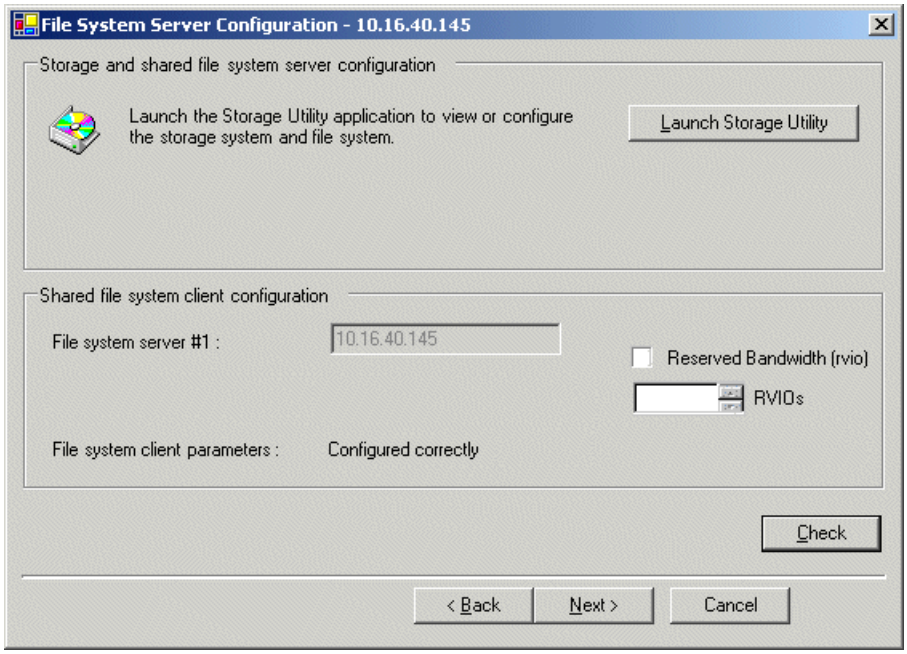
   NOTE: Do not attempt to start SAN-attached systems or otherwise bring the SAN online until instructed to do so by the documented procedure.

Next, continue with configuring the server using the K2Config application.

Configuring NH server - Part 2

Configure File System Server Configuration page - NH server

- Network and SNMP must be settings configured
- Disks must be bound
- A new file system must be made



This page checks on the file system server role. The server also functions as a file system client, which is also checked from this page.

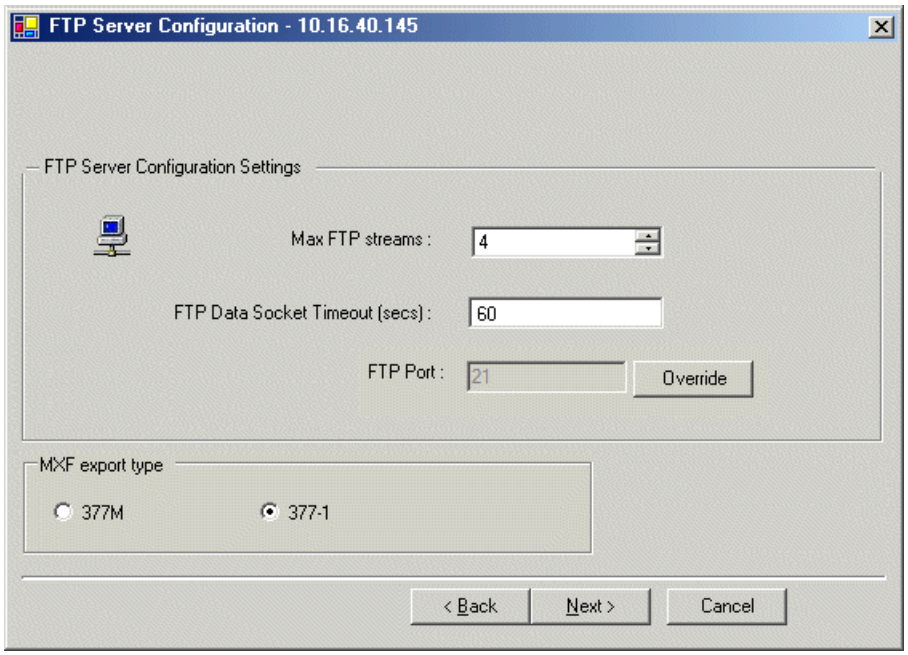
1. In K2Config open the server's File System Server Configuration page, if the page is not already open.
2. Do not select **Reserved Bandwidth** unless instructed to do so by Grass Valley. This system is usually not configured for RVIO.
3. Click **Check**.

4. When the wizard reports that the configuration is correct, click **Next**.

   If you get a "The V: will not be available until this device is rebooted…" message, you can safely continue now and reboot later when instructed to do so.

The FTP Server Configuration page opens.

Configure FTP Server Configuration page



This page appears only if the server has the role of FTP server.

Do not modify these settings. Leave at default values of Max FTP streams = 4, FTP Data Socket Timeout = 60, and FTP Port = 21. Only qualified Grass Valley personnel should specify other values, as these settings are intended for use only with custom systems designed by Grass Valley.

1. Select MXF export type as follows:

   - **377M**: Original SMPTE 377M style. Ensures compatibility with older products.
   - **377-1**: Newer SMPTE 377-1 style.

   Refer to related topics in the "Configuring the K2 System" section of this Topic Library for more information.

2. Click **Next**.

   The Completing the Configuration Wizard page opens.

3. Click **Finish**.

   The wizard closes. The server restarts.

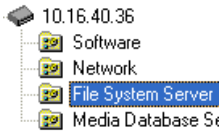
Wait until all startup processes have completed before continuing.

Check the V: drive

- The K2 Media Server must be configured
- The restart of the K2 Media Server after it is configured must be complete

This task is required for NAS server functionality.

1. Verify that the K2 Media Server has restarted by opening the MS-DOS command prompt and use the "ping" command.
2. In the K2Config application tree view, under the K2 Media Server select the File System Server node.



   The File System Server Configuration page appears.

3. Click **Check** and verify that the V: drive is shared.

The K2 Nearline SAN configuration is complete.

Configuring the redundant nearline K2 SAN

Work through the topics in this section sequentially to configure a redundant nearline (Tier 3) K2 SAN.

Prerequisites for initial configuration - Nearline K2 SAN

Before beginning your initial configuration, make sure the devices of the K2 SAN meet the following prerequisites.

Control point PC

- Ethernet cable connected
- Control Point software must be installed
- Control network IP address must be assigned
- There must be network communication over the control network with all other K2 devices
- Power must be on

Ethernet switch

- Ethernet cables connected
- Control network IP address must be assigned
- VLANs must be set up
- Trunks must be set up
- Power must be on

K2 Media Server

- Ethernet cables must be connected
- Fibre Channel cable must be connected

- Redundant servers must be connected by serial cable
- Software must be installed, as from the factory, including QuickTime 7
- MPIO software must be installed.
- Control network IP address must be assigned
- Power must be on for all servers

K2 RAID chassis

- Fibre Channel cable(s) must be connected
- Ethernet cable(s) must be connected
- Power must be on

K2 RAID Expansion chassis (optional)

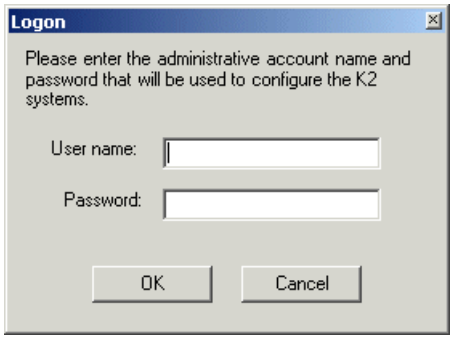
- Fibre channel cable(s) must be connected
- Power must be on

Defining a new K2 SAN

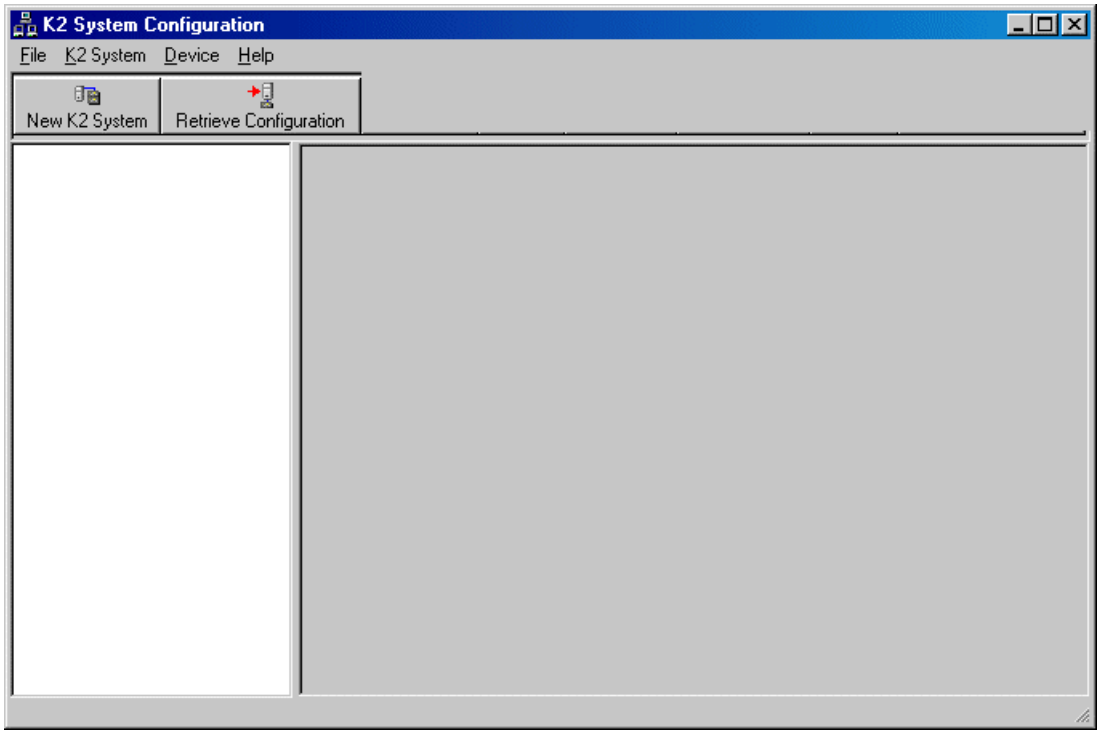
If you import a SiteConfig system description file in which the SAN is defined, you do not need to define a new SAN. You can skip this task and instead start by configuring the first K2 Media Server.

1. On the control point PC, open the K2Config application.

   A log on dialog box opens.



2. Log on to the K2Config application with the Windows administrator account.
   The K2Config application opens.



3. Click **New K2 System**.

The New K2 System wizard opens to page 1.

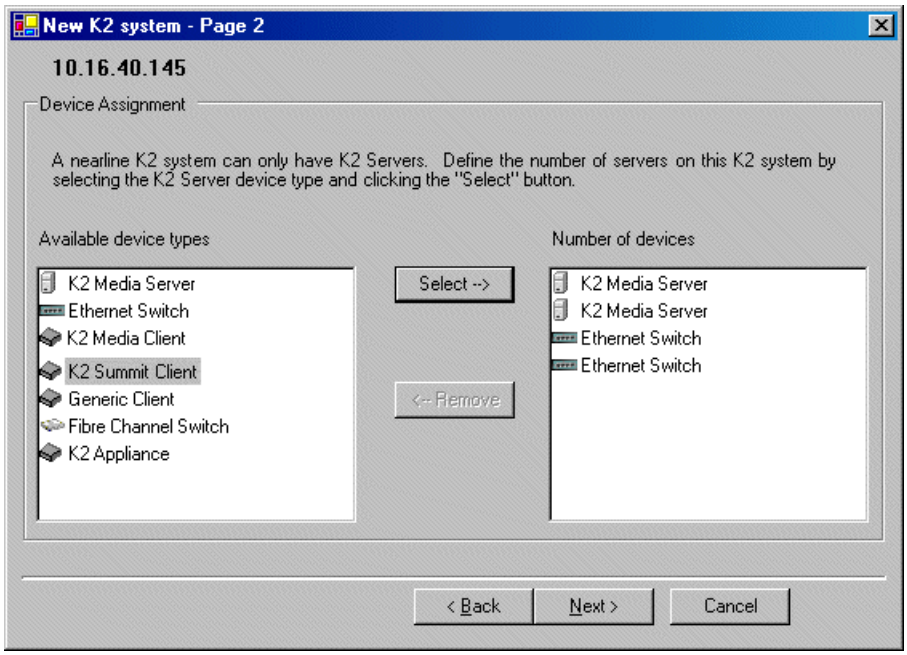
Configure New K2 System page 1 - Nearline K2 SAN

1. Create a name for your system and type it in the Name box.
2. Select **Nearline**.

   The Server redundancy option is not selected and is disabled. This option applies to media database redundancy. Since the Nearline system has no media database, this setting is correct for both redundant and non-redundant Nearline systems.
3. Click **Next**.

Page 2 opens.

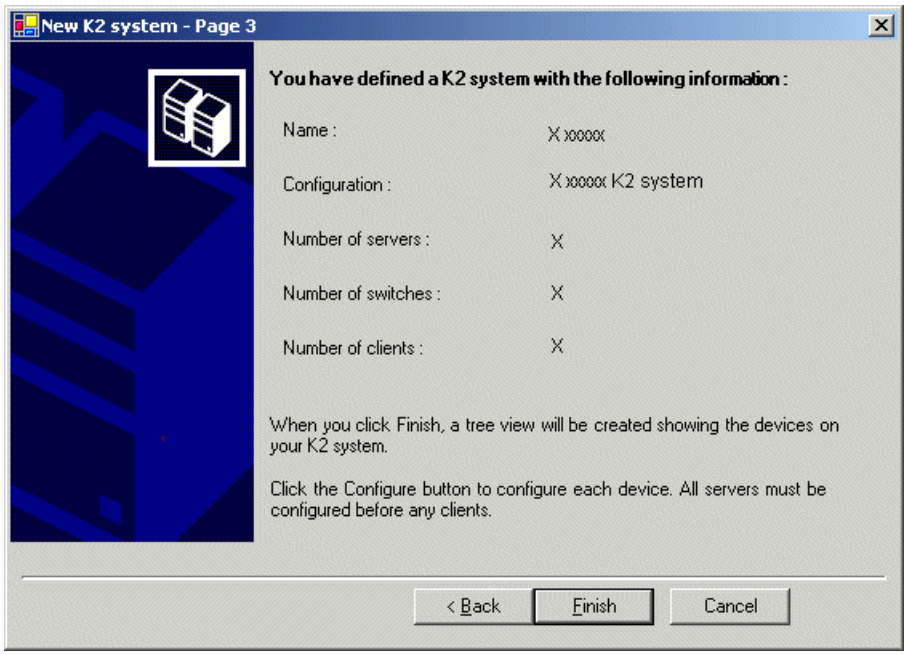
Configure New K2 System page 2 - Nearline K2 SAN



1. Move the following into the Number of devices box:
   - Two K2 Media Servers
   - Two Ethernet switches
2. Click **Next**.

Page 3 opens.

Configure New K2 System page 3 - Nearline K2 SAN



1. Review the information on this page and verify that you have correctly defined your K2 SAN.
   For a redundant nearline K2 SAN you should have the following:
   - Two Gigabit Ethernet switches
   - Two K2 Media Servers
2. Click **Finish**.
   The Define New K2 Storage System wizard closes.

Your storage system appears in the tree view of the K2Config application.

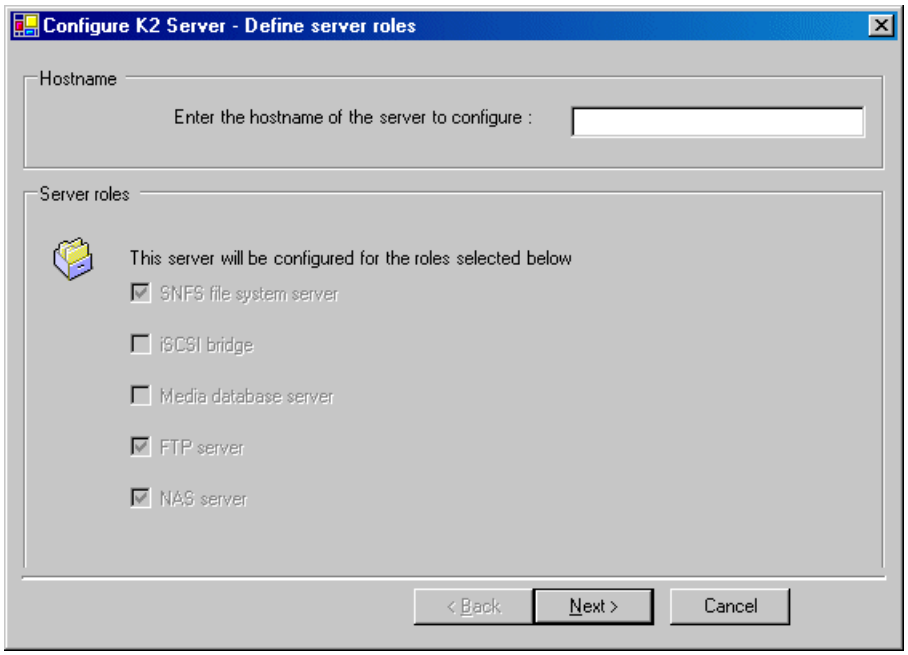
Next, configure the server.

Configuring NH server A - Part 1

1. In the K2Config application tree view, select **[K2Server1]**.
   For the nearline K2 SAN, this is NH server A.
2. Click the **Configure** button.

The Configure K2 Server wizard opens to the Define server roles page.

Configure Define Server Roles page - NH server



1. Enter the name for the K2 Media Server, as currently configured on the machine.

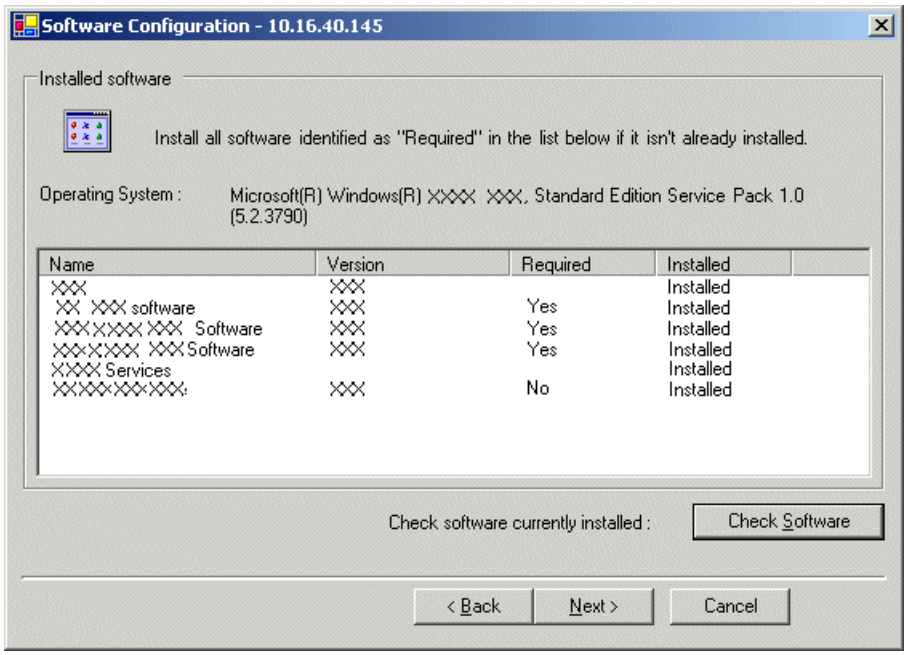
   For Nearline server roles, selections are disabled. Leave SNFS file system server, FTP server, and NAS server selected.

   The wizard does not allow you to select Media Database Server. There is no Media Database Server in a nearline system.

2. Click **Next**.

The Software Configuration page opens.

Configure Software Configuration page - NH server

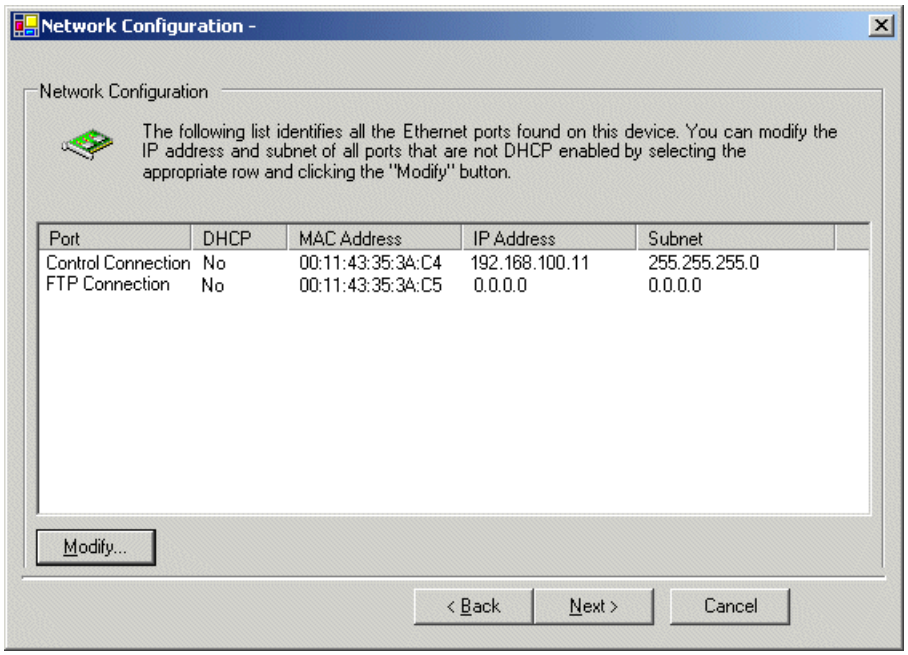


This page checks for the software required to support the roles you selected on the previous page.
NOTE: MPIO software is required on servers in redundant systems.

1. If software with **Yes** in the Required column reports as **Not Installed**, install the software.
2. Click **Check Software**.
3. When all required software reports as **Installed**, click **Next**.

The Network Configuration page opens.

Configure Network Configuration page - NH server



This page displays the control network Ethernet port, and allows you to configure the FTP/Streaming network Ethernet port.

1. Verify that the top port is configured correctly.

   The top port is the port over which the K2Config application is communicating. If correctly configured, it is already assigned the control network IP address, as displayed on this page.

2. Verify that the FTP/Streaming port is configured correctly. If not configured correctly, do the following:

   a) Select the other port and click **Modify**.

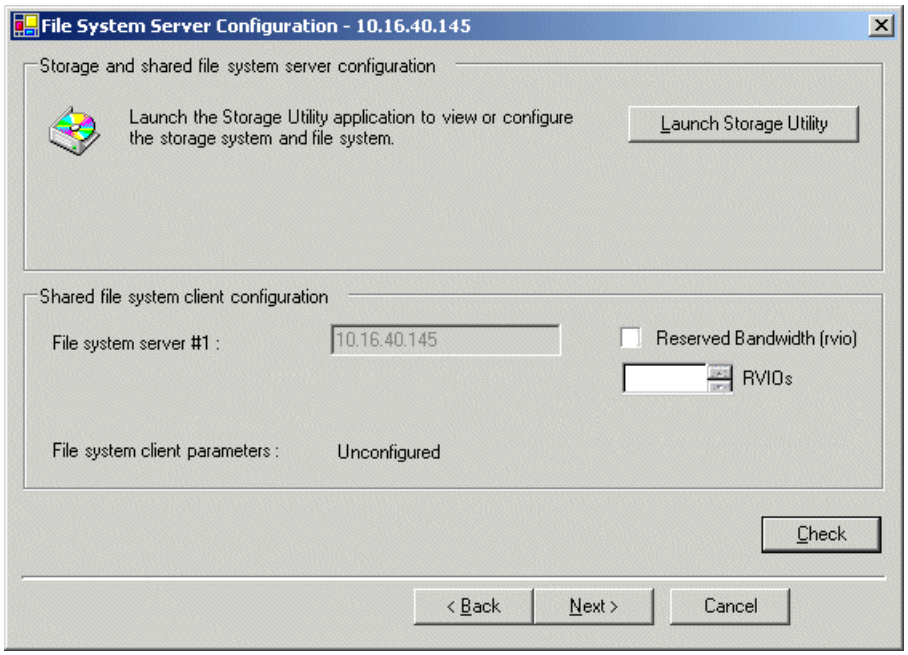
      A network configuration dialog box opens.

   b) Enter the FTP/Streaming IP address and the subnet mask and click **Apply**.

3. Click **Next**.

The File System Server Configuration page opens.

Configure File System Server Configuration page - NH server



This page checks on the file system server role. The server also functions as a file system client, which is also checked from this page.

1. Do not select **Reserved Bandwidth** unless instructed to do so by Grass Valley. This system is usually not configured for RVIO.
2. Click **Launch Storage Manager**.

   Storage Utility opens.
3. Leave the Configure K2 Server wizard open while you use Storage Utility.

   When you are done with Storage Utility, you continue with the wizard.

Next, use Storage Utility to configure the RAID storage and file system.

Configuring RAID

Use Storage Utility to complete the configuration of the K2 RAID storage devices, as explained in the following topics.

Configuring RAID network and SNMP settings

- Fibre Channel cable(s) must be connected
- Ethernet cable(s) must be connected
- Power must be on
- Fibre channel cable(s) must be connected
- Power must be on

Use the Storage Utility to configure the following settings for the K2 RAID controller:

- IP address

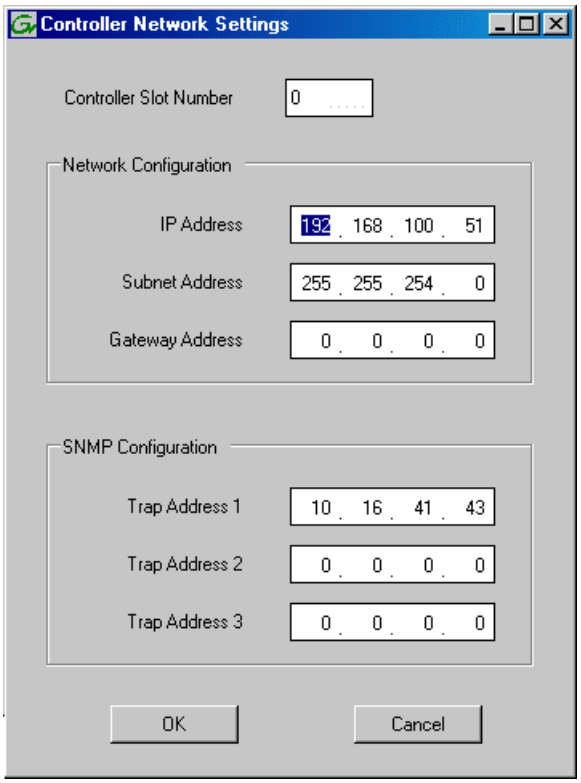
- Subnet mask
- Gateway Address
- SNMP trap destinations

For K2 RAID, network and SNMP settings are set and stored on the RAID controller module. For the RAID chassis with two controllers, each controller has its own network settings and the RAID chassis exists as two entities on the control network.

The RAID storage device is configured by default for the SNMP community name “public”. If your site’s policies require using a different SNMP community name, contact your Grass Valley representative.

1. Launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.
3. In Storage Utility tree view, expand the node for the K2 RAID, right-click the icon for a RAID controller, and select **Configuration I Network Properties**.

   The Controller Network Settings dialog box opens.



4. In the Controller Slot Number field enter **0** and then press **Enter**.

   The settings from controller 0 are loaded into the Controller Network Settings dialog box and are available for you to modify.
5. Enter the control network IP address and other network settings.

6. For SNMP Configuration, enter the IP address of the SNMP manager PC.

   You can also enter IP addresses for other SNMP managers to which you want to send SNMP trap messages.

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

7. For the RAID chassis with two controllers, in the Controller Slot Number field enter **1** and then press **Enter**.

   The settings from controller 1 are loaded into the Controller Network Settings dialog box and are available for you to modify.

8. Repeat the previous steps to configure controller 1.
9. Click **OK** to save settings and close.
10. In Storage Utility click **View | Refresh**.

Next, bind disk modules.

Binding disk modules - Nearline K2 SAN

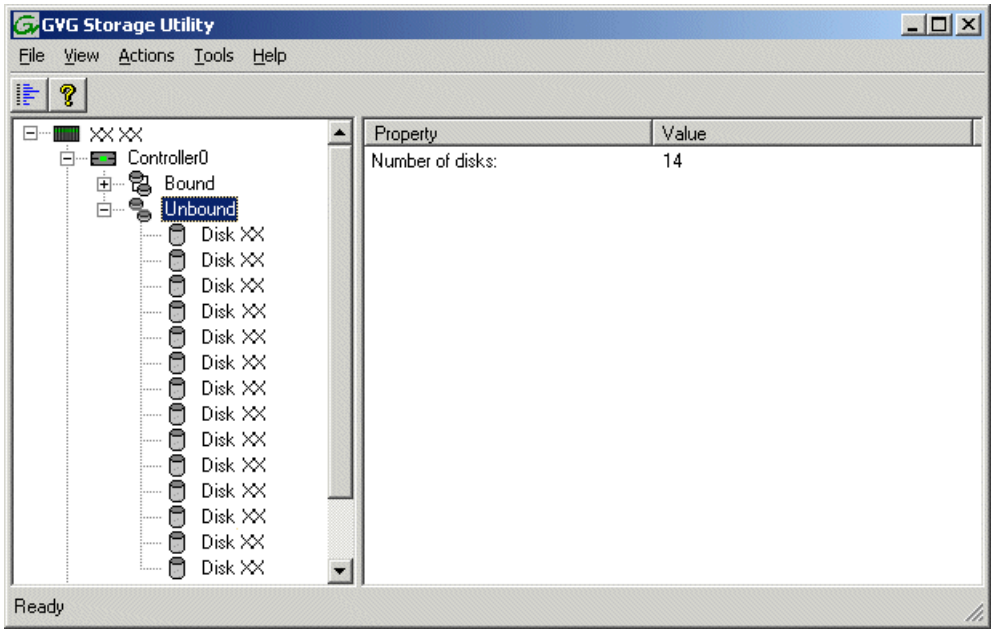
- Fibre Channel cable(s) must be connected
- Ethernet cable(s) must be connected
- Power must be on

- Fibre channel cable(s) must be connected
- Power must be on

NOTE: Binding destroys all user data on the disks.

1. If you have not already done so, launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.

3. In the Storage Utility main window, identify bound RANKs and unbound disks by their placement in the hierarchy of the tree view. In the following illustration, disk numbers are represented by "XX".



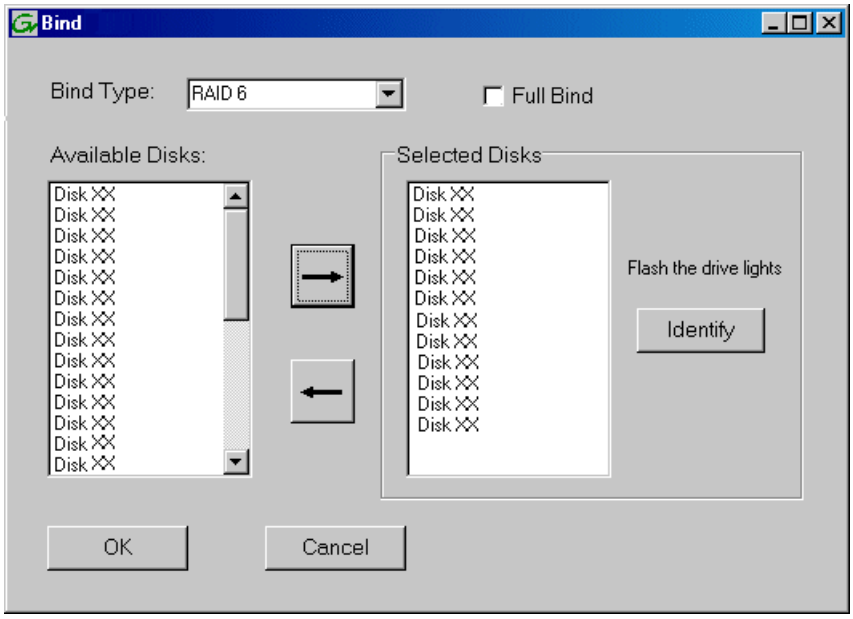
Nearline systems store media files across both the primary RAID chassis and the optional Expansion chassis. In addition, file system metadata files and journal files are mixed in with the media files.

The RAID configuration is the same on all chassis. Each chassis contains disks, which are bound as RAID 6 in a RANK of twelve disks. One twelve disk RANK fills one chassis.

4. Right-click the **Unbound** node for a controller, then select **Bind** in the context menu.

   If the RAID chassis has two controllers, both controllers are represented by the single “Controller” node.

   The Bind dialog box opens showing all unbound disks for the controller listed in the Available Disk list.



5. Leave **Full Bind** unchecked.
6. In the **Bind Type** drop down box, select **RAID 6**.
7. In the Available Disks box, select twelve contiguous disks at the top of the list.

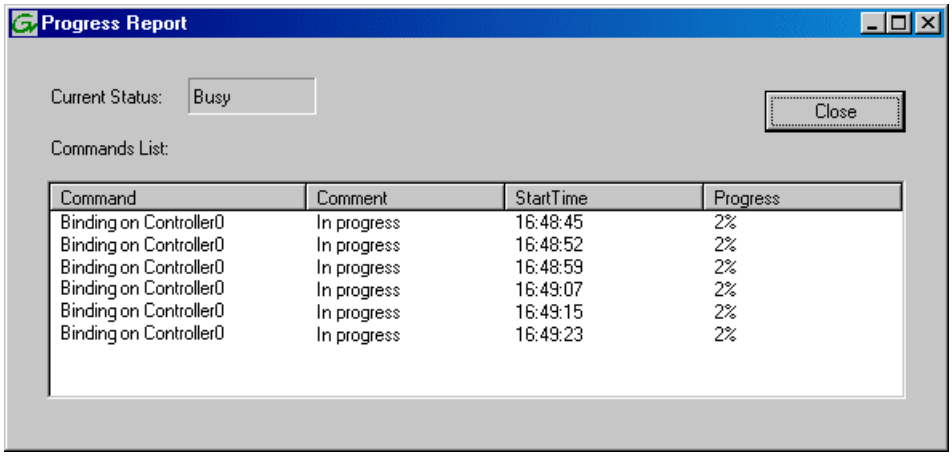
   Use ‘shift-click’ or ‘control-click’ to select disks.

8. Click the add (arrow) button to add disks to the Selected Disks list.

   NOTE: As an aid in identifying a disk module’s physical location, select it in the Selected Disks list, then click Identify Disks. This causes the disk drive light to flash.

9. Click **OK** to close the Bind dialog box and begin the binding process.

   The Progress Report dialog box opens, showing the status of the binding process.



10. Close the Progress Report and repeat these steps for other unbound disks.

    If specified by your system design, you can bind some disks as Hot Spares.

    When you are done, if you did not bind any extra Hot Spares, you should have the following results:

    The disks in the primary RAID chassis and in optional Expansion chassis should be bound as RAID 6 RANKs, with twelve disks to a RANK.

11. Click **Close** in Progress Report window.
12. Restart the K2 Media Server.

    NOTE: Make sure start up processes on the K2 Media Server are complete before proceeding.

Next, create a new file system.

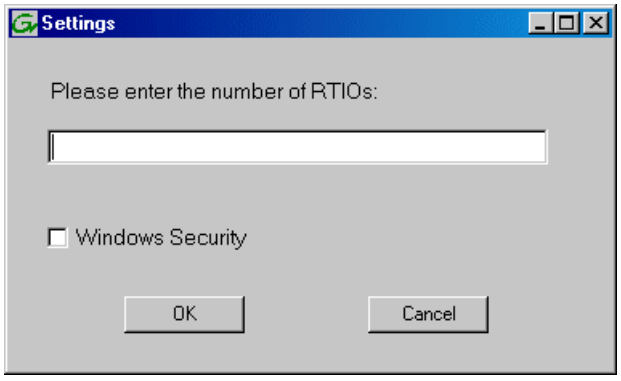
Creating a new file system - Nearline K2 SAN

- Fibre Channel cable(s) must be connected
- Ethernet cable(s) must be connected
- Power must be on
- Disks must be bound

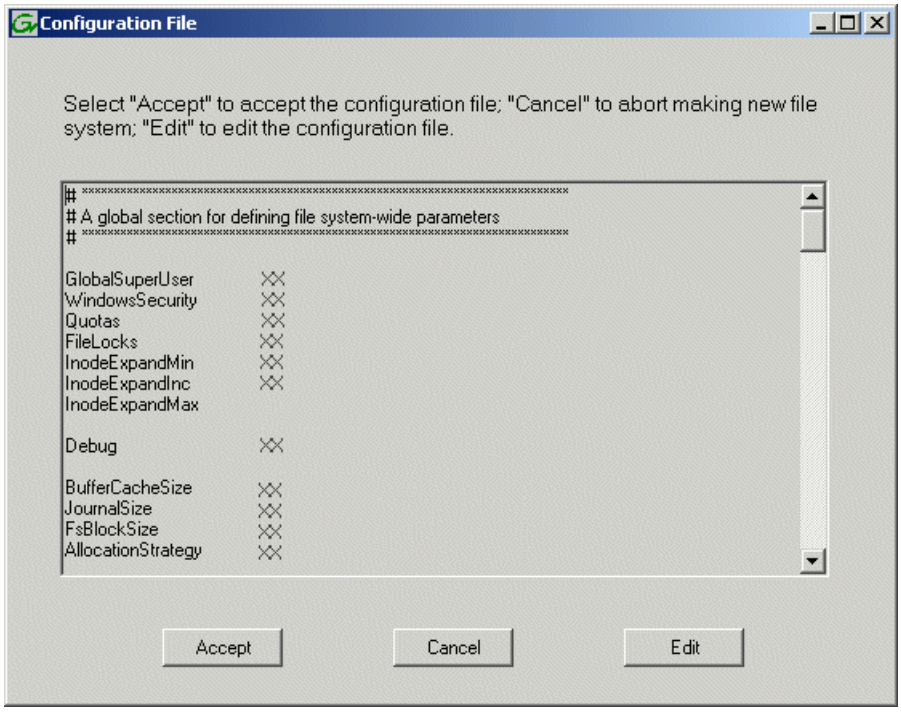
- Fibre channel cable(s) must be connected
- Power must be on
- Disks must be bound

1. If you have not already done so, launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.

3. In Storage Utility, click **Tools | Make New File System**.
   The Setting dialog box opens.



4. For a Nearline system, enter zero as the Real Time Input/Output (RTIO) rate.
5. Leave Windows Security unchecked.
6. Click **OK**.
   The Configuration File dialog box opens.



   The configuration file for the media file system is displayed.

7. Verify media file system parameters.
   Do not edit the configuration file for the media file system.

8. Click **Accept**.

   A "…Please wait…" message box displays progress and a "…succeeded…" message confirms the process is complete.

   A message informs you that you must restart the server, however the restart at the end of the Configure K2 Server wizard suffices, so you do not need to restart now.

9. Close the Storage Utility.

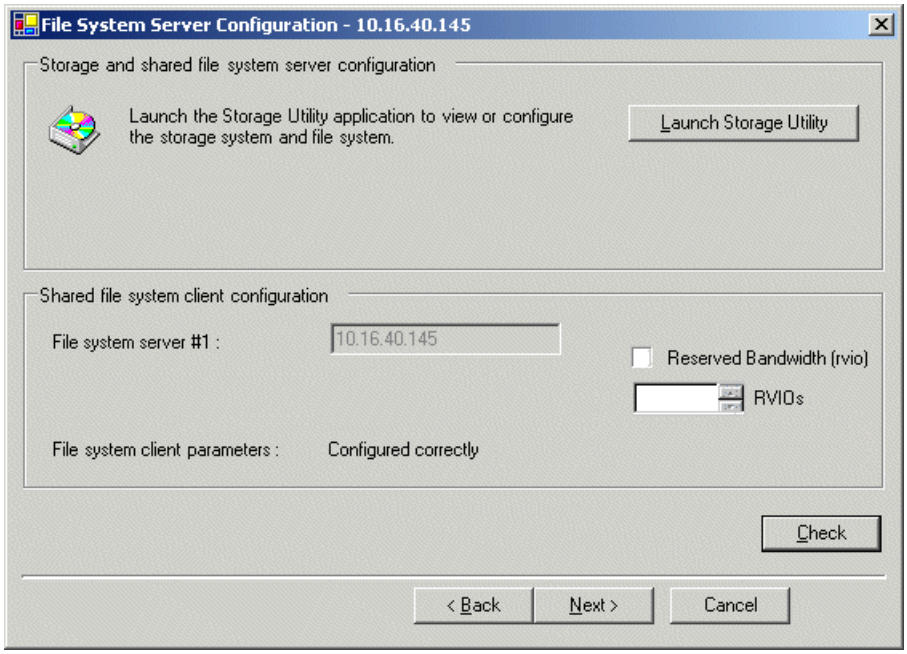
   NOTE: Do not attempt to start SAN-attached systems or otherwise bring the SAN online until instructed to do so by the documented procedure.

Next, continue with configuring the server using the K2Config application.

Configuring NH server A - Part 2

Configure File System Server Configuration page - NH server

- Network and SNMP must be settings configured
- Disks must be bound
- A new file system must be made



This page checks on the file system server role. The server also functions as a file system client, which is also checked from this page.

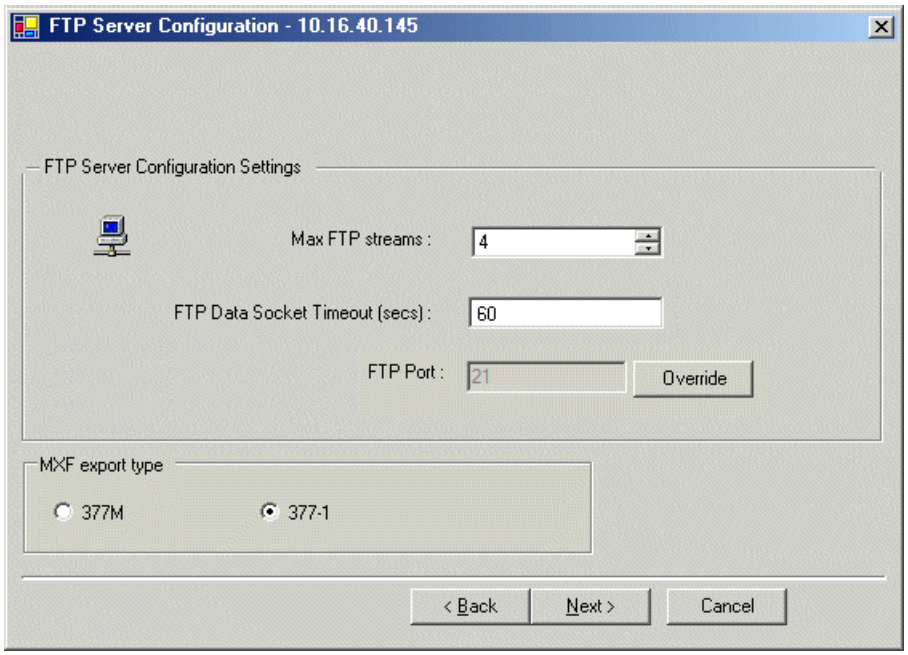
1. In K2Config open the server's File System Server Configuration page, if the page is not already open.
2. Do not select **Reserved Bandwidth** unless instructed to do so by Grass Valley. This system is usually not configured for RVIO.
3. Click **Check**.

4. When the wizard reports that the configuration is correct, click **Next**.

   If you get a "The V: will not be available until this device is rebooted…" message, you can safely continue now and reboot later when instructed to do so.

The FTP Server Configuration page opens.

Configure FTP Server Configuration page - NH server A



This page appears only if the server has the role of FTP server.

Do not modify these settings. Leave at default values of Max FTP streams = 4, FTP Data Socket Timeout = 60, and FTP Port = 21. Only qualified Grass Valley personnel should specify other values, as these settings are intended for use only with custom systems designed by Grass Valley.

1. Select MXF export type as follows:

   - **377M**: Original SMPTE 377M style. Ensures compatibility with older products.
   - **377-1**: Newer SMPTE 377-1 style.

   Refer to related topics in the "Configuring the K2 System" section of this Topic Library for more information.

2. Click **Next**.

   The Completing the Configuration Wizard page opens.

3. Click **Finish**.

   The wizard closes. The server restarts.

Wait until all startup processes have completed before continuing.

Next, configure the other NH server.

Configuring NH server B

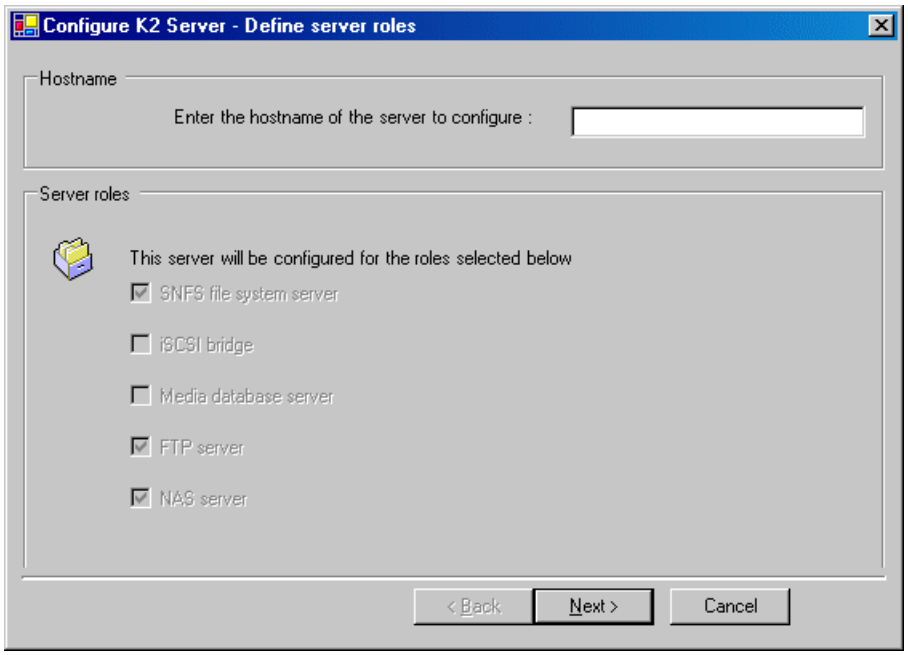
- Server A must be configured
- The restart of server A after it is configured must be complete

On nearline systems, both NH K2 Media Servers are identical, with the exception that only one server can be the active media file system server at any time. For this reason the K2Config application embeds the configuration and start of the media file system into the wizard when you configure the first NH K2 Media Server, as in the previous procedure. That server is now the acting media file system server. You can now configure the remaining server using the following procedure.

1. Verify that server A has restarted by opening the MS-DOS command prompt and use the "ping" command.
2. In the K2 System Configuration application tree view, select the K2 Media Server you are configuring as server B.
3. Click the **Configure** button.

The Configure K2 Server wizard opens to the Define server roles page.

Configure Define Server Roles page - NH server



1. Enter the name for the K2 Media Server, as currently configured on the machine.

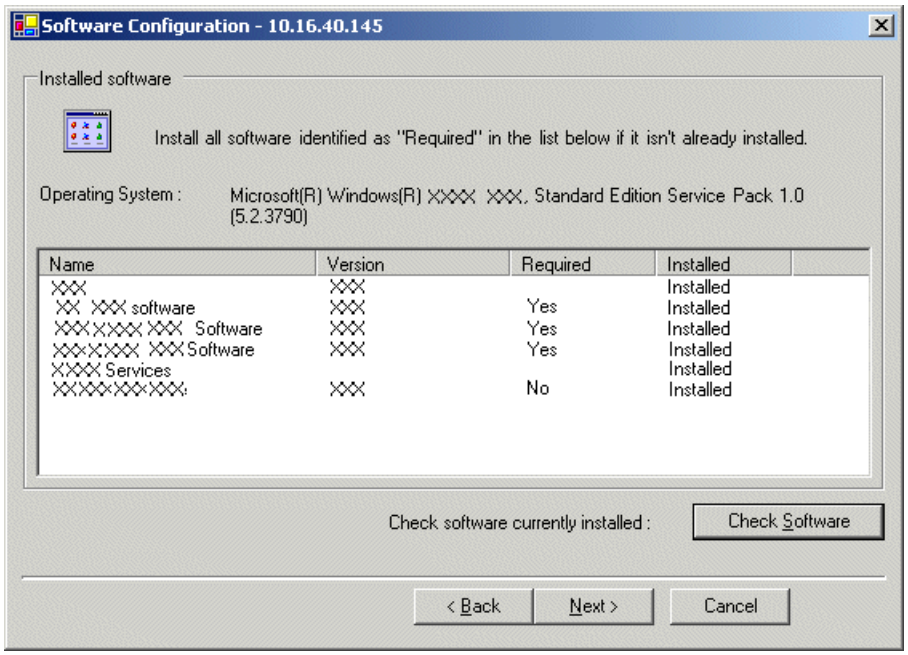
   For Nearline server roles, selections are disabled. Leave SNFS file system server, FTP server, and NAS server selected.

   The wizard does not allow you to select Media Database Server. There is no Media Database Server in a nearline system.

2. Click **Next**.

The Software Configuration page opens.

Configure Software Configuration page - NH server

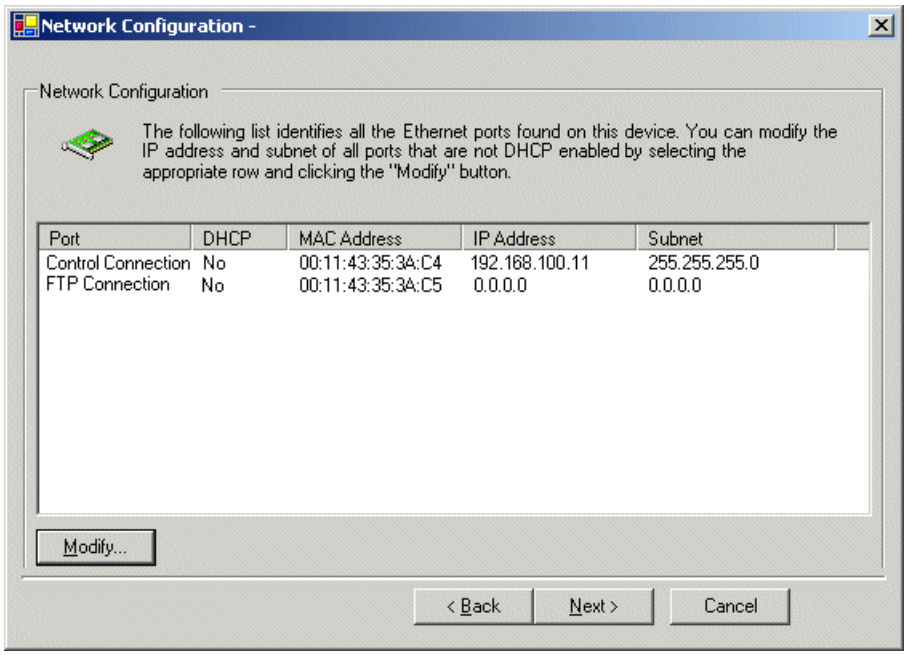


This page checks for the software required to support the roles you selected on the previous page.
NOTE: MPIO software is required on servers in redundant systems.

1. If software with **Yes** in the Required column reports as **Not Installed**, install the software.
2. Click **Check Software**.
3. When all required software reports as **Installed**, click **Next**.

The Network Configuration page opens.

Configure Network Configuration page - NH server



This page displays the control network Ethernet port, and allows you to configure the FTP/Streaming network Ethernet port.

1. Verify that the top port is configured correctly.

   The top port is the port over which the K2Config application is communicating. If correctly configured, it is already assigned the control network IP address, as displayed on this page.

2. Verify that the FTP/Streaming port is configured correctly. If not configured correctly, do the following:

   a) Select the other port and click **Modify**.

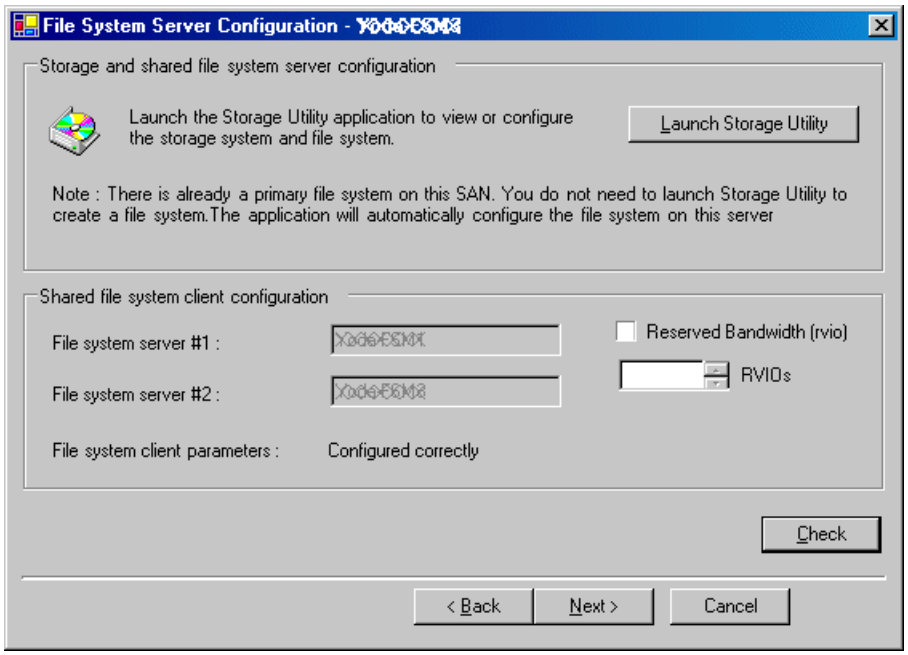
      A network configuration dialog box opens.

   b) Enter the FTP/Streaming IP address and the subnet mask and click **Apply**.

3. Click **Next**.

The File System Server Configuration page opens.

Configure File System Server Configuration page - NH server B



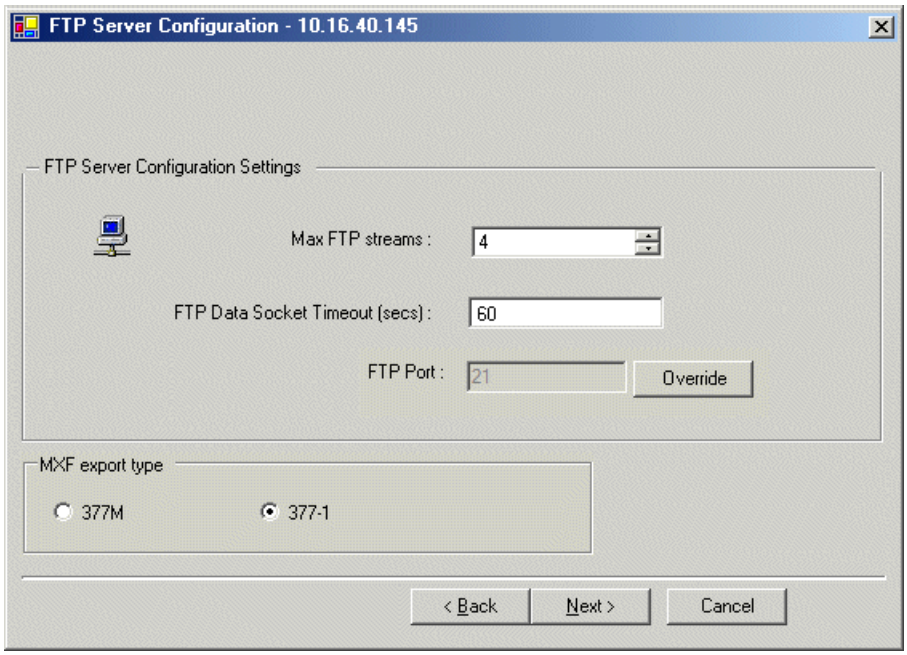
This page checks on the configuration of the K2 Media Server in one of its main roles as a file system server. The K2 Media Server also functions as a file system client, which is also checked from this page. It is not necessary to bind RANKs or create a file system, since this task was completed when you configured the previous K2 Media Server.

1. Do not select **Reserved Bandwidth** unless instructed to do so by Grass Valley. This system is usually not configured for RVIO.
2. Click **Check**.
3. Confirm a "… file copied…" message.
4. When the wizard reports that the configuration is correct, click **Next**.
5. Confirm messages about copying the file system configuration file to the other server.

   If you get a "The V: will not be available until this device is rebooted…" message, you can safely continue now and reboot later when instructed to do so.

The iSCSI Bridge Server Configuration page opens.

Configure FTP Server Configuration page - K2 SAN server B



This page appears only if the server has the role of FTP server.

Do not modify these settings. Leave at default values of Max FTP streams = 4, FTP Data Socket Timeout = 60, and FTP Port = 21. Only qualified Grass Valley personnel should specify other values, as these settings are intended for use only with custom systems designed by Grass Valley.

1. Select MXF export type as follows:

   - **377M**: Original SMPTE 377M style. Ensures compatibility with older products.
   - **377-1**: Newer SMPTE 377-1 style.

   Refer to related topics in the "Configuring the K2 System" section of this Topic Library for more information.

2. Click **Next**.

   The Completing the Configuration Wizard page opens.

3. Click **Finish**.

   The wizard closes. The server restarts.

Wait until all startup processes have completed before continuing.

Next, check the V: drive

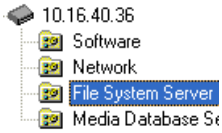
Check the V: drive

- The K2 Media Server must be configured

- The restart of the K2 Media Server after it is configured must be complete

This task is required for NAS server functionality.

1. Verify that the K2 Media Server has restarted by opening the MS-DOS command prompt and use the “ping” command.
2. In the K2Config application tree view, under the K2 Media Server select the File System Server node.



The File System Server Configuration page appears.

3. Click **Check** and verify that the V: drive is shared.

The K2 Nearline SAN configuration is complete.

Configuring clients on the K2 SAN

About iSCSI bandwidth

When you purchase a K2 SAN to provide the shared storage for your K2 clients, your Grass Valley representative sizes the storage system and recommends the appropriate license level and QOS level based on your bandwidth requirements. These bandwidth requirements are based on how you intend to use the channels of your K2 clients. The bit rates, media formats, and ratio of record channels to play channels all effect your bandwidth requirements.

As you add your K2 clients to the K2 SAN, you must assign a bandwidth value to each K2 client. This value is based on your intended use of the channels of that K2 client. There is a page in the K2Config application on which you enter parameters such as channel count, bit rate, and track count per channel to calculate the bandwidth value for a K2 client. The K2Config application takes that bandwidth value and assigns it to the total bandwidth available, so that the K2 client has adequate bandwidth for its intended media access operations. When the bandwidth values you enter in the K2Config application match the overall bandwidth requirements upon which your K2 shared storage is sized and licensed, you have sufficient bandwidth for all your K2 clients.

The K2 SAN uses a mechanism called a TCP/IP Offload Engine (TOE) as a bridge across which all media must travel between the iSCSI/Ethernet world and the SCSI/Fibre Channel world. A TOE is hosted by the iSCSI interface board, which also provides the connection to the Ethernet switch. In addition, the K2Config application restricts the amount of bandwidth available based on the level at which you have licensed your K2 SAN.

As you configure your K2 SAN, the K2Config application assigns a K2 client to a TOE and keeps track of the bandwidth so subscribed to each TOE. A single K2 client can only subscribe to a single TOE. However, a single TOE can have multiple K2 clients subscribed to it. It is important to realize that this does not adjust itself dynamically. If you change your intended use of a K2 client and

increase its bandwidth requirements, you risk oversubscribing the TOE to which that K2 client is assigned.

The K2Config application provides a report of iSCSI assignments, which lists for each TOE the iSCSI clients assigned and their bandwidth subscription.

Determining K2 client bandwidth requirements

The K2Config application provides a page in the Configure K2 Client wizard that calculates the bandwidth requirement for a K2 client. On this page you enter information regarding the channel count, bit rate, and tracks per channel for your intended use of the K2 client. The page then calculates the bandwidth requirement and make it available for load balancing.

K2 SAN prerequisites for adding clients

The following K2 SAN preparations are required to support adding SAN clients:

- All K2 Media Servers and/or K2 RAID storage devices must be installed and cabled.
- The control network must be operational with K2 devices communicating. At the command prompt, use the ping command to verify.
- For basic, non-redundant K2 SANs, the media network must be operational. You can check this with the K2Config application.
- For redundant K2 SANs, media network A and media network B must be operational. You can check this with the K2Config application.
- K2 RAID devices must have disks bound and be configured as required for operation on the K2 SAN.
- K2 Media Servers must be configured such that an operational media file system is present.
- K2 Ethernet switches must be configured and have V-LANs set up.
- The SAN to which you are adding your clients must be defined with the appropriate number and type of clients. In other words, in the K2Config application tree view you should see the clients you are about to add represented as unconfigured devices.
- The K2 Media Server with role of file system server must be licensed as appropriate for the design of your K2 SAN.

NOTE: Do not run Storage Utility on a shared storage client. For shared storage, run Storage Utility only via the K2Config application.

Verify license on K2 Media Server

The K2 SAN license is installed on K2 Media Servers with role of iSCSI bridge. If a redundant system and/or a large system with multiple servers, the license must be installed on each K2 Media Server with role of iSCSI bridge. Use the following steps to verify the license on each K2 Media Server with role of iSCSI bridge.

1. On the K2 Media Server, open SabreTooth License Manager.
2. Verify that a license identified as K2-ISCSI-SVR is installed.

If the license for your K2 SAN license is not installed, you must install it before proceeding.

Preparing K2 clients

Do the following to each system in preparation for its addition as a client to the K2 SAN:

1. If you have not already done so, rack, cable, and provide power.
2. Power on the K2 client and log on to Windows as Windows administrator, which is username *Administrator* and password *adminK2* by default. Ignore startup messages referring to a missing media storage system.
3. Assign a control network IP address and configure other network settings for the K2 client. Use SiteConfig for this step. The two control ports are teamed, so even if are making a connection to port 1 only, you must configure network settings for the Control Team.
4. Optionally, use SiteConfig to configure media (iSCSI) networks at this time. You can use either SiteConfig or K2Config to configure media networks. If you use SiteConfig, then you must open the relevant page in K2Config so that K2Config reads the settings in from the system you are adding as a SAN client. This also allows you to verify the media network configuration in the context of K2Config.
5. Configure SNMP properties so the trap destination points to the SNMP manager PC. Use standard Windows procedures.

   Refer to related topics about Grass Valley recommended deployment and monitoring solutions in the "About This Release" section of the K2 Topic Library.
6. If the K2 client connects to the K2 SAN with a redundant Ethernet (iSCSI) fabric, install Multi-Path I/O software.
7. Copy the K2 SAN hosts file onto the system you are adding as a SAN client. You can use SiteConfig for this task.

Installing Multi-Path I/O Software

If a K2 Solo 3G system with K2 software version lower than 9.0, before doing this task make sure the write filter is disabled.

The following procedure is required for shared storage K2 clients that have their Gigabit Media ports connected to the two iSCSI Media networks. This configuration is used for redundant K2 SANs. The procedure is also required on K2 Media Servers on a redundant nearline SAN.

The files for the Multi-Path I/O software are copied on to the K2 client or K2 Media Server when the K2 software is installed.

1. Access the Windows desktop on the computer on which you are installing MPIO.

   You can do this locally with a connected keyboard, mouse, and monitor or remotely via the Windows Remote Desktop Connection.
2. Stop all media access. If AppCenter is open, close it.
3. Click **Start | Run**, type `cmd` and press **Enter**.

   The MS-DOS command prompt window opens.
4. From the command prompt, navigate to the `C:\profile\mpio` directory.

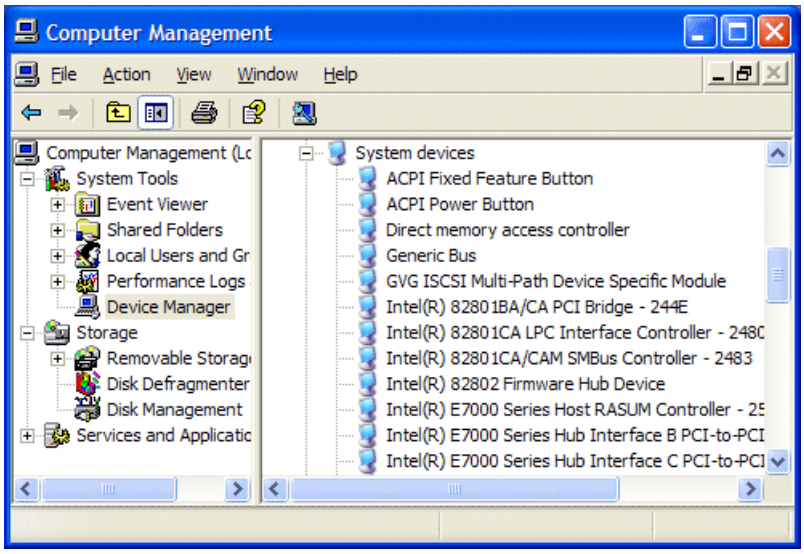
5. Type one of the following at the command prompt:
   - If installing on a 32-bit computer:

     ```
     gdsminstall.exe -i c:\profile\mpio gdsm.inf Root\GDSM
     ```
   - If installing on a 64-bit computer:

     ```
     gdsminstall64.exe -i
     ```
6. Press **Enter**.

   The software is installed. The command prompt window reports progress.
7. Restart the computer on which you installed MPIO.
8. After restart, to verify that the software is installed, on the Windows desktop right-click **My Computer** and select **Manage**.

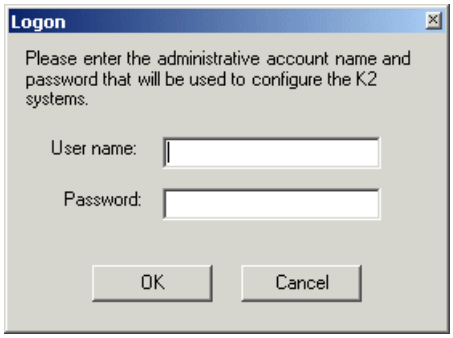
   The Computer Management window opens.



9. In the left pane select **Device Manager**.
10. In the right pane open the **System devices** node and verify that **GVG ISCSI Multi-Path Device Specific Module** is listed.

Configuring a K2 client for the K2 Storage System

1. On the PC that hosts K2Config, open the K2Config application.
   A log on dialog box opens.

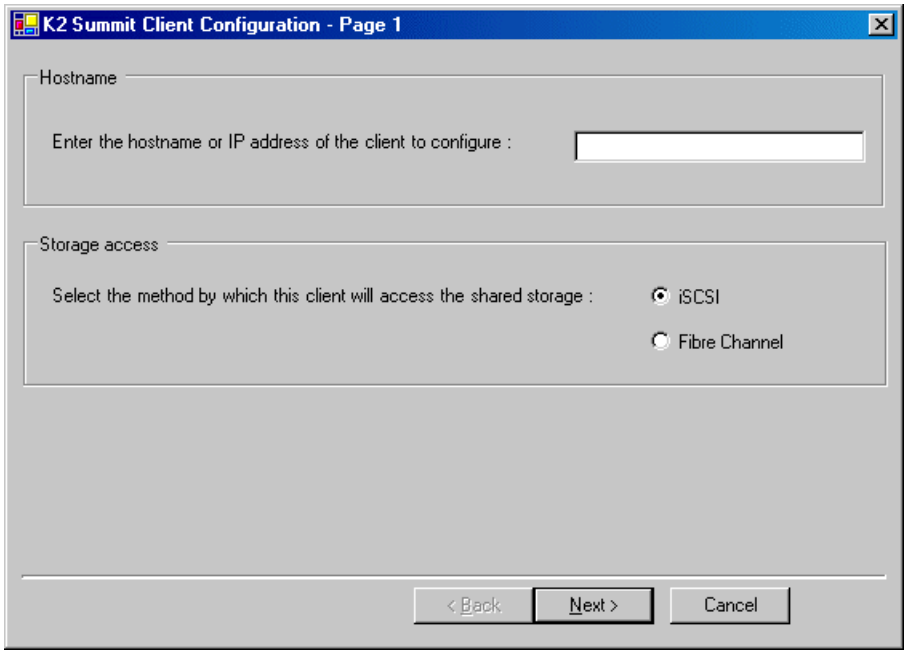


2. Log on to the K2Config application with the administrator account.
   The K2Config application opens.
3. In the K2Config application tree view, verify that the K2 SAN has the correct number of clients, according to your system design.
   If the correct number of clients is not currently added to the K2 SAN, you can add or remove clients now (before clients are configured), as follows:
   - To add a client, select the top node of the storage system and click the **Add Device** button.
   - To remove a client, select an unconfigured client and click the **Remove** button.
4. In the K2Config application tree view, select the system you are adding to the K2 SAN.
5. Select a client and click the **Configure** button.

The configuration wizard opens to page 1.

NOTE: If your system has a large number of iSCSI clients, you are prompted to restart the server that has the role of SNFS file system server when you configure clients and cross the following thresholds: 64 clients; 80 clients; 96 clients.

Configure page 1 - K2 client

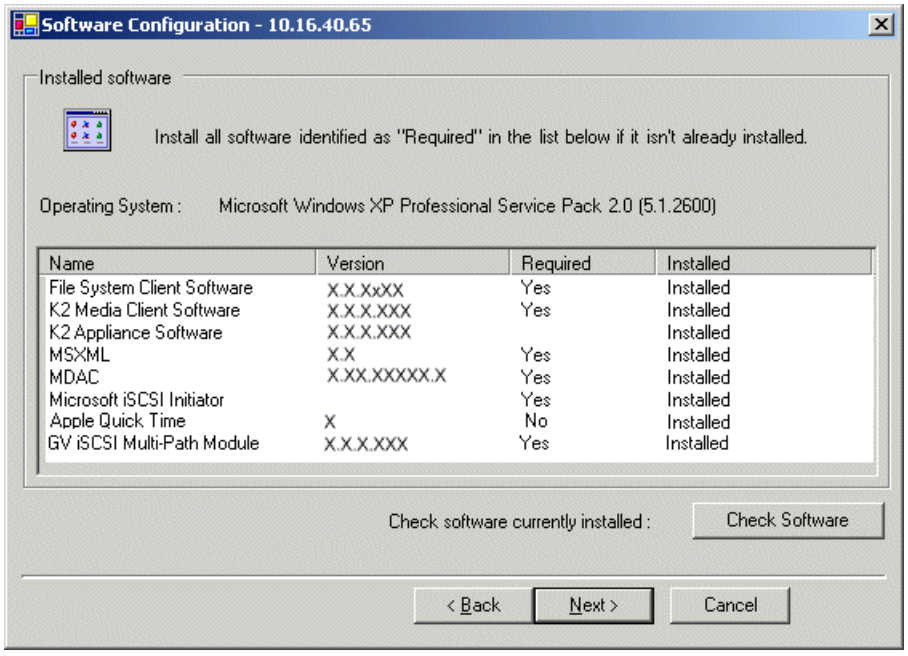


1. Enter the IP address or network name for a SAN client, as currently configured on the client system.

   You should configure your highest bandwidth SAN clients first, as this ensures load balancing is correct.
2. For the Storage Access settings, leave iSCSI selected.
3. Click **Next**.

The Software Configuration page opens.

Configure Software Configuration page - K2 client



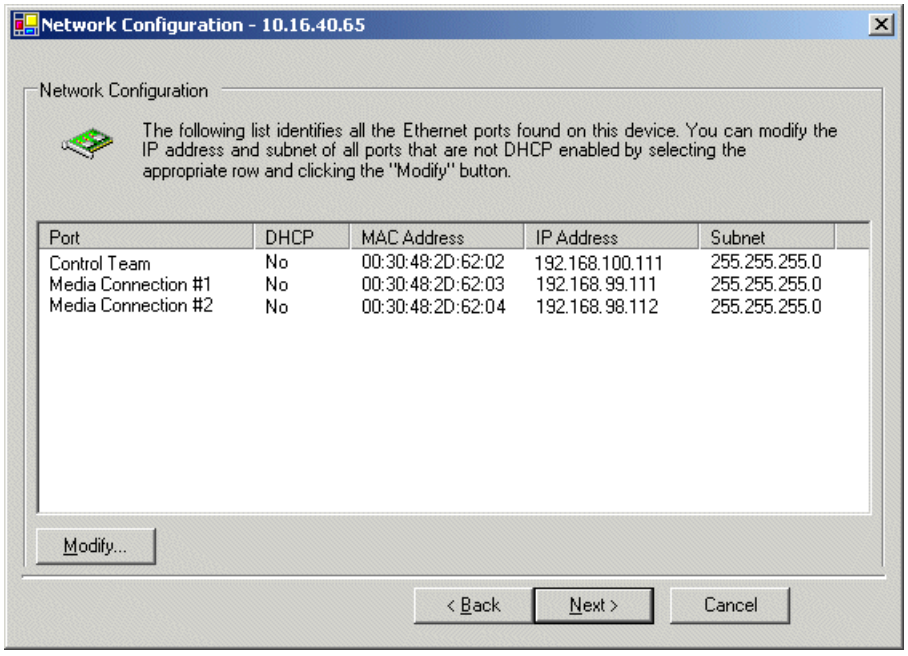
This page checks the client for required software.

NOTE: Multi-Path I/O software must be installed on K2 clients connected to a redundant K2 SAN.

1. If software with **Yes** in the Required column reports as **Not Installed**, install the software.
2. Click **Check Software**.
3. When all required software reports as **Installed**, click **Next**.

The Network Configuration page opens.

Configure Network Configuration page - K2 client



This page configures both control and media (iSCSI) network connections.

The K2 client actually has four Gigabit Ethernet ports, but two ports are configured as a teamed pair (the control team), while the other two ports (the media connections) are individual. The teamed pair shares an IP address and appears on this page as a single port.

1. Verify that the top port is configured correctly.

   The top port is the port over which the K2Config application is communicating. If correctly configured, it is already assigned the control network IP address, as displayed on this page.

2. Select **Media Connection #1** and then click **Modify**.

   A network configuration dialog box opens.

3. Verify or configure Media Connection #1 as follows:

   - If a basic (non-redundant) K2 SAN, verify or enter the media network IP address. Also enter the subnet mask.
   - If a redundant K2 SAN, verify or enter an IP address for the “A” media (iSCSI) network. Also enter the subnet mask.

4. Do one of the following:

   - If a basic (non-redundant) K2 SAN, skip to the last step in this procedure. Do not configure Media Connection #2.
   - If a redundant K2 SAN, proceed with the next step and configure Media Connection #2.

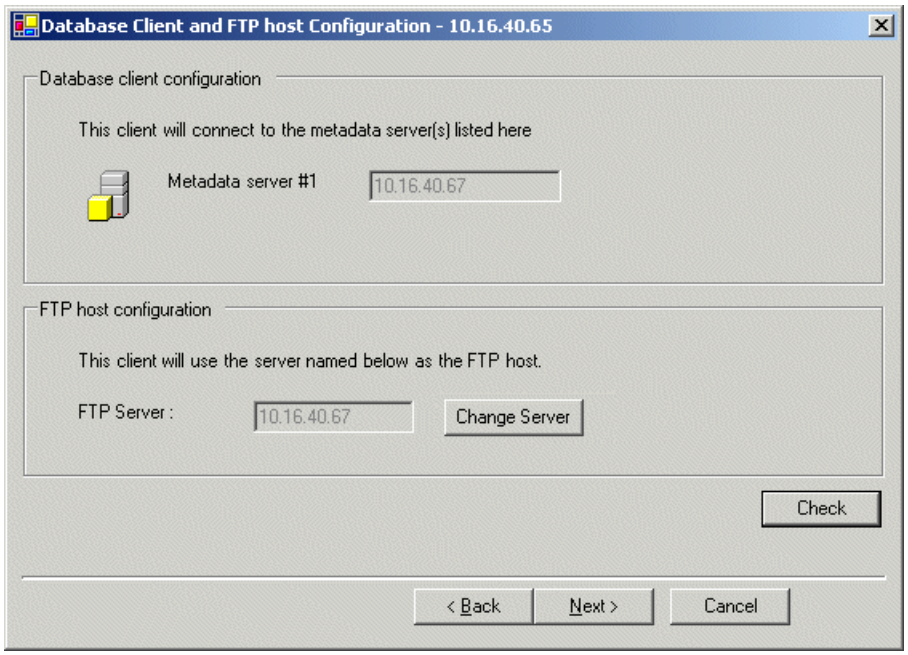
5. Select **Media Connection #2** and then click **Modify**.

   A network configuration dialog box opens.

6. Verify or enter an IP address for the “B” media (iSCSI) network. Also enter the subnet mask.
7. Click **Next**.

The Database Client Configuration page opens.

Configure Database Client Configuration page - K2 client



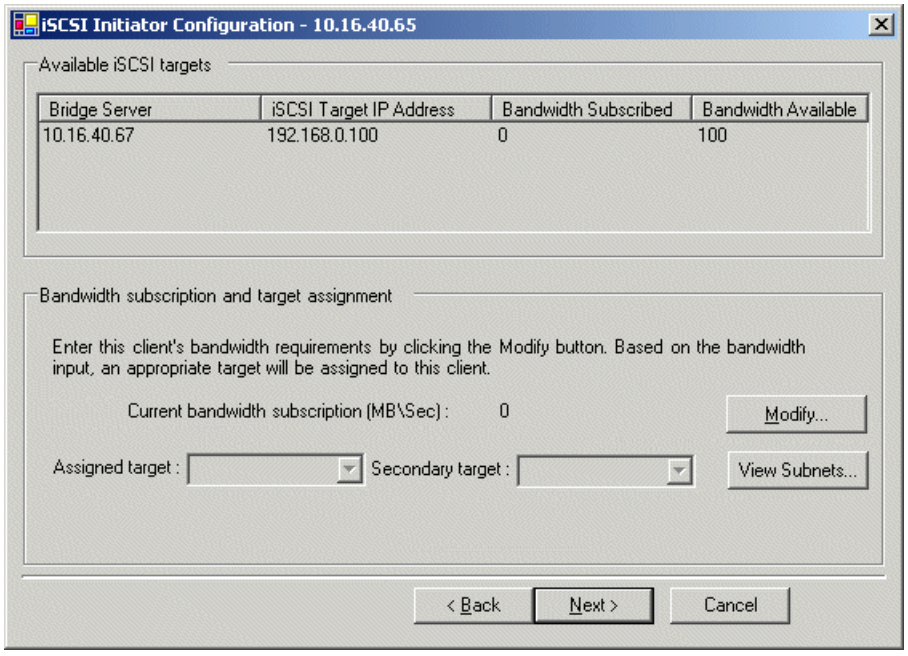
This page connects the SAN client as a media database client to the K2 Media Server taking the role of metadata (database) server. If there are redundant K2 Media Servers, both are listed on this page as database servers.

1. Verify that the K2 client is connecting to the correct K2 Media Server or Servers, as follows:
   - For a basic (non-redundant) K2 SAN, the client connects to the only server.
   - For a redundant K2 SAN, the client connects to server A as database server 1 and server B as database server 2.

   If there are multiple FTP servers (such as the optional NH servers), the K2Config application automatically assigns the SAN client to an FTP server to provide optimum FTP bandwidth across the system. Do not attempt to change the assignment to a different FTP server while you are doing this initial configuration.
2. Click **Check**.
3. When the wizard reports that the configuration check is successful, click **Next**.

The iSCSI Initiator Configuration page opens.

Configure iSCSI Initiator Configuration page - K2 client

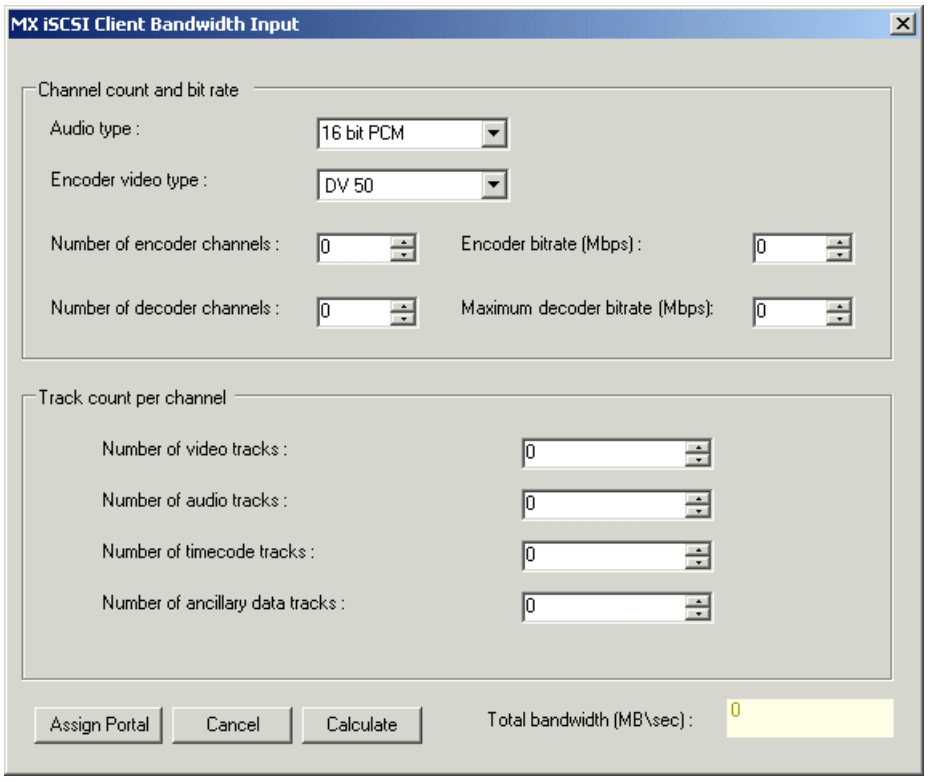


This page lists the iSCSI adapter on your K2 Media Server as an iSCSI target. The K2Config application subscribes the SAN client to the iSCSI target and allocates bandwidth, based on the bandwidth values that you enter. The K2Config application keeps track of each SAN client's bandwidth, and when the total amount allowed by the K2 SAN license is consumed, the K2Config application displays an informative message and then disables your ability to add more SAN clients. For large systems the K2Config application can load balance SAN clients across multiple iSCSI targets.

If a custom K2 SAN, qualified system designers can view subnets to help assign iSCSI targets.

1. Click **Modify**.

   The Bandwidth Input dialog box opens.



2. Enter the channel count, bit rate, and track count per channel information according to your intended use of the K2 client.

   If using ChannelFlex Suite with multiple inputs and/or outputs per channel, do not enter the number of channels. Instead do the following:

   - For **Number of encoder channels** enter the total number of inputs.
   - For **Number of recorder channels** enter the total number of outputs.

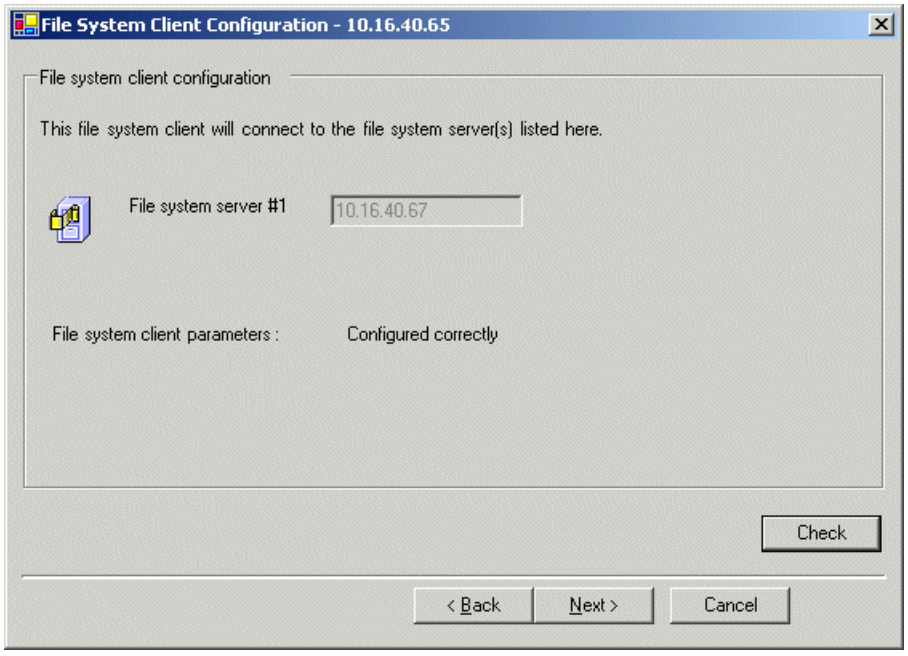
3. Click **Calculate**.
4. Click **Assign Portal**, then **OK** to confirm.

   If you have a redundant K2 SAN, the K2Config application makes the appropriate assignment to the redundant server, as reported in the Secondary target box.

5. Click **Next**.

The File System Client Configuration page opens.

Configure File System Client Configuration page



This page connects the SAN client 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.

1. Verify that the K2 client is connecting to the correct K2 Media Server or Servers, as follows:
   - For a basic (non-redundant) K2 SAN, the client connects to the only server.
   - For a redundant K2 SAN, the client connects to server A as file system server 1 and server B as file system server 2.
2. Click **Check**.
3. When the wizard reports that the configuration check is successful, click **Next**.

Repeat these tasks to add remaining SAN clients to the K2 SAN.

Adding a generic client device

- You must be logged in to the K2Config application with permissions equivalent to K2 administrator or higher.
- The devices of the K2 SAN are not required to be offline, and a restart of devices is not required.

1. In SiteConfig, add the client device to the appropriate group and verify that it is communicating correctly on networks.
2. In the K2Config application tree view, select the name of the K2 SAN, which is the top node of the storage system tree.
3. Click **Add Device**. The Add Device dialog box opens.
4. Select the type of client you are adding.

5. Click **OK**. The new client appears in the tree view.
6. Configure the client as appropriate. Refer to the documentation for the device.

   Enter the RVIO value as provided by Grass Valley. Do not attempt to calculate the RVIO value on your own.

   When configuring editors on a K2 SAN with 1 Gig TOEs, do not assign editors and K2 clients (K2 Summit or K2 Media Client) to the same TOE. Instead, assign editors to their own TOE.

Assigning a SAN client to different FTP server

If your K2 SAN has multiple K2 Media Servers that take the role of FTP server, such as when you have one or more options NH servers, you can change the FTP assignment of a SAN client so that it uses a different FTP server. This is helpful if one of the FTP servers requires service work or otherwise becomes unavailable. In this case, you might want a SAN client assigned to that FTP server to use a different FTP server, so that its FTP access can continue.

1. From the Control Point PC, open the K2Config application.
2. For each SAN client, open the Media Database page.
3. Identify the SAN clients assigned to the FTP server that is about to become unavailable.
4. For those K2 clients, click **Change Server**.

   A message box appears that asks if you are sure you want to change the FTP server.
5. In the message box, click **Yes**.

   The K2Config application finds the FTP server with the most available FTP bandwidth and re-assigns the K2 client to that FTP server.
6. On each SAN client for which you changed the FTP server assignment, restart the client. This puts the change into effect, so that the next time the SAN client needs FTP access, it uses the newly assigned FTP server.

Powering on/off a SAN client

As long as the K2 SAN remains operational, you can use the standard power on and power off procedures appropriate for the SAN client. When a SAN client goes offline or comes online it does not disrupt the K2 SAN.

However, if you are powering down or otherwise taking the K2 SAN itself out of service, you must follow the correct SAN power down procedure. You must first stop all media access on your SAN clients to ensure that they do not cause error conditions. You can power off the SAN clients or take them offline using the K2Config application.

When powering up the K2 SAN, power on the SAN clients last so that they can verify their media storage as part of their start up processes.

Taking a SAN client offline

1. Stop all media operations on the device. This includes, play, record, and transfer operations.
2. Shut down the SAN client.

Operating the K2 SAN

Powering off the K2 SAN

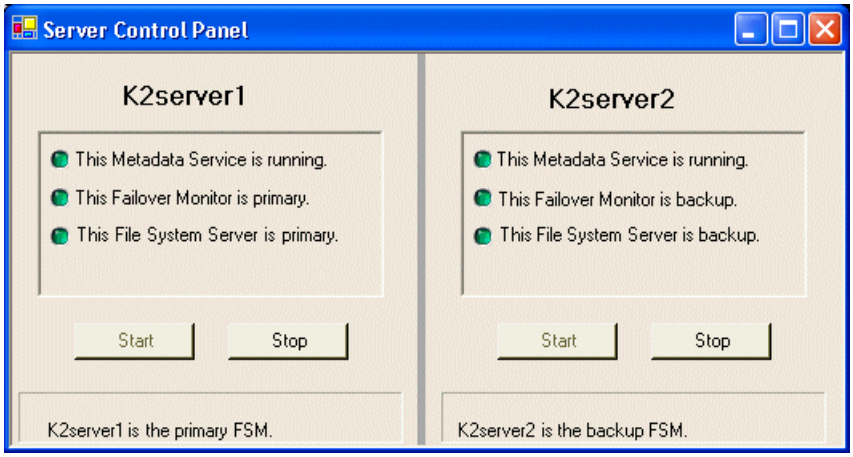
Use the following procedures to do an orderly power off of the complete K2 SAN.

Power off K2 Media Servers

1. Stop all media access as follows:
   - For nearline systems, stop all FTP streams or other media operations.
   - For online systems, power-off all K2 clients or other iSCSI clients.
2. Shut down K2 Media Servers as follows:
   - For nearline systems, shut down all K2 Media Servers.
   - For basic (non-redundant) online or production systems, shut down the K2 Media server that is the media file system and metadata server.
   - For redundant online or production systems, manage redundant server shutdown as follows:

   a) From the K2 System Configuration application, in the tree view select the name of the K2 SAN, which is the top node of the storage system tree. Then click the **Server Control Panel** button. 

   The Server Control Panel opens.



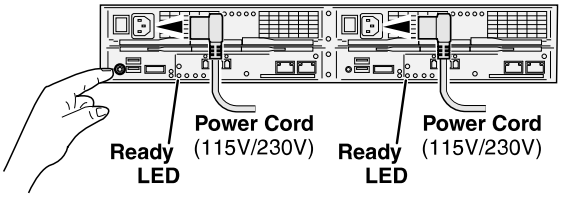
   b) Take note of which is the primary K2 Media Server and which is the backup K2 Media Server.
   c) For the backup K2 Media Server, click **Stop**. This takes the server out of service.
   d) Shut down the backup K2 Media Server, if it does not shut down automatically.
   e) For the primary K2 Media Server, click **Stop**. This takes the server out of service.
   f) Shut down the primary K2 Media Server, if it does not shut down automatically.
3. Shut down any remaining K2 Media Servers, such as NH FTP servers.

Next, power off K2 RAID devices.

Powering off K2 G10v2 RAID

- K2 Media Servers must be powered off

1. On the primary RAID chassis controller, identify the Ready LED. It blinks at a rate of 1 blink per second during normal operation.



2. Tap the power button on a RAID controller. If you have two controllers, you can tap the power button on either RAID controller 0 or RAID controller 1.

   NOTE: Do not press and hold down the power button.

   After tapping the power button, the Ready LED blinks more quickly, at a rate of about 2 blinks per second.

   The power button on the RAID controller turns off power for the primary RAID chassis and any connected Expansion chassis. Power-off normally occurs within 20 seconds and is indicated when LEDs other than those on the power supplies go off and the fans stop rotating.

3. Wait for RAID power-off to complete before proceeding.
4. Power-off all Ethernet switches.
5. Power-off the control point PC and/or the SNMP manager PC, if necessary.

Next, power off remaining SAN devices.

Power off remaining K2 SAN devices

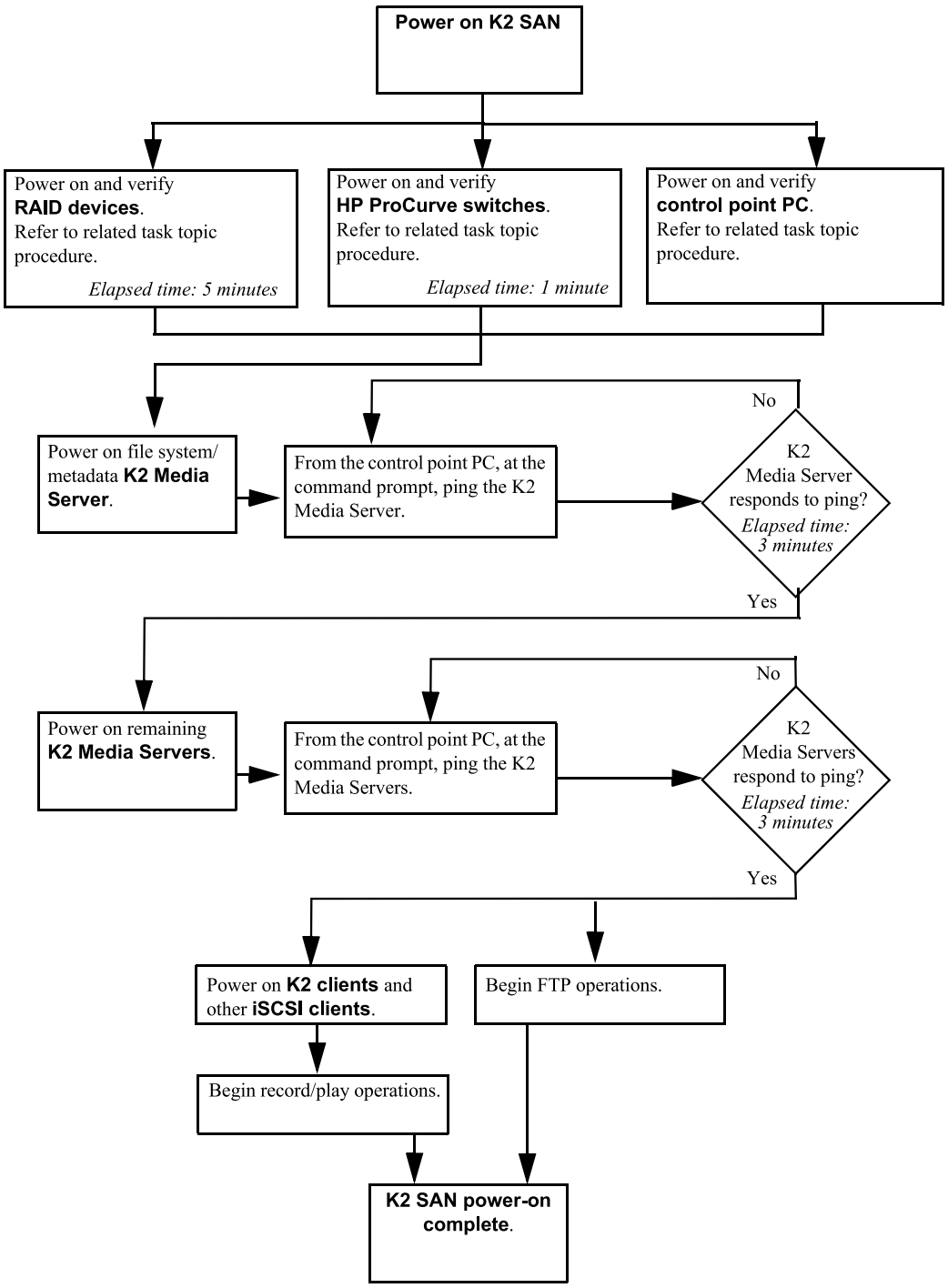
1. Power-off all Ethernet switches.
2. Power-off the control point PC and/or the SNMP manager PC, if necessary.

The K2 SAN is powered off.

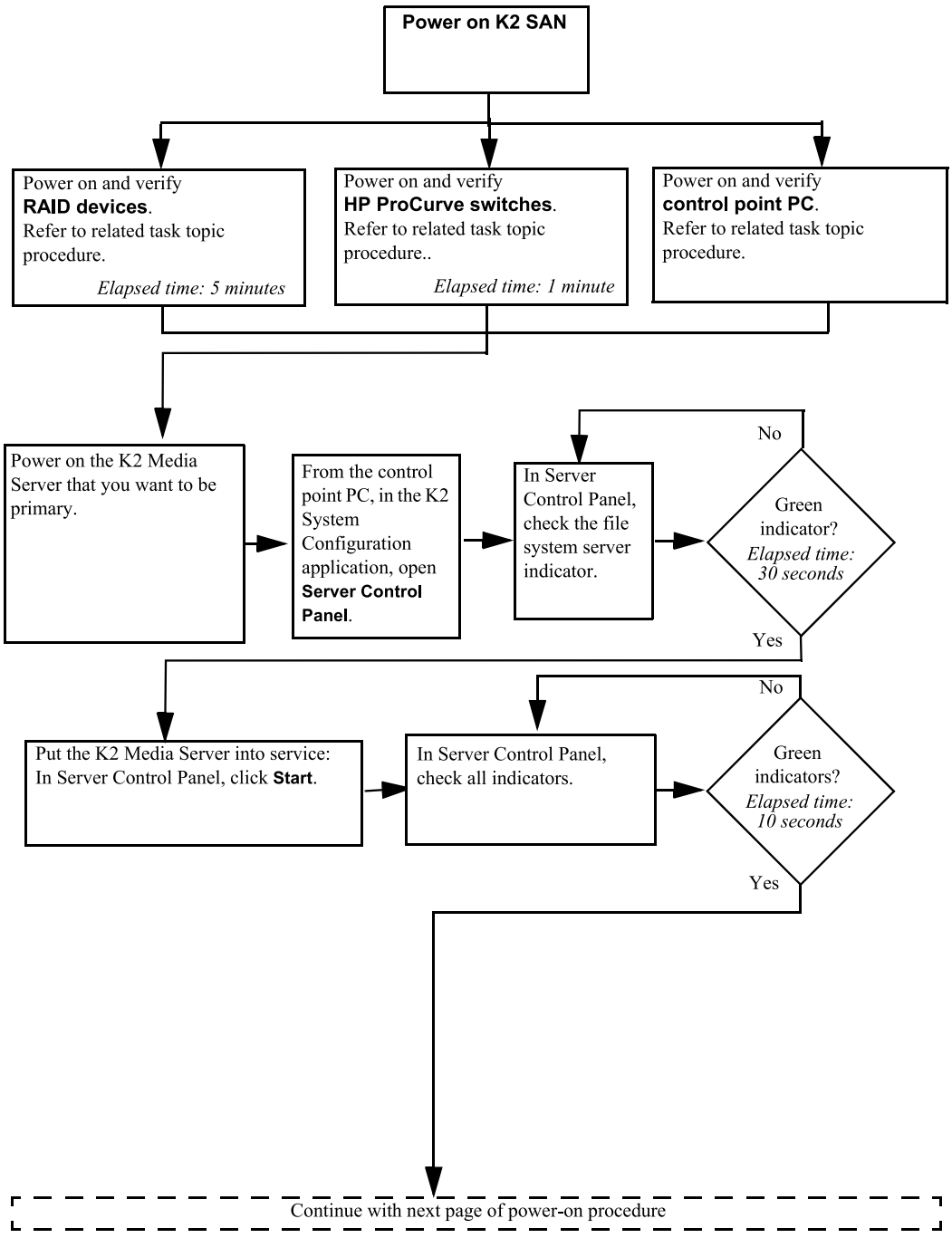
Powering on the K2 SAN

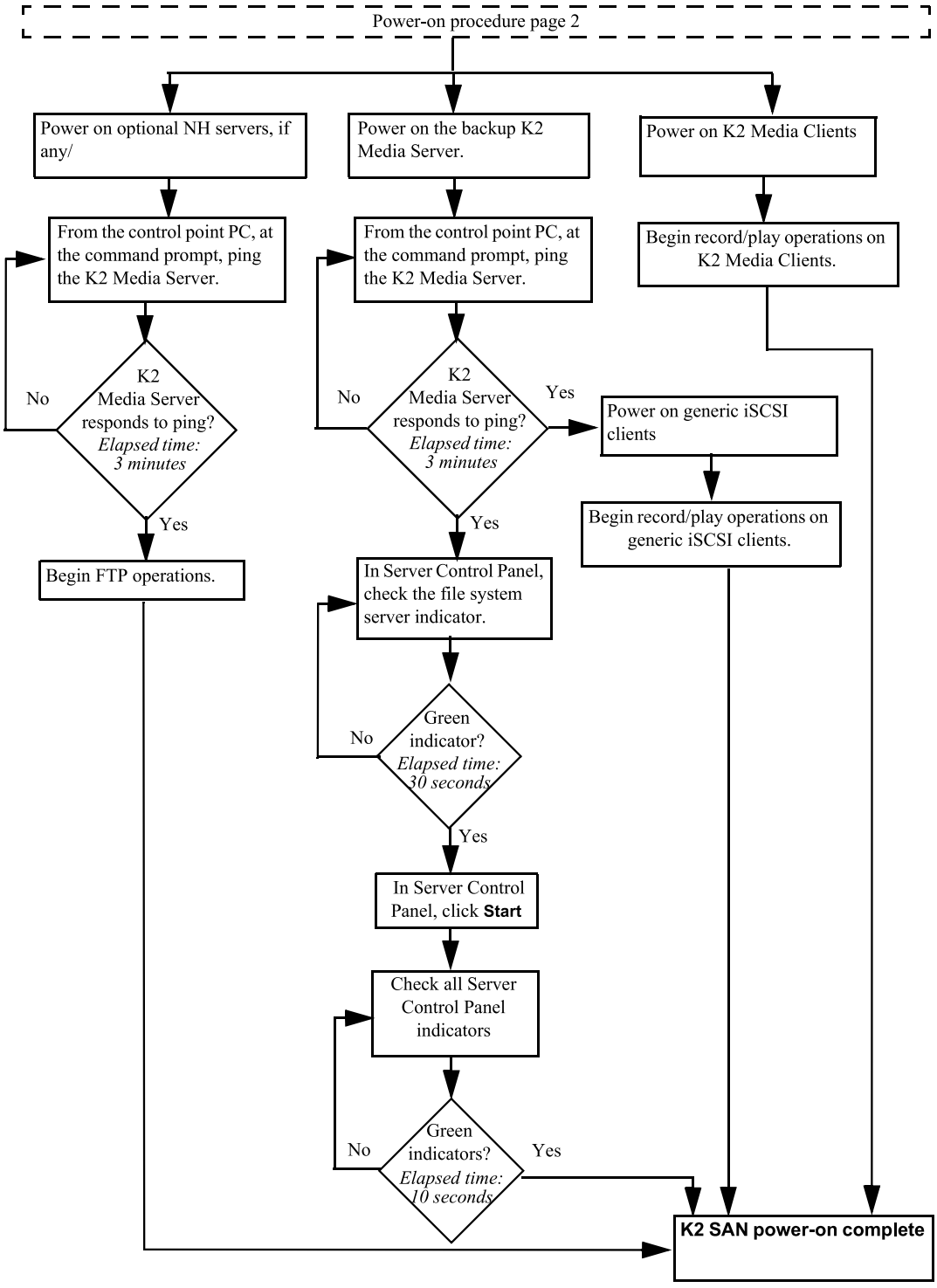
Use the following procedures to do an orderly power on of the complete K2 SAN.

Basic K2 SAN power on procedure

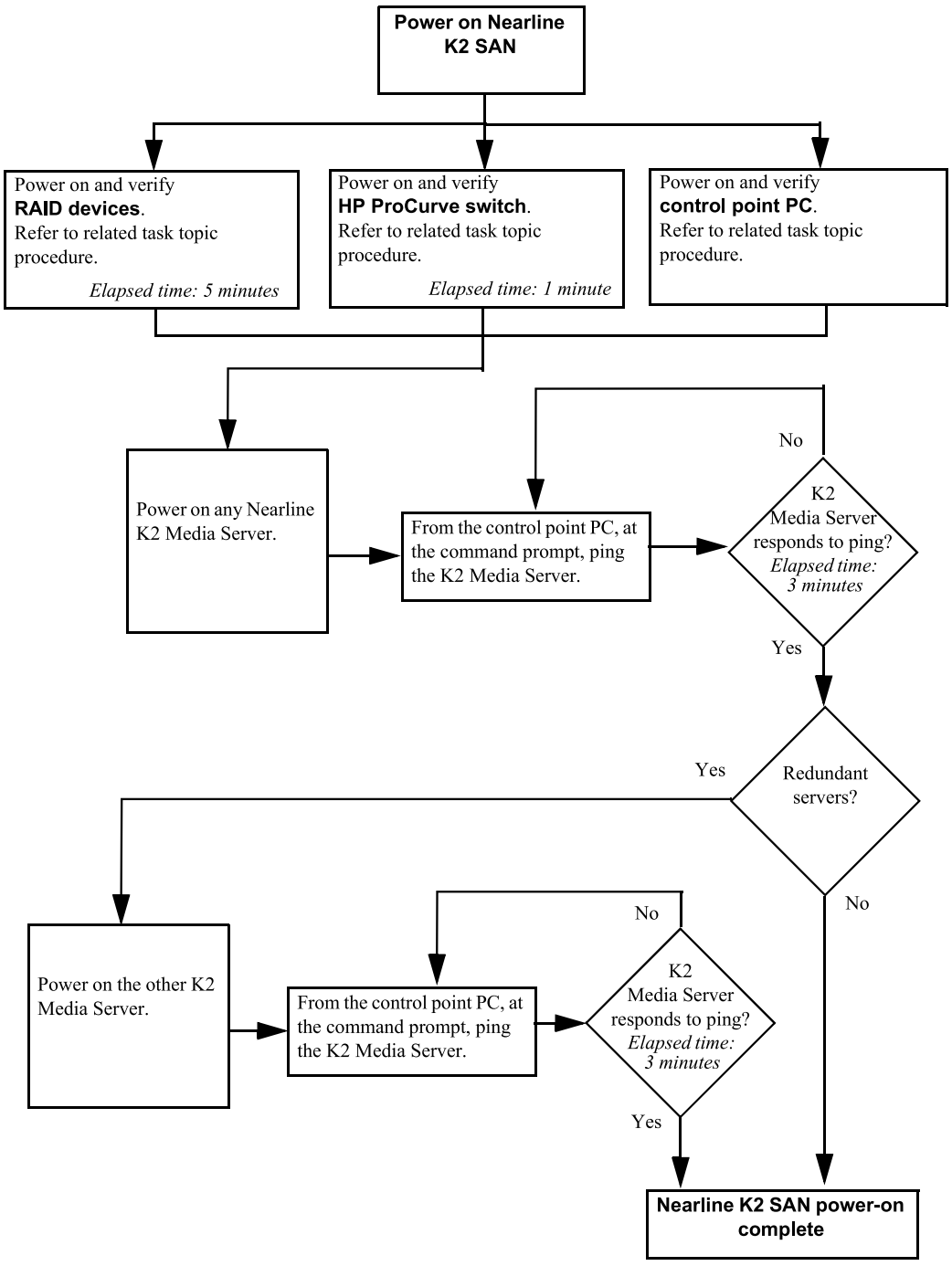


Redundant K2 SAN power on procedure




Power-on procedure page 2
Power on optional NH servers, if any/
Power on the backup K2 Media Server.
Power on K2 Media Clients
From the control point PC, at the command prompt, ping the K2 Media Server.
From the control point PC, at the command prompt, ping the K2 Media Server.
Begin record/play operations on K2 Media Clients.
K2 Media Server responds to ping? Elapsed time: 3 minutes
No
Yes
K2 Media Server responds to ping? Elapsed time: 3 minutes
No
Yes
Power on generic iSCSI clients
Begin FTP operations.
Yes
Begin record/play operations on generic iSCSI clients.
In Server Control Panel, check the file system server indicator.
Green indicator? Elapsed time: 30 seconds
No
Yes
In Server Control Panel, click Start
Check all Server Control Panel indicators
Green indicators? Elapsed time: 10 seconds
No
Yes
K2 SAN power-on complete

Nearline K2 SAN power on procedure

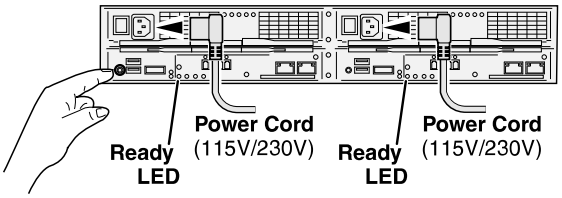


Powering on K2 G10v2 RAID

This topic applies to K2 G10v2 (M100) RAID.

1. Verify power and cabling.
2. Tap the power button on the controller, as shown.

   NOTE: Do not press and hold down the power button.



   If the RAID chassis has two controllers, you can tap the power button on either controller. You do not need to tap both power buttons.

   Tapping the power button on a controller also powers on any connected Expansion chassis. There are no power buttons on Expansion chassis.

3. Wait while the primary RAID chassis performs self-test and initialization. This takes 6-8 minutes. While this is taking place, the Ready LED is illuminated with a steady on light.
4. Watch for the Ready LED to begin blinking at one second intervals. The LED might turn off and back on two times before starting the one second blink pattern. When the Ready LED is blinking at one second intervals, the self-test and initialization is complete and the chassis is ready for use.

Powering on the HP ProCurve switch

Use the following procedure to power on and verify proper operation of the HP ProCurve switch.

1. Power up the switch.
2. Watch LEDs to verify proper operation.

   The diagnostic self test LED Behavior is as follows:

   - Initially, all the status, LED Mode and port LEDs are on for most of the duration of the test.
   - Most of the LEDs go off and then may come on again during phases of the self test. For the duration of the self test, the Test LED stays on.

   If the ports are connected to active network devices, the LEDs behave according to the LED Mode selected. In the default view mode (Link), the LEDs should be on.

   If the ports are not connected to active network devices, the LEDs will stay off.

Powering on the control point PC

Use the following procedure to power on K2 SAN's control point PC and verify proper operation during power up of the system.

1. Power up and log on to the PC using standard Windows procedures.
2. Start and log on to the SNMP manager.

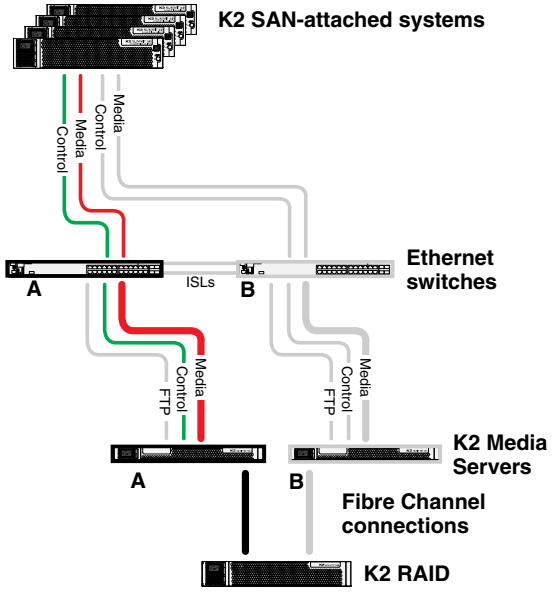
3. The SNMP manager reports devices as offline. As each device of the K2 SAN is powered on, check the SNMP manager to verify the device's status.

Failover behaviors

If a fault occurs and one of the failover mechanisms is triggered, an online redundant iSCSI K2 SAN behaves as explained in the following sections.

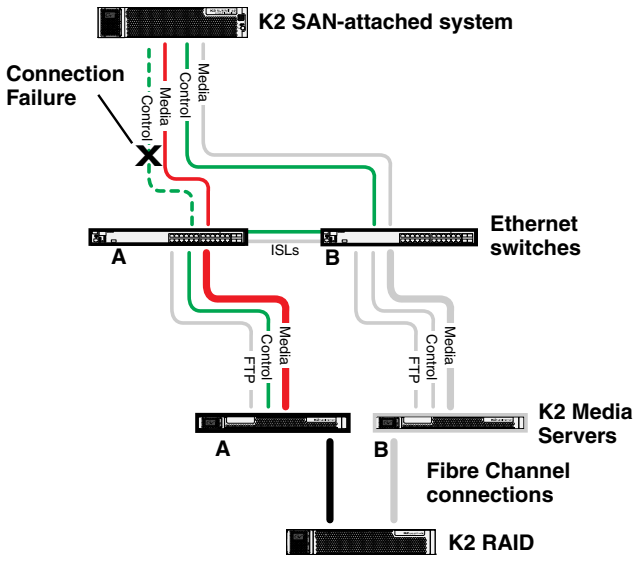
The diagrams that follow are representative of a generic redundant K2 SAN. Some details, such as the number of media connections, might not be the same as your K2 SAN. These diagrams illustrate the media (iSCSI) and control paths as they interact with the redundant K2 Media Servers in their role of media file system/metadata server and iSCSI bridge. Interactions of FTP traffic and/or paths involving K2 Media Servers with other roles are not illustrated.

Pre-failover behavior



The system operates initially with both media and control traffic on GigE switch "A" and K2 Media Server "A". Media (iSCSI) traffic is using media network "A". The iSCSI adapters (TOEs) on the "A" K2 Media Server provide access to the Fibre Channel connected RAID storage. K2 Media Server "A" is the media file system/metadata server.

Control Team failover behavior



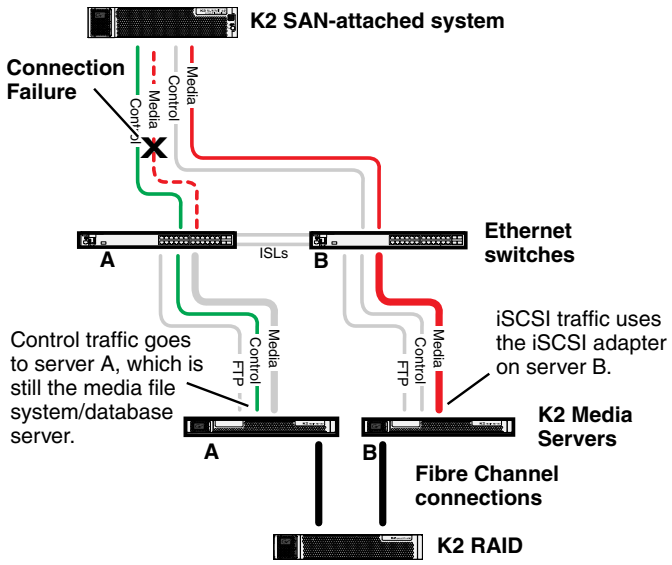
If the following system connection or component fails to respond to network communication:

- The control connection between a K2 SAN-attached system and GigE switch “A”.

Then the following failover behavior occurs:

1. The control team on the K2 SAN-attached system fails over and communication begins on the other control port.
2. The control communication finds a path through GigE “B” switch and across an ISL to GigE switch “A” to reach the same control port on the same K2 Media Server.
3. Media (iSCSI) traffic keeps using the same path.
4. K2 Media Server “A” is still the media file system/metadata server. The media file system (SNFS) and media database do not fail over.
5. The other K2 SAN-attached systems (not affected by the connection failure) keep using the same paths for media and control, as in pre-failover behavior.

K2 client media (iSCSI) connection failover behavior



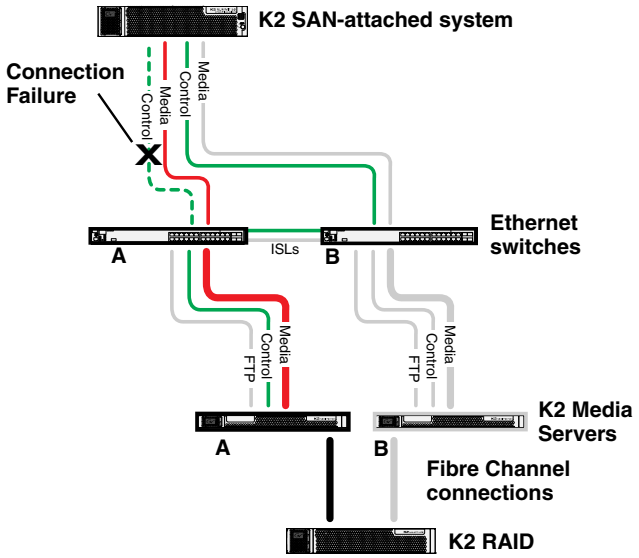
If the following system connection or component fails to respond to network communication:

- Media (iSCSI) network “A” connection between a K2 SAN-attached system and the GigE switch

Then the following failover behavior occurs:

1. The K2 SAN-attached system drops communication on its “A” media port and begins using its “B” media port and the “B” media (iSCSI) network. The iSCSI adapter (TOE) on the “B” K2 Media Server provides access to the Fibre Channel connected RAID storage.
2. Control traffic keeps using the same path to K2 Media Server “A”.
3. K2 Media Server “A” is still the media file system/metadata server. The media file system (SNFS) and media database do not fail over.
4. The other K2 SAN-attached systems (not affected by the component failure) keep using the same paths for media and control, as in pre-failover behavior. This means the K2 SAN-attached systems unaffected by the failover are using the iSCSI adapter (TOE) on the “A” K2 Media Server to provide access to the Fibre Channel connected RAID storage, while at the same time the affected K2 SAN-attached systems are using the iSCSI adapter (TOE) on the “B” K2 Media Server to provide access to the Fibre Channel connected RAID storage. In this case both RAID controller are simultaneously providing disk access.

Control Team failover behavior



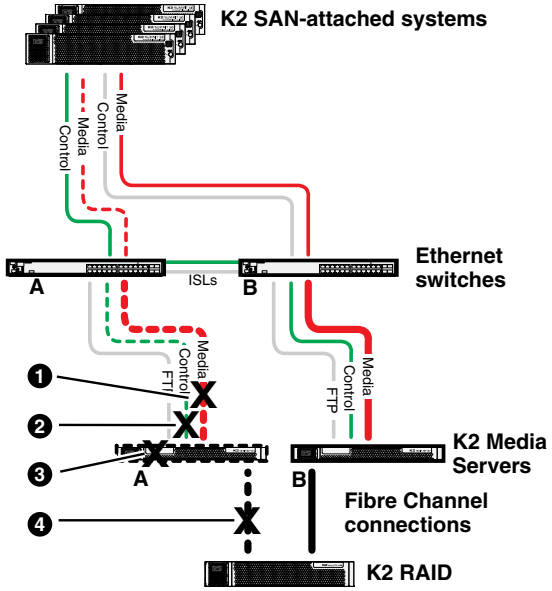
If the following system connection or component fails to respond to network communication:

- The control connection between a K2 SAN-attached system and GigE switch “A”.

Then the following failover behavior occurs:

1. The control team on the K2 SAN-attached system fails over and communication begins on the other control port.
2. The control communication finds a path through GigE “B” switch and across an ISL to GigE switch “A” to reach the same control port on the same K2 Media Server.
3. Media (iSCSI) traffic keeps using the same path.
4. K2 Media Server “A” is still the media file system/metadata server. The media file system (SNFS) and media database do not fail over.
5. The other K2 SAN-attached systems (not affected by the connection failure) keep using the same paths for media and control, as in pre-failover behavior.

K2 Media Server failover behavior



If the following system connection or component fails to respond to network communication:

❶ Either of the Media (iSCSI) network “A” connections between the GigE switch and the K2 Media Server

❷ The control connection between GigE switch “A” and K2 Media Server “A”

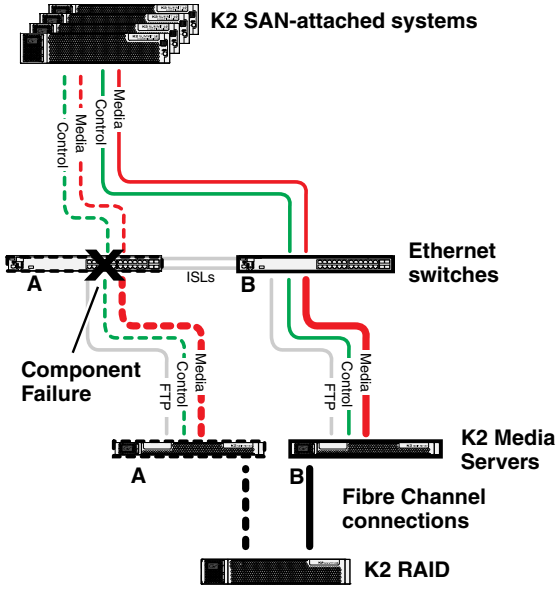
❸ K2 Media Server “A”

❹ The Fibre Channel connection between K2 Media Server “A” and RAID controller “A”

Then the following failover behavior occurs:

1. The media file system (SNFS) and media database on K2 Media Server “A” fail over and K2 Media Server “B” becomes the active media file system/metadata server.
2. All K2 SAN-attached systems drop communication on the “A” media port and begin using the “B” media port, finding a path through GigE switch “B” to K2 Media Server “B”. All K2 SAN-attached systems use an iSCSI adapter (TOE) on the “B” K2 Media Server to provide access to the Fibre Channel connected RAID storage.
3. All K2 SAN-attached systems keep communicating on the same control port, finding a new path through GigE switch “A” and across an ISL to GigE switch “B” to reach K2 Media Server “B”.

K2 Media Server failover with Control team failover behavior



If the following system connection or component fails to respond to network communication:

- The “A” GigE switch

Then the following failover behavior occurs:

1. The media file system (SNFS) and media database on K2 Media Server “A” fail over and K2 Media Server “B” becomes the active media file system/metadata server.
2. All K2 SAN-attached systems drop communication on the “A” media port and begin using the “B” media port, finding a path through GigE switch “B” to K2 Media Server “B”. All K2 SAN-attached systems use an iSCSI adapter (TOE) on the “B” K2 Media Server to provide access to the Fibre Channel connected RAID storage.
3. For all K2 SAN-attached systems, communication fails on the control port, so the control team fails over and communication begins on the other control port.
4. For all K2 SAN-attached systems, control communication finds a path through GigE switch “B” to K2 Media Server “B”.

Description of K2 SAN Devices

Device terminology

K2 Media Client

The K2 product originally released with version 3.x K2 software. It can have internal storage, direct-connect storage, or shared (SAN) storage.

First generation K2 Summit system

The K2 Summit Production Client product originally release with version 7.x K2 software. It can have internal storage, direct-connect storage, or shared (SAN) storage.

K2 Summit 3G system

The K2 Summit 3G Production Client product originally release with version 8.1 K2 software. It can have internal storage, direct-connect storage, or shared (SAN) storage.

K2 client

Either a K2 Media Client or a K2 Summit Production Client. This term is used for K2 clients with internal storage, direct-connect storage, or shared (SAN) storage.

K2 SAN client

A device that is an iSCSI or Fibre Channel client to the K2 SAN.

Control point PC description

A control point PC runs applications from which you operate, configure, and monitor the K2 SAN. You can have one or more PCs that provide control point functionality. You must have at least one control point PC on which you install and run the K2Config application.

The primary applications that run on a control point PC are as follows:

- The K2 System Configuration application
- SiteConfig
- Storage Utility
- AppCenter
- SNMP manager

In addition, you can use the control point PC for the following applications:

- QuickTime
- Adobe Acrobat Reader
- Windows Remote Desktop Connection

You can purchase a control point PC from Grass Valley. In this case the PC has all the above software pre-installed at the factory. When you receive the PC it is ready to install on the K2 SAN control network and begin using with minimal configuration.

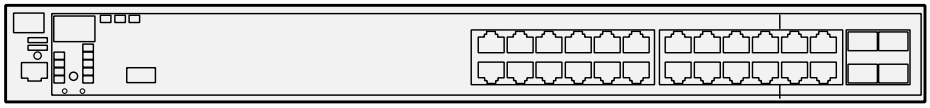
You can also build your own control point PC by installing and configuring software on an existing PC. Refer to the *K2 System Guide* for specifications and instructions.

K2 Ethernet switch description

The K2 Ethernet switch provides the primary network fabric of the K2 SAN. The switch supports Gigabit Ethernet connections, which provides the bandwidth required for the iSCSI media traffic.

The HP ProCurve switch is qualified as the K2 Ethernet switch.

The 29xx series switch is qualified for all K2 SANs. This section provides information on the 29xx series switch.



The HP ProCurve switch is a store-and-forward device offering low latency for high-speed networking. In addition, the switch offers full network management capabilities.

Refer to the manuals that you receive with the switch for more information.

K2 Ethernet switch specifications

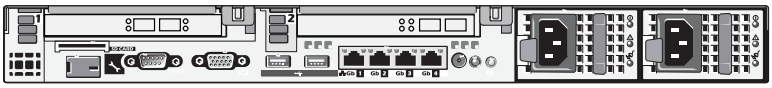
The K2 Ethernet switch is a HP ProCurve switch, with specifications as follows:

ProCurve switch 2920-24G

Characteristic	Specification
Ports	20 auto-sensing 10/100/1000 ports (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T) 2 SFP+ 10-GbE ports 1 RS-232C DB-9 console port 4 dual-personality ports
Dimensions	13.2(d) x 17.4(w) x 1.75(h) in. (33.6 x 44.2 x 4.4 cm) (1U height)
Weight	11.57 lb. (5.25 kg)
Voltage	100-127 / 200-240 VAC
Power consumption	Idle power: 26 W; Maximum power rating: 58 W
Temperature	Operating: 32ºF to 131ºF (0ºC to 55ºC); Non-operating: -40ºF to 158ºF (-40ºC to 70ºC)
Relative humidity: (non-condensing)	Operating: 15% to 95% @ 104ºF (40ºC) 15% to 95% @ 149ºF (65ºC)
Maximum altitude	Up to 10,000 ft. (3 km)

K2 Media Server description

The central component of the K2 SAN is the K2 Media Server. The Dell PowerEdge R610 and R620 are qualified as the platform for the K2 Media Server.



The following interfaces provide K2 SAN functionality with Dell PowerEdge R610:

- Two GigE ports on the motherboard. The R610 has four GigE ports, but only two are used.
- One iSCSI interface card. A port on this card is also referred to as a TOE (TCP/IP Offload Engine).
- One Fibre Channel card.

The following interfaces provide K2 SAN functionality with Dell PowerEdge R620:

- Broadcom Dual Port 10GbE SFP+ with two 1GbE (TOE and iSCSI offload available on 10GbE ports)
- Fibre channel adapter: ATTO Celerity FC-81EN Single-Channel 8Gb/s Fibre Channel PCIe 2.0 Host Adapter.
- QLogic QLE8262 Dual-Port, 10Gbps Ethernet-to-PCIe® Converged Network Adapter.

K2 Media Server specifications

The K2 Media Server is built on a Dell PowerEdge R610 and R620 server platform. Specifications that are unique to it purpose as a K2 Media Server are listed in the following table. For a complete list of specifications, refer to Dell documentation.

Dell PowerEdge R610 server

Characteristic	Specification
Operating System	Microsoft® Windows® Server 2008 R2
Fibre Channel Adapter	ATTO Celerity FC-81ENSingle-Channel 8Gb/s Fibre Channel PCIe 2.0 Host Adapter
iSCSI Adapter	QLogic QLE8240 Single Port 10-Gbps iSCSI TOE to PCI Express HBA
Communications	Two dual port embedded Broadcom NetXtreme II 5709c Gigabit Ethernet NIC
Form Factor	1U

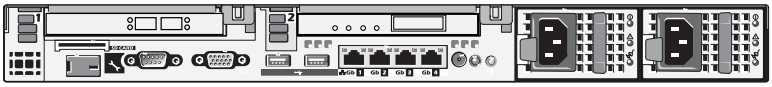
Dell PowerEdge R620 server

Characteristic	Specification
Operating System	Microsoft® Windows® Server 2008 R2 SP1, x64 (includes Hyper-V® v2)
Fibre Channel Adapter	ATTO Celerity FC-81EN Single-Channel 8Gb/s Fibre Channel PCIe 2.0 Host Adapter
iSCSI Adapter	QLogic QLE8262 Dual-Port, 10Gbps Ethernet-to-PCIe® Converged Network Adapter

Characteristic	Specification
Communications	Broadcom Dual Port 10GbE SFP+ with two 1GbE (TOE and iSCSI offload available on 10GbE ports)
Form Factor	1U

NH K2 Media Server

The NH K2 Media Server is an optional server. The Dell PowerEdge R610 is qualified as the platform for the NH K2 Media Server.



The NH K2 Media Server provides 10 Gig FTP bandwidth. The following interfaces provide K2 SAN functionality:

- One GigE port on the motherboard. The R610 has four GigE ports, but the additional ports are not used.
- One 10 Gig port.
- One Fibre Channel card.

NH K2 Media Server specifications

The NH K2 Media Server is built on a Dell PowerEdge R610 and R620 server platform. Specifications that are unique to it purpose as a K2 Media Server are listed in the following table. For a complete list of specifications, refer to Dell documentation.

Dell PowerEdge R610 server

Characteristic	Specification
Operating System	Microsoft® Windows® Server 2003, Standard Edition
Fibre Channel Adapter	ATTO Celerity FC-81EN Single-Channel 8Gb/s Fibre Channel PCIe 2.0 Host Adapter for online systems ATTO Celerity FC-82EN Dual-Channel 8Gb/s Fibre Channel PCIe 2.0 Host Adapter for nearline systems.
Communications	Two dual port embedded Broadcom NetXtreme II 5709c Gigabit Ethernet NIC Intel® Single-port 10 Gigabit SFP+ Ethernet Server Adapter x520
Form Factor	1U

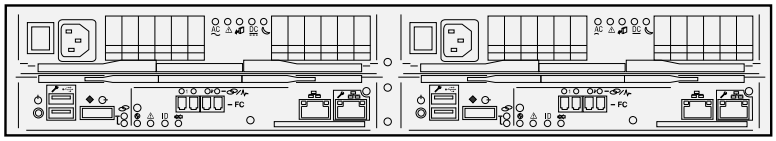
Dell PowerEdge R620 server

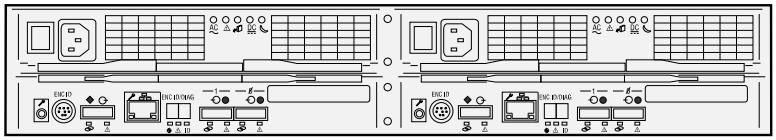
Characteristic	Specification
Operating System	Microsoft® Windows® Server 2008 R2 SP1, x64 (includes Hyper-V® v2)
Fibre Channel Adapter	ATTO Celerity FC-81EN Single-Channel 8Gb/s Fibre Channel PCIe 2.0 Host Adapter
iSCSI Adapter	QLogic QLE8262 Dual-Port, 10Gbps Ethernet-to-PCIe® Converged Network Adapter
Communications	Broadcom Dual Port 10GbE SFP+ with two 1GbE (TOE and iSCSI offload available on 10GbE ports)
Form Factor	1U

K2 RAID storage description

This section refers to K2 10Gv2 RAID storage devices.

The K2 RAID storage device is a high performance, high availability mass storage system. The RAID chassis 8Gb/s host interface supports industry standard Fibre Channel technology. K2 RAID is available with either SAS drives for online storage or SATA drives for nearline storage. There are two types of chassis: one type has 2.5 inch drives, with a capacity of 24 drives; the other type has 3.5 inch drives, with a capacity of 12 drives.





The RAID Expansion Chassis provides additional storage capacity. The Expansion Chassis has two Expansion Adapters installed.

Refer to the installation chapters earlier in this manual for connection and configuration instructions.

The K2 10Gv2 RAID is NEC Storage M100 Series. For specifications and servicing information, refer to NEC Storage M100 Series manuals.

Overview of K2 Storage Tools

About SiteConfig

SiteConfig is Grass Valley's tool for network configuration and software deployment. SiteConfig is a ProductFrame application. ProductFrame is an integrated platform of tools and product distribution processes for system installation and configuration.

You can use SiteConfig as a stand-alone tool for planning and system design, even before you have any devices installed or cabled. You can define networks, IP addresses, hostnames, interfaces, and other network parameters. You can add devices, group devices, and modify device roles in the system.

As you install and commission systems, SiteConfig runs on a designated PC. It discovers devices, configures their network settings, and manages host files. SiteConfig also manages software installations and upgrades and provides a unified software package with compatible versions for deployment across multi-product systems.

You should use SiteConfig for network configuration and software deployment at installation and throughout the life of the system in your facility. This enforces consistent policy and allows SiteConfig to keep a record of changes, which makes the system easier to maintain and aids in troubleshooting should a problem arise.

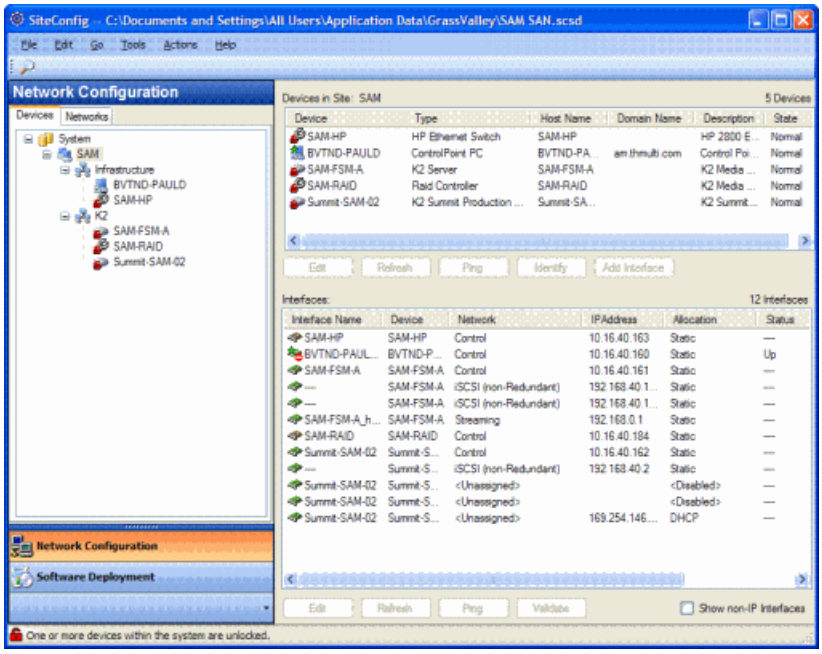
SiteConfig displays information from a system description file, which is an XML file.

Opening SiteConfig

1. Do one of the following: Use the SiteConfig shortcut on the Windows desktop or in the Start menu to open SiteConfig.
   - On the Windows desktop, click the **Grass Valley SiteConfig** shortcut. 
   - On the Windows **Start** menu, in the **Grass Valley** folder, click the **SiteConfig** shortcut. 
2. SiteConfig opens as follows:
   - If you have previously opened SiteConfig, the SiteConfig main window opens with the most recently used system description loaded.
   - If you have not previously used SiteConfig or if SiteConfig does not have access to a system description file, you are prompted to create a new system description or to import an existing system description.
3. Respond as appropriate.

SiteConfig main window

The SiteConfig main window is as follows:



The left side of the screen shows the tree view of the currently loaded system description. The Network Configuration and Software Deployment buttons at the bottom of the tree view activate either the network configuration workspace or the software deployment workspace.

The network configuration workspace on the left has two tabs: a Devices tab to display the tree of devices in the system and a Networks tab to show the hierarchy of networks defined in the system.

The software deployment workspace also has two tabs: a Devices tab that displays the same tree view of devices but provides information about the software roles assigned to the devices and the software currently installed on devices. The Deployment Groups tab provides the interface to manage software deployment tasks.

Select an item in the tree and the view on the right side of the screen shows details about the item selected. Select a site or group to show information about all the items that fall under the selected item.

Right-click an item to access a context menu of operations.

Icon overlays on items and tooltips provide status and warning feedback.

K2Config

The K2 System Configuration application (K2Config) is the primary tool for configuring systems in the category of a K2 SAN, which include online or production K2 SANs, K2 Nearline systems, and GV STRATUS Proxy Storage systems. Once the devices of the storage system are cabled and are communicating on the control network, you can do all the configuration required to create a working K2 SAN using the K2Config application. When you use SiteConfig for network configuration, you can import the SiteConfig system description file into the K2Config application to get you started with your SAN configuration.

After your K2 SAN is initially installed and configured, if you need to reconfigure the system you should do so using SiteConfig and the K2Config application. This enforces consistent policy and sequencing for configuration tasks, which makes the system easier to maintain and aids in troubleshooting should a problem arise.

The K2Config application runs on a control point PC and accesses the devices of the K2 SAN via the control network. You can configure the devices of the K2 SAN as follows:

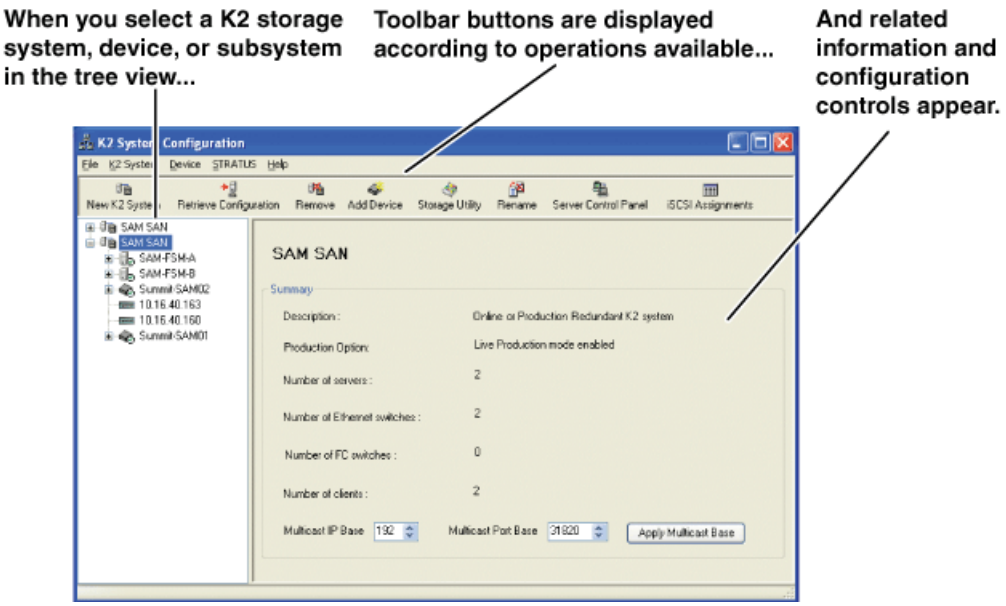
- SAN-attached K2/Summit systems and K2 Media Server — These devices are configured directly by the K2Config application.
- K2 RAID storage devices — The K2Config application launches a remote instance of Storage Utility, which configures RAID storage devices. Storage Utility components run on the K2 Media Server and the configuration actually takes place via the Fibre Channel connection between the K2 Media Server and the RAID storage device.
- Ethernet switches — The K2Config application can launch a switch's web-based configuration application.

You can expand and select nodes in the tree view to view K2 SANs, individual devices, and configuration settings. The configuration file is saved on the V: drive, along with the media files in the shared storage system. The configuration file is updated and saved whenever you change a configuration using the K2Config application. That is why you must always use the K2Config application to change settings on the storage system, so the most recently changed configurations will always be stored in the configuration file and displayed.

Opening the K2Config application

1. On the control point PC open the K2Config application shortcut on the desktop. The K2Config application log in dialog box opens.
2. Log in using the designated administrator account for configuring K2 SAN devices.

3. The K2Config application opens.



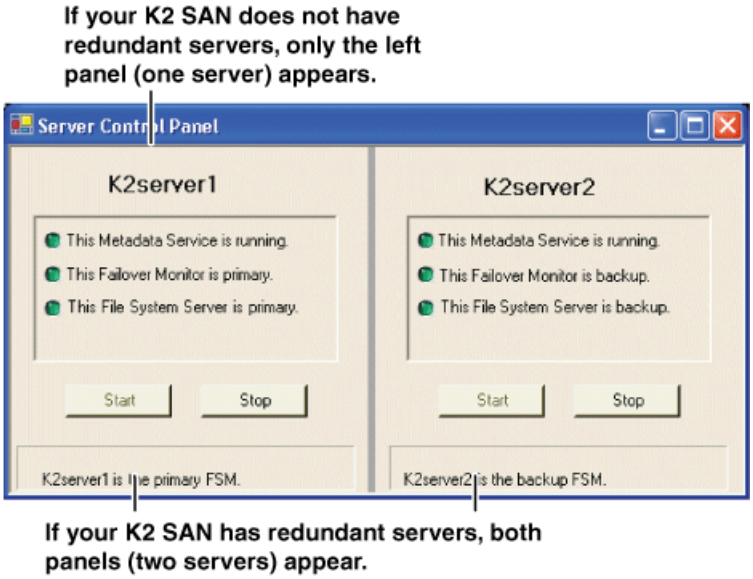
If you have one or more K2 SANs currently configured, the K2Config application displays the systems in the tree view.

If you have not yet configured a K2 SAN, the K2Config application opens with the tree view blank.

Server Control Panel

Server Control Panel allows you to monitor and control the current status of a K2 Media Server in its roles as the media file system server and the metadata server. This is especially useful for redundant K2 SANs, as you must know if a server is currently acting as primary or as backup before attempting any troubleshooting or service work.

Server Control Panel displays information about the metadata service and the media file system server primary/redundant roles.



NOTE: Do not click Stop or Start unless you intend to manually control the current primary/redundant roles. Using these buttons can trigger an automatic system recovery (failover) event.

To launch Server Control Panel, in the K2Config application, click the **Server Control Panel** button.

On the local K2 Media Server, you must log in with administrator-level privileges in order to use Server Control Panel.

Storage Utility for K2 SAN

There are two versions of Storage Utility:

- Storage Utility for the K2 SAN
- Storage Utility for stand-alone K2 systems

This section explains Storage Utility for the K2 SAN. Refer to the *K2 System Guide* to learn about Storage Utility for stand-alone K2 Solo 3G system.

NOTE: For shared storage, run Storage Utility only via the* K2Config *application.

The Storage Utility is your primary access to the media file system, the media database, and media disks of the K2 SAN for configuration, maintenance, and repair. It is launched from the K2Config application.

⚠ ***CAUTION: Use the Storage Utility only as directed by a documented procedure or by Grass Valley Support. If used improperly, the Storage Utility can render your K2 system inoperable or result in the loss of all your media.***

The Storage Utility's primary functionality is hosted by the K2 Media Server. The Storage Utility uses the Fibre Channel connection between the K2 Media Server and the RAID storage device for

access and configuration. When you launch Storage Utility from the K2Config application on the control point PC, you use a Storage Utility remote interface to control the main application as it runs on the K2 Media Server.

The Storage Utility requires that the storage system be in an offline operating mode before it allows any configuration to take place. Take your K2 SAN devices offline before configuring with Storage Utility. This means all media access operations are disabled while you are using the Storage Utility.

NOTE: Do not run Storage Utility as a stand-alone application, separate from the* K2Config *application. To maintain a valid K2 SAN all configuration must be controlled and tracked through the* K2Config *application.

NOTE: Do not use the MegaRAID utility on a K2 system. This utility is for use by qualified Grass Valley Service personnel only. When this utility is opened it scans the SCSI bus and interferes with record and play operations.

About RANKs and LUNs in Storage Utility

With Storage Utility you bind disks into a group. This group is a logical unit recognized by the Windows operating system, the media file system, and other software. A logical unit is called a LUN, which stands for Logical Unit Number. You can combine one or more LUNs into a group called a RANK.

Storage Utility for K2 SAN uses RANK to define the group. In contrast, Storage Utility for stand-alone K2 storage uses LUN to define the group.

The distinction between LUN and RANK is necessary because the maximum disk size recognized by some older Windows operating systems is relatively low, and in a K2 SAN with large capacity disks, a group of disks can exceed this maximum size. To solve the problem, Storage Utility binds disks as smaller size LUNs which can be recognized by the Windows operating system as a logical disk. Then multiple LUNs are combined into a RANK, as required to support the K2 SAN.

K2 software version 9.0 and higher takes advantage of recent Windows operating systems that have a much higher maximum disk size and are able to accommodate LUNs with large capacity disks. So for systems new with K2 software version 9.0 and higher, all binding of disks must be one LUN per RANK. However, for the purpose of expanding existing storage pools, binding multiple LUNs per RANK is still available.

In Storage Utility, there is no operational difference between what is currently labeled a RANK and what was previously labeled a LUN. The tasks you perform are identical. However, Storage Utility reports the number of LUNs in each RANK, which is useful information if you need to view disks from Windows operating system administrative tools.

In systems on which Storage Utility bound disks to fit the limitations of the older Windows operating systems, LUNs per RANK are as follows:

Drives	RAID 5	RAID 6
500 GB 7.2K	2 LUNs/RANK	1 LUN/RANK
600 GB 15K	4 LUNs/RANK	4 LUNs/RANK
1 TB 7.2K	4 LUNS/RANK	2 LUNS/RANK

Windows Remote Desktop Connection

You can use the Microsoft Windows Remote Desktop Connection application to make a remote connection to a Grass Valley system that runs the Windows operating system.

Take the following into consideration when connecting to K2 systems:

- Before you can use the Remote Desktop Connection, you need network access and permissions to connect to the K2 system.
- You can use either the name or the IP address to access the K2 system.
- Do not use the Remote Desktop Connection to access the PC running the Control Point software or to access the AppCenter application; results may be unreliable.
- Take care when accessing an online K2 system on which media access is underway. The additional load on network and system resources could cause unpredictable results.
- Lack of robust video/graphic support can cause video display problems. Remote desktop connections can interrupt proxy and live streaming. AppCenter video monitoring is not supported through Remote Desktop Connection.

Accessing Remote Desktop Connection

1. Do one of the following:
   - Click the **Start** button on the Windows task bar
   - Press the Windows key on the keyboard.
2. Select **Programs | Accessories | Communications | Remote Desktop Connection**.
   The Remote Desktop dialog box opens.
3. Enter the name or IP address of the system to which you are making the remote connection and click **Connect**.

Grass Valley Recommended Deployment and Monitoring Solutions

To maximize up-time, a maintenance strategy must provide the ability to easily identify the root cause of an unanticipated hardware or software failure and to quickly compile failure data. The ability to proactively predict failures and to quickly notify those who can rectify them makes the maintenance strategy even more powerful. Grass Valley has a long history of building the necessary functionality into critical broadcast products. Beginning with Grass Valley's longstanding monitoring application NetCentral and progressing to the next generation tool GV GUARDIAN, remote monitoring and proactive predictive failure analysis are important contributors to Grass Valley system solutions. Both NetCentral and GV GUARDIAN run on commercial off-the-shelf server PCs, such as the K2 system control point PC. Grass Valley and 3rd party devices report status via Window Messaging, Simple Network Management Protocol (SNMP), or syslog to the NetCentral or GV GUARDIAN application. Each application provides easy to use, fully autonomous remote monitoring to predict errors, provide proactive notifications, and centrally consolidate error logs and hardware failure information. Grass Valley recommends using a remote monitoring tool like NetCentral or GV GUARDIAN. With NetCentral, and even more so with GV GUARDIAN, you can maximize your up-time with less manpower, as compared to manual system monitoring. Watching for indicator lights, physically scanning logs, and other manual monitoring is far more time

consuming, more error-prone, and much less accurate. If you have an existing NetCentral installation you install a NetCentral device provider on the NetCentral server PC for each type of device you are monitoring. Refer to NetCentral product documentation for installation and operating instructions. With GV GUARDIAN, only SNMP MIBs are required. Separate device providers are not necessary. Refer to the on-line GV GUARDIAN Topic Library for information.

Administering and maintaining the K2 SAN

Passwords and security on Grass Valley systems

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

The following table shows the different types of users and their privileges. Passwords are case sensitive.

	Windows administrator	Grass Valley product administrator	K2 product administrator	Grass Valley product user
User name	Administrator	GVAdmin	K2Admin	GVUser
Password	adminGV!	adminGV!	adminK2	userGV!
AppCenter Configuration Manager	Full access	Full access	Full access	Can view
AppCenter	Full access	Full access	Full access	Full access; requires an account on the K2 Summit/Solo system
Storage Utility	Full access	Full access	Full access	Can’t access
K2Config	Full access	Full access	Full access	Can’t access
Server Control Panel	Full access	Full access	Can view	Can view
Windows Operating System	Full access	Full access	Limited access (based on Windows user account privileges).	Limited access (based on Windows user account privileges)

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

About application security on the K2 SAN

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

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

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

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

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

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

About credentials in SiteConfig

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

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

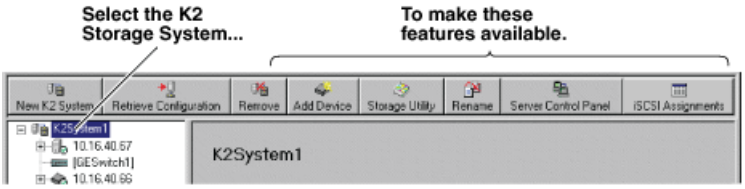
It is possible to also override the default credentials for a single device.

Modifying K2 SAN settings

Use the topics in this section when changing or viewing settings on an existing K2 SAN. These are the settings that define the K2 SAN.

Accessing K2 SAN features

In the K2Config, use the following features to K2 SAN settings:



About SiteConfig and K2Config settings

Many settings and operations, such as network settings, adding/removing devices, and software versions, are managed by both the SiteConfig application and the K2Config application. Each application has its own XML file in which information is stored. You can keep the applications in synch by using an orderly task flow as you configure the K2 SAN.

When doing initial installation and configuration tasks, you can export/import system information from one application's XML file to the other application's XML file. You can also merge from K2Config into an existing SiteConfig system description. These export/import/merge features support a one-time process in which a system as described in the XML file of one application is imported into the XML file in the other application. The target XML must not already contain the system being imported.

When you change a setting in one application, it is not automatically updated directly in the other application. The applications do not communicate dynamically with one another. However, both applications can read settings as currently configured on the actual physical device and update their XML file accordingly. This is the method you must use to keep the applications in synch.

When you change a setting that is managed by both applications, you should change it first in SiteConfig, as a general rule. This application gives you the best context for the system as a whole and provides features to identify and verify changes. Once the change is implemented on the actual physical device, you must then open the relevant page in the K2Config application. This causes the K2Config application to refresh its settings from the device and write the change to its XML file. It also allows you to verify your change within the context of the K2Config application.

The following table summarizes operations that involve interaction between SiteConfig and K2Config.

Operation	Task flow context and policies	Additional information
Import SiteConfig system description file into K2Config	Use this operation for initial install/commission (greenfield) sites. First define the site topology using SiteConfig and complete network configuration and software deployment. Then import the SiteConfig system description into K2Config and complete the K2 SAN configuration.	This operation creates a K2 SAN in K2Config with SiteConfig defined devices. Uses the site name to check if the K2 SAN already exists. The operation will not import if the K2 SAN exists with the same name. The operation can import all sites which are K2 SANs from a single system description file in a single import step.
Import K2Config XML into SiteConfig	Use this operation when you're running SiteConfig for the first time at a site with existing K2 SANs that have already been configured with K2Config. This allows you to seed the SiteConfig system description with device information that is already in the K2Config XML file. After you have done this operation for the first time, do not do it again.	This operation creates a SiteConfig site with K2Config defined devices. The operation removes all other sites.
Merge K2Config XML into SiteConfig system description	Use this operation when you've already defined some sites using SiteConfig and you later want to bring in another K2Config defined K2 SAN that doesn't exist in SiteConfig. Do not merge a K2Config XML that you've already merged. If you do so, it is likely that SiteConfig will create a new site with the same devices.	This operation creates a SiteConfig site with K2Config defined devices but leaves existing sites as is.
Rename Site\SAN	Rename first in SiteConfig. Then rename in K2Config. Do not import\merge into SiteConfig or K2Config.	—
Remove Site\SAN	Remove first in SiteConfig. Then remove in K2Config. Do not import\merge into SiteConfig or K2Config.	—
Remove device	Remove from both SiteConfig and K2Config.	—
Add device	Add in SiteConfig first, do network configuration and software deployment. Then, add in K2Config and configure using K2Config.	—
Create a new site\SAN	Use SiteConfig to create site, add devices, configure network and deploy software, then import into K2Config and configure each device	—
Change hostname	Perform hostname change using SiteConfig. Remove and re-add to K2Config. If changing the hostname of a media file system/metadata K2 Media Server, re-configure all clients on the K2 SAN using K2Config	—

Operation	Task flow context and policies	Additional information
Change IP address (except address of TOE on K2 Media Server)	Use SiteConfig for IP address changes. Then in K2Config, click on the changed device's network configuration node. This refreshes the K2Config view of IPs from the device.	—
Change IP address of TOE on K2 Media Server	For TOE IP changes and/or TOE card removal, use K2Config.	—
Modify K2 SAN redundancy - redundant to non-redundant or vice versa	Use SiteConfig to recreate the site using the appropriate redundancy models and configure network and deploy software. Remove K2 SAN from K2Config. Import site into K2Config. Configure using K2Config.	—

About Control Panel, SiteConfig, and K2Config settings

During system commissioning or system reconfiguration, the SiteConfig and K2Config applications are first used to set up or modify K2 SAN and network configurations. The GV STRATUS Control Panel application is then used to complete the setup of the GV STRATUS system-wide workflow components.

The GV STRATUS Control Panel application imports the configuration information and populates the GV STRATUS view of the available K2 systems. For example, information about K2 SANs comes from K2Config while information about standalone K2 Summit systems comes from SiteConfig. The information transfer is uni-directional, where the GV STRATUS Control Panel application imports the SiteConfig/K2Config generated configurations.

Use of the GV STRATUS Control Panel application requires the GV STRATUS Core server to be running. If, during maintenance or commissioning, SiteConfig and K2Config are used to setup or modify systems while the GV STRATUS Core server is turned off, it is important to synchronize K2Config information to GV STRATUS Control Panel before attempting to use the GV STRATUS Control Panel application.

NOTE: While the* GV STRATUS Control Panel *application allows you to enter device names and other values as free-form text, it is not recommended for use at customer sites as manual entry can result in text errors.

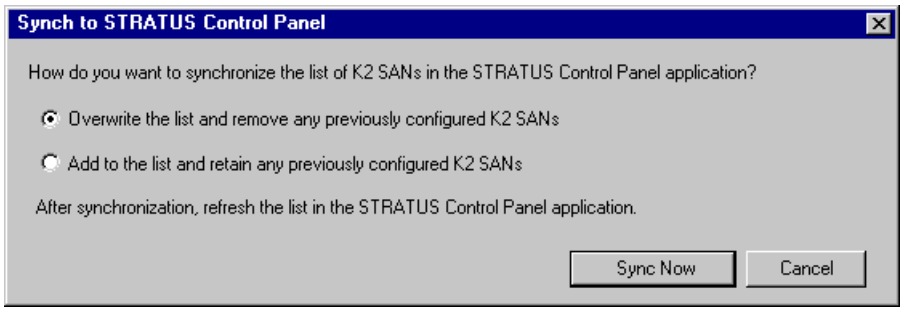
Synchronizing K2Config information to GV STRATUS Control Panel

The K2Config application writes its configuration file to the GV STRATUS server that hosts the Control Panel Service. Typically this is the GV STRATUS Core server. If the Control Panel Service is running, the K2Config application automatically does this whenever you change K2 SAN information. In most cases, this automatic operation should be sufficient. For example, when you add or remove a K2 SAN, the K2Config application adds or removes that K2 SAN in the configuration file that is on the Control Panel Service host. If the configuration file does not already exist on the Control Panel Service host, the file is created. If the file already exists, the K2 SAN is added or remove in the configuration file, but any information in the configuration file about other K2 SANs is not removed or modified.

However, if a situation arises in which you want to purge the information in the configuration file or otherwise control the rules for writing the K2Config information to the Control Panel Service host, you can do so as explained in this topic.

1. Make sure the GV STRATUS Core server is running.
2. Open the K2Config application.
3. In the K2Config application click **STRATUS | Network Configuration** and verify that the machine that hosts the Control Panel Service is correctly configured. Typically this is the GV STRATUS Core server.
4. Click **STRATUS | Sync to Control Panel**.

   The Synch to STRATUS Control Panel dialog box opens.



5. Select the synchronization option as follows:

   - Overwrite the list... — This overwrites the K2Config configuration file currently on the Control Panel Service host. Any K2 SAN information currently in the file is lost and replaced by the K2 SAN information currently in K2Config. Take care when selecting this option, especially if you previously configured a K2 SAN from a different instance of K2Config. This practice is not recommended, but if you are doing this, you could lose the information from that other K2Config instance.
   - Add to the list... — This is the same action that K2Config does automatically when you add a K2 SAN. The SAN's information is written to the configuration file on the Control Panel Service host, replacing any information for that same K2 SAN that is already in the configuration file. By selecting this option, you are triggering the same operation that would take place if you removed a K2 SAN from K2Config and then added the SAN back to K2Config.

6. Click **Sync Now** to write the K2 SAN information to the K2Config file on the Control Panel Service host.
7. Close the K2Config application.
8. Open the GV STRATUS Control Panel application and click **Core | K2 Storage | K2 SAN Storage.**

   K2 SAN Storage settings open.

9. Click **Refresh**.

   The Control Panel application reads the information from its local K2Config file and updates the list of K2 SANs.

Renaming a K2 SAN

- 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 are not required to be offline, and a restart of devices is not required.

1. In the K2 System Configuration application tree view, select the current name of the K2 SAN, which is the top node of the storage system tree.
2. Click **Rename**. The Rename dialog box opens.
3. Enter the new name of the SAN and click **Apply**.
4. If the SAN name is used similarly in SiteConfig, make the appropriate change in SiteConfig.

Adding devices to a K2 SAN

Refer to the topics in this section to add devices to an existing K2 SAN.

Adding a generic client device

- You must be logged in to the K2Config application with permissions equivalent to K2 administrator or higher.
- The devices of the K2 SAN are not required to be offline, and a restart of devices is not required.

1. In SiteConfig, add the client device to the appropriate group and verify that it is communicating correctly on networks.
2. In the K2Config application tree view, select the name of the K2 SAN, which is the top node of the storage system tree.
3. Click **Add Device**. The Add Device dialog box opens.
4. Select the type of client you are adding.
5. Click **OK**. The new client appears in the tree view.
6. Configure the client as appropriate. Refer to the documentation for the device.

   Enter the RVIO value as provided by Grass Valley. Do not attempt to calculate the RVIO value on your own.

   When configuring editors on a K2 SAN with 1 Gig TOEs, do not assign editors and K2 clients (K2 Summit or K2 Media Client) to the same TOE. Instead, assign editors to their own TOE.

Adding an Ethernet switch

- 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 SiteConfig, add the switch to the appropriate group.
2. 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.
3. Click **Add Device**. The Add Device dialog box opens.
4. Select **Ethernet Switch**.
5. Click **OK**. The new switch appears in the tree view.

6. Configure the switch as appropriate.

Adding a K2 Media Server

With online and production K2 SANs, the K2Config application enforces the number of K2 Media Servers, as pre-defined for the system. The application does not allow you to add K2 Media Servers. Refer to the installation chapter for each type of SAN for more information.

For all system levels and designs, adding a K2 Media Server with the role of media file system/metadata server to an existing K2 SAN is not supported as a customer procedure. Adding a server with these roles fundamentally changes the baseline design of the system, which means you must dismantle one or more pieces of the existing system and create a new system. This requires custom design and implementation services that should only be attempted by qualified Grass Valley personnel.

On some K2 SANs, the system design supports adding an optional NH K2 Media Server, as follows:

1. If you have not already done so, in SiteConfig, add the server to the appropriate group and verify that it is communicating correctly on networks.
2. In the K2Config application tree view, select the name of the K2 SAN, which is the top node of the storage system tree.
3. Click **Add Device**. The Add Device dialog box opens.
4. Select **K2 Media Server**.
5. Click **OK**. The new server appears in the tree view.

Next, configure the server as instructed in the installation chapter for the level of the K2 SAN.

Removing a K2 SAN

- You must be logged in to the K2Config application with permissions equivalent to GV administrator or higher.
- For ongoing maintenance and support, you must always have at least one control point from which you can access the K2 SAN with the SiteConfig application and with the K2Config application. If you have installations of these applications on multiple control point PCs, do not remove the K2 SAN from all control point PCs at the same time.

The K2 SAN can continue operations while it is removed from the K2Config application. As long as you are removing only the complete K2 SAN and not removing any individual devices, there is no need to put devices offline or restart devices.

1. In the SiteConfig application, remove the devices of the K2 SAN.
2. In the K2Config application tree view, select the name of the K2 SAN, which is the top node of the storage system tree.
3. Click **Remove**. The SAN is removed from the tree view.

Accessing a K2 SAN from multiple PCs

It is recommended that you install the SiteConfig application and the K2 System Configuration (K2Config) application on one PC only in your facility. This eliminates potential problems in the installation, configuration, and maintenance of your K2 SAN.

If you run SiteConfig and/or the K2Config application on multiple PCs in your facility, you must enforce an operational policy whereby you constrain your use of the applications as follows:

- Designate a control point PC as the configuration PC and then make changes from that PC only.
- On the other control point PCs, limit operations to view-only when accessing the K2 SAN. Do not make changes. With the K2Config application there is some basic protection, in that the first instance of the application in essence "locks out" any other instances. However, SiteConfig has no such protection and making changes on devices from multiple SiteConfig instances can result in configuration and software deployment errors.

SiteConfig has no features that are designed to support access from multiple instances. If you access systems from multiple instances of SiteConfig, you must define and enforce your own policy. For example, you can import system descriptions or otherwise create systems and discover devices in each instance of SiteConfig and then enforce policy whereby instances are kept in synch.

1. Install Control Point software on the designated K2Config control point PC and complete the initial system configuration. Close the K2Config application on that PC.
2. Install Control Point software on another control point PC and open the K2Config application.
3. Select **Retrieve Configuration** and enter the name or IP address of the K2 Media Server for the K2 SAN. If the K2 SAN has multiple K2 Media Servers, you must enter the name or IP address of the server configured first.

   If there is another instance of the K2Config application on a different control point PC currently accessing the K2 SAN, a message informs you of this and you are not allowed to access the system.

   If access is allowed, a Retrieving Configuration message box shows progress. It can take over 30 seconds to retrieve the configuration. When the configuration is retrieved, the K2 SAN appears in the tree view. Make sure that you only attempt view-only operations from this PC. Do not configure the K2 SAN from this PC.
4. Repeat the previous steps for other control point PCs from which you need access to the K2 SAN.

When you expand and select nodes in the tree view to view K2 SANs, individual devices, and configuration settings, the K2Config application displays information as found in a configuration file, rather than continuously polling devices to get their latest information. The configuration file is saved on the V: drive, along with the media files in the shared storage system. When you use the Retrieve Configuration feature, you are connecting to the configuration file.

Taking a K2 SAN offline

1. Stop all media access.
2. Shut down all K2 clients and all generic clients. You can do this via SiteConfig.
3. Take all K2 Media Servers out of service.

   If you have redundant servers, make sure that you know which server is the current primary and which server is the current backup, and that you take primary/backup servers out of service in the proper order.

Bringing a K2 SAN online

1. Verify that RAID storage devices, Ethernet switches, and other supporting system are powered up. Refer to the section earlier in this manual for power on procedures.
2. If K2 Media Servers are powered down, power them up. Refer to the section earlier in this manual for power on procedures.
3. Place K2 Media servers in service.

   If you have redundant servers, make sure that you place primary/backup servers in service in the proper order.
4. Power on all K2 clients and all generic clients.

Viewing iSCSI assignments

You can review a report of clients and their iSCSI configuration on a K2 SAN as follows:

1. In the K2Config application tree view, select the name of the K2 SAN, which is the top node of the storage system tree.
2. Click **iSCSI Assignments**.

   The iSCSI Port Assignments report opens.

   The report displays the following information.

   - K2 Media Servers with the role of iSCSI bridge
   - Each server's iSCSI ports, identified by IP address
   - For each iSCSI port, the iSCSI clients assigned and their bandwidth subscription.

Using reference files

When you create a simple K2 clip on a K2 system, K2 software can create a corresponding reference file. The reference file is stored in a directory in the clip's folder on the V: drive. You can configure the software to create QuickTime reference files or no reference files. The following topics provide information about reference files on K2 systems.

About QuickTime reference files

The following formats are supported as QuickTime reference files:

- DV
- AVC-Intra
- XDCAM-EX
- XDCAM-HD
- XDCAM-HD 422
- IMX
- Avid DNxHD

The K2 clip must be a simple clip in order to create the reference file. With the QuickTime reference file you can open the K2 clip with QuickTime tools, such as Final Cut Pro, for playback and editing. For some formats the QuickTime tool does not provide default support, so you must configure the

tool as necessary to support the format. The QuickTime tool must be run on another system. Running the QuickTime player or other QuickTime tools on the K2 system is not supported. You have options for connections, access, and software to support your workflow requirements.

Configuring reference file type on a K2 SAN system

1. In the K2Config application, for the K2 Media Server with role of file system server, access the File System Server Configuration page as follows:
   - On a SAN that is already configured, in the tree view click **File System Server**.
   - On a SAN that is not yet fully configured, work through the Configure K2 Server wizard until you reach the File System Server Configuration page.
2. On the File System Server Configuration page select one of the following:
   - No reference file — K2 software does not create reference files.
   - QuickTime reference file — K2 software creates QuickTime reference files.
3. Click **Check** to apply the setting.
4. Manage the required K2 Media Server restart as follows:
   - On a SAN that is already configured, you must restart the K2 Media Server to put the change into effect. Follow the restart procedure appropriate for the basic or redundant K2 SAN.
   - On a SAN that is not yet fully configured, continue to work through the Configure K2 Server wizard. The restart at the end of the configuration process is sufficient.

If a redundant K2 SAN, you must configure similarly and restart both K2 Media Servers with role of file system server.

Managing redundancy on a K2 SAN

If you have a redundant K2 SAN, use the procedures in this section to control the primary/redundant roles of the K2 Media Servers.

Identifying current primary/backup K2 Media Servers

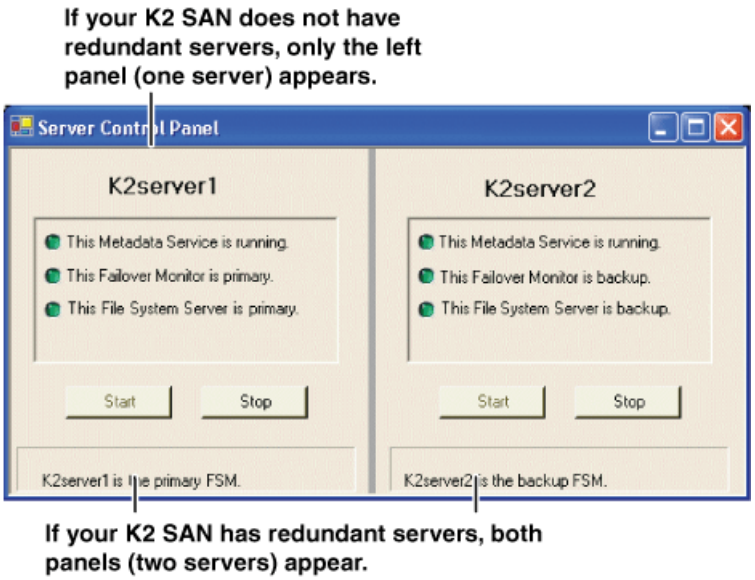
Before attempting any configuration or service work on a redundant K2 Media Server, you must know if the server is the current primary server or the current backup server for the media file system and the metadata service. While most configuration and service work can be accomplished on a backup server without affecting the operation of the SAN, if you attempt configuration or service work on the operating primary server, it will likely result in record/play failures and/or a loss of media.

To identify the current primary/backup K2 Media Server, use one or more of the methods described in the following procedures.

Identifying primary/backup from the K2Config application

1. In the tree view, select the name of the K2 SAN, which is the top node of the storage system tree.

2. Click the **Server Control Panel** button. The Server Control Panel opens.



3. Identify the primary K2 Media Server and the backup K2 Media Server.

   If the K2 SAN does not have redundant servers, only one server (the left half of the Server Control Panel) is displayed.

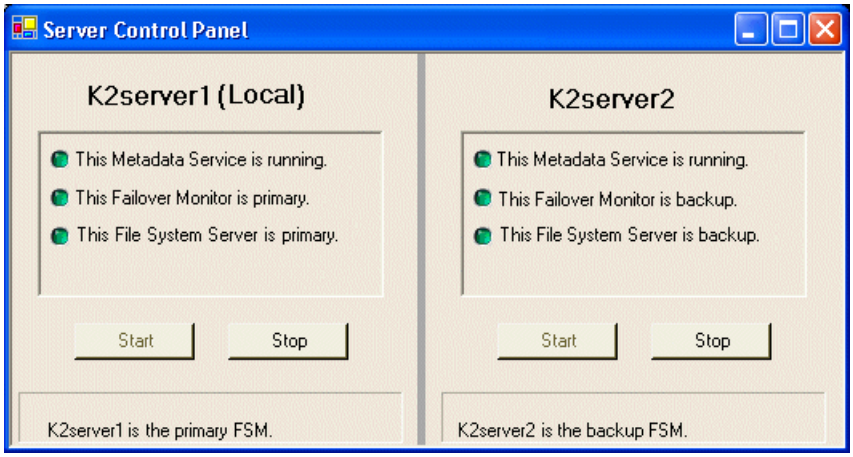
   For Nearline K2 SANs, the Server Control Panel is not available from the K2Config application.

Identifying primary/backup from the local K2 Media Server

The following procedure assumes that you are at the local K2 Media Server and you need to check its status in its role of media file system/metadata server, especially regarding redundancy. The recommended mode for local operation of a K2 Media Server is to use a connected keyboard, monitor, and mouse. You can also use Windows Remote Desktop Connection from a network-connected PC to access the Windows desktop for "local" operation, but this is not recommended if the system is currently online with media access underway. The additional load on network and local system resources could cause unpredictable results.

1. If you have not already done so, connect keyboard, monitor, and mouse to the K2 Media Server and log on to Windows.
2. If Server Control Panel is not already open, on the Windows desktop, click **Start | Grass Valley | Server Control Panel**.

3. Log on to Server Control panel with administrator-level permissions. The Server Control Panel opens.



4. Determine if the local machine is currently the primary K2 Media Server or the backup K2 Media Server.

   If the K2 SAN does not have redundant servers, only one server (the left half of the Server Control Panel) is displayed.

   For the K2 Media Servers of a Nearline K2 SAN, Server Control Panel on the local K2 Media Server reports if the server is the current active media file system (SNFS) server. No metadata information is displayed, since the Nearline system does not have a media database.

Triggering an intentional failover

⚠ ***WARNING: Do not attempt this procedure except under the supervision of qualified Grass Valley personnel.***

The following procedure renders the primary K2 Media Server unqualified to carry out its role in managing the K2 SAN. The backup K2 Media Server detects this condition and triggers a failover in which it takes the primary server out of service and takes control of the K2 SAN. Therefore, before using these procedures, verify that the backup K2 Media Server is fully operational and qualified to take control of the K2 SAN. Be aware that the failover capabilities of the -K2 SAN are degraded until you place the machine back into service as the backup K2 Media Server.

You should stop all media access before attempting this procedure. If media access is underway, there will be period of time in which media loss will occur.

In the following procedures, K2server1 and K2server2 represent your redundant K2 Media Servers. The procedure begins with K2server1 acting as the primary K2 Media Server.

1. Verify primary/backup roles and make sure K2server2 (the backup) is qualified and ready to become primary.
2. From the K2Config application, open **Server Control Panel**.
3. In Server Control Panel for K2server1 click **Stop**. This triggers the failover process.

   K2server1 shuts down. K2server2 detects (via the absence of the heartbeat signal on the serial cable) that K2server1 is gone, so K2server2 takes over as primary.

4. Allow the failover process to complete, until K2server2 is operating correctly in its new role as the primary K2 Media Server for the K2 SAN.
5. Verify K2server2 as primary.
6. Start up K2server1. It is now out of service. If you need to do service work on K2server1, you can do it now. After your work is complete, proceed with the next step.
7. If there are K2 Media Servers with role of iSCSI bridge or Fibre Channel switches on the same redundant "side" as K2server1, start or restart them.
8. In Server Control Panel, for K2server1, click **Start**. This notifies K2server2 (via a heartbeat signal on the serial cable) that K2server1 is coming online as backup.
9. Verify K2server1 as backup.
10. All failover processes are complete. All media management mechanisms are now running and K2server1 is now qualified and acting as the backup.

Recovering from a failover

⚠ ***WARNING: Do not attempt this procedure except under the supervision of qualified Grass Valley personnel.***

In the following procedures, K2server1 and K2server2 represent your redundant K2 Media Servers. The procedure begins with K2server1 being the server on the failed side of the SAN. K2server2 is acting as the primary K2 Media Server.

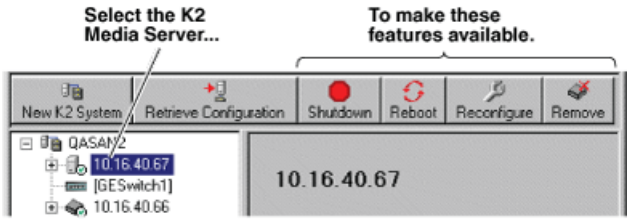
1. Verify primary/backup roles and make sure K2server2 is the primary.
2. Start up K2server1. It is now out of service.
3. Determine the cause of the failover and take corrective action as necessary. If you need to do service work on K2server1 or other devices on the failed side of the SAN, you can do it now. After your work is complete, proceed with the next step.
4. If there are K2 Media Servers with role of iSCSI bridge, Ethernet switches, or Fibre Channel switches on the same redundant "side" as K2server1, start or restart them. Make sure they have been started up at least once before putting K2server1 into service.
5. In Server Control Panel, for K2server1, click **Start**. This notifies K2server2 (via a heartbeat signal on the serial cable) that K2server1 is coming online as backup.
6. Verify K2server1 as backup.
7. All failover processes are complete. All media management mechanisms are now running and K2server1 is now qualified and acting as the backup.

Working with K2 Media Servers

Use the procedures in this section when doing configuration or service work on a K2 Media Server that is part of an operational K2 SAN.

Accessing K2 Media Server features in the K2Config application

In the K2 System Configuration (K2Config) application , features for working on a K2 Media Server are as follows:



Taking a K2 Media Server out of service

This procedure applies to K2 Media Servers that are taking the role of media file system and metadata server.

When you take a K2 Media Server out of service you stop services such that the K2 Media Server is prevented from functioning as a media file system and/or metadata server. In this state no media operations can take place.

If there is just one K2 Media Server in the role of media file system and metadata server, before you take the K2 Media Server out of service, you should stop all media access on the K2 SAN.

If there are redundant K2 Media Servers currently in service (both primary and backup) in the role of media file system and metadata server, take only the backup out of service. Do not take the primary out of service. If you take the primary out of service it will trigger a failover event. If the K2 Media Server that you want to take out of service is currently the primary, you have the following options:

- Make the current primary K2 Media Server the backup in an orderly fashion by triggering an intentional failover. Then, when the K2 Media Server is the backup, you can take it out of service.
- Take the current backup out of service (shutdown) so that the primary K2 Media Server is the only file system/metadata server currently in service. You can then take the primary K2 Media Server out of service without triggering a failover event.

1. Stop all media access on the K2 SAN.
2. In the K2Config application tree view, select the K2 SAN.
3. Select **Server Control Panel**. The Server Control Panel opens.
4. Identify the K2 Media Server you intend to take out of service. If there are redundant K2 Media Servers, consider that you might trigger a failover event.

   Use the Stop button in Server Control Panel as appropriate for the action that you want to take.
5. When you are sure that you understand the implications of taking the K2 Media Server out of service, click the **Stop** button for that server.
6. Proceed as follows:

   - If the server shuts down automatically, allow the shutdown processes to complete. Then start the server. When a redundant server restarts, it comes up in an out of service state.
   - If the server continues to run, it is in an out of service state.

Using the Stop button in Server Control Panel

In Server Control Panel, the following behaviors occur when using the Stop button.

On a system with this configuration of media file system/metadata K2 Media Servers…	With server(s) in this state…	When you click the Stop button on this server…	The following behavior occurs.
Redundant servers	Both primary and backup are in service (online)	Primary	The server automatically powers itself down. This causes a failover event to occur and the backup server becomes primary. When you restart the former primary server, it comes up out of service.
		Backup	The server automatically powers itself down. When you restart the server, it comes up out of service.
Redundant servers	Only the primary is in service. The other server is either shut down or it is powered on but out of service.	Primary	The media file system services stop, but the server continues to run. It does not automatically shut down. The server is now out of service.
One (non-redundant) server	The server is in service	Primary (the only server)	The media file system services stop, but the server continues to run. It does not automatically shut down. The server is now out of service.

For Nearline K2 SANs, the Server Control Panel is not available from the K2Config application.

Placing a K2 Media Server in service

This procedure applies to K2 Media Servers that have the role of media file system and metadata server.

When you put a K2 Media Server in service it is capable of taking the role of media file system and metadata server.

1. In the K2 System Configuration application tree view, select the K2 SAN.
2. Select **Server Control Panel**. The Server Control Panel opens.
3. For the K2 Media Server that you want to place in service, click the **Start** button.

Shutting down or restarting a K2 Media Server

- To shut down or restart a K2 Media server that is in the role of media file system and metadata server, first put the server out of service, as explained in the procedures earlier in this section. Then you can shut down or restart the K2 Media Server.

- To shut down or restart a K2 Media server that is not in the role of media file system and metadata server, consider that the K2 Media Server can host the iSCSI interface adapters (TOEs) by which clients access the shared storage. You should stop all media access before shutting down or restarting any K2 Media Server that hosts an iSCSI interface adapter.

Identifying K2 Media Server software versions

Use one or more of the following options to identify K2 Media Server software versions:

- In the K2Config application tree view, open the node for the K2 Media Server. This exposes the nodes for individual configuration pages. Select the **Software** configuration page to view software version information. To check for recent changes in software, click the **Check** button.
- Use SiteConfig software deployment features.

Modifying K2 Media Server network settings

Read the following sections for considerations and procedures for modifying network settings on a K2 Media Server.

Whenever you modify control network settings or FTP/streaming network settings on any device, you must then redeploy the hosts file if that is your name resolution mechanism.

Modifying K2 Media Server control network settings

If the K2 Media Server takes the role of media file system and metadata server, modifying its control network settings on an existing K2 SAN is not supported as a customer procedure. This is because the network identity of the K2 Media Server is embedded throughout the K2 SAN. To reconfigure this network identity, you must reconfigure the entire system from the start. Contact your Grass Valley representative for assistance.

Modifying K2 Media Server FTP network settings

You can modify the FTP network settings using SiteConfig without directly affecting the media file system or metadata service. However, you must be aware of the requirements of your site's FTP, file transfer, and streaming system design, as the FTP network settings will likely need to be changed elsewhere.

After modifying FTP network settings using SiteConfig, open the Network Configuration page in the K2Config application. The settings should automatically update. Verify that the settings are correct.

Modifying K2 Media Server media network settings

Use this procedure if you must change the IP address assigned to an iSCSI interface board on a K2 Media Server. This should not be necessary for a normally operating system and in fact it should be avoided if possible.

1. Put all the devices of the K2 SAN in an offline or out of service state. Refer to the appropriate procedures in this chapter.
2. Open the K2 System Configuration (K2Config) application on the control point PC.
3. In K2Config, make sure you know the load balancing bandwidth parameters for each of the iSCSI clients, as you must re-enter these values later in this procedure.

4. In K2Config, remove all iSCSI clients from the K2 SAN. To do this, select each iSCSI client and click **Remove**.
5. Use SiteConfig to change the IP address. Make sure that the IP address is within the range designated for the network.
6. Restart the K2 Media Server.
7. In the K2Config tree view, expand the node for the media server that has the iSCSI interface adapter for which you need to change the IP address and click the **iSCSI Bridge** node. The iSCSI Bridge Server configuration page opens.
8. In K2Config, identify the iSCSI adapter for which you are changing the IP address. Since you changed it in SiteConfig, K2Config should now display the new IP address.
9. In K2Config, add each iSCSI client again and reconfigure. Make sure you add them in the correct order (highest bandwidth first) and enter the same bandwidth values (load balancing) for each client as the values originally configured.
10. Place the devices of the K2 SAN back online.

Configuring Server 2008 for domain

This topic applies to Grass Valley servers with a base disk image created prior to mid-2011. Server disk images created after that time do not require this special configuration.

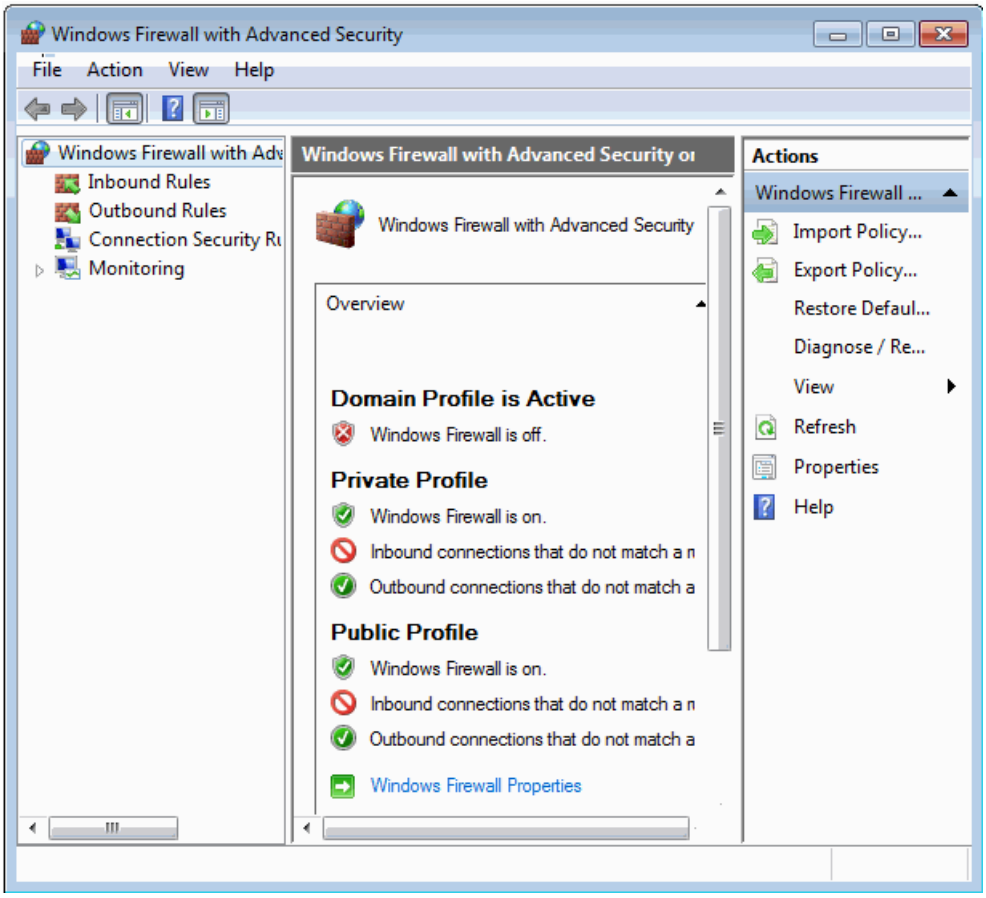
Systems with the Microsoft Windows Server 2008 R2 operating system require special configuration. A server must have its firewall disabled for proper K2 system operation. This includes the Windows firewall that has different profiles for workgroup, domain, etc. You must do the following steps to disable the firewall.

1. Log in to the server with Windows administrator privileges.

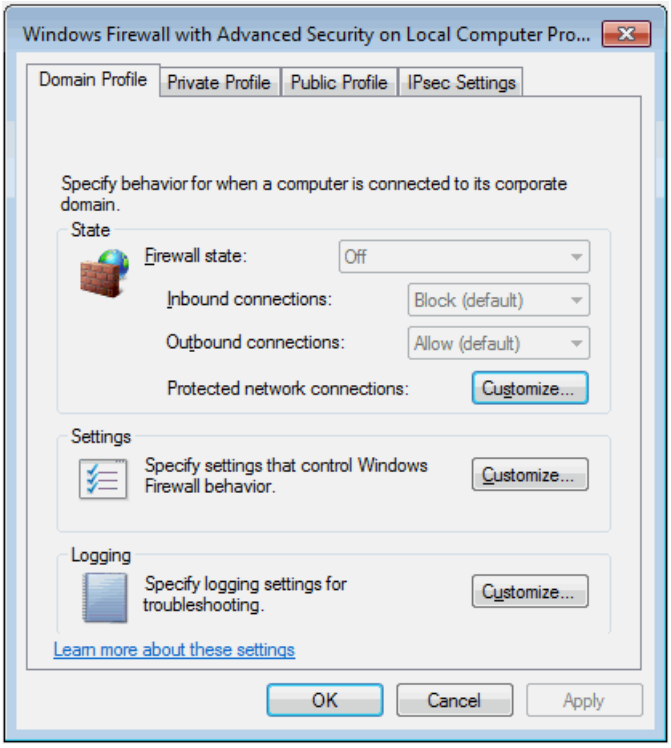
2. From the Windows desktop click **Start** and in the **Search programs and files** box type the following and then press **Enter**.

   ```
   wf.msc
   ```

   The Windows Firewall with Advanced Security window opens.



3. At the bottom of the Overview section, click **Windows Firewall Properties**.
   The Properties dialog box opens.



4. On the **Domain Profile** tab, set **Firewall state** to **Off**.
5. On the **Private Profile** tab, set **Firewall state** to **Off**.
6. On the **Public Profile** tab, set **Firewall state** to **Off**.
7. Click **OK** to save settings and close.

Restoring network configuration

When you restore a system from its system specific image, network configuration is also restored to the factory default settings. This is the recommended method of restoring network configuration. However, if for some other reason you must configure network settings manually, use the tasks in this section to restore the default network configuration.

Verify adapter names

1. If not already open, open Network Connections as follows:
   a) Open the Windows **Network and Sharing Center** control panel.
   b) Click **Change Adapter Settings**.
      Network Connections opens.
2. In Network Connections, click **View | Details**.

3. Verify adapter names.
   - On a Dell R620 or R610 system with four 1 Gig adapters only, the required names are specified as follows:

Adapter name
Control Connection
FTP-Streaming Connection
Unused Connection 1
Unused Connection 2

   - On a Dell R620 system with two 1 Gig adapters and two 10 Gig adapters, the required adapter names are specified as follows:

Adapter name
Control Connection
Unused Connection 1
FTP-Streaming Connection
Unused Connection 2

   - On a Dell R610 system with a 10 Gig network interface card installed, the required adapter names are specified as follows:

Adapter name
Control Connection
Unused Connection 0
Unused Connection 1
Unused Connection 2
FTP 10G Connection

     The 10 Gig network interface adapter is named `FTP 10G Connection`. If it has dual-ports, the other connection is named `Unused Connection 3 10G`.

4. Proceed as follows:
   - If all the names on this system are configured correctly to locations, skip the rest of this procedure.
   - If names on this system are not configured correctly, for each adapter name incorrectly configured, complete the remaining steps of this procedure.
5. Select the name in the Name column.
6. Select **File | Rename** to enter rename mode.
7. Type the name required.

Next, reorder adapters.

Reorder adapters

- Adapters must be named correctly
- The control team must be created
- The team and loopback must be named

1. If not already open, open Network Connections as follows:
   a) Open the Windows **Network and Sharing Center** control panel.
   b) Click **Change Adapter Settings**.
   Network Connections opens.
2. Select **Advanced**, then **Advanced Settings...**
3. On the **Adapters and Bindings** tab, order adapters as follows:
   - On a Dell R620 or R610 system with four adapters only, the specified order is as follows

Control Connection
FTP-Streaming Connection
Unused Connection 1
Unused Connection 2

   - On a Dell R610 system with four adapters and a 10 Gig network interface card installed, the specified order is as follows

Control Connection
FTP 10G Connection
Unused Connection 1
Unused Connection 2
Unused Connection 3 10G

4. Click **OK** to close and accept the changes.
5. Close Network Connections.

If continuing with network configuration, next set power management settings.

Set power management settings

1. If not already open, open Network Connections as follows:
   a) Open the Windows **Network and Sharing Center** control panel.
   b) Click **Change Adapter Settings**.
   Network Connections opens.
2. Right-click one of the adapters and select **Properties**.
   The Properties dialog box opens.

3. Click **Configure**.
4. On the **Power Management** tab, uncheck all checkboxes, if they are not already unchecked.
5. Click **OK**.
6. If a "…lose connectivity…" message opens, click **Yes**.
7. Repeat these steps on the remaining network connection in the Network Connections window.

Configure static IP address on Server 2008

This task required on systems with Microsoft Windows Server 2008 operating system only.

SiteConfig cannot discover systems with the Microsoft Windows Server 2008 operating system that have no IP address, such as those that are configured for DHCP. Therefore you must configure the system with a static IP address. You can use any IP address.

Removing a K2 Media Server

In a functioning K2 SAN, you should not permanently remove a K2 Media Server that takes the role of media file system/metadata server, as this changes system capabilities and results in the failure of some or all of the media operations for which the system was designed. Remove a K2 Media Server only under the direct supervision of qualified Grass Valley personnel.

If you are replacing a faulty server with a replacement server, follow the documented procedure.

Replacing a K2 Media Server

The requirements for replacing a K2 Media Server on an existing K2 SAN are as follows:

- You must be logged in to the K2Config application with permissions equivalent to K2 administrator or higher.

Use this procedure if a K2 Media Server in a working system is faulty or otherwise needs to be replaced with a new K2 Media Server.

NOTE: If you are replacing a non-redundant media file system/metadata server, you lose all media during the replacement process.

1. If the server hosts an iSCSI interface adapter, copy down iSCSI bandwidth settings for K2 clients and other iSCSI clients that use the faulty server as their iSCSI target, as follows:
   a) In the K2Config application, select the K2 SAN in the tree view and then click the button in the toolbar to view client iSCSI assignments. A page opens that displays each client's primary and secondary iSCSI targets.
   b) In the tree view, select one of the clients that have the faulty server as a primary or secondary iSCSI target.
   c) Open the client's iSCSI Initiator Configuration page and click **Modify**. The Bandwidth Input dialog box opens.
   d) Copy down the bandwidth settings configured for that client and then close the Bandwidth Input dialog box.
   e) Repeat these steps for each client that has the faulty server as a primary or secondary iSCSI target.
2. If the server hosts an iSCSI interface adapter, in the K2 System Configuration application, for the faulty K2 Media Server, open the iSCSI bridge page and make a note of the IP addresses.

3. Copy down network and hostname settings for the faulty K2 Media Server. You can do this from SiteConfig or from the K2Config application Network Configuration page.
4. Save a copy of the host table from the faulty K2 Media Server. You can use SiteConfig hosts file features or you can find the host table at the following location on the K2 Media Server:

   C:\WINDOWS\system32\drivers\etc\hosts
5. If the server hosts an iSCSI interface adapter, in the K2Config application, remove the K2 clients and other iSCSI clients that use the faulty server as their iSCSI target, as determined earlier in this procedure.
6. Stop all media access and power down all K2 clients and other iSCSI clients.
7. If the faulty server is a media file system/metadata server, take the K2 Media Server out of service. If it is a redundant server, it must be the backup before you take it out of service.
8. In the K2Config application, remove the faulty K2 Media Server as follows:
   a) In the tree view, select the K2 Media Server
   b) Click **Remove** and **Yes** to confirm. The K2 Media Server is removed from the tree view.
9. In SiteConfig, remove the K2 Media Server.
10. Physically remove the faulty K2 Media Server and put the replacement server in its place. Reconnect all cables to the replacement server as they were to the faulty server.

    NOTE: If the replacement server was previously configured on a K2 SAN, you must restart it before adding it to a K2 SAN or in any other way reconfiguring it for use.
11. In SiteConfig, add, discover, and assign the replacement server. Configure the hostname and all network settings on the replacement server to be the same as they were on the faulty server.
12. Copy the host table onto the replacement server. You can use SiteConfig for this task.
13. In the K2Config application, add and configure the replacement server. Refer to the installation chapter for the level of your system earlier in this manual for specific procedures, with the following special instructions:
    a) Add the server to the K2 SAN, using the **Add Device** button.
    b) Configure the replacement server so that its settings are all the same as they were on the faulty server.

       - On the Define Server Roles page, assign the same roles.
       - On the Network Configuration page, verify the same network settings for the FTP network.
       - If the server hosts an iSCSI interface adapter, on the iSCSI Bridge Server Configuration page, verify the same settings.

    c) After completing the configuration, restart the machine to put changes into effect.
14. If the server hosts an iSCSI interface adapter, in the K2 System Configuration application, add the clients that you removed in step 5 earlier in this procedure, with the following special instructions:
    a) Add the client with the highest iSCSI bandwidth first.
    b) On each client, configure iSCSI bandwidth settings so they are the same as they were before.
15. Power up all K2 clients and other iSCSI clients and test media access.

The replacing a server procedure is complete.

Replacing an iSCSI interface adapter (TOE card)

- The K2 SAN must be at K2 system software version 3.2.7 or higher before you begin this procedure.
- K2 system software version must be the same on all K2 Media Servers, before and after you replace the iSCSI interface adapter or adapters.
- If the K2 Media Server has two single-port adapters and the replacement adapter is a dual port adapter, you must remove both single-port adapters, even though only one adapter is faulty, and replace them with the dual-port adapter.

1. In the K2Config application, for the K2 Media Server with the adapter or adapters you are replacing, open the iSCSI bridge page and identify the ports on the adapter or adapters.
2. For the ports on the adapter or adapters you are replacing, make a note of the IP addresses and subnet mask settings.

   Later in this procedure you must assign these same settings to ports on the replacement adapter.
3. Close the K2Config application.
4. Take the clients of the K2 SAN offline and take all K2 Media Servers out of service.
5. If you are replacing two single-port adapters with a dual-port adapter, uninstall K2 system software from the K2 Media Server.
6. Power down the K2 Media Server and replace the iSCSI interface adapter or adapters. Refer to the service documentation on the Dell Documentation CD for procedures. If you are replacing two single-port adapters with a dual-port adapter, install the dual-port adapter in slot 2. Leave slot 3 empty.
7. Power up the K2 Media Server.
8. If you are replacing two single-port adapters with a dual-port adapter, install the current versions of K2 system software (version 3.2.7 or higher is required) on the K2 Media Server and then restart the K2 Media Server.
9. In the K2Config application, open the iSCSI bridge page for that K2 Media Server. It displays iSCSI interface adapters on the K2 Media Server, identified by MAC address. Notice that on replacement adapter ports the MAC address is different than it was on the former adapter, the IP addresses is set to 0.0.0.0, and bandwidth subscription set to 0.
10. Do the following for the replacement iSCSI interface adapter or adapters on the K2 Media Server:
    a) Select each port and set it to the same IP addresses\subnet mask as formerly assigned.
    b) Apply the settings.

       When the IP address is set successfully, the K2Config application automatically applies the same bandwidth subscription that was previously assigned to that IP address. The iSCSI bridge page updates and displays the bandwidth subscription.
11. After making settings on the iSCSI interface adapter or adapters, on the iSCSI bridge page, click **Check**.

    A "…Replaced iSCSI port…" message and a "…Added iSCSI port…" message appears for each port on the adapter or adapters that you replaced.
12. If you are replacing iSCSI interface adapters on multiple K2 Media Servers, repeat this procedure on the remaining K2 Media Servers.
13. Place the devices of the K2 SAN back online.

Installing the Fibre Channel card driver

When you restore a K2 Media Server from the generic disk image, the 8Gb Fibre Channel card driver is not on the disk image. After restoring the disk image, you must install the Fibre Channel card driver as instructed in this procedure.

1. After restoring the disk image and restarting the K2 Media Server, a Found New Hardware wizard opens. Dismiss the wizard and continue with this procedure.
2. Navigate to the following directory:

   C:\Profile\Drivers\Atto 8Gb HBA Drivers

3. Open the directory for the K2 Media Server platform on which you are installing, as follows:

Directory	Platform type
x64	64 bit
x86	32 bit

4. Open *setup.exe*.

   An install wizard opens.

5. Restart the K2 Media Server

Recovering from a failed K2 Media Server system battery

The following procedure applies to K2 Media Servers based on the Dell 2850/2950 platform. K2 Media Servers on other Dell models can have similar procedures. Refer to the service documentation on the Dell Documentation CD for specific procedures.

When the system battery in a K2 Media Server fails (non rechargeable) the system configuration is lost, and the system will not complete startup processes when the battery is replaced.

1. Restart the K2 Media Server.

   A startup screen displays the message "Invalid configuration information - Please run setup program. Time of day not set - Please run setup program."

2. Press **F2** to enter setup.
3. Set the system date and time
4. Select **System Setup | Integrated Devices**
5. Select **RAID**. This also sets ChA and ChB to RAID
6. Restart the K2 Media Server.

   A startup screen displays the message "Warning: Detected mode change from SCSI to RAID on ChA of the embedded RAID system."

7. Select **Yes**.

   A startup screen displays the message "Warning: Detected mode change from SCSI to RAID on ChB of the embedded RAID system."

8. Select **Yes**.

   The K2 Media Server restarts as normal.

When startup completes, normal operation is restored.

Checking K2 Media Server services

The following table specifies the startup type of services for the different K2 Media Server roles. Depending on a K2 Media Server's roles, some services have different startup types. Unless otherwise noted, services with startup type Automatic are started, while services with startup type Manual or Disabled are not started. You can use this table to check services if you suspect that they have been tampered with or for any reason are not set correctly.

To reset services, reconfigure the server with the K2Config application, starting at the beginning of the configuration wizard. Do not manually change the way services run on a configured K2 Media Server.

Service	SNFS file system server	iSCSI bridge	Metadata server	FTP server	NAS server
*CvfsPM[21]	Automatic[22]	Automatic	Manual	Automatic	Automatic
Grass Valley AppService	Automatic	Automatic	Automatic	Automatic	Automatic
Grass Valley Extent Manager Service	Manual	Manual	Manual	Manual	Manual
*Grass Valley FTP Dameon	Manual	Manual	Manual	Automatic[23]	Manual
Grass Valley Import Service	Manual	Manual	Manual	Manual	Manual
Grass Valley K2 Config	Automatic	Automatic	Automatic	Automatic	Automatic
Grass Valley MegaRaid Server[24]	Manual	Manual	Manual	Manual	Manual
Grass Valley MetaDataService	Manual	Manual	Manual	Manual	Manual
Grass Valley Performance Status	Manual	Manual	Manual	Manual	Manual
Grass Valley Performance Status Maker	Manual	Manual	Manual	Manual	Manual

[22] This startup type is top priority for servers with this role. In other words, if a server has this role, then this is always the service's startup type, regardless of other roles that specify a different startup type.

[21] With SNFS version 3.5, this is the only service. Previous versions had StorNext File System service and StorNext File System RPC Port Mapper service

[23] This startup type is top priority for servers with this role. In other words, if a server has this role, then this is always the service's startup type, regardless of other roles that specify a different startup type.

[24] This service has no purpose on a K2 Media Server. It is only used on a K2 client.

Service	SNFS file system server	iSCSI bridge	Metadata server	FTP server	NAS server
Grass Valley SabreToothWS	Manual	Manual	Manual	Manual	Manual
Grass Valley Server Monitor	Automatic	Automatic	Automatic	Automatic	Automatic
Grass Valley SNFS SetRtio	Automatic	Automatic	Automatic	Automatic	Automatic
Grass Valley Storage Utility Host	Automatic	Automatic	Automatic	Automatic	Automatic
GV STRATUS Summit Services	Automatic	Automatic	Automatic	Automatic	Automatic
ProductFrame Discovery Agent Service	Automatic	Automatic	Automatic	Automatic	Automatic
SabreTooth License Server	Automatic	Automatic	Automatic	Automatic	Automatic
SabreTooth Protocol Service	Automatic	Automatic	Automatic	Automatic	Automatic
SNMP Service	Automatic	Automatic	Automatic	Automatic	Automatic
SNMP Trap Service[25]	Automatic	Automatic	Automatic	Automatic	Automatic
STRATUS K2 Configuration Service	Automatic	Automatic	Automatic	Automatic	Automatic

*Startup type set by the K2Config application.

Licensing a K2 Media Server

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

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

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

[25] This service has no purpose on a K2 Media Server. It is only used for receiving traps on a SNMP manager.

Use these procedures to license a K2 Media Server for your K2 SAN as designed by Grass Valley. Consult with Grass Valley before attempting to add a license to an existing K2 SAN.

To license a K2 SAN, the license must be installed on the K2 Media Server with role of file system server.

Requesting a license

This topic applies to Grass Valley SabreTooth licenses. For the system you are licensing, you must provide a generated unique ID to Grass Valley. Grass Valley uses the ID 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 shortcut on the Windows desktop or in the `Grass Valley License Requests` folder.

   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 from Grass Valley.

   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. 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.

8. 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.

9. 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, or the License wizard is not available, try this alternate method:

1. Generate a unique ID of the device where you will install software, as follows:
   a) Double click on the License Manager icon on the Windows Desktop.
      The SabreTooth License Manager opens.
   b) Choose **File | Generate Unique Id** the License Manager.
   c) Click **Copy to clipboard** to copy the generated ID, and **OK** to exit.
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.
   - The license types you are requesting.
3. Send the email to GrassValleyLicensing@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. Double click on the License Manager icon on the Windows Desktop.
   The SabreTooth License Manager opens.
2. Do one of the following:
   - Choose **File | Import License** and navigate to the file location to open the text file.
   - Drag and drop the text file onto the License Manager.

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

You should archive the permanent license to a backup system.

Deleting licenses

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

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

Archiving licenses

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

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

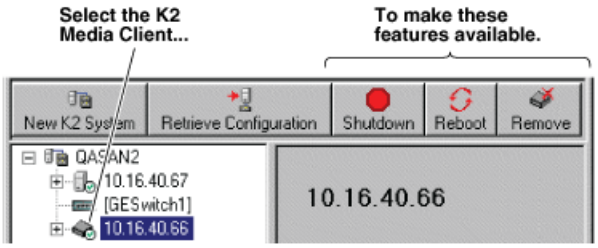
1. In the SabreTooth License Manager, select the license or licenses.
2. Choose **File | Export License** to open the Save As dialog box.
3. Assign a meaningful name to the file, and save it to the desired location. Grass Valley recommends saving the license file to a USB drive or other external location.

Working with K2 clients

Use the procedures in this section when doing configuration or service work on a shared storage K2 client that is part of an existing K2 SAN.

Accessing K2 client features in the K2Config application

In the K2 System Configuration (K2Config) application , features for working on a shared storage K2 client are as follows:



Shutting down or restarting a K2 client

- All media access on the K2 client must be stopped.

Your options for shutting down a K2 client are as follows:

- Do a local shutdown/restart via AppCenter. Assuming a keyboard, monitor, and mouse is connected to the local K2 client, in AppCenter select **System | Shutdown**, then select **Shutdown** or **Restart** and **OK**. AppCenter exits, Windows shuts down and powers off the K2 client.
- Do a local shutdown/restart via Windows. Assuming a keyboard, monitor, and mouse is connected to the local K2 client, if AppCenter is not open, you can use the normal Windows procedure to shutdown. You can also do this type of shutdown/restart using the Windows Remote Desktop Connection.
- In the SiteConfig tree view right-click the K2 Client and select **Shutdown** or **Restart**.
- Do a remote shutdown/restart via the K2Config application. In the tree view select the K2 client and then click **Shutdown** or **Restart**.

- Do a local hard shutdown. Use this method only when there is a problem that prevents you from using one of the other methods for an orderly shutdown. To do a hard shutdown, hold down the standby button for approximately five seconds. To restart, press the standby button again.

Taking a K2 client offline

- To take a K2 client offline, simply stop all media access and then shut down the K2 client.

Bringing a K2 client online

- To bring a K2 client online, simply restart the K2 client. When the K2 client starts up, it is always in the online state.

Adding a K2 client

- You must be logged in to the K2Config application with permissions equivalent to K2 administrator or higher.
- The K2 SAN must have adequate bandwidth available to meet the bandwidth needs of the K2 client you are adding.
- The devices of the K2 SAN are not required to be offline, and a restart of devices is not required.
- The K2 client must be connected to appropriate networks and be powered up.

1. In SiteConfig, add the K2 client to the SAN as follows:
   a) In the Network Configuration tree view, add the client as a placeholder device next to existing clients.
   b) Discover devices.
   c) Identify the K2 client you are adding.
   d) Assign the discovered K2 client to placeholder K2 client.
   e) Verify that networks are assigned and planned network interface settings applied.
2. In the K2Config application tree view, select the name of the K2 SAN, which is the top node of the storage system tree.
3. Click **Add Device**. The Add Device dialog box opens.
4. Select the appropriate type of client.
5. Click **OK**. The new client device appears in the tree view.
6. Configure the K2 client as appropriate.

Removing a K2 client

- You must be logged in to the K2Config application with permissions equivalent to K2 administrator or higher.
- Media access must be stopped on the K2 client you are removing.

You can remove a K2 client without disrupting the operation of the rest of the SAN.

1. Stop media access on the K2 client.
2. In SiteConfig, remove the K2 client.
3. In the K2Config application tree view, select K2 client.
4. Click **Remove** and **Yes** to confirm. The K2 client is removed from the tree view.

Identifying K2 client software versions

Your options for identifying K2 client software version are as follows:

- In the K2Config application tree view, open the node for the K2 client. This exposes the nodes for individual configuration pages. Select the **Software** configuration page to view software version information. To check for recent changes in software, click the **Check** button.
- Use SiteConfig software deployment features.

Modifying K2 client control network settings

To modify the hostname or IP address of a K2 client, use the following procedure. Refer to other procedures for the details of individual steps.

Whenever you modify control network settings or FTP/streaming network settings on any device, you must then redeploy the hosts file if that is your name resolution mechanism.

1. Make sure you know the load balancing (bandwidth) parameters currently set for the K2 client in the K2Config application. You must reconfigure these parameters later in this procedure.
2. In SiteConfig, remove the K2 client.
3. In the K2Config application, remove the K2 client from the K2 SAN.
4. In SiteConfig, add the K2 client to a K2 SAN as follows:
   a) In the Network Configuration tree view, add the client as a placeholder device next to existing clients.
   b) Discover devices.
   c) Identify the K2 client you are adding.
   d) Assign the discovered K2 client to placeholder K2 client.
   e) Verify that networks are assigned and planned network interface settings applied.
5. Edit hosts files or other name resolution mechanisms for all the devices of the K2 SAN. You can use SiteConfig for this task.
6. In the K2Config application, add the K2 client as a new device to the K2 SAN, load balancing the K2 client just as it was previously. This is important, as you want the K2Config application to assign it to the same available bandwidth on the same iSCSI target as previously.

Modifying K2 client media (iSCSI) network settings

If IP address to which you are changing is in a different subnet, do not use this procedure. Instead, remove, then add the K2 client.

If the iSCSI network address to which you are changing is within the same subnet and range as the current iSCSI network, use the following procedure.

1. Stop media access on the K2 client.
2. Use SiteConfig to change the IP address. Make sure that the IP address is within the subnet and range designated for the network.
3. In the K2 System Configuration application, open the Network configuration page for the K2 client.
4. Verify that the IP address updates correctly.

5. Restart the K2 client.

Using Storage Utility

When doing configuration or service work on the media file system, the media database, or the RAID storage devices of an existing K2 SAN, the primary tool is the Storage Utility.

⚠ ***CAUTION: Use the Storage Utility only as directed by a documented procedure or by Grass Valley Support. If used improperly, the Storage Utility can render your K2 SAN inoperable or result in the loss of all your media.***

Use K2 SAN installation instructions to using Storage Utility as you initially set up and configure a K2 SAN. You should refer to those instructions for information that is specific to your K2 SAN.

Accessing Storage Utility

- You must open Storage Utility from within the K2Config application.

Access permissions are passed from the K2Config application to the Storage Utility as it opens, so make sure that you are logged in with sufficient permissions.

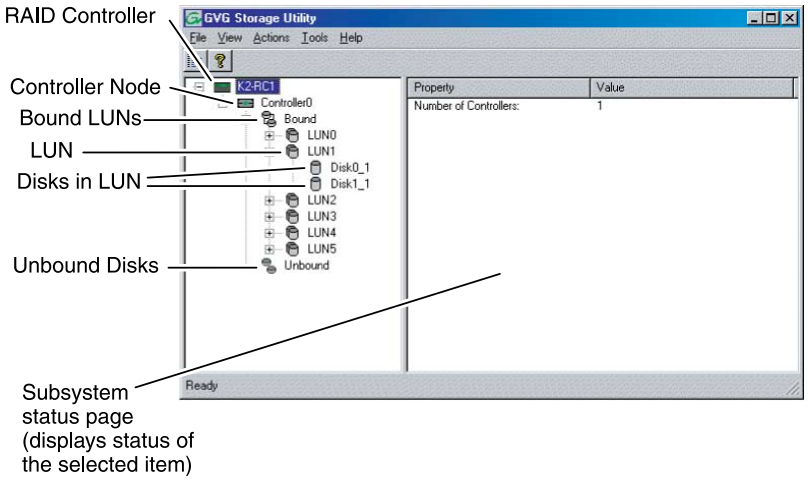
You can open Storage Utility in the following ways:

- In the K2Config application tree view, select the name of the K2 SAN, which is the top node of the storage system tree. Then click the **Storage Utility** button. Storage Utility opens. In this case the connection to the RAID storage devices is via the K2 Media Server first configured, depending on the level of the SAN.
- In the K2Config application tree view, open the node for a K2 Media Server and select the **File System Server** node to open its property page. On the property page click **Launch Storage Utility**. Storage Utility opens. In this case the connection to the RAID storage devices is via the selected K2 Media Server. Use this method for nearline SANs.

NOTE: Do not run Storage Utility on a shared storage K2 client.

NOTE: Do not run Storage Utility as a stand-alone application, separate from the K2Config application. To maintain a valid K2 SAN all storage configuration must be controlled and tracked through the K2Config application.

Overview of Storage Utility



The Storage Utility user interface includes a tree view in the left-hand pane, and a status information area displayed in the right-hand pane. The tree view displays the hardware that make up the RAID storage system. The context menus in the tree view are used to configure storage. The right-hand status pane displays information about the item selected in the tree view. The tree view hierarchy is as follows:

- Controllers in device - Provides a logical grouping of the RAID Controllers in a primary RAID chassis.
- Controller - Represents the RAID Controllers found. These are numbered in the order discovered. The controller icon represents both RAID Controller A and, if installed, RAID Controller B. To determine if an optional RAID Controller B is installed, select the Controller icon in the tree view, then examine the status pane for peer status.
- Bound Disks - Expanding the Bound node displays all bound disks.
- RANK - Represents a bound RANK. Expanding the RANK node displays the disk modules that make up the RANK.
- UnBound disks - Expanding the UnBound node, displays all unbound disk modules.
- Disks - Represents the disk modules. The Storage Utility detects disks available and lists them on the opening screen.

Use Storage Utility for working on the media file system and database.

Working on the media file system and database

Use the procedures in this section when doing configuration or service work on the media file system or the media database of an existing K2 SAN.

Checking the media file system

- You must access Storage Utility (via the K2Config application login) with permissions equivalent to K2 administrator or higher.

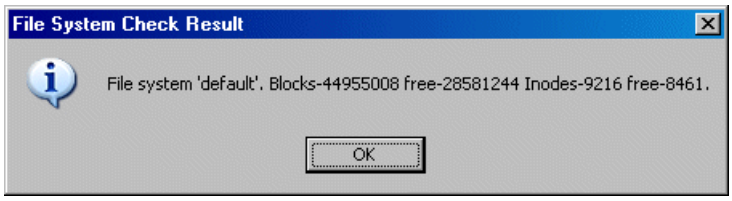
- When you access Storage Utility, the K2 SAN must be offline.
- All iSCSI clients and K2 clients in the K2 SAN must be offline.
- K2 Media Servers with role of file system/metadata server, both primary and redundant, must be powered up but offline.

This procedure checks the media file system but retains current media files.

NOTE: This procedure can take 20 hours or more on a large SAN. Do not start this process unless you have adequate time set aside.

1. In Storage Utility, click **Tools | Check File System**.
2. A message box appears "Checking media file system. Please wait". Observe progress.

   If problems are discovered they are reported. If the check process passes, when the process is complete a message appears to confirm success.



3. Click **OK** to dismiss the results.
4. Messages appear "…online mode now?" and "…continue?". Do one of the following:
   - Click **Yes** to put the system in online mode. This is the recommended option in most cases. For example, even if you plan to next clean unreferenced files and/or movies, that operation requires that the system be online, so you should put it online now. When you click Yes, AppCenter channels go online.
   - Click **No** to keep the system in offline mode. This is not recommended for most cases. Only do this when you are sure that subsequent operations require the system to be offlline.

Your file system has been checked.

Cleaning unreferenced files and movies

- You must access Storage Utility (via the K2Config application login) with permissions equivalent to K2 administrator or higher.
- When you access Storage Utility, the K2 SAN must be online.
- All iSCSI clients and K2 clients in the K2 SAN must be online.
- K2 Media Servers with role of file system/metadata server, both primary and redundant, must be powered up but online.

These procedures allow you to keep the media database and the media files in sync. You can check the movies (clips) in the media database for the references to media files that should be currently stored on the media disks. Likewise, you can check for media files that are not referenced by a movie in the media database. If you find any unreferenced files or movies, you can delete them.

Clean unreferenced files

1. In Storage Utility, click **Tools | Clean Unreferenced Files**.
2. A message box appears "…searching …Please wait". Observe progress.

3. A message box reports results. Respond as follows:
   - If no unreferenced files are found, click **OK** to dismiss the results.
   - If unreferenced files are discovered, you are prompted to delete them. Click **Yes** to delete the files or **No** to leave the files intact.

The process writes a log file to `C:\profile\logFS.txt`, which you can check for more information.

Clean unreferenced movies

1. In Storage Utility, click **Tools | Clean Unreferenced Movies**.
2. A message box appears "…searching …Please wait". Observe progress.
3. A message box reports results. Respond as follows:
   - If no unreferenced movies are found, click **OK** to dismiss the results.
   - If unreferenced movies are discovered, you are prompted to delete them. Click **Yes** to delete the movies or **No** to leave the movies intact.

The process writes log files to `C:\profile\cleanupDB.txt` and `C:\profile\MediaDB.txt`, which you can check for more information.

Making a new media file system

The requirements for this procedure are as follows:

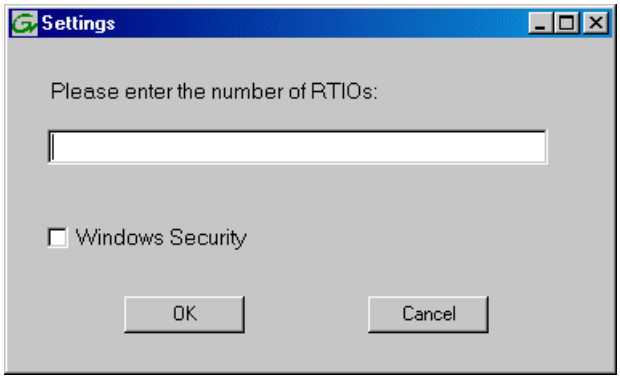
- You must access Storage Utility (via the K2Config application login) with permissions equivalent to K2 administrator or higher.
- When you access Storage Utility, the K2 SAN must be offline.
- All iSCSI clients and K2 clients in the K2 SAN must be shut down.

If your SNFS file system name is currently "default", when you make a new file system the name changes to "gvfs_hostname", where hostname is the name of the primary FSM.

NOTE: You lose all media with this procedure.

1. If you have not already done so, launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.
3. In Storage Utility, click **Tools | Make New File System**.

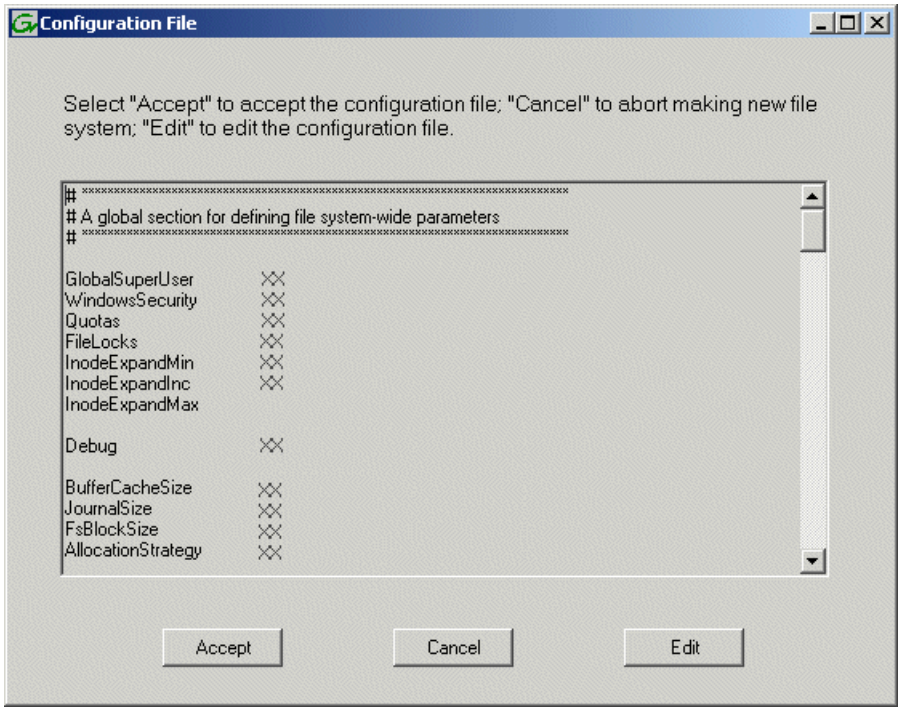
   The Setting dialog box opens.



4. For the Real Time Input/Output (RTIO) rate, enter the value specified by your system design. If you do not know this value, contact your Grass Valley representative.
5. Configure Windows Security as follows:
   - If the K2 SAN is on a network Workgroup (not domain), do not select **Windows Security** .
   - If the K2 SAN is on a network domain, you may select **Windows Security**.

   NOTE: Only select Windows Security if the K2 SAN is on a domain. Never select Windows Security if the K2 SAN is on a workgroup.
6. Click **OK**.

   The Configuration File dialog box opens.



   The configuration file for the media file system is displayed.
7. Verify media file system parameters.

   Do not edit the configuration file for the media file system.
8. Click **Accept**.

   A "…Please wait…" message box displays progress and a "…succeeded…" message confirms the process is complete.
9. Restart the K2 Media Server.

10. You now have a blank (empty) file system. Proceed as follows:
    - On a 7.x SAN, you also have a blank database. Do not perform additional operations on the database. Skip to the next step in this procedure.
    - On a 3.x SAN, the media database still contains references to media files which are no longer present in the file system. To clear the media database do the following:

    a) In the K2Config application tree view, open the node for the K2 Media Server and select the **Database Server** node to open its property page.
    b) On the Database Server property page click **Erase media database**.

       A message box displays progress.
    c) Wait until a message confirms that the process is complete. This can take several minutes.
    d) If you have redundant K2 Media Servers, repeat these steps to clear the media database on the other (redundant) server.
11. Close Storage Utility.
12. If you have Macintosh systems accessing the K2 SAN, you should check that the SNFS file system volume is configured correctly on the Macintosh systems.
13. Place the K2 SAN back online.

Expanding the media file system by capacity

- The system must have one LUN per RANK. Expansion by capacity is not supported on systems with multiple LUNs per RANK.
- The expansion chassis that you add to your K2 SAN must have unbound, unlabeled disks.

NOTE: This procedure should only be attempted under the supervision of qualified Grass Valley support personnel. Contact your Grass Valley representative for assistance.

If you need to increase the storage capacity of your K2 SAN, you can do so by adding one or more Expansion Chassis, up to the maximum number of chassis allowed for your level of storage.

1. Rack the Expansion Chassis.
2. If a redundant K2 SAN, do the following:
   a) Verify that MPIO is updated to the latest version on all shared storage K2 clients.
   b) Put the system into an "original primary" state. This means that for all redundant devices (switches, servers, RAID controllers, etc.) the current device acting as primary is the one that was initially configured as primary when the system was originally installed.
3. On the K2 Media Server with the role of primary media file system/metadata server, save a copy of the following files to a different location:

   `D:\snfs\config\default.cfg` (on some systems this file is named `gvfs_hostname.cfg`, where hostname is the name of the SNFS file system server.)

   `D:\snfs\config\cvlabels`
4. Power down the K2 SAN, including RAID storage devices.
5. Power up the RAID storage devices. Verify that they stabilize in an operational state with no errors indicated.
6. Power down RAID storage devices.
7. Cable and configure the Expansion Chassis.

8. Power up the RAID storage devices. Verify that they stabilize in an operational state with no errors indicated.
9. Start up the K2 SAN.
10. Bind the RANKs in the Expansions Chassis using Background Bind.
11. When binding is complete, put the K2 SAN in an offline state as follows:
    a) You must access Storage Utility (via the K2Config application login) with permissions equivalent to K2 administrator or higher.
    b) When you access Storage Utility, the K2 SAN must be offline.
    c) All iSCSI clients and K2 clients in the K2 SAN must be shut down.
12. Restart all K2 Media Servers. Do not use the standard startup processes here. Just start up the server(s) and wait until the Windows desktop appears. Especially do not use Server Control Panel or start Failover Monitor.
13. In Storage Utility, select **Tools | Expand File System By Capacity**.

    The first of a series of informational screens opens.
14. Work through the informational screens to verify information. When the option to retry becomes available, if the new disks are not labeled correctly, retry to start the process. If you are not sure, you can retry to be sure. Doing so does not cause problems.
15. A message box reports progress. When a message reports success, the process is complete.
16. Restart the K2 SAN.
17. If a redundant K2 SAN, test failover capabilities.

Expanding the media file system by bandwidth

If you want to retain your media file system and yet expand the bandwidth of your K2 SAN, you must use the following procedures for dynamic bandwidth expansion. This process allows you to add RANKs to the stripe group, thereby expanding its width, without reinitializing the file system. This keeps the existing media intact. The additional RANKs can be made up of new disks in existing RAID chassis, disks in new Expansion Chassis, or disks in new primary RAID chassis.

After the file system is expanded, existing media is still striped across the original narrower stripe group, so it can not take advantage of the increased bandwidth. Also, if there is a significant portion of the storage pool occupied by this existing media, its presence reduces the extent to which new media can use the increased bandwidth. For this reason the dynamic bandwidth expansion process provides the Restripe Utility, which restripes the existing media across the new wider stripe group. This enables both the existing media and new media to get full benefit of the increased bandwidth.

If the media on your file system has a high turnover rate and you know existing media is to be deleted soon, you have the option of disabling the Restripe Utility. This saves the system resources and time required to restripe media.

The expansion chassis that you add to your K2 SAN must have unbound, unlabeled disks. If it currently has disks bound or labeled, connecting it to your system can cause errors.

Dynamic bandwidth expansion is supported only with K2 system software version 3.2 and higher.

Dynamic bandwidth expansion is supported on systems with one LUN per RANK and on systems with multiple LUNs per RANK.

NOTE: Adding RAID storage devices changes your system design and must be specified for your K2 SAN by Grass Valley. Do not attempt to add RAID storage devices without support from Grass Valley.

Procedures for expanding the media file system by bandwidth

Grass Valley personnel who have received K2 SAN training can use the following procedures.

Prepare system for bandwidth expansion

1. If a redundant K2 Storage System, do the following:
   a) Verify that MPIO is updated to the latest version on all shared storage K2 clients.
   b) Put the system into an "original primary" state.

      This means that for all redundant devices (switches, servers, RAID controllers, etc.) the current device acting as primary is the one that was initially configured as primary when the system was originally installed.
2. Back up configuration files from the primary K2 Media Server. To do this, save a copy of the following files to a different location:

   `D:\snfs\config\cvlabels`

   `D:\snfs\config\default.cfg`

   On some systems this file is named `gvfs_hostname.cfg`, where hostname is the name of the SNFS file system server.

   If there is a problem with the expansion process, contact Grass Valley Support for instructions on using these files to recover.
3. If K2 storage contains Aurora media, do additional steps.
4. Verify recovery disk images. Update if necessary

Set up and configure RAID for bandwidth expansion

1. Rack any new RAID equipment
2. Stop all media access and power down K2 clients and other clients.
3. Clean unreferenced files and movies.

   K2 Media Servers with role of file system/metadata server, both primary and redundant, must be powered up but offline.
4. Power down the remaining devices of the K2 SAN.
5. Add disks or RAID equipment to support the additional RANKs

   As applicable, remember to set Fibre Channel addresses on RAID controllers and chassis addresses on Expansion Adapters.
6. Start up the RAID equipment.
7. Start up the primary K2 Media Server.

   If there are multiple K2 Media Servers, this is the server that takes the role of media file system server. On a redundant K2 SAN, this is the server functioning as primary when the system was last powered down.

8. From the control point PC, open the K2Config application and launch Storage Utility.

   Make sure that versions are correct and consistent on both new and existing RAID storage devices.

9. Verify versions of controller microcode and disk firmware. Update if necessary.

   Make sure that versions are compatible on both new and existing disks and RAID storage devices.

10. Bind RANKs using the new disks.

    Wait for the binding process to complete.

    Do not unbind or bind existing RANKs. Doing so destroys all data. If in doubt, flash drive lights to identify disks.

11. Close Storage Utility.
12. Restart the primary K2 Media Server.

    Do not use the standard startup processes here. Just start up the server and wait until the Windows desktop appears. On a redundant K2 SAN, do not use Server Control Panel or manually start.

13. Check the Windows Device Manager to verify that the server "sees" both the old RANKs and the new RANKs.
14. Start up the remaining K2 Media Servers that are connected to the K2 SAN.

    Do not use the standard startup processes here. Just start up the server(s) and wait until the Windows desktop appears. On a redundant K2 SAN, do not use Server Control Panel or manually start.

Configure the media file system for bandwidth expansion

1. If Aurora media is present, modify *`VolumeConfig.xml`*.
2. Stop services (if running) on K2 Media Servers. .

   On a redundant K2 SAN stop the Server Monitor Service. On a non-redundant K2 SAN stop the MetaData service.

3. From the control point PC, open the K2Config application and launch Storage Utility.
4. In Storage Utility make sure both old RANKs and new RANKs are displayed.
5. In Storage Utility, select **Tools | Expand File System By Bandwidth** and answer **Yes** to confirm.
6. A dialog box opens asking if you want to restripe existing media after bandwidth expansion. Proceed as follows:

   - Click **Yes** in most cases. This is the typical response. In any case this does no harm.
   - Click **No** only if you are sure you do not need to restripe existing media, such as in the following cases:

     - You have very little existing media so the fact that it cannot use the new stripe group does not impact future media operations or capacity.
     - Your existing media is to be deleted soon so you don't care if it uses the new stripe group.

   The first of a series of informational screens opens.

7. Work through the informational screens.

   When prompted to retry, if you are not sure if the process started, you can retry to be sure. Doing so does not cause problems.

   The expansion process runs. A dialog box displays progress

8. Wait for the process to complete. On a large system this can take over 30 minutes.
9. A "…succeeded…" message is displayed when done. Click **OK** and Storage Utility closes.
10. The K2Config application displays a message informing you to restart servers. Click **OK**.
11. Make sure Storage Utility is closed before proceeding.
12. If directed, modify RTIOS.

    Depending on your use of the expanded file system, you might need to change the RTIOS value. This value can be calculated only by Grass Valley Support. Do this step only under the direction of Grass Valley Support.

    As directed, use a text editor to modify the SNFS configuration file on K2 Media Servers (both primary and backup) with the role of media file system/database server.

    NOTE: Don't use the SNFS configuration tool to modify the system configuration. Doing so causes unexpected changes in the configuration file, resulting in a failure of the expansion process.

13. Restart all K2 Media Servers.

    Make sure to first start servers with the role of media file system/metadata server.

    When the server that takes the role of FTP server starts, one of the following happens:

    - If you answered "Yes" to restripe existing media in the step above, the Restripe Utility automatically launches and begins restriping media.
    - If you answered "No" to restripe existing media in the step above, the Restripe Utility does not launch.

14. In the K2Config application, do the following for each K2 Media Server with role of iSCSI bridge to verify that you see the correct number of drives:
    a) On the **iSCSI Bridge Server Configuration** page, click **View Target Drives** and proceed as follows:
       - If you see all drives, both old and new, no further sub-steps are necessary. Skip to the next step in this procedure.
       - If some drives are listed as unexposed, continue with the remaining sub-steps in this step.

    b) Click **Check**.
    c) Restart the K2 Media Server.
    d) Repeat this step to make sure you now see the correct number of drives.
15. Monitor the Restripe Utility.

    On a file system with a large amount of existing media, this can take days.

    NOTE: Do not stop the FTP server once the restripe process begins.

    a) Record system information

       Make sure you keep diagrams and other on-site documentation up to date.

Managing the Restripe Utility

If you answer "Yes" to the dialog box that asks about restriping existing media, after the bandwidth expansion process completes, Storage Utility exits with a special code. On receiving the special exit code, the K2 System Configuration application sets the current date in the registry of the K2 Media Server that takes the role of FTP server.

When the FTP server restarts, the Restripe Utility automatically opens. The Restripe Utility reads the date set in the registry, finds clips and files created before that date, and restripes the clips and files, one at a time.

1. You can monitor the Restripe Utility in the following ways:
   - While the Restripe Utility is running, it is represented by an icon in the system tray. You can right-click this icon and open the Restripe Utility window.
   - The Restripe Utility window reports first on the progress of K2 clips being restriped, then on the progress of files being restriped.
   - Click the Report button for a list of clips and files that failed to be restriped, if any.
   - When the Restripe Utility completes its processes, it reports its results to *C:\profile\RestripeResult.txt*. Open this file in Notepad to verify successful results.
2. You can start and stop the Restripe Utility manually as follows:
   - At any time while the Restripe Utility is in the process of restriping clips, you can right-click the icon in the system tray, and select **Abort**. This stops the restripe process and closes the Restripe Utility.

     NOTE: Stopping the Restripe Utility before it completes its processes leaves some of your existing media still striped across the original narrower stripe group. Once the Restripe Utility is stopped, you cannot restripe that existing media.

Recovering the media database

Use the topics in this section to understand and implement recovery strategies for your K2 storage media database.

About the automatic database backup process

Every 15 minutes the K2 system checks to see if any media operations have changed the media database. If a change has occurred, the K2 system creates a backup file of the media database. The backup file is saved in the same directory as the media database using a rotating set of three file names. These files are named `media.db_bakX` where `X` is the number in the rotation. Each time a backup occurs, the oldest backup file is overwritten. If some condition renders one of the backup files un-writable, the backup file following that in the rotation is subsequently used for every backup until the condition is resolved.

Identifying a corrupt media database

1. Check the following symptoms, as they could indicate a corrupt media database:
   - On startup, the Grass Valley MetaDataService is unable to start. This is indicated in the Services control panel if the Grass Valley MetaDataService does not display as Started.
   - The K2 log displays a "…file is encrypted or is not a database…" error.
2. As soon as you suspect a corrupt media database, stop all media access and take the K2 system offline.

Restoring the media database

1. Stop all media access and take the K2 system offline.

   If a K2 SAN, follow procedures to take connected K2 client systems and K2 Media Servers offline. Shutdown connected K2 client systems. Refer to the *K2 SAN Installation and Service Manual*.
2. Navigate to the V:\media directory.

   If a K2 SAN, access this directory from a K2 Media Server with role of media file system server.
3. Make a copy of the media.db and media.db_bak* files and store them in a secure location.
4. Stop the Grass Valley MetaDataService as follows:
   - If a stand-alone K2 system, use the Services control panel to stop the service.
   - If a K2 SAN, use Server Control Panel to stop the service on primary, and if present, backup K2 Media Server with role of file system server.
5. Determine which backup file is the most recent good file by examining the file modification date on each backup file.
6. Rename the current *media.db* file (which is assumed to be corrupt) to another name, and rename the most recent good *media.db_bakX* file to *media.db*.
7. Restart the K2 system following normal procedures.
8. Confirm that the systems come up correctly with the restored database now in place.
9. Use Storage Utility **Clean Unreferenced Files** and **Clean Unreferenced Movies** to repair any inconsistencies between the contents of the database and the file system.

Working with RAID storage

This section refers to K2 10Gv2 RAID storage devices.

K2 Level 2, 3, 10, 20, 30, 35 and 10G RAID storage devices were released with previous versions of K2 SANs. Refer to previous versions of this manual for information about those levels.

Use the procedures in this section when doing configuration or service work on the RAID storage devices of an existing K2 SAN.

Checking RAID storage subsystem status

Some limited status information for storage subsystems is displayed in the Storage Utility. This can be helpful when configuring storage. You can view status information by selecting items in the tree view.

Item in tree view	Status information displayed
Controllers in Device	Number of Controllers
Controller	Peer Status
	Primary IP
	Serial Number
	Slot
	Peer Slot
	Microcode Version
Bound	Number of RANKS or LUNs
RANK	Binding Type, such as RAID 1
	State (online or offline)
	Number of Logical Units
Disk	Firmware
	Vendor
	State
	Product ID
	Capacity
Unbound	Number of disks

Checking controller microcode

As explained in the previous section, to check controller microcode, in Storage Utility select the controller in the tree view and the microcode version is displayed.

Identifying disks

When you do maintenance or service work on your RAID storage, it is important for many tasks that you positively identify the disk or disks on which you are working. Your primary indicators for this are the numbering of the disks in Storage Utility and the ability to flash the disk LED on a physical disk or a group of disks.

Disk numbering for 2.5 inch disks

In Storage Utility, RAID disks are numbered with a hexadecimal convention. Disk modules are identified based on the chassis address and physical location as follows:

Chassis	Disk numbering							
Primary	00	01	02	03	04	05	06	07
	08	09	0A	0B	0C	0D	0E	0F
	10	11	12	13	14	15	16	17
Expansion 1	20	21	22	23	24	25	26	27
	28	29	2A	2B	2C	2D	2E	2F
	30	31	32	33	34	35	36	37
Expansion 2	40	41	42	43	44	45	46	47
	48	49	4A	4B	4C	4D	4E	4F
	50	51	52	53	54	55	56	57
Expansion 3	60	61	62	63	64	65	66	67
	68	69	6A	6B	6C	6D	6E	6F
	70	71	72	73	74	75	76	77

Disk numbering for 3.5 inch disks

In Storage Utility, RAID disks are numbered with a hexadecimal convention. Disk modules are identified based on the chassis address and physical location as follows:

Chassis...	With disk numbering as follows:			
Primary	00	01	02	03
	04	05	06	07
	08	09	0A	0B
Expansion 1	10	11	12	13
	14	15	16	17
	18	19	1A	1B
Expansion 2	20	21	22	23
	24	25	26	27
	28	29	2A	2B
Expansion 3	30	31	32	33
	34	35	36	37
	38	39	3A	3B

Chassis...	With disk numbering as follows:			
Expansion 4	40	41	42	43
	44	45	46	47
	48	49	4A	4B
Expansion 5	50	51	52	53
	54	55	56	57
	58	59	5A	5B
Expansion 6	60	61	62	63
	64	65	66	67
	68	69	6A	6B
Expansion 7	70	71	72	73
	74	75	76	77
	78	79	7A	7B

Flashing disk LEDs

Storage Utility's Identify feature allows you to flash the disk LEDs so that you can physically locate a specific disk module or group of disk modules that make up a RANK. Always use the disk identify feature before removing and replacing a failed disk module. Accidentally removing the wrong disk module can destroy data.

1. Open Storage Utility and in the tree view expand all nodes so that all disks are displayed.
2. Open the bezel on the RAID storage chassis or otherwise make sure you can see disk LEDs.
3. Identify the disks in a RANK or identify a single disk, as follows:
   a) In the Storage Utility tree view, right-click a RANK or right-click a single disk, then select **Identify RANK** or **Identify Disk** in the context menu. A message box opens with a message that informs you that a disk or disks are blinking.
   b) The LEDs for the disk or disks display a flashing pattern. Verify the location of the disk or disks.

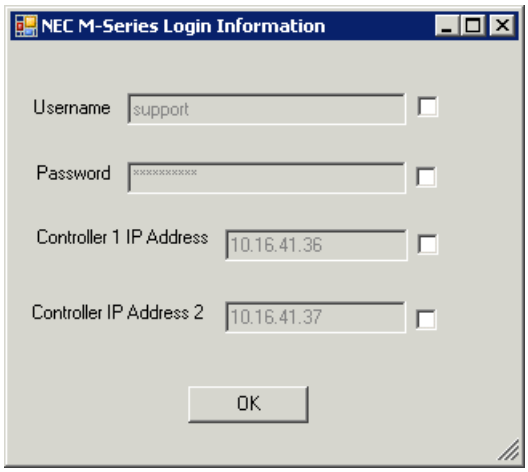
Get K2 10Gv2 RAID controller logs

The K2 10Gv2 RAID controller(s) must be connected to the control network and must have IP address(es) set (using Storage Utility) to support the operations in this topic.

1. In the Storage Utility tree view, select the controller.

2. Click **Actions | Get Controller Logs**.

   The Login Information dialog box opens.



3. If necessary, enable fields and enter username, password, or controller IP address, then click **OK**.

   The Gather Logs wizard opens.

4. At each wizard page, read messages in the center window to follow progress and wait until the green indicator verifies that operations are complete. Then click **Next** to proceed.
5. A message informs you of that logs have been successfully gathered.
6. Find the log files on the K2 Media Sever at *C:\logs*.

Unbind RANK

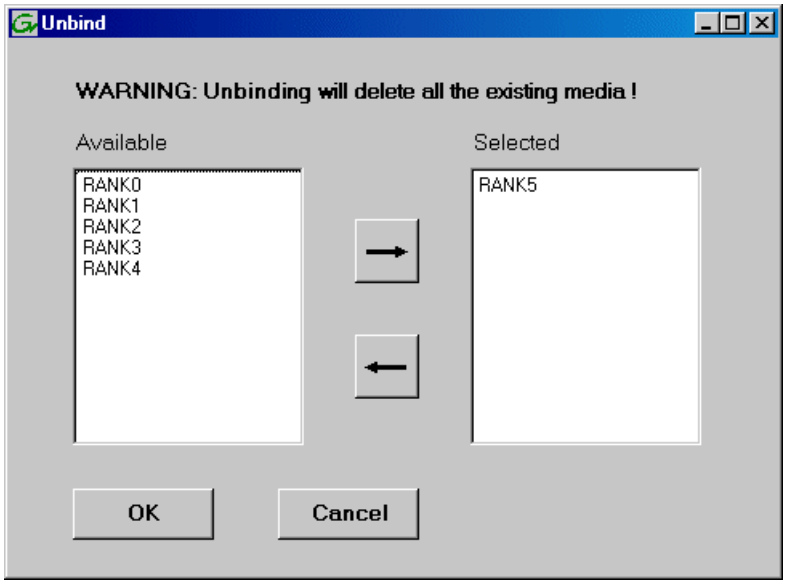
- You must access Storage Utility (via the K2Config application login) with permissions equivalent to K2 administrator or higher.
- All iSCSI clients and K2 clients in the K2 SAN must be shut down.

Unbinding reverses the bind process. Unbinding might be needed when reconfiguring a SAN.

⚠ ***CAUTION: Unbinding destroys all data stored on disk modules***

1. In the tree view, right-click the RANK and select **Unbind**.

2. When warning messages appear "…destroy all existing media…" and "Are you sure?", click **OK** to continue. The Unbind dialog box opens.



3. Verify that the RANK or RANKs you intend to unbind is in the Selected box. If not, select RANKs and click the arrow buttons until the RANKs you intend to bind are in the Selected box and the RANKs you do not intend to unbind are in the Available box.

   NOTE: As an aid in identifying a disk module's physical location, select it in the Selected Disks list, then click Identify Disks. This causes the disk drive LED to flash.

4. Click **OK** to close the Unbind dialog box and begin the unbinding process. The Progress Report dialog box opens, showing the status of the unbinding process.
5. When progress reports 100% complete, the RANK is unbound.
6. Restart the K2 Media Server.

About full/background bind

When binding RAID disks, you can choose to do either a full bind or a background bind. Background bind is recommended. These binding processes are described as follows:

- Full bind — During this process, the K2 SAN must be in the offline mode. While the full bind process is underway, disks are not available for data access of any kind. On a large SAN, the full bind process can take many hours, so you should plan ahead for this process. For example, binding 750 Gig SATA drives can take up to 3 days.

- Background bind — During this process, the K2 SAN can be in a restricted online mode. Disks are available for data access, but the overall performance of the RAID storage is significantly reduced. While the background bind process is underway, you can initiate media access on your SAN for limited testing of operations, such as record, play, and transfer, but do not run media access at full bandwidth. The background bind process is useful when doing initial system installation and configuration, as it does not require the long wait time required for full bind. You can have RAID disks binding while you move on to other tasks that require RAID media access.

With either type of binding process, you should bind multiple RANKs simultaneously, to reduce the overall time required to bind disks.

Bind RANK

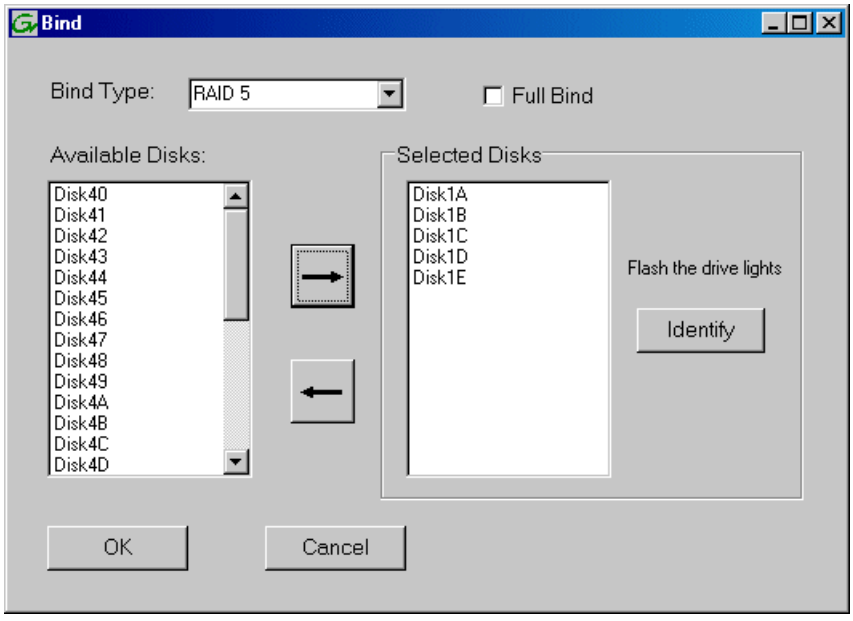
- You must access Storage Utility (via the K2 System Configuration application login) with permissions equivalent to K2 administrator or higher.
- When you access Storage Utility, the K2 SAN must be offline.
- All iSCSI clients and K2 clients in the K2 SAN must be shut down.

Binding disk modules formats them into a logical units called RANKs. The disks that make up a RANK are accessed as a contiguous disk space. Disk modules must be bound before they can be part of the video storage file system.

For simplicity, the Storage Utility only allows binding the first available (at the top of the Available Disks list) contiguous disk modules into RANKs. After binding, disk modules become slot specific and cannot be moved to other disk module slots.

1. In the tree view, right-click the **Unbound** node and select **Bind**. (Peer controllers that share the same set of disks are automatically selected as a pair.)

   The Bind dialog box opens showing all unbound disks for the controller listed in the Available Disk list.



2. Leave **Full Bind** unchecked. Refer to the previous section "About full/background bind".
3. In the **Bind TYPE** drop down box, select the RAID type. Refer to the installation chapter earlier in this document for your level of SAN for specific instructions.
4. In the Available Disks box, select contiguous disks at the top of the list as appropriate for the RAID type. (TIP: Use 'shift-click' or 'control-click' to select disks.)
5. Click the add (arrow) button to add disks to the Selected Disks list.

   NOTE: As an aid in identifying a disk module's physical location, select it in the Selected Disks list, then click Identify Disks. This causes the disk drive LED to flash.

6. Click **OK** to close the Bind dialog box and begin the binding process. The Progress Report dialog box opens, showing the status of the binding process.
7. Close the Progress Report and repeat these steps for other unbound disks.
8. Upon 100% completion, click **Close** in Progress Report window.
9. Restart the K2 Media Server.

Binding Hot Spare drives

- You must access Storage Utility (via the K2 System Configuration application login) with permissions equivalent to K2 administrator or higher.
- When you access Storage Utility, the K2 SAN must be offline.
- All iSCSI clients and K2 clients in the K2 SAN must be shut down.

You can bind disks as hot spare drives. Hot spare drives are on standby and are used in the event of a drive failure in a RANK. If a drive fails, the RAID Controller automatically selects a hot spare drive to use in place of the failed drive. This prevents the system from operating in a degraded state.

If the drives you want to designate as hot spares are bound as part of a RANK, you must unbind the drives first, then bind them as hot spares. To function as a Hot Spare, the drive must be at least as fast and have at least as much capacity as the failed drive it replaces.

1. In Storage Utility, right-click the **Unbound** node for a controller, then select **Bind** in the context menu. (Peer controllers that share the same set of disks are automatically selected as a pair.)

   The Binding dialog box opens showing all unbound disks for the controller listed in the Available Disk list.

2. Select **Hot Spare** using the BIND TYPE drop-down box.
3. In the Available Disks box, select the disk(s) to be used as hot spares, then click the add (arrow) button to add them to the Selected Disks list.

   NOTE: As an aid in identifying a disk module's physical location, select it in the Selected Disks list, then click Identify Disks. This causes the disk drive LED to flash.

4. Click **OK** to close the Binding… dialog box and begin the binding process. The Progress Report dialog box opens, showing the status of the binding process.
5. Upon 100% completion, click **Close** in Progress Report window.
6. Restart the K2 Media Server.

Loading K2 10Gv2 RAID controller and expansion chassis microcode

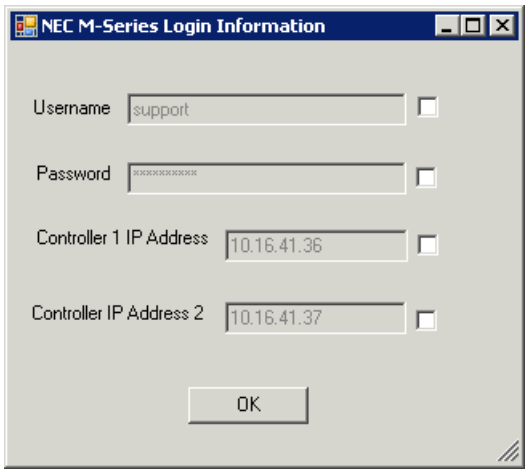
The K2 10Gv2 RAID controller must be connected to the control network to support the operations in this topic.

You might be instructed in K2 Release Notes to upgrade the RAID Controller microcode and/or expansion chassis on the RAID chassis. This allows you to take advantage of the RAID enhancements and benefit from improved reliability.

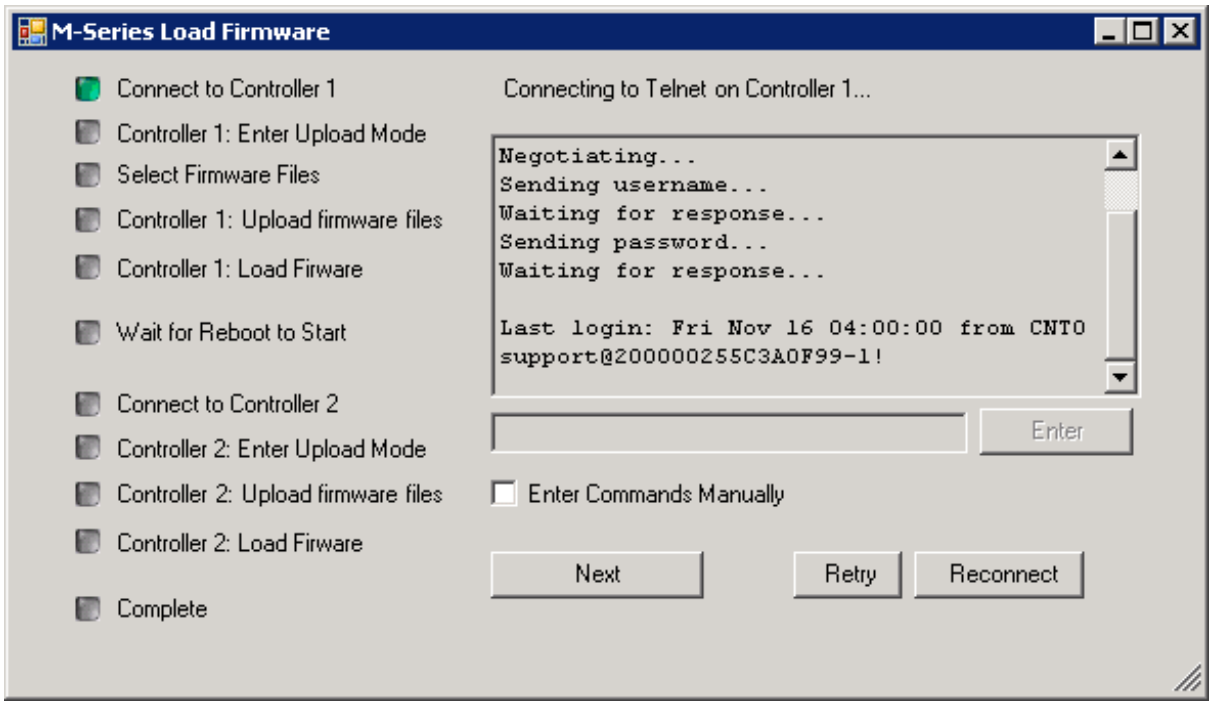
1. If upgrading expansion chassis microcode, take the RAID system offline.
2. In Storage Utility, right-click a controller in the tree view, then do one of the following:
   - To load controller microcode select **Advanced | Load Controller Microcode**
   - To load expansion chassis microcode select **Advanced | Load Disk Enclosure Microcode**

   Redundant controllers that share the same set of disks are automatically selected and upgraded as a pair.

   The Login Information dialog box opens.



3. If necessary, enable fields and enter username, password, or controller IP address, then click **OK**.
   The Load Firmware wizard opens.



4. Work through the wizard as follows:
   a) At each wizard page, read messages in the center window to follow progress and wait until the green indicator verifies that operations are complete. Then click **Next** to proceed.
   b) When prompted, browse to and select the folder that contains the controller microcode.
   c) When waiting for the controller to reboot, proceed after a "Controller...back online" message is displayed in the center window.
   d) If the RAID controller chassis has redundant controllers, after working through pages for Controller 1, work through similar pages for Controller 2.

      You do not need to select microcode for Controller 2. The microcode you selected for Controller 1 is automatically loaded onto Controller 2.

5. On completion, proceed as follows:

   - If the RAID controller chassis has redundant controllers, power cycle the RAID controller chassis, then restart the K2 Media Server.
   - If the RAID controller chassis does not have redundant controllers, no power cycle is required. The firmware download is complete.

Downloading disk drive firmware

- All K2 clients and other clients must be powered down, or in some other way disconnected from the K2 SAN.
- The K2 Media Server through which Storage Utility is connected to the RAID Storage must be powered up.

- All other K2 Media Servers must be powered down.

You might be instructed in K2 Release Notes to upgrade disk drive firmware. This allows you to take advantage of the disk drive enhancements and benefit from improved performance and reliability.

To determine your disk drive type and current firmware version, select a disk drive icon in the Storage Utility tree view, then note the drive properties reported in the right-hand pane. Use the following procedure if you need to download disk drive firmware.

NOTE: The disk drives on each controller are upgraded one at a time which can take as long as 2 minutes per drive. Take this into consideration when scheduling the upgrade.

1. Refer to *K2 Release Notes* to determine firmware types, versions, files, and any other special instructions regarding the particular disk drive firmware you are downloading.
2. In the Storage Utility, right-click a controller in the tree view, then select **Advanced | Download Disk Firmware** in the context menu.

   The Open File dialog box opens.

   ⚠ ***CAUTION: Do not attempt to download firmware to a single disk, unless directed to do so by Grass Valley. Downloading to a single disk can trigger a disk rebuild, with potential loss of data.***

3. In the Open File dialog box, browse to the desired firmware file for your disks, select the file, and click **OK**.

   As instructed by a message that appears, watch the lights on the drives. For each drive, one at a time, the lights flash as firmware loads. Wait until the lights on all the drives on which you are downloading firmware have completed their flashing pattern. This can take several minutes.

   The Progress Report window appears showing the disk firmware download task and the percentage complete.

4. When finished, restart the K2 Media Server.

Replacing a disk module

If the RAID chassis has a single controller (non-redundant), you must take the K2 SAN offline before replacing a failed controller. Refer to procedures in the Instruction Manual for your RAID storage chassis. The remainder of this procedure does not apply to non-redundant systems.

If the RAID chassis has redundant controllers and is properly cabled and configured for a redundant K2 SAN, you can replace a failed controller while media access is underway, as described in this procedure. When a controller detects a fault on its redundant partner controller, the good controller disables the faulty controller automatically. In most cases an error message informs you of the fault and when you check the controller's status in Storage Utility it reports as disabled.

However, you can also manually disable a controller. In the event that one of the RAID controllers appears operational, but also reports faults through various log files and status indicators, you can choose to disable the controller and replace it. Disabling the controller and removing it in this way avoids interruptions in signal output that can occur if the module fails or if it is simply hot swapped while it is the active controller. When the replacement RAID controller module is installed, it is automatically enabled and becomes the backup controller.

On a RAID chassis with two controllers, if the replacement controller's firmware is not the same as the firmware on the redundant (currently installed) controller, the firmware on the replacement controller is automatically upgraded or downgraded to match the current system level firmware.

NOTE: Refer to the Instruction Manual for your RAID storage chassis for procedures on removing and replacing the RAID controller module.

1. Open the Storage Utility.
2. Expand the tree view to display the controllers.
3. Select the controller and check its status, then proceed as follows:
   - If the faulty controller reports as disabled, proceed to the next step in this procedure.
   - If the faulty controller reports as online, right-click the controller icon in the tree view, and select **Advanced | Disable Controller 0** or **Disable Controller 1**, then click **OK** to continue.

   The RAID controller is disabled. You can check controller status in the Storage Utility. You may need to refresh the display.

   NOTE: If you accidentally disable the wrong controller, you can enable it again by removing it and then replacing it in the chassis.
4. Remove and replace the disabled RAID controller module.

   Refer to procedures in the Instruction Manual for your RAID storage chassis.
5. On inserting the replacement RAID controller, it initializes and is automatically enabled to become the "backup" RAID controller.

Replacing a K2 10Gv2 RAID controller

The K2 10Gv2 RAID controller must be connected to the control network to support the operations in this topic.

If the RAID chassis has a single controller (non-redundant), you must take the K2 SAN offline before replacing a failed controller. Refer to procedures in the Instruction Manual for your RAID storage chassis. The remainder of this procedure does not apply to non-redundant systems.

If the RAID chassis has redundant controllers and is properly cabled and configured for a redundant K2 SAN, you can replace a failed controller while media access is underway, as described in this procedure. When a controller detects a fault on its redundant partner controller, the good controller disables the faulty controller automatically. In most cases an error message informs you of the fault and when you check the controller's status in Storage Utility it reports as disabled.

However, you can also manually disable a controller. In the event that one of the RAID controllers appears operational, but also reports faults through various log files and status indicators, you can choose to disable the controller and replace it. Disabling the controller and removing it in this way avoids interruptions in signal output that can occur if the module fails or if it is simply hot swapped while it is the active controller. When the replacement RAID controller module is installed, it is automatically enabled and becomes the backup controller.

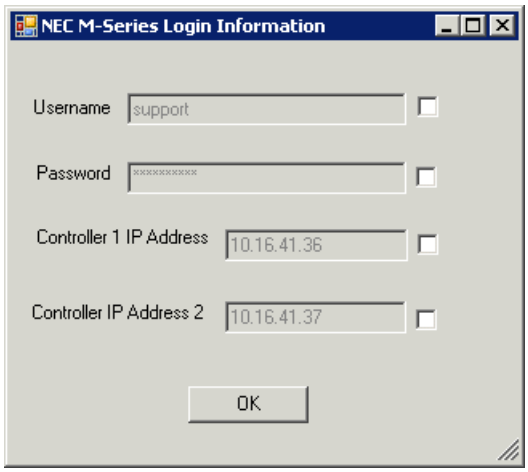
On a RAID chassis with two controllers, if the replacement controller's firmware is not the same as the firmware on the redundant (currently installed) controller, the firmware on the replacement controller is automatically upgraded or downgraded to match the current system level firmware.

NOTE: Refer to the Instruction Manual for your RAID storage chassis for procedures on removing and replacing the RAID controller module.

1. Open the Storage Utility.
2. Expand the tree view to display the controllers.

3. Select the controller and check its status, then proceed as follows:
   - If the faulty controller reports as disabled, proceed to the next step in this procedure.
   - If the faulty controller reports as online, right-click the controller icon in the tree view, and select **Advanced | Disable Controller 0** or **Disable Controller 1**, then click **OK** to continue.

   The Login Information dialog box opens.



4. If necessary, enable fields and enter username, password, or controller IP address, then click **OK**.

   The Disable Controller wizard opens.
5. At each wizard page, read messages in the center window to follow progress and wait until the green indicator verifies that operations are complete. Then click **Next** to proceed.
6. When a "Controller...disabled" message opens, click **Yes** to confirm and close the wizard.

   The RAID controller is disabled. You can check controller status in the Storage Utility. You may need to refresh the display.

   NOTE: If you accidentally disable the wrong controller, you can enable it again by removing it and then replacing it in the chassis.
7. Remove and replace the disabled RAID controller module.

   Refer to procedures in the Instruction Manual for your RAID storage chassis.
8. On inserting the replacement RAID controller, it initializes and is automatically enabled to become the “backup” RAID controller.

Configuring RAID chassis network and SNMP settings

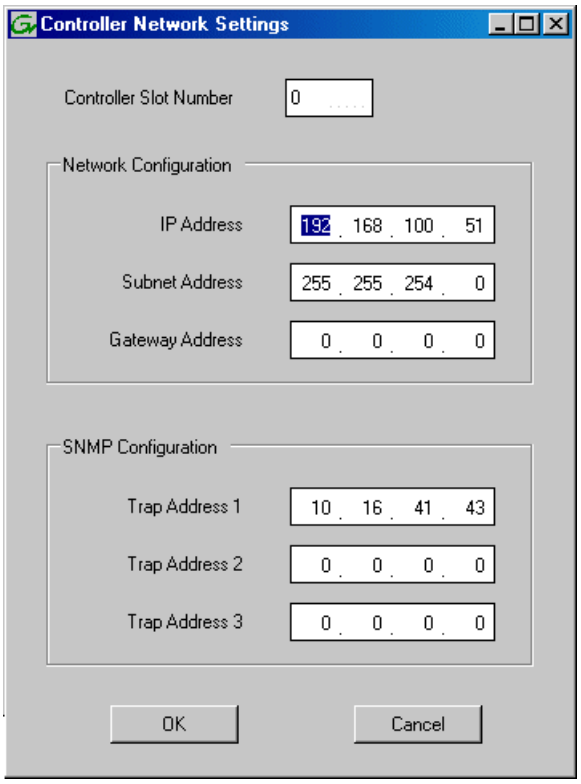
Through Storage Utility you can configure the following settings on a RAID chassis:

- IP address
- Subnet mask
- Gateway Address
- SNMP trap destinations

Whenever you modify control network settings or FTP/streaming network settings on any device, you must then redeploy the hosts file if that is your name resolution mechanism.

Network and SNMP settings are set and stored on the RAID controller. Therefore, if the RAID chassis has two controllers, each controller must be configured separately, as in the following procedure.

1. In the K2Config application tree view, open the node for a K2 Media Server and select the **File System Server** node to open its property page. On the property page click **Launch Storage Utility**. Storage Utility opens. You can now configure the network settings on the controller connected to the selected K2 Media Server.
2. In the Storage Utility, right-click the icon for a RAID controller and select **Configuration | Network Properties**. The Network Settings dialog box opens.



3. In the Controller Slot Number field enter **0** and then press **Enter**. The settings from controller 0 are loaded into the Controller Network Settings dialog box and are available for you to modify.
4. Enter the control network IP address and other network settings.
5. You want SNMP trap messages go to a SNMP manager, so for SNMP Configuration enter the IP address of the SNMP manager PC. You can also enter IP addresses for other SNMP managers to which you want to send SNMP trap messages.

   Refer to related topics about Grass Valley recommended deployment and monitoring solutions in the "About This Release" section of the K2 Topic Library.
6. If the RAID chassis has two controllers, in the Controller Slot Number field enter **1** and then press **Enter**. The settings from controller 1 are loaded into the Controller Network Settings dialog box and are available for you to modify. Repeat the previous steps to configure controller 1.
7. Click **OK** to save settings and close.

8. Restart the RAID chassis to put SNMP configuration changes into effect.

Replacing a controller

If the RAID chassis has a single controller (non-redundant), you must take the K2 SAN offline before replacing a failed controller. Refer to procedures in the Instruction Manual for your RAID storage chassis. The remainder of this procedure does not apply to non-redundant systems.

If the RAID chassis has redundant controllers and is properly cabled and configured for a redundant K2 SAN, you can replace a failed controller while media access is underway, as described in this procedure. When a controller detects a fault on its redundant partner controller, the good controller disables the faulty controller automatically. In most cases an error message informs you of the fault and when you check the controller's status in Storage Utility it reports as disabled.

However, you can also manually disable a controller. In the event that one of the RAID controllers appears operational, but also reports faults through various log files and status indicators, you can choose to disable the controller and replace it. Disabling the controller and removing it in this way avoids interruptions in signal output that can occur if the module fails or if it is simply hot swapped while it is the active controller. When the replacement RAID controller module is installed, it is automatically enabled and becomes the backup controller.

On a RAID chassis with two controllers, if the replacement controller's firmware is not the same as the firmware on the redundant (currently installed) controller, the firmware on the replacement controller is automatically upgraded or downgraded to match the current system level firmware.

NOTE: Refer to the Instruction Manual for your RAID storage chassis for procedures on removing and replacing the RAID controller module.

1. Open the Storage Utility.
2. Expand the tree view to display the controllers.
3. Select the controller and check its status, then proceed as follows:
   - If the faulty controller reports as disabled, proceed to the next step in this procedure.
   - If the faulty controller reports as online, right-click the controller icon in the tree view, and select **Advanced | Disable Controller 0** or **Disable Controller 1**, then click **OK** to continue.

   The RAID controller is disabled. You can check controller status in the Storage Utility. You may need to refresh the display.

   NOTE: If you accidentally disable the wrong controller, you can enable it again by removing it and then replacing it in the chassis.
4. Remove and replace the disabled RAID controller module.

   Refer to procedures in the Instruction Manual for your RAID storage chassis.
5. On inserting the replacement RAID controller, it initializes and is automatically enabled to become the "backup" RAID controller.

Custom K2 SAN systems

About custom K2 SAN systems

Custom systems extend the infrastructure of standard K2 SAN product bundles. For example, a custom K2 SAN has multiple primary RAID chassis connecting to K2 Media Servers via a Fibre

Channel fabric consisting of one or more Fibre Channel switches. This is an extension of the Fibre Channel infrastructure of a standard K2 SAN, which has a single primary RAID chassis connecting to one or more K2 Media Servers via direct Fibre Channel connection. Only qualified Grass Valley personnel that have received K2 SAN technical training should attempt to design, install, and configure custom K2 SAN systems. Refer to related topics in this document for more information on custom K2 SAN systems.

About custom K2 SAN information

The information in this section applies to custom-designed K2 SAN systems, built with recently released Grass Valley hardware and software products. Custom systems of this type are also called Level 40 systems.

This information assumes that the reader understands and has access to the baseline information about standard, pre-defined K2 SAN systems as presented in customer documentation. The customer documents that relate to the K2 SAN system are as follows:

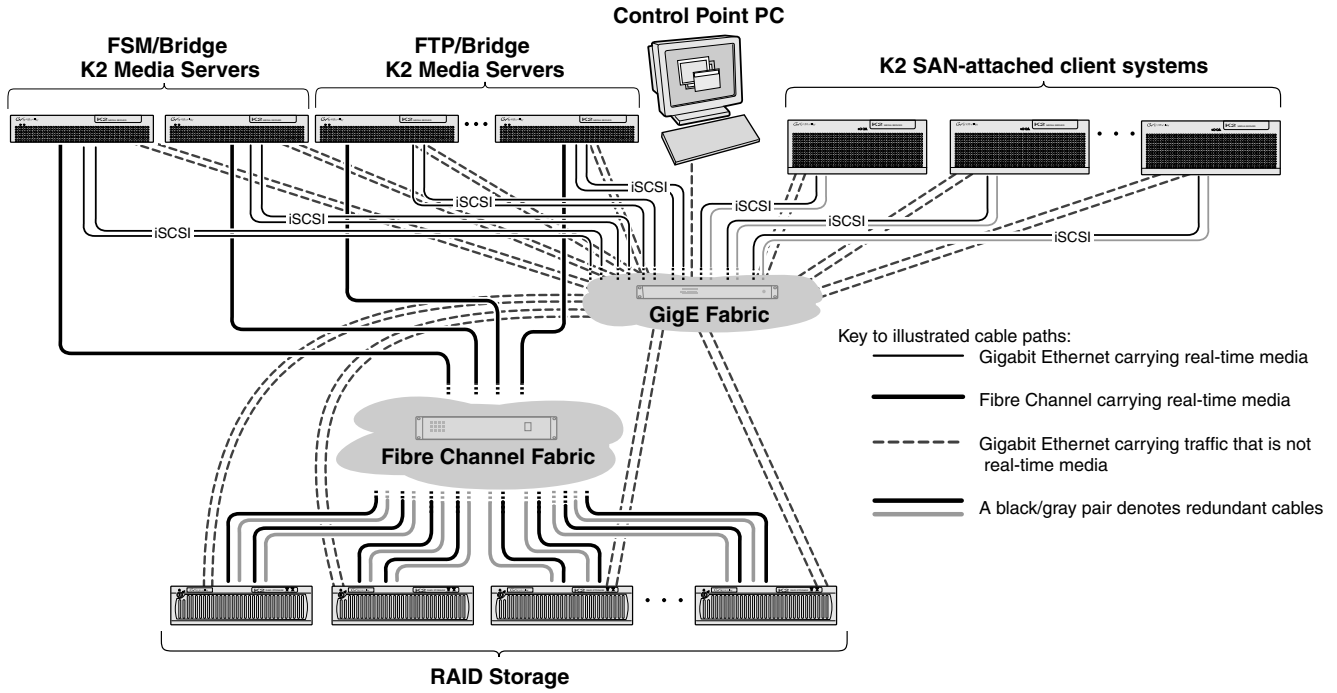
- K2 SAN Installation and Service Manual
- K2 System Guide
- K2 Release Notes

These documents are intended for customers with standard systems. While much of the information in these customer documents also applies to custom systems, in most cases you must interpret and extend the information in order to apply the procedures to a custom system.

System diagrams

The following sections provide high-level diagrams of example systems with guidelines for commissioning and operating.

iSCSI extended (redundant FSMs)



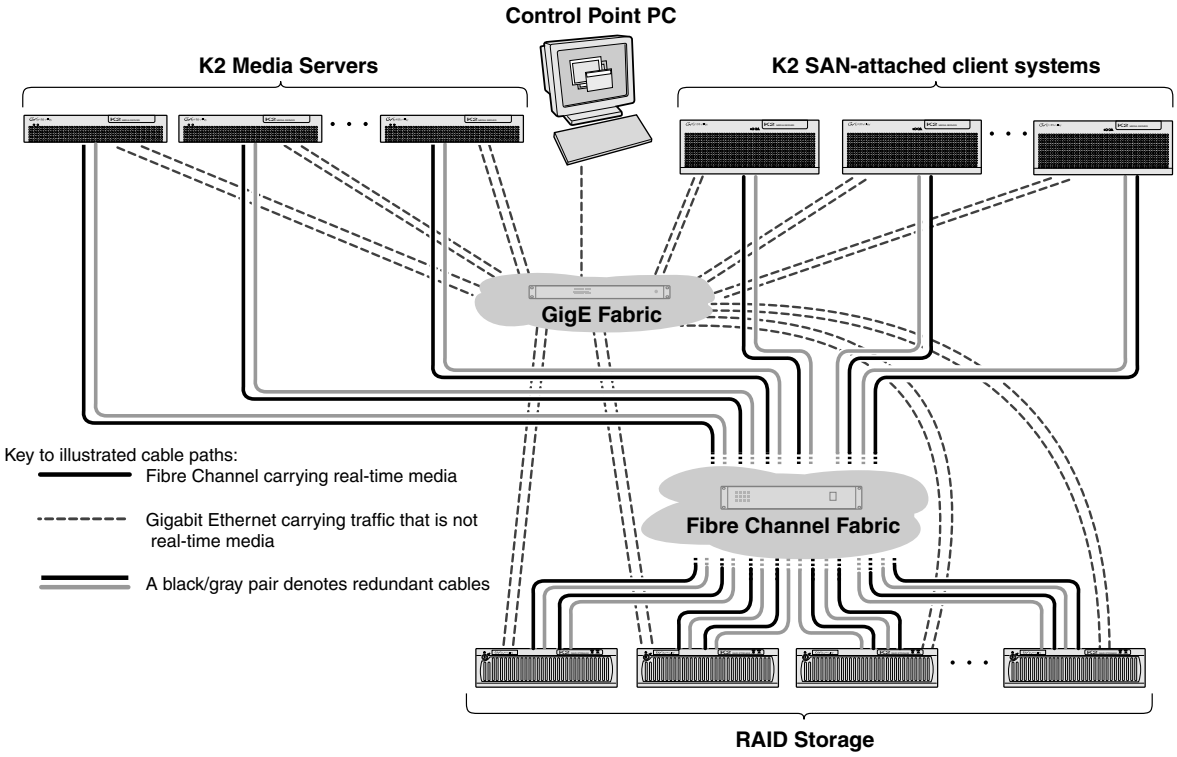
This system differs from the Level 3R system as follows:

- A Fibre Channel switch fabric, comprised of one or more Fibre Channel switches, is interposed between K2 Media Servers and the RAID Storage devices. This allows more RAID Storage devices to be connected, which provides higher bandwidth and more storage space.
- Additional FTP/Bridge K2 Media Servers are added, providing additional iSCSI bridges to support more clients and higher bandwidth clients.

Guidelines for this system are as follows:

- The Fibre Channel switch fabric must be zoned.

Fibre Channel connected clients (redundant FSMs)



This system differs from the iSCSI extended system as follows:

- K2 SAN-attached client systems have a Fibre Channel card installed and are connected directly to the Fibre Channel Fabric. This replaces the iSCSI layer.
- Because there is no iSCSI, there is no need for multiple K2 Media Servers to act as iSCSI bridges, reducing the total number of K2 Media Servers required.
- There is a RAID chassis dedicated for file system metadata.
- The FSM K2 Media Servers read/write data over Fibre Channel only to the metadata RAID chassis.
- The FSM K2 Media Servers must "see" (be on the same Fibre Channel fabric with) the media RAID, even though they do not read/write data to the media RAID.

Guidelines for this system are as follows:

- When adding a K2 SAN-attached client system in K2Config, set the Storage access option to **Fibre Channel**.
- When configuring the system in K2Config, select the **Server redundancy** option.

Explanations and procedures

The following information might or might not apply to your particular custom system. Make sure you understand the application of the information to your own custom system.

General guidelines

The following guidelines apply to all systems:

- Update to version 3.0.1.21 or higher before attempting to configure a custom system.
- When you change the RTIOS, you must reboot the system for it to take effect.
- For a Fibre Channel SAN, the 8 Gig controller must be set to Fabric.
- When connecting iNavi make sure the browser has scripting turned on.

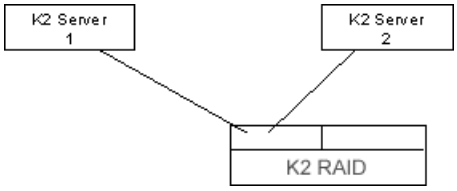
K2 RAID Fibre Channel port redundant configuration

In addition to the Level 3 non-redundant and Level 3 redundant configurations, you can also cable and use K2 RAID Fibre Channel ports for Fibre Channel port redundancy, as explained in this section.

For clarity, Level 3 non-redundant and Level 3 redundant configurations are included in the following illustrations:

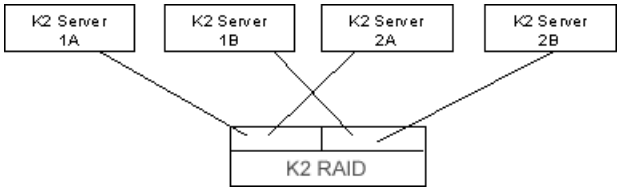
L3 non-redundant

Two K2 Servers connect to one RAID controller.



L3 redundant

Four K2 Servers connect to two RAID controllers. Servers 1A and 1B are redundant. Servers 2A and 2B are redundant.

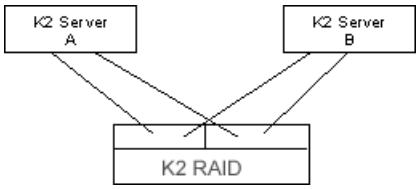


In the above examples, one K2 Server connects to one RAID controller only. This means there is no redundancy (failover) at the Fibre Channel port level. Redundancy in a system that uses this configuration must therefore be at the K2 Client/K2 Server level. For example, in a L3 redundant system, K2 clients can connect to either of a redundant K2 Server pair. This means that if K2 Server 1A goes down, K2 Clients connect to K2 Server 1B.

FC port redundant

NOTE: Do not use the FC port redundant configuration without first consulting with Grass Valley Server Engineering.

Two K2 Servers each connect to two RAID controllers. Servers A and B are redundant.



With this configuration the redundancy is at the Fibre Channel port level. If one of the FC ports, cables, or RAID controllers fails, the redundant connection takes over.

The following rules and policies apply to the FC port redundant configuration:

- Only use this configuration on systems that do not have a conflicting failover policy. For example, if a system is assembled with an iSCSI failover mechanism AND a Fibre Channel port failover mechanism, the policies of these two failover mechanisms can conflict during a failover event and result in scrambled data pathways. Examples of systems without conflicting failover policies are as follows:
  - A system with iSCSI clients that are non-redundant. This means the clients have just one connection to the iSCSI VLAN (media ports on GigE switch). Since there is no iSCSI failover in this type of system, there is no conflict with the Fibre Channel failover policy.
  - A system with Fibre Channel connected clients. Fibre Channel clients can be non-redundant (one FC cable connected to the FC switch) or redundant (two FC cables connected to the FC switch). The Fibre Channel failover policy is cohesive between FC client connections and FC RAID connections, so there is no conflict.
- Do not use this configuration on a system with redundant iSCSI clients, as this introduces a conflicting failover policy. If iSCSI clients are redundant and K2 Server FC ports are redundant, failover conflicts occur that render the system inoperable.

Installing SANsurfer Switch Manager software

Use the SANsurfer Switch Manager application to configure the QLogic Fibre Channel Switch. Install the software on the Control Point PC.

1. Close all programs currently running and insert the SANsurfer Switch Manager Installation Disk into CD-ROM drive.
2. Open the CD with Windows Explorer. Locate and run the following installation program file:

   `Windows_5.00.xx.xx.exe`

3. Follow on-screen instructions to install the software. Click Next to accept defaults.

Uninstalling SANsurfer Switch Manager software

When uninstalling the software, use the QLogic uninstall program in Program Files.

NOTE: Do not attempt to use Windows Control Panel Add/Remove Programs to uninstall SANsurfer Switch Manager.

The *UninstallerData* folder in the Install directory contains the uninstall program. Also, a shortcut/link to the uninstall program was installed in the installation directory during the SANsurfer Switch Manager installation process. The default installation directory is:

C:\Program Files\QLogic_Corporation\SANsurfer

1. Browse for the uninstall program file or the shortcut/link that points to the uninstall program file.

   The uninstall program shortcut is in the same folder as the program shortcut (Start menu, program group, on desktop, or user specified) that is used to start the SANsurfer Switch Manager application.

2. Double-click the uninstall program file or shortcut/link, and follow the instructions to uninstall the SANsurfer Switch Manager application.

Fibre Channel switch domains

If a system has more than one SCSI Fibre Channel switch, such as in a redundant system, it is required that each switch have a unique domain number. This is a requirement for switches with ISLs and for switches without ISLs.

Configuring Fibre Channel switch

- For a direct console connection, a 9-pin serial cable must be connected from a test PC to the QLogic Fibre Channel switch serial port.
- A crossover Ethernet cable must be connected from the test PC to the QLogic Fibre Channel switch Ethernet port.
- The correct version of firmware and license must be installed.

1. Install the TeraTerm application on the test PC or start a Telnet session to configure the switch.

   The switch logon prompt displays in the HyperTerminal window. The command line interface should start with: `SANbox#>`

2. Log on with the following:

   - User: `admin`
   - Password: `password`

3. At the SANbox prompt, type `admin start` and press **Enter**.

   The prompt changes to `SANbox(admin)#>`

4. Type set `setup system` and press **Enter**.
5. Do the following to set the IP address:
   a) At **EthIPv4NetworkEnable**: type `True` and press **Enter**.
   b) At **EthIPv4NetworkDiscovery**: type `1` (for Static) and press **Enter**.
   c) At **EthIPv4NetworkAddress**: type the IP address and press **Enter**.
   d) At **EthIPv4NetworkMask**: type the subnet address and press **Enter**.
6. For the remainder of entries, press **Enter** until **Do you want to save and activate this system setup (y/n)** appears.
7. Type `y` to save the setup.

8. At the SANbox (admin) prompt, type `show setup system` and press **Enter** to verify the IP address.
9. At the SANbox (admin) prompt, type `config edit` and press **Enter** to continue with the configuration.
10. At the SANbox (admin-config) prompt, type `set config switch` and press **Enter**.
11. Press **Enter** until **SymbolicName** displays.
12. Type the name of the Fibre Channel switch and press **Enter**.
13. Continue to press **Enter** until you are returned to the SANbox (admin-config) prompt.
14. Type `config save` and press **Enter**.

    The config named default has been saved displays.
15. Type `config activate` and press **Enter**.
16. Type `show switch` and press **Enter** to verify the switch name is the same with the one you entered earlier.
17. Type `exit` and press **Enter** to log off.

Fibre Channel fabric cabling

Make your cable connections symmetrical when cabling a multiple switch fabric. For example, for a K2 SAN-attached client system (or Server) that has redundant connections that each go to a different switch, if you make one connection to port 1 on switch A, make the other connection to port 1 on switch B. This is especially important on switches that are not interconnected by ISLs, as the Fibre Channel failover path can get confused if redundant cable connections are not in the same order on both switches.

To cable the Fibre Channel fabric for such a system, do the following:

- Each K2 Media Server is connected to a different zone. For example, connect as follows:
  - Connect K2 Media Server 1 to switch A port 0 (Zone 1)
  - Connect K2 Media Server 2 to switch A port 8 (Zone 2)
  - Connect K2 Media Server 3 to switch B port 0 (Zone 3)
  - Connect K2 Media Server 4 to switch B port 8 (Zone 4)

  There is only one Fibre Channel connection at each K2 Media Server. The second Fibre Channel port on each K2 Media Server not used.
- Each K2 RAID storage chassis is connected to all four zones. For example, connect RAID chassis 1 as follows:
  - Connect controller 0 port HP0 to switch A port 1 (Zone 1)
  - Connect controller 0 port HP1 to switch A port 9 (Zone 2)
  - Connect controller 1 port HP0 to switch B port 1 (Zone 3)
  - Connect controller 1 port HP1 to switch B port 9 (Zone 4)

  Connect RAID chassis 2, 3, and 4 similarly.

Upgrading K2 systems in the field

Upgrade instructions

Use these installation instructions to upgrade your K2 system. Refer to the section in this document that applies to the upgrade kit that you received.

Upgrade kit	Section
K2-XDP2-CPU-FK	*Installing software and CPU carrier module upgrades* on page 784.
K2-XDP2-V9-FK	*Installing software and CPU carrier module upgrades* on page 784.
K2-XDP2-3G-FK	*Install codec module upgrade* on page 807.
K2-XDPSVR-V9-FK	*Upgrading a K2 Media Server to version 9.x* on page 809.
CP-XDPCP-V9-FK	*Upgrading a Control Point PC* on page 811.
K2-XDP2-2IO-FK	*Installing a two channel upgrade* on page 815.
K2-XDP2-AVC-2CH-FK K2-XDP2-3XP-SSM-FK K2-XDP2-6X-SSM-FK K2-XDP2-TRIPLE-FK K2-XDP2-UHDTV1-FK	*Installing an upgrade license* on page 818.
K2-XDP2-MPG2-MC-FK	*Installing a MPEG/Multi-Cam codec option upgrade* on page 820.
K2-DYNOZOOM-FK	*Install DynoZoom upgrade* on page 822

Safety Summaries

⚠ ***WARNING: In order to avoid personal injury and prevent damage to this product and its peripheral products, be sure to review all safety and ESD precautions listed in the K2 product Service Manual.***

Installing software and CPU carrier module upgrades

Tools and materials needed:

- Hardware as provided by upgrade kit. See descriptions below.
- Torx tool with T15 magnetic tip

This section provides instructions for the following field kits:

Upgrade Nomenclature	Description
K2-XDP2-CPU-FK	Processor upgrade Field Kit. Includes updated Type IV CPU carrier module required for advanced features such as ShareFlex. NOT AVAILABLE for K2-SOLO models.

Upgrade Nomenclature	Description
K2-XDP2-V9-FK	K2 Summit / K2 Solo 9.x Upgrade Field Kit. Includes 9.x system software license, 16GB CompactFlash system drive with image, and 16GB USB recovery flash drive with Acronis backup software and new Windows Embedded System 7 license with Embedded Security Solution. Requires either Type II, Type III, or Type IV CPU carrier module.

For any upgrade from a software version lower than 9.0 to a 9.x version, you must reimage the system and do all the steps as directed in the procedure to ensure the system is properly initialized.

⚠ ***CAUTION: This system contains board-level components that must be protected from static discharge and physical shock. Wear a wrist strap grounded to the system chassis when handling system components.***

Work through the tasks in this section sequentially.

Saving settings

Do this task for both software and CPU carrier module upgrade kits.

Before doing this task, the 16GB USB Recovery Flash Drive that you received with the kit must have the serial number of the K2 Solo 3G system written on it to identify it as belonging to that individual system.

NOTE: Do not attempt to use a single Recovery Flash Drive on multiple systems. This can overwrite saved settings and lose the ability to restore settings on one or more systems. Also, software licensing requires one Recovery Flash Drive for each system.

1. If you are working on a K2 client SAN-attached system, record iSCSI bandwidth settings, so you can reconfigure after removing and readding to SAN.
2. Make sure you are logged in to the K2 Solo 3G system with administrator privileges.
3. Connect the USB Recovery Flash Drive to a USB port on the K2 Solo 3G system.
4. On the USB Recovery Flash Drive, navigate to the following location:

   `\tools\SaveRestoreScripts.`

   NOTE: Do not attempt to use the same Recovery Flash Drive on multiple systems.
5. Run the following and wait for the process to complete:

   `ssave.bat`

   This saves current settings onto the USB Recovery Flash Drive in the `\settings` directory.
6. Disconnect the USB Recovery Flash Drive.

Next, do one of the following:

- If you are installing K2-XDP2-V9-FK on a K2 Summit 3G system with mSATA system drive, skip ahead and reimage.
- If you are installing K2-XDP2-V9-FK on a K2 Solo 3G system with CompactFlash system drive, skip ahead and replace the CompactFlash boot media with the new larger 16GB CF.
- If you are installing K2-XDP2-CPU-FK on a K2 Solo 3G system, replace the CPU carrier module.

Replace CPU carrier module

Do this task if installing K2-XDP2-CPU-FK on a K2 Solo 3G system.

NOTE: Do not attempt to replace the CPU carrier module on a K2 Solo Media Server. K2-XDP2-CPU-FK does not apply to K2 Solo Media Server.

1. Shutdown the K2 Solo 3G system.
2. Disconnect all power cables from the K2 Solo 3G system.
3. Press the power button on the K2 Solo 3G system to drain off power from boards.
4. Remove any cables connected to the CPU carrier module.
5. Replace the current CPU carrier module with the new CPU carrier module.
6. Reconnect cables to the CPU carrier module.
7. Reconnect power cables.

Next, do one of the following:

- If you are installing K2-XDP2-V9-FK on a K2 Summit 3G system with mSATA system drive, skip ahead and reimage.
- If you are installing K2-XDP2-V9-FK on a K2 Solo 3G system with CompactFlash system drive, replace the CompactFlash boot media with the new larger 16GB CF.

Replace CompactFlash boot media

Do not do this task if:

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

Do this task if:

- A K2 Solo 3G system with CompactFlash system drive.

Before doing this task, make sure the K2 Solo 3G system is powered off.

1. Remove the front bezel assembly.
2. Replace the current CompactFlash boot media with the new CompactFlash boot media.
3. Replace the front bezel assembly.

Next, reimage the K2 Solo 3G system.

Reimage K2 Solo 3G system

Do this task for both software and CPU carrier module upgrade kits.

- Settings must be saved using the `ssave.bat` script.
- Hardware must be replaced, as supplied by your upgrade kit.
- Cables must be reconnected.
- The iSCSI-SVR (FSM TOE) licenses must be backed up prior to reimaging the file system server (FSM).

1. If you have not already done so, connect keyboard, monitor, and mouse.

2. Do the following:
   a) Insert the Recovery Flash Drive into a USB port.
   b) Restart the machine, or power on if currently shut down.

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

      A MS-DOS command window opens.

   c) When prompted with a list of options, type `2` to select the Acronis option and then press **Enter**.

   The Acronis program loads.
3. In the Acronis main window, click **Recovery**.

   The Restore Data Wizard opens.
4. On the Welcome page, click **Next**.
5. On the Backup Archive Selection page, do the following:
   a) In the tree view expand the node for *`Computer/SummitBoot9_0_2_1803(D:)`*. This is the Recovery Flash Drive.
   b) In the Images folder, select the correct version of the image file such as *`Summit_WES7_7.0.13.tib`*.
   c) Click **Next**.
6. On the Restoration Type Selection page, select **Restore disks or partitions** and then click **Next**.
7. On the Partition or Disk to Restore page, select **MBR and Track 0** and then click **Next**.
8. On the Disk Selection page, select **Disk 1** and then click **Next**.

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

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

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

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

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

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

    The machine restarts automatically.
22. Remove the recovery media while the machine is shutting down.
23. Upon startup, wait for initialization processes to complete. This can take several minutes, during which time USB keyboard/mouse input is not operational. The system might automatically restart. Do not attempt to shutdown or otherwise interfere with initialization processes.
24. When prompted, enter the K2 Solo 3G system machine name.

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

    After start up, one or more device discovery windows can open. Allow processes to complete without interference. Refer to Release Notes for informaion on compatible driver versions. If a Fibre Channel card driver, ignore until instructed later in this process.

    At first start up after reimage, the system is in Embedded Security Update mode by default.

Next, restore settings.

Restore settings after generic reimage

Do this task for both software and CPU carrier module upgrade kits.

Settings must be saved using *ssave.bat* before reimaging the K2 Solo 3G system, and the reimage (Acronis) process must be complete.

NOTE: Do not attempt to use a single Recovery Flash Drive on multiple systems. This can overwrite saved settings and lose the ability to restore settings on one or more systems. Also, software licensing requires one Recovery Flash Drive for each system.

1. If you have not already done so, start up the K2 Solo 3G system and log on with administrator privileges.

   The administrator password is `adminGV!`.
2. Connect the USB Recovery Flash Drive to a USB port on the K2 Solo 3G system.
3. From the USB Recovery Flash Drive, run the following and wait for the process to complete:

   Tools\SaveRestoreScripts\srestore.bat

Next, restore network configuration.

Restore network configuration

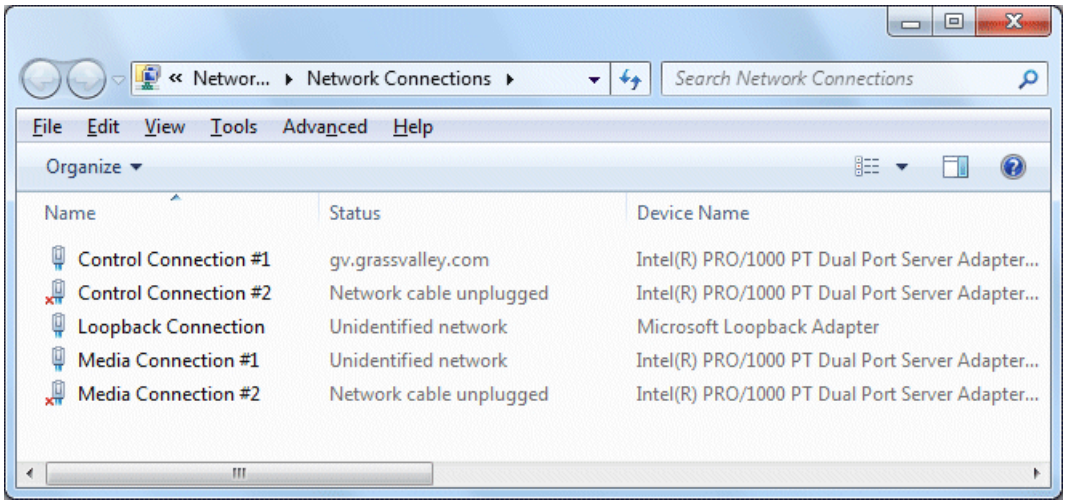
Do this task for both software and CPU carrier module upgrade kits.

Work through the tasks in this section sequentially to restore the default network configuration. As you do so, refer to `C:\ipconfig.txt` for the complete listing of the network settings that the K2 Solo 3G system had before reimaging.

Create the Control Team

NOTE: Team control ports only. Do not team media ports.

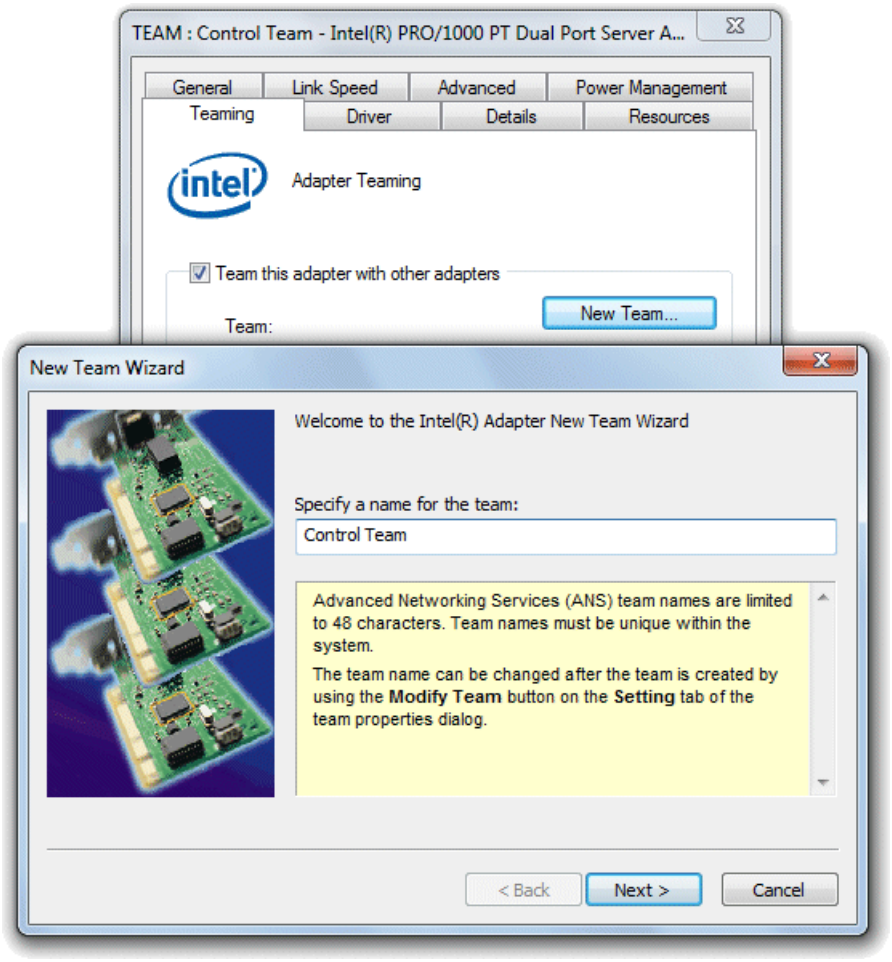
1. Open Network Connections, if it is not already open.
   a) From the Windows **Start** menu, in the **Run** or the **Search programs and files** box, type `ncpa.cpl` and press **Enter**.
2. In Network Connections, view **Details** and identify the adapter name that maps to Control Connection #1 and the adapter name that maps to Control Connection #2.



3. Right-click the adapter name that maps to Control Connection #1.
4. Select **Properties**, then click **Configure**.

   The Properties dialog box opens.

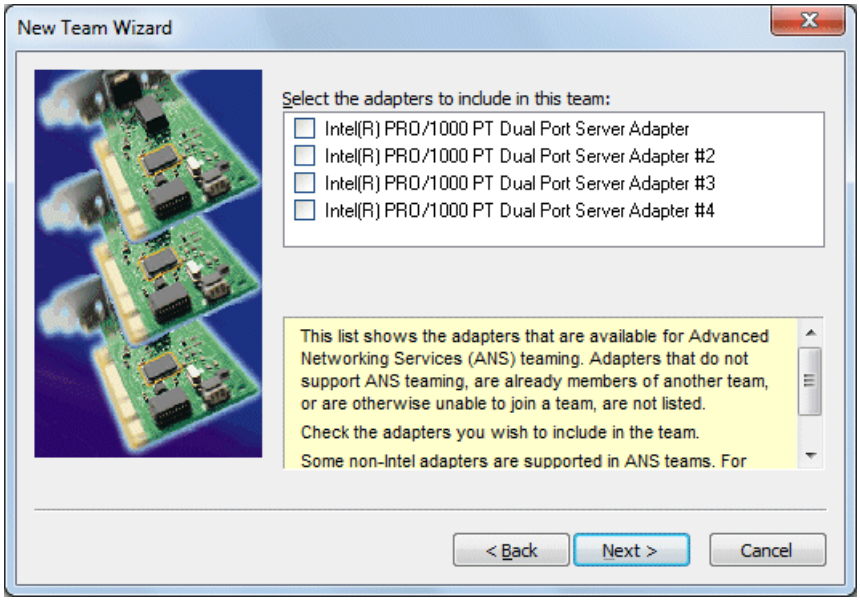
5. Select the **Teaming** tab.



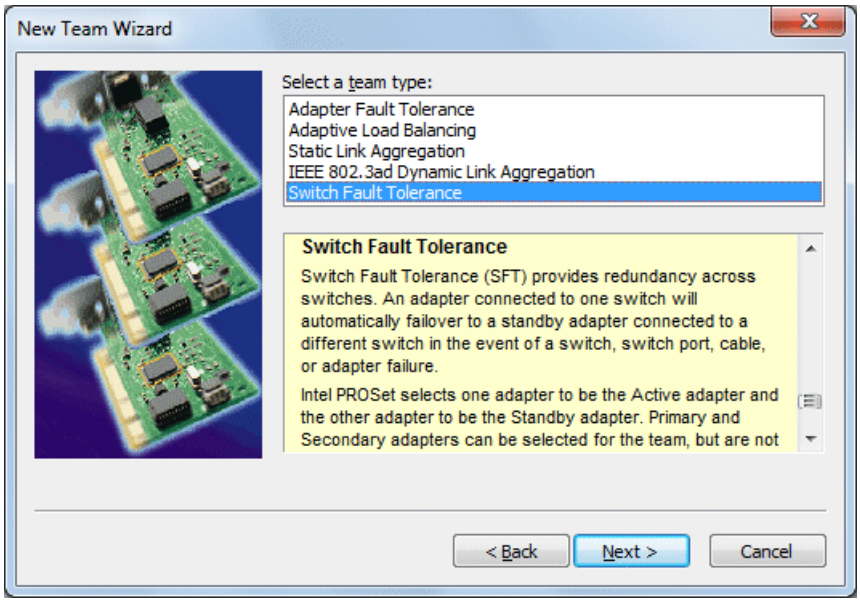
6. Select **Team this adapter with other adapters**, then click **New Team**. The New Team Wizard opens.

7. Enter Control Team.

   Click **Next**.



8. Select the check box for the adapter name that maps to Control Connection #1 and for the adapter name that maps to Control Connection #2. Click **Next**.



9. Select **Switch Fault Tolerance**. Click **Next**.
10. Click **Finish** and wait a few seconds for the adapters to be teamed.

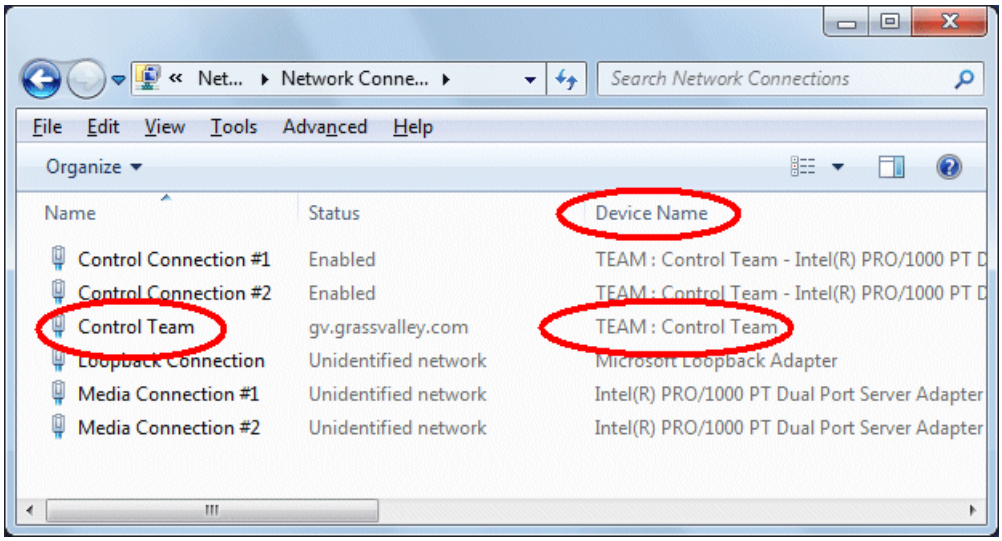
11. Open the Modify Team dialog box as follows:
    a) In **Device Manager | Network Adapters**, right-click **Control Team** and select **Properties**. The Properties dialog box opens.
    b) Select the **Settings** tab.
    c) Click **Modify Team**. A dialog box opens.
12. On the **Adapters** tab, do the following:
    a) Select the top entry, which is the adapter name that maps to Control Connection #1 and click **Set Primary**.
    b) Select the adapter name that maps to Control Connection #2 and click **Set Secondary**.
13. Click **OK** and **OK** and to close dialog boxes.
14. Restart the K2 Solo 3G system.

If continuing with network configuration, your next task is to name team and loopback.

Name team and loopback

- Adapters must be named
- The control team must be created

1. On the Windows desktop right-click **Start | Control Panel | Network and Sharing Center | Change adapter settings**. The Network Connections window opens.



2. For the Control Team and the loopback, select adapter names in the "Device Name" column and rename them as follows:
    a) Select the adapter name.
    b) Select **File | Rename** to enter rename mode.
    c) Type the name, as specified in the following table:

In the Device Name column, select this adapter name…	And rename it as follows:
TEAM : Control Team	Control Team

3. Do one of the following:
   - If you intend to use SiteConfig for device discovery and IP address configuration, you do not need to set an IP address for the Control Team at this time. You are done with this procedure.
   - If you are not using SiteConfig, set an IP address for the Control Team at this time. Use standard Windows procedures.

   NOTE: Do not set IP addresses for the two Media Connections.

If continuing with network configuration, your next task is to reorder adapters.

Reorder adapters

- Adapters must be named correctly
- The control team must be created
- The team and loopback must be named

1. Open Network Connections, if it is not already open.
   a) From the Windows **Start** menu, in the **Run** or the **Search programs and files** box, type `ncpa.cpl` and press **Enter**.

   The Network Connections window opens.
2. Select **Advanced**, then **Advanced Settings…**
3. On the **Adapters and Bindings** tab, depending on the K2 system storage, order adapters as follows:

Internal or direct-connect storage	Shared (SAN) storage
Loopback	Control Team
Control Team	Control Connection #1
Control Connection #1	Control Connection #2
Control Connection #2	Media Connection #1
Media Connection #1	Media Connection #2
Media Connection #2	Loopback
1394 Connection	1394 Connection

   If controlled by Dyno Production Assistant, refer to Dyno PA documentation for adapter order.
4. Click **OK** to close and accept the changes.
5. Close Network Connections.

Network configuration is complete.

Next, enhance network bandwidth.

Enhance network bandwidth

On K2 Summit/Solo systems with K2 system software 9.x, the on-board network adapters have a performance limitation that causes them to function at half the expected bandwidth. On most systems, there are no symptoms related to this limitation, as network traffic is below the limitation. Systems

using ShareFlex or having other requirements for high network bandwidth might be impacted to some degree. Symptoms include general network bandwidth restrictions, slow iSCSI I/O performance, slower than expected FTP traffic, and other slowness not caused by other factors.

Grass Valley requires that you remove the limitation and enhance the network performance. Once the limitation is removed, the change persists throughout normal software upgrades. However, if you reimage the K2 Summit/Solo system you must check and reapply the change if necessary.

To remove the limitation, disable "Large Send Offloads" on the network adapters and disable "CPU Power Technology" in the BIOS.

Refer to Grass Valley Knowledge Base Article *#000011688* for more information.

Disable Large Send Offloads

1. From the Windows operating **Start** menu, open **Control Panel**.
2. In **Control Panel**, open **Network and Sharing Center**.
3. In **Network and Sharing Center**, select **Change adapter settings**.
   Network Connections opens and displays network adapters, including the following:
   - Control Connection #1
   - Control Connection #2
   - Media Connection #1
   - Media Connection #2
4. For each Control Connection and each Media Connection, do the following:
   a) Right-click the connection and select **Properties**.
      The **Connection Properties** dialog box opens.
   b) In the **Connection Properties** dialog box, click **Configure**.
      The **Adapter Properties** dialog box opens.
   c) In the **Adapter Properties** dialog box, click the **Advanced** tab.
   d) On the Advanced tab, in the Settings list select **Large Send Offload v2 (IPv4)** and then in the Value drop-down list select **Disabled**.
   e) Click **OK** to save settings and close.
   f) Repeat these steps for each Control Connection and each Media Connection.

Next, disable CPU power technology.

Disable CPU Power Technology

1. Restart the K2 Summit/Solo system.
2. During the BIOS startup screen, press **F2** repeatedly until `Entering Setup...` appears.
   The BIOS screen opens.
3. On the BIOS screen, use arrow keys and select the **Advanced** tab.
4. On the Advanced tab select **CPU Core Configuration** and then press **Enter**.
   The CPU Core Configuration screen opens.

5. On the CPU Core Configuration screen, select **Power Technology** and then press **Enter**.
   A **Power Technology** dialog box opens.
6. In the **Power Technology** dialog box select **Disable** and then press **Enter**.
7. Press **F4** to save and exit.
   A **Save & Exit Setup** dialog box opens.
8. In the **Save & Exit Setup** dialog box, select **Yes** and then press **Enter**.
9. The K2 Summit/Solo system restarts.

Next, install the SiteConfig Discovery Agent.

Install the Discovery Agent on a K2 Summit/Solo system

Do this task for both software and CPU carrier module upgrade kits.

Find the Discovery Agent installation files on the USB Recovery Flash Drive you received with the upgrade kit. The files are in the `\release\DiscoveryAgent` folder.

1. Navigate to your SiteConfig files.
2. To launch the program that installs the ProductFrame Discovery Agent Service do the following:
   a) Copy the `Discovery Agent` directory to the device.
   b) In the directory, double-click the `DiscoveryAgentServiceSetup.msi` file.
      The setup program launches to install the SiteConfig Discovery Agent.
   c) Follow the setup wizard.
3. When presented with a list of device types, select one of the following as appropriate:
   - K2SummitSanClient
   - K2SummitStandaloneClient
   - K2SoloStandaloneClient
4. Complete the setup wizard and restart the device.
   The restart is required after the installation.

Next, do one of the following:

- Install software using SiteConfig.
- Install software manually.

If you install software with SiteConfig

Do not do the tasks in this section if:

- You install/upgrade software on the K2 Solo 3G system manually, rather than using SiteConfig.

Do the tasks in this section if:

- You use SiteConfig to install/upgrade software on the K2 Solo 3G system.

NOTE: You must use the same install/upgrade method now, either SiteConfig or manual, as you will use for installations and upgrades in the future. Do not switch between methods, using one method now and a different method for future installations and upgrades.

Follow the task in this section sequentially.

Deploy Embedded Security solution - One-time process

You must have a system system-specific recovery disk image of the computer on which you are doing the Embedded Security one-time process.

NOTE: A re-image of the computer might be necessary if the Embedded Security one-time process is done incorrectly. Follow instructions carefully.

This is a two-phase task:

1. Run a script on the local system to which you are deploying software.
2. Deploy software with SiteConfig.

NOTE: You must carefully read and verify that you have completed each step in the task. Do not assume the task is the same as other software install tasks with which you are familiar.

On the computers in your system that are running the Grass Valley Embedded Security solution, you must do a one-time initial deployment process, as instructed by this task. This task isolates the steps required for the one-time process. If you have sufficient knowledge of systems and upgrades, you can modify your software upgrade steps as necessary to do the one-time process at the same time as your other software upgrades, rather than as isolated steps. After you have done this one-time process, you can do future upgrades using the normal upgrade process.

This applies to the following:

- K2 Summit/Solo system
- All types/roles of K2 Media Server
- All types/roles of GV STRATUS server

1. Determine the status of the Embedded Security solution on the computer. You can use SiteConfig check/view software to make this determination or on the local computer you can use the Programs and Features Control Panel to make this determination. Proceed as follows:
   - If the computer does not have **McAfee Solidifier**, which is a component of the Embedded Security solution, do not continue with these steps. The computer must already have the Embedded Security solution before the one-time process is applied.
   - If the computer has **McAfee Solidifier** at version 6.1.1.369, do not continue with these steps. That version indicates that the computer already has the one-time process applied, through either a software installation or a disk image process.
   - If the computer has **McAfee Solidifier** at a version lower than 6.1.1.369, continue with these steps.
2. Procure the McAfee script from the software download page on the Grass Valley website.

   The filename to download is `McAfee-6.1.1.zip`.
3. Unzip and copy the directory containing the McAfee script files to any location on the local computer.
4. Use Embedded Security Manager and put the local computer in Update Mode.
5. On the local computer, in the directory of McAfee script files that you downloaded from the Grass Valley website, run `UpdateMcAfee.cmd`.
6. Delete the directory of McAfee script files from the local computer.

7. In SiteConfig, do the following:
   a) Add the **GV Embedded Security Manager** role to the device.
   b) Add cab file as necessary to the device's deployment group so that the `GVEmbeddedSecurityManager` cab file is available for deployment.
   c) Do a **Check Software** operation on the device.
   d) Deploy software to the device.
8. Use Embedded Security Manager and leave the Update Mode.

   Embedded Security Manager now reports **Enabled**.
9. Do Windows updates on the local computer.

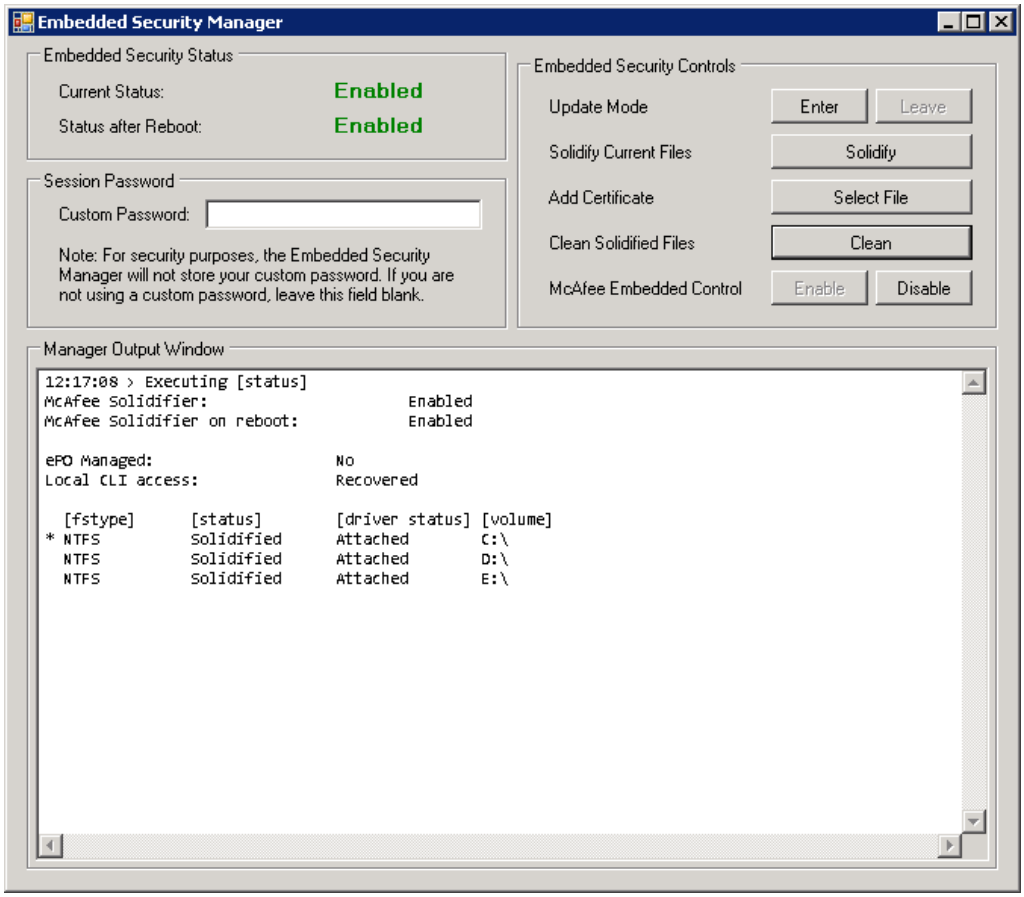
   You can now install Windows updates KB2859537 and KB2872339, which were previously not allowed on Grass Valley systems.

- For future Windows updates, it is no longer necessary to exclude KB2859537 and KB2872339.
- For future deployment of K2 and GV STRATUS software using SiteConfig, it is no longer necessary to put Embedded Security in Update Mode.

  NOTE: If not using SiteConfig, it can still be necessary to put Embedded Security in Update Mode. Refer to your product's software install/upgrade instructions.

Leave the embedded security solution Update mode

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



   Interpret Current Status as follows:

   - **Enabled**: Embedded Security is enabled but is not in Update mode.
   - **Update**: Embedded Security is enabled and is in Update mode, ready for software installation.

2. Under **Update**, manage the Update mode as follows:

   - Click **Leave** to take Embedded Security out of Update mode.

   A restart is not required after you leave the Update mode.

Install software using SiteConfig

1. Find SNFS software, K2 software, and a PDF file with instructions from the "About This Release" section of the K2 Topic Library on the USB Recovery Flash Drive that you received with the upgrade kit.

2. If you have reimaged 32-bit Windows XP K2 Summit system so that it is now a 64-bit Windows 7 system, do the following:
   a) Remove the K2 Summit system from the SiteConfig system descriptions.
   b) Add the K2 Summit system as a 64-bit system to the SiteConfig system description.

   SiteConfig generates an "RPES Service Error 2" if you do not do this step.
3. Use your normal methodology with SiteConfig to install the following software:
   - SNFS software
   - K2 system software

   NOTE: When checking software, if an "Unable to copy ... to target" error appears for a device that has Grass Valley Embedded Security, put Embedded Security in Update mode.

Next, restore licensing.

Restore licensing

1. On the Windows desktop, click **License Manager**.

   SabreTooth License Manger opens.
2. If the License Manager says the licenses are not for this machine then the hardware for the network interfaces has changed. Contact Grass Valley Customer Service to order new replacement licenses.

Next, from the following list, do those tasks that apply to the K2 Solo 3G system. Follow instructions in related topics later in this document as necessary.

- If a K2 Solo 3G system with direct-connect storage or shared storage on a redundant K2 SAN, install MPIO software.
- If a K2 Solo 3G system with a Fibre Channel card, install the Fibre Channel card driver.

If none of the tasks above apply to the K2 Solo 3G system, skip ahead and do final steps.

If you install software manually

Do not do the tasks in this section if:

- You use SiteConfig to install/upgrade software on the K2 Solo 3G system.

Do the tasks in this section if:

- You install/upgrade software on the K2 Solo 3G system manually, rather than using SiteConfig.

NOTE: You must use the same install/upgrade method now, either SiteConfig or manual, as you will use for installations and upgrades in the future. Do not switch between methods, using one method now and a different method for future installations and upgrades.

Follow the task in this section sequentially.

Install software manually

Do not do this task if:

- You use SiteConfig to install/upgrade software on the K2 Solo 3G system.

Do this task if:

- You install/upgrade software on the K2 Solo 3G system manually, rather than using SiteConfig.

NOTE: You must use the same install/upgrade method now, either SiteConfig or manual, as you will use for installations and upgrades in the future. Do not switch between methods, using one method now and a different method for future installations and upgrades.

Find K2 software, SNFS software, and installation instructions in the "About This Release" section of the K2 Topic Library, or on the USB Recovery Flash Drive that you received with the upgrade kit.

1. Install SNFS software. Refer to installation instructions in the "About This Release" section of the K2 Topic Library for procedures.

   SNFS uses the settings restored from `srestore.bat`.

2. Install K2 software. Refer to installation instructions in the "About This Release" section of the K2 Topic Library for procedures.

Deploy Embedded Security solution - One-time process

You must have a system system-specific recovery disk image of the computer on which you are doing the Embedded Security one-time process.

NOTE: A re-image of the computer might be necessary if the Embedded Security one-time process is done incorrectly. Follow instructions carefully.

This is a two-phase task:

1. Run a script on the local system to which you are deploying software.
2. Deploy software with SiteConfig.

NOTE: You must carefully read and verify that you have completed each step in the task. Do not assume the task is the same as other software install tasks with which you are familiar.

On the computers in your system that are running the Grass Valley Embedded Security solution, you must do a one-time initial deployment process, as instructed by this task. This task isolates the steps required for the one-time process. If you have sufficient knowledge of systems and upgrades, you can modify your software upgrade steps as necessary to do the one-time process at the same time as your other software upgrades, rather than as isolated steps. After you have done this one-time process, you can do future upgrades using the normal upgrade process.

This applies to the following:

- K2 Summit/Solo system
- All types/roles of K2 Media Server

- All types/roles of GV STRATUS server

1. Determine the status of the Embedded Security solution on the computer. You can use SiteConfig check/view software to make this determination or on the local computer you can use the Programs and Features Control Panel to make this determination. Proceed as follows:
   - If the computer does not have **McAfee Solidifier**, which is a component of the Embedded Security solution, do not continue with these steps. The computer must already have the Embedded Security solution before the one-time process is applied.
   - If the computer has **McAfee Solidifier** at version 6.1.1.369, do not continue with these steps. That version indicates that the computer already has the one-time process applied, through either a software installation or a disk image process.
   - If the computer has **McAfee Solidifier** at a version lower than 6.1.1.369, continue with these steps.
2. Procure the McAfee script from the software download page on the Grass Valley website.

   The filename to download is *McAfee-6.1.1.zip*.
3. Unzip and copy the directory containing the McAfee script files to any location on the local computer.
4. Use Embedded Security Manager and put the local computer in Update Mode.
5. On the local computer, in the directory of McAfee script files that you downloaded from the Grass Valley website, run *UpdateMcAfee.cmd*.
6. Delete the directory of McAfee script files from the local computer.
7. In SiteConfig, do the following:
   a) Add the **GV Embedded Security Manager** role to the device.
   b) Add cab file as necessary to the device's deployment group so that the *GVEmbeddedSecurityManager* cab file is available for deployment.
   c) Do a **Check Software** operation on the device.
   d) Deploy software to the device.
8. Use Embedded Security Manager and leave the Update Mode.

   Embedded Security Manager now reports **Enabled**.
9. Do Windows updates on the local computer.

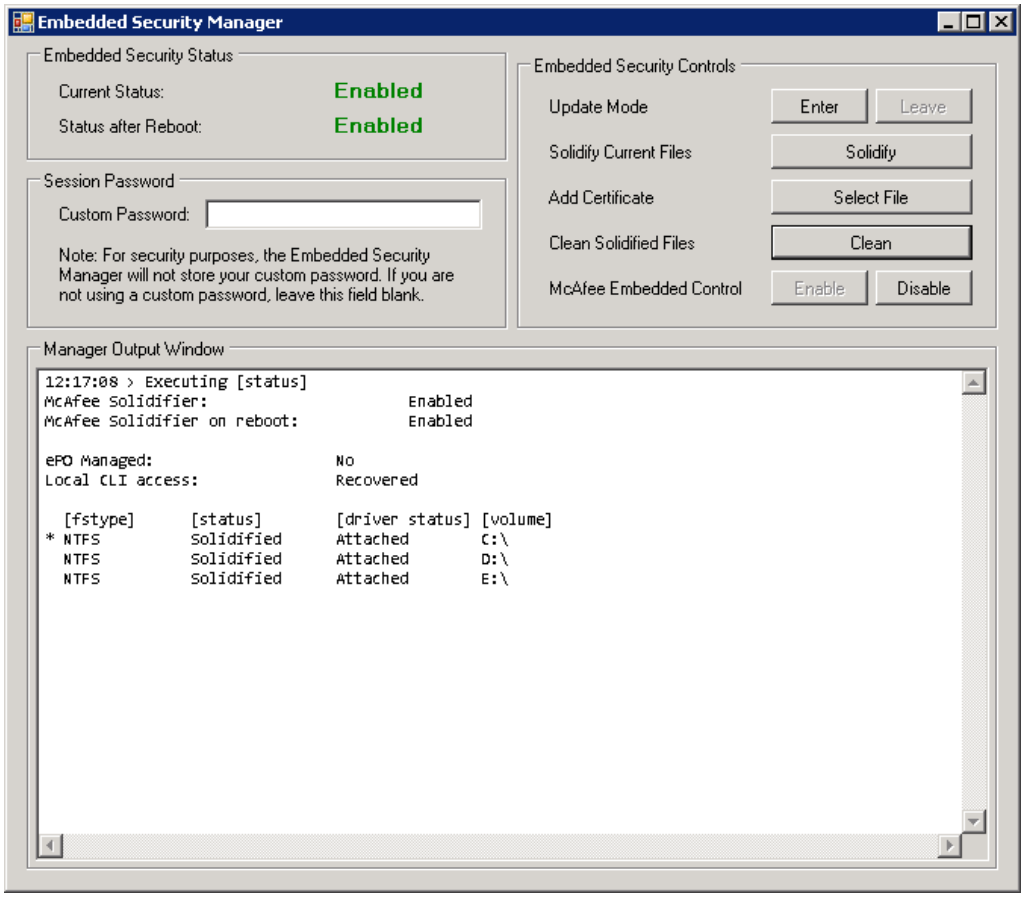
   You can now install Windows updates KB2859537 and KB2872339, which were previously not allowed on Grass Valley systems.

- For future Windows updates, it is no longer necessary to exclude KB2859537 and KB2872339.
- For future deployment of K2 and GV STRATUS software using SiteConfig, it is no longer necessary to put Embedded Security in Update Mode.

  NOTE: If not using SiteConfig, it can still be necessary to put Embedded Security in Update Mode. Refer to your product's software install/upgrade instructions.

Leave the embedded security solution Update mode

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



   Interpret Current Status as follows:

   - **Enabled**: Embedded Security is enabled but is not in Update mode.
   - **Update**: Embedded Security is enabled and is in Update mode, ready for software installation.

2. Under **Update**, manage the Update mode as follows:

   - Click **Leave** to take Embedded Security out of Update mode.

   A restart is not required after you leave the Update mode.

Restore licensing

1. On the Windows desktop, click **License Manager**.

   SabreTooth License Manger opens.

2. If the License Manager says the licenses are not for this machine then the hardware for the network interfaces has changed. Contact Grass Valley Customer Service to order new replacement licenses.

Next, from the following list, do those tasks that apply to the K2 Solo 3G system. Follow instructions in related topics later in this document as necessary.

- If a K2 Solo 3G system with direct-connect storage or shared storage on a redundant K2 SAN, install MPIO software.
- If a K2 Solo 3G system with a Fibre Channel card, install the Fibre Channel card driver.

If none of the tasks above apply to the K2 Solo 3G system, skip ahead and do final steps.

Install Multi-Path I/O software

Do this task on a 64-bit K2 Solo 3G system with direct-connect storage or shared storage on a redundant K2 SAN.

1. Access the Windows desktop on the computer on which you are installing MPIO.

   You can do this locally with a connected keyboard, mouse, and monitor or remotely via the Windows Remote Desktop Connection.

2. Access the Windows desktop on the computer on which you are installing MPIO.

   You can do this locally with a connected keyboard, mouse, and monitor or remotely via the Windows Remote Desktop Connection.

3. Stop all media access. If AppCenter is open, close it.
4. Click **Start | Run**, type `cmd` and press **Enter**.

   The MS-DOS command prompt window opens.

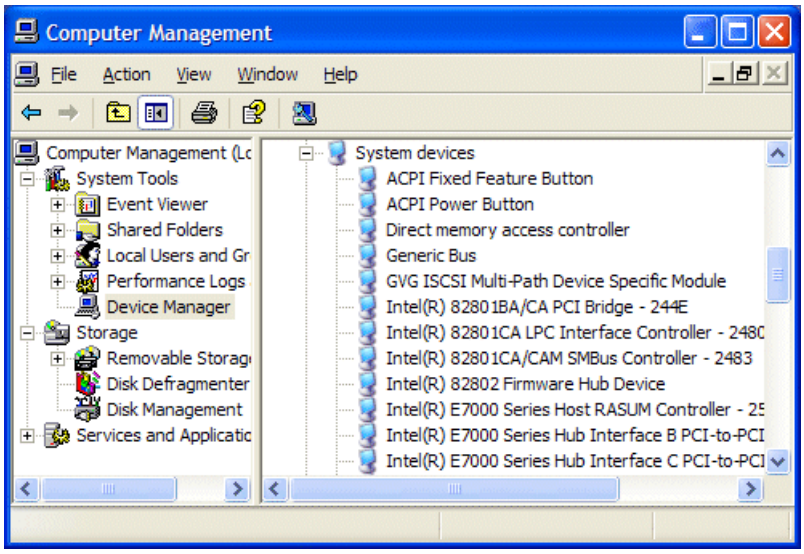
5. From the command prompt, navigate to the *`C:\profile\mpio`* directory.
6. Type the following at the command prompt:

   ```
   gdsminstall64.exe -i
   ```

7. Restart the computer on which you installed MPIO.

8. After restart, to verify that the software is installed, on the Windows desktop right-click **My Computer** and select **Manage**.

   The Computer Management window opens.



9. In the left pane select **Device Manager**.
10. In the right pane open the **System devices** node and verify that **GVG ISCSI Multi-Path Device Specific Module** is listed.

Next, do one of the following:

- If the K2 Solo 3G system does not have a Fibre Channel card, skip ahead and do final steps.
- If the K2 Solo 3G system has a Fibre Channel card, install the Fibre Channel card driver.

Install the Fibre Channel card driver

If the K2 Solo 3G system is on a redundant K2 SAN or is connected to direct-connect storage, MPIO software must be installed.

If your K2 Solo 3G system has the optional Fibre Channel card, the driver for the Fibre Channel card is not installed on the recovery image provided by Grass Valley for that K2 Solo 3G system. Therefore, after restoring the image, you must install the Fibre Channel card driver.

A K2 Solo 3G system can have one of the following types of Fibre Channel cards:

- LSI
- ATTO

Depending on the type of Fibre Channel card in the K2 Solo 3G system, do the appropriate task from this section to install the Fibre Channel card driver.

Install the LSI Fibre Channel card driver

1. Make sure that you have access to the Fibre Channel card driver file. K2 software installation copies the driver to the local K2 Solo 3G system, in `C:\Windows`. In that location, look for *LSI_SCSIPORT_1.21.25.00*, then do one of the following:
   - If the file is present, continue with the next step in this procedure.
   - If the file is not present, procure the file from `ftp://ftp.grassvalley.com/pub/K2/Microcode_and _Drivers/LSI_SCSIPORT`. The filename is *LSI_SCSIPORT_1.21.25.00.zip.* Then continue with this procedure.
2. Upon restart a Found New Hardware wizard opens for the Fibre Channel controller. Install the driver on the first FC port as follows:
   a) Select **Install from a list or specific location**. Click **Next**.
   b) Select **Don't search. I will choose the driver to install** and then click **Next**.
   c) Select **SCSI and Raid Controllers** and **Have Disk**.
   d) Browse to `C:\Windows` and find *LSI_SCSIPORT_1.21.25.00*. Click **Open** and **OK**.
   e) Start the driver install by selecting **Next**.
   f) On the Hardware Installation page, click **Continue Anyway**.
   g) Click **Finish**.
3. If the K2 Solo 3G system has a dual port Fibre Channel card, on the Found New Hardware wizard, install the driver on the second FC port as follows:
   a) Select **Install from a list or specific location** and then click **Next**.
   b) Select **Don't search. I will choose the driver to install**. Click **Next**.
   c) Select **Have Disk**.
   d) Browse to `C:\Windows` and find *LSI_SCSIPORT_1.21.25.00*. Click **Open** and **OK**.
   e) Start the driver install by selecting **Next**.
   f) On the Hardware Installation page, click **Continue Anyway**.
   g) Click **Finish**.
4. On the Found New Hardware wizard, install the first LSI Pseudo Device as follows:
   a) Select **Install from a list or specific location**. Click **Next**.
   b) Select **Don't search. I will choose the driver to install** and then click **Next**.
   c) Select **Have Disk**.
   d) Browse to `C:\Windows` and find *LSI_SCSIPORT_1.21.25.00*. Click **Open** and **OK**.
   e) Start the driver install by selecting **Next**.
   f) On the Hardware Installation page, click **Continue Anyway**.
   g) Click **Finish**.

5. If the K2 Solo 3G system has a dual port Fibre Channel card, on the Found New Hardware wizard, install the driver on the second LSI Pseudo Device port as follows:
   a) Select **Install from a list or specific location** and then click **Next**.
   b) Select **Don't search. I will choose the driver to install** and then click **Next**.
   c) Select **Have Disk**.
   d) Browse to `C:\Windows` and find *LSI_SCSIPORT_1.21.25.00*. Click **Open** and **OK**.
   e) Start the driver install by selecting **Next**.
   f) On the Hardware Installation page, click **Continue Anyway**.
   g) Click **Finish**.
6. If the K2 Solo 3G system is on a redundant K2 SAN or is connected to direct-connect storage, make the following registry settings:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Symmpi\Parameters\Device]

"DriverParameter"="MPIOMode=2"

"MaximumSGList"=dword:000000ff

"NumberOfRequests"=dword:00000020
```

Next, do final steps.

Install the ATTO Fibre Channel card driver

1. Open Device Manager.
2. Right-click on **K2 Summit Client** and select **Manage.**
3. Click **Device Manager**
4. Install the first Fibre Channel driver as follows:
   a) Right click on the upper Fibre Channel Controller and select **Update Driver…**
   b) On the Welcome page, select **No, not this time** and then click **Next**.
   c) Select **Install from a list or specific location** and then click **Next**.
   d) Browse to `C:\Profile\Drivers\ Atto 8Gb HBA Drivers\x86`.
   e) Click **OK**.
   f) Click **Next**.
   g) Click **Finish** when prompted.
   h) In the Found new hardware wizard that will open for the ATTO Phantom device, select **No, not this time**.
   i) Select **Install from a list or specific location** and then click **Next**.
   j) Browse to `C:\Profile\Drivers\ Atto 8Gb HBA Drivers` and select the `x86` directory if installing on a 32-bit computer or the `x64` directory if installing on a 64-bit computer.
   k) Click **OK** .
   l) Click **Next.**.
   m) Click **Finish** when prompted.

5. Repeat the process for the second Fibre Channel Controller as follows:
   a) Right-click on the remaining Fibre Channel Controller and select **Update Driver…**
   b) On the Welcome page, select **No, not this time** and then click **Next**.
   c) Select **Install from a list or specific location** and then click **Next**.
   d) Browse to *C:\Profile\Drivers\ Atto 8Gb HBA Drivers* and select the *x86* directory if installing on a 32-bit computer or the *x64* directory if installing on a 64-bit computer..
   e) Click **OK**.
   f) Click **Next**.
   g) Click **Finish** when prompted.
6. Verify that the two "ATTO" devices are now listed under the SCSI and RAID Controllers
7. Close the Device Manager and System windows

Next, do final steps.

Final steps for software and CPU carrier module upgrades

Do this task for both software and CPU carrier module upgrade kits.

1. If you have not already done so, manage the Embedded Security. Make sure Update mode is ended.
2. Check the Windows operating system clock and, if necessary, set it to the correct time.
3. If you installed K2-XDP2-V9-FK, apply the Windows operating system sticker that you received with the upgrade kit. Attach it to the K2 Summit/Solo system, in the same location as the previous Windows operating system sticker.
4. If you are upgrading a K2 Summit SAN-attached system, on the K2 SAN's control point PC, use the K2Config application to add the K2 Solo 3G system back to the SAN.
5. When the K2 Solo 3G system is fully configured, licensed, and operational, create a disk image and store it on the USB Recovery Flash Drive. Refer to the K2 product's service procedures.
6. Disconnect the USB Recovery Flash Drive and store it in the front bezel assembly.

   If present, discard the previous USB Recovery Flash Drive.

The upgrade process is complete for the following upgrade kits:

- K2-XDP2-CPU-FK
- K2-XDP2-V9-FK

For a K2 Solo 3G system upgraded with the K2-XDP2-CPU-FK kit, if you do any service work or replace any Field Replaceable Units (FRUs), first consult 3G service procedures in the "Servicing the K2 Summit system" section of the K2 Topic Library. This is true even if replacing an original FRU that has not been upgraded. System dependencies involving FRUs require 3G service procedures.

Install codec module upgrade

Before installing a codec module upgrade, the K2 Solo 3G system must have either Type II, Type III or Type IV CPU carrier module, 16 GB system drive, 16 GB or 32 GB USB Recovery Flash Drive, and K2 software version 9.x or higher.

Tools and materials needed:

- Hardware as provided by upgrade kit. See description below.
- Torx tool with T15 magnetic tip

This section provides instructions for the following field kit:

Upgrade Nomenclature	Description
K2-XDP2-3G-FK	K2 Summit Production Client XDP Series 3G SDI Interface field kit for K2-XDP series platforms. Includes 2ea - 3G codec modules, 2 - ea. 550W power supplies, and installation instructions. NOTE: This kit cannot be used with K2-XDT Series Summit Transmission Clients and Servers or K2-SOLO models.

⚠ ***CAUTION: This system contains board-level components that must be protected from static discharge and physical shock. Wear a wrist strap grounded to the system chassis when handling system components.***

Work through the task in this section.

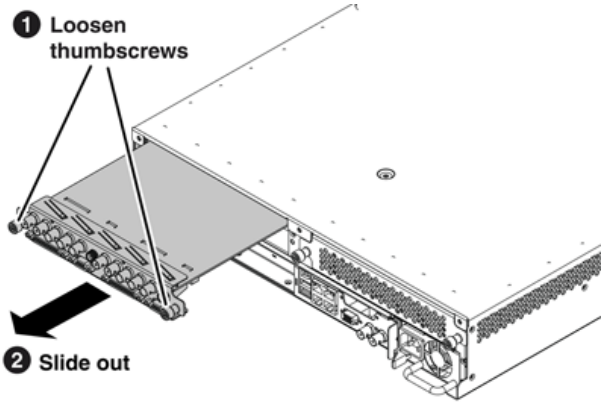
Replace codec module and power supplies

Do this task if installing K2-XDP2-3G-FK on a K2 Solo 3G system.

NOTE: Do not attempt to replace the CPU carrier module on a K2 Solo Media Server. K2-XDP2-3G-FK does not apply to K2 Solo Media Server.

- The K2 Solo 3G system must be shut down.
- The K2 Solo 3G system must have all power cables disconnected.
- The K2 Solo 3G system must have the power button pressed to drain off power from boards.

1. Remove any cables connected to the codec modules.
2. Access the rear panel and remove as illustrated.



NOTE: With a firm grip on the metal (EMI) bracket, ensure the board is level and parallel to the card guides to avoid damage to the components on the edge opposite the rear panel.

⚠ ***CAUTION: Improper handling can damage components on the board. Do not allow the board to come in contact with the chassis sheet metal during removal or installation. The components on the edge opposite the rear panel are the most susceptible to damage.***

3. Install the new codec modules.
4. Replace the current power supply modules with the new power supply modules.
5. Reconnect cables to the codec modules and power supplies.
6. After installing the card, start up and log on to the K2 Solo 3G system with administrator privileges, then load software onto the codec board as follows:
   a) Stop all Grass Valley services except for **Grass Valley Host File Service**.
   b) From the Windows command prompt, navigate to the following directory:
      `C:\profile`
   c) Type the following and press **Enter**.
      `srtploader -U`

   This ensures that the board is flashed with the proper version to be compatible with K2 software.

The upgrade process is complete for the following upgrade kit:

- K2-XDP2-3G-FK

For a K2 Solo 3G system upgraded with the K2-XDP2-3G-FK kit, if you do any service work or replace any Field Replaceable Units (FRUs), first consult the "Servicing the K2 Summit system" section of the K2 Topic Library. This is true even if replacing an original FRU that has not been upgraded. System dependencies involving FRUs require procedures found only in the "Servicing the K2 Summit system" section of the K2 Topic Library.

Upgrading a K2 Media Server to version 9.x

Software needed:

- K2 software version 9.x. Refer to the "About This Release" section of the K2 Topic Library to determine your compatible version.
- SNFS software version 4.1
- SNFS software version 4.2

Do not do this task if one of the following is true:

- The server has a version 8.1.x or higher disk image and you do not require the Embedded Security solution on the server. If this is the case, you can do a software-only upgrade on the server, as instructed by the "About This Release" section of the K2 Topic Library upgrade instructions.
- The server is a Dell 1910 or 2850. Version 9.x supports Dell 2950, Dell R610, and newer Dell platforms only.

Do this task if either of the following is true:

- The server has a disk image version lower than 8.1.x.
- You require the Embedded Security solution on the server.

This section provides instructions for the following field kit:

Upgrade Nomenclature	Description
K2-XDPSVR-V9-FK	K2 Server 9.x Upgrade Field Kit. Includes 9.x system software license, 32GB USB Thumb drive with Windows Server 2008 64bit, McAfee Embedded Server; CD with Acronis True Image Server.

This section provides instructions for servers that have the role of K2 file system server, such as the following:

- K2 SAN system:
  - The FSM on a basic (non-redundant) K2 SAN
  - The two FSMs on a redundant K2 SAN
- K2 Nearline system:
  - The NH server on a basic (non-redundant) system
  - The two NH servers on a redundant system

In addition to the instructions in this section, review the "About This Release" section of the K2 Topic Library upgrade instructions. When you upgrade the server, do so in the proper sequence with the other devices of the system. Also refer to this document as necessary to accomplish the tasks in this section.

These instructions are for upgrading from a K2 system software 7.4.x or 8.x version to a 9.x version. Part of the upgrade is re-imaging the K2 Media Server. You must do all the steps as directed in the procedure to ensure the system is properly upgraded. When you upgrade to version 9.x, all connected devices that run K2 system software must also upgrade to version 9.x.

1. Check the current base image version on the K2 Media Server to verify prerequisites stated earlier in this topic.
   - On a 32-bit K2 Media Server, use registry key
     `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Grass Valley Group\Base`
   - On a 64-bit K2 Media Server, use registry key
     `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Grass Valley Group\Base`
2. If you have not already done so, download the required software from the Grass Valley website. Use the following URL and then browse to the required version.
   http://www.grassvalley.com/dl/k2_summit
3. On the K2 Media Server, open SabreTooth License Manager. If a K2-ISCSI-SVR license is installed, archive the license to a different location so that you can reinstall the license at the end of this process.
4. From the Control Point PC, remove the server from K2Config.
5. Remove SAN-attached K2 Summit systems and other K2 SAN clients from K2Config.
6. On the K2 Media Server, create a backup recovery disk image of the server's C and D partitions.
7. Restore the server's C partition from the disk image provided on the USB thumb drive you received with the upgrade kit.
   NOTE: To preserve existing media, only restore the C partition from the generic disk image.
   At first start up after reimage, the system is in Embedded Security Update mode by default.
8. Set up Windows.
9. Restore network configuration.
10. Install SiteConfig Discovery Agent.
11. At the server, manually install SNFS 4.1.
12. Restart the server and wait for all start up processes to complete.

13. Manually uninstall SNFS 4.1.
14. Restart the server and wait for all start up processes to complete.
15. Manually install SNFS 4.2.
16. Restart the server and wait for all start up processes to complete.
17. Manually install K2 9.x software.

    While manually installing software, accept any hardware installation or driver/security prompts that appear. Also refer to related topics in the "About This Release" section of the K2 Topic Library.
18. Restart the server and wait for all start up processes to complete.
19. Install Fibre Channel Card driver.
20. If you archived the K2-ISCSI-SVR Sabretooth license earlier in this process, reinstall it on the K2 Media Server.
21. Launch the Embedded Security Manager and select **Leave** to exit out of Update mode.
22. From the Control Point PC, use K2Config and add the server to the K2 SAN.
23. In K2Config, configure the server's File System Server page as follows:

    - If a redundant K2 SAN, copy file system config settings from the redundant K2 Media Server, as prompted by K2Config.
    - If a basic (non-redundant) K2 SAN, launch Storage Utility, identify a disk, then exit Storage Utility.

    NOTE: Do not make a new file system.

    K2Config does not allow you to proceed until you do these steps.
24. In K2Config, add SAN-attached K2 Summit systems and other K2 SAN clients.
25. Verify the server operates as expected.
26. Activate Windows within 30 days.

Upgrading a Control Point PC

Software needed:

- K2 software version 9.x.
- SiteConfig software

Refer to the "About This Release" section of the K2 Topic Library to determine your compatible versions.

This section provides instructions for the following field kit:

Upgrade Nomenclature	Description
CP-XDPCP-V9-FK	K2 Server 9.x Upgrade Field Kit. Includes 9.x system software license, 32GB USB Thumb drive with Windows Server 2008 64bit, Windows Server 2003 HyperV, McAfee Embedded Server, NetCentral 5.2.2; CD with Acronis True Image Server.

These instructions apply to the upgrade of a Grass Valley supplied, Dell platform, Control Point PC. As part of the upgrade you re-image the Control Point PC. On the Windows Server 2008 R2

64-bit image there is a Virtual Machine that has a Windows Server 2003 32-bit operating system. This is required to support NetCentral.

Re-image Control Point PC

1. Make a record of your current NetCentral licenses, as you must request new licenses later in this process.
2. Backup the current Grass Valley Control Point image to an external USB drive.
3. Reimage the Grass Valley Control Point Dell R610 to the image on the USB thumb drive you received with the upgrade kit. At the time of this writing, it is a version C9.0.3 base image.
4. Install K2 Control Point, SiteConfig, and other software as required for your use of the Control Point PC.

Set BIOS prerequisites

1. In the BIOS set **EXECUTE DISABLE** to **ENABLED.**
2. In the BIOS set **VIRTUALIZATION TECHNOLOGY** to **ENABLED**.

Configure Virtual Machine

- The base image must be version C9.0.3.

1. Check the current base image version to verify prerequisites stated earlier in this topic.
   - On a 64-bit machine, use registry key `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Grass Valley Group\Base`
2. From the Windows desktop, right-click **Computer** and select **Manage**.
   Server Manager opens.
3. In the tree-view, expand nodes **Roles | Hyper-V | Hyper-V Manager**.
4. Select **BASEPC**.
5. Under Actions, select **Virtual Network Manager**.
   Virtual Network Manager opens.
6. Identify the physical network adapter to use for the Virtual Network. You do this using Windows Network Connections.
   a) To open Network Connections, from the Windows **Start** menu, in the **Run** or the **Search programs and files** box, type `ncpa.cpl` and press **Enter**.
   The Network Connections window opens.
   b) Find the connection that is the physical network adapter (not a virtual adapter) that you use for connection to your network.
   For example, if the connection named "Control Connection" is currently connected to your network, then that is the connection to use for the Virtual Network.
   c) Take note of the adapter and its number, as specified in the **Device Name** column.
   In next steps, you must select this adapter to use it for the Virtual Network.
7. In Virtual Network Manager, click **Add**.

8. Under New Virtual Network, Connection Type, in the **External** drop-down list, select the network adapter that you identified to use for the Virtual Network.
9. Verify that **Allow management operating system to share this network adapter.** is selected.
10. Click **Apply** and when prompted to apply network changes, click **Yes**.
    Progress is reported for applying changes. Wait until changes are complete.
11. Click **OK** to close the connection set-up.
12. Under BASEPC, select **NetCentral**.
13. Under Actions, NetCentral, select **Settings**.
    Setting for NetCentral opens.
14. Under Hardware, click **Memory**.
15. Under Memory management settings, click **Static**.
16. Verify that Static RAM is specified as **2048** MB.
17. Under Hardware, click **Network Adapter**.
18. In the **Network** drop-down list, select the network you created, which is **New Virtual Network**.
19. Under Management, click **Automatic Start Action**.
20. Select the **Always start this virtual machine automatically** option.
21. Under Management, click **Automatic Stop Action**.
22. Select the **Save the virtual machine state** option.
23. Click **Apply** and **OK**.
24. Verify that the physical network adapter that you used for the Virtual Network is connected to your network.
25. Restart the Control Point PC.
26. From the Windows desktop, right-click **Computer** and select **Manage**.
    Server Manager opens.
27. In the tree-view, expand nodes **Roles | Hyper-V | Hyper-V Manager**.
28. Select **BASEPC**.
29. Under BASEPC, verify that the NetCentral Virtual Machine is running.

Next, do Windows setup on the NetCentral Virtual Machine.

Setting up Windows on the Virtual Machine

- The NetCentral Virtual Machine must be configured on the Control Point PC.

1. From the Windows desktop, right-click **Computer** and select **Manage**.
   Server Manager opens.
2. In the tree-view, expand nodes **Roles | Hyper-V | Hyper-V Manager**.
3. Select **BASEPC**.
4. Under BASEPC, verify that the NetCentral Virtual Machine is running.
5. To connect to the NetCentral Virtual Machine, under NetCentral click **Connect**.
   A **Virtual Machine Connection** window opens.
   If you have not yet done Windows setup, a Windows Setup Wizard is displayed.

6. Work through the Windows Setup Wizard, clicking **Next** and **I accept** and entering other information as desired.
7. On the Product Key page, key in your 25-character Product Key to authenticate your Microsoft Windows Server 2003.
8. On the Workgroup or Computer Domain page, choose one of the following:
   - Workgroup: GRASSVALLEY
   - Computer Domain: Enter your own domain.
9. Click **Finish** to complete the Windows Setup Wizard.

   The Virtual Machine restarts.

Next, log on to the Virtual Machine and license NetCentral.

Logging on to the Virtual Machine

- The Virtual Machine must be configured
- Windows must be set up

1. From the Control Point PC Windows desktop, right-click **Computer** and select **Manage**.

   Server Manager opens.
2. In the tree-view, expand nodes **Roles | Hyper-V | Hyper-V Manager**.
3. Select the Virtual Machine name, as named in Windows setup.
4. Under the Virtual Machine name, verify that the NetCentral Virtual Machine is running.
5. To connect to the NetCentral Virtual Machine, under NetCentral click **Connect**.

   A **Virtual Machine Connection** window opens.
6. If a **Welcome to Windows** log on message is displayed, do the following to log on to the Virtual Machine.
   a) On the **Virtual Machine Connection** window tool bar, click the **Ctrl + Alt + Delete** button.

   Ctrl + Alt + Delete is sent to the Virtual Machine.

   b) Enter your user name and password and click **OK**.

   The Virtual Machine Windows desktop opens.

Next, license NetCentral.

License NetCentral on the Virtual Machine

You must request new NetCentral licenses and add them to the Virtual Machine. You do this on the Virtual Machine (not on the Control Point PC), using the SabreTooth License Manager. Because the NetCentral Virtual Machine desktop does not have a License Request Wizard, start by following the instructions in the next topic *If you encounter difficulties when requesting a license* on page 815.

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

If you encounter difficulties when requesting a license

If you encounter difficulties running the License wizard, or the License wizard is not available, try this alternate method:

1. Generate a unique ID of the device where you will install software, as follows:
   a) Double click on the License Manager icon on the Windows Desktop.
      The SabreTooth License Manager opens.
   b) Choose **File | Generate Unique Id** the License Manager.
   c) Click **Copy to clipboard** to copy the generated ID, and **OK** to exit.
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.
   - The license types you are requesting.
3. Send the email to GrassValleyLicensing@grassvalley.com.

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

Adding a license to the Virtual Machine

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

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

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

You should archive the permanent license to a backup system.

Installing a two channel upgrade

Tools and materials needed:

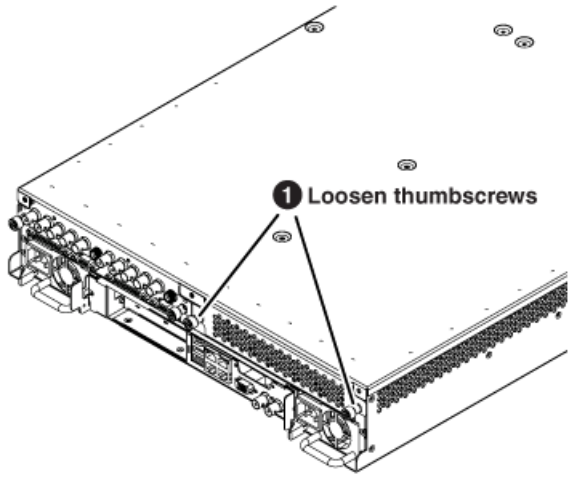
- Upgrade codec module.

This section provides instructions for the following field kits.

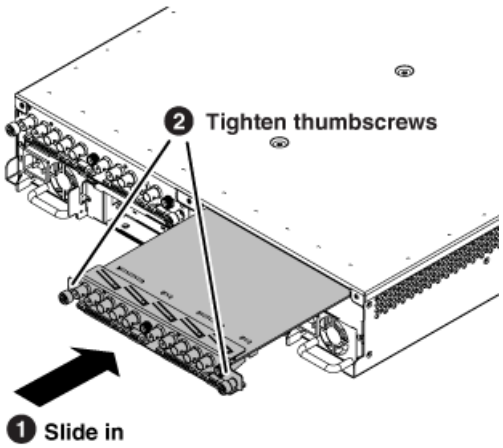
Upgrade Nomenclature	Description
K2-XDP2-2IO-FK	K2 Summit 3G 2 HD/SD channel I/O field kit. Adds 2 HD/SD bi-directional channels to the K2-XDP2-02 or any of the K2- XDP Series clients. When used with the K2-XDP Series clients all codec modules must be replaced with the Summit 3G module.

⚠ ***CAUTION: This system contains board-level components that must be protected from static discharge and physical shock. Wear a wrist strap grounded to the system chassis when handling system components.***

1. If you intend to upgrade K2 software along with this Field Kit upgrade, upgrade K2 software first, completing all upgrade processes as documented in the "About This Release" section of the K2 Topic Library, then proceed with this procedure.
2. Restart the K2 system.
3. Log in to Windows.
4. When the AppCenter logon box appears, click **Cancel** and **Abort**.
5. Delete the channel suites file in the `C:\profile\ChannelSuites` directory. The file name begins with the K2 system's name. For example, if the name is k2client1, then the file name is `K2CLIENT1_localConnection.xml`.
6. Shutdown the K2 system.
7. From the rear panel, remove the blank plate that covers the empty codec module slot, as illustrated.



8. Install the upgrade codec module as illustrated.



NOTE: With a firm grip on the metal (EMI) bracket, ensure the board is level and parallel to the card guides to avoid damage to the components on the edge opposite the rear panel.

⚠ ***CAUTION: Improper handling can damage components on the board. Do not allow the board to come in contact with the chassis sheet metal during removal or installation. The components on the edge opposite the rear panel are the most susceptible to damage.***

9. Start up the K2 system.

   On restart, the K2 sysem rescans hardware and automatically discovers the new codec module.

10. If a message appears, follow the instructions in the message to either restart or shutdown/startup. This second startup process is necessary so that the K2 system can reconfigure appropriately.
11. After installing the replacement codec module, install the current version of K2 software and restart.

    This is a re-install of current software, not an upgrade. You must install the same version of software that is currently on the K2 system now, regardless of whether you did or did not upgrade software earlier in this procedure. You install software now to ensure that the board is flashed with the proper version to be compatible with software currently on the K2 system. An over-install is all that is required. You do not need to first un-install the software.

12. Log in to Windows and AppCenter, and open Configuration Manager. The new channels are available for configuration.

Configure channels as follows:

- If you are installing a codec license field kit, do not configure your new channels yet. First install the codec license field kit, then configure your new channels.

Installing an upgrade license

Tools and materials needed:

- The license sheet you received with the upgrade kit.

This section provides instructions for the following field kits:

Upgrade Nomenclature	Description
K2-XDP2-AVC-2CH-FK	K2 Summit 3G AVC-Intra 2 channel codec license. Includes AVC-Intra level 50 and 100 and decoding of H.264 L4.2. Two required for 4 channel model (K2-XDP2-04) Field kit.
K2-XDP2-3XP-SSM-FK	K2 Summit 3G single channel 3x 1080p SSM option. Adds 3x 1080p SSM record capability. Includes license for single camera ingest. Two required for dual camera ingest (K2-XDP2-02/04).
K2-XDP2-6X-SSM-FK	K2 Summit 3G single channel 6x SSM option. Adds 6x SSM record capability. Includes license for single camera ingest. Two required for dual camera ingest (K2-XDP2-02/04).
K2-XDP2-TRIPLE-FK	K2 3 Input Multicam License. Enables support for 3 Input Multicam on a single K2 channel. A single license will only enable a single channel. Multiple licenses required for multiple K2 channel support. Only supports AVC-I, DNxHD, and DVCPro-HD.
K2-XDP2-UHDTV1-FK	K2 UHD/4K License. Enables support for a single 4K/UHD camera input or 4K/UHD output. Two licenses required to support simultaneous record and playout of 4K/UHD. Requires separate K2-XDP2-3G-2CH 1080p licenses (2 Required).

Work through the tasks in this section sequentially.

Requesting a license

1. If you have not already done so, log on to the K2 Solo 3G system.

   NOTE: You must log in as an Administrator with a local account, not a domain account.

2. On the Windows desktop in the Grass Valley License Requests folder, open the appropriate license request shortcut.

   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 from Grass Valley.

   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 Solo 3G system at a K2 software version lower than 9.0 and 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, when you receive the email from Grass Valley with your license, add the license to the K2 Solo 3G system.

Adding a license

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

1. Double click on the License Manager icon on the Windows Desktop.

   The SabreTooth License Manager opens.

2. Do one of the following:

   - Choose **File | Import License** and navigate to the file location to open the text file.
   - Drag and drop the text file onto the License Manager.

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

You should archive the permanent license to a backup system.

Installing a MPEG/Multi-Cam codec option upgrade

- K2 software version 8.1 or higher is required.

Tools and materials needed:

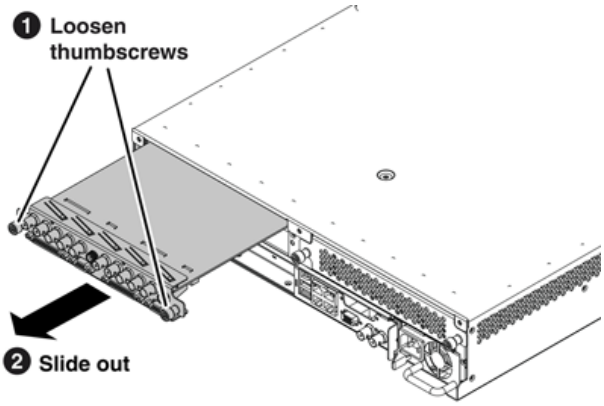
- Codec option card
- #1 Phillips screwdriver

This section provides instructions for the following field kits:

Upgrade Nomenclature	Description
K2-XDP2-MPG2-MC-FK	K2 Summit 3G MPEG2 Multicam encoding field. Adds the ability to record up to 4 video streams per codec module using MPEG2 compression when used in ChannelFlex mode. Includes hardware and additional MPEG encoding license and K2_APPCENTER_ELITE. Two K2-XDP2-MPG-FK kits are required for the K2-XDP2-04 and enables up to 8 video streams to be recorded.

⚠ ***CAUTION: This system contains board-level components that must be protected from static discharge and physical shock. Wear a wrist strap grounded to the system chassis when handling system components.***

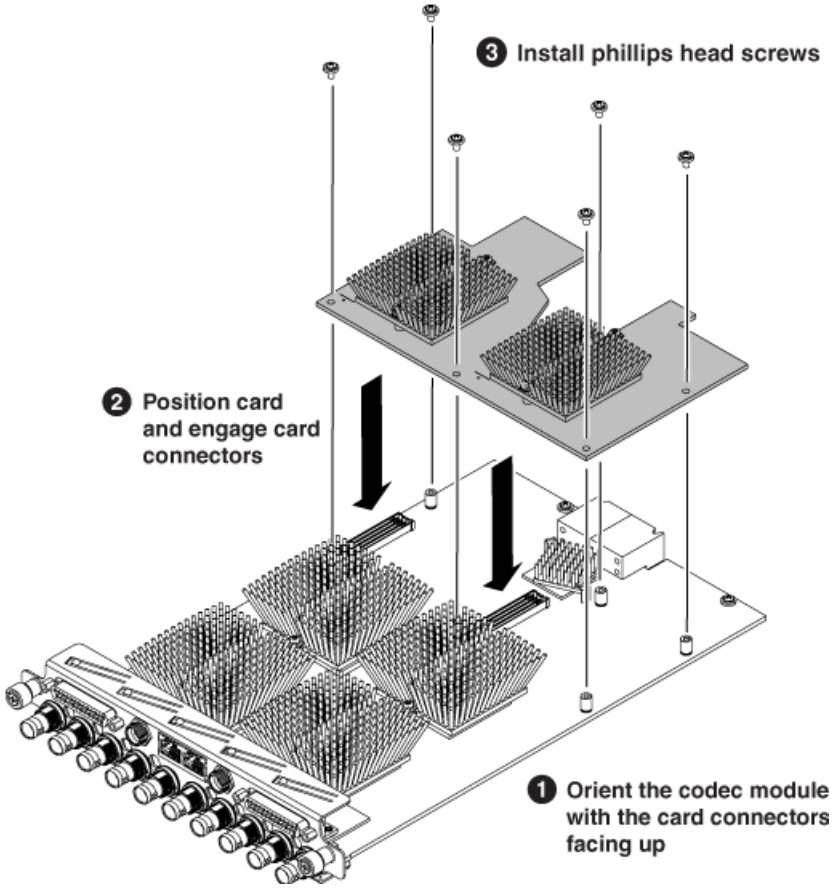
1. If you intend to upgrade K2 software along with this Field Kit upgrade, upgrade K2 software first, then continue with this procedure.
2. Shutdown the K2 Solo 3G system.
3. Access the rear panel and remove as illustrated.



NOTE: With a firm grip on the metal (EMI) bracket, ensure the board is level and parallel to the card guides to avoid damage to the components on the edge opposite the rear panel.

⚠ ***CAUTION: Improper handling can damage components on the board. Do not allow the board to come in contact with the chassis sheet metal during removal or installation. The components on the edge opposite the rear panel are the most susceptible to damage.***

4. Install codec option card as shown.



5. Install the codec module into the K2 Solo 3G system.
6. Start up the K2 Solo 3G system.

   On restart, the K2 Solo 3G system rescans hardware and automatically discovers the codec option card.

7. If a message appears, follow the instructions in the message to either restart or shutdown/startup. This second startup process is necessary so that the K2 Solo 3G system can reconfigure appropriately.
8. After installing the card, start up and log on to the K2 Solo 3G system with administrator privileges, then load software onto the codec board as follows:
   a) Stop all Grass Valley services except for **Grass Valley Host File Service**.
   b) From the Windows command prompt, navigate to the following directory:

      ```
      C:\profile
      ```

   c) Type the following and press **Enter**.

      ```
      srtploader -U
      ```

   This ensures that the board is flashed with the proper version to be compatible with K2 software.

Next, license the K2 Solo 3G system for K2 AppCenter Elite, if it is not already licensed. The license enables the ChannelFlex functionality supported by the codec option card.

NOTE: Once a channel is operational, if you then remove the codec option card from the codec module you must also delete `C:/profile/config/config.xml`. Failure to do so causes errors in Configuration Manager.

Install DynoZoom upgrade

Before installing a DynoZoom upgrade, the K2 Summit 3G system must be capable of 4K record/play, which includes the following:

- K2 Summit 3G system chassis. First generation K2 Summit system chassis not supported.
- SSD disk modules
- Type IV CPU carrier module
- 3G codec module
- Codec option cards
- K2 software 9.3.x or higher
- K2-APPCENTER-ELITE license
- K2-XDP2-3G-2CH 1080p licenses (two required)
- K2-XDP2-UHDTV1 4K licenses (two required)

Tools and materials needed:

- Hardware as provided by upgrade kit. See description below.
- Torx tool with T15 magnetic tip

This section provides instructions for the following field kit:

Upgrade Nomenclature	Description
K2-DYNOZOOM-FK	K2 DynoZoom UltraHD/4K Pan & Zoom option adds DynoZoom Pan & Zoom. Includes: DynoZoom Software with License on USB drive; DynoZoom Frame, DynoZoom Scaler; DynoZoom PCIe Control Card; DynoZoom PCIe Connection Cable; Installation Instructions. Compatible with K2-XDP2-02/04.

⚠ ***CAUTION: This system contains board-level components that must be protected from static discharge and physical shock. Wear a wrist strap grounded to the system chassis when handling system components.***

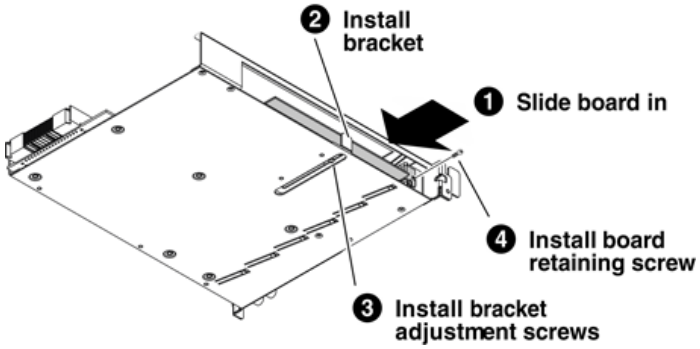
Work through the tasks in this section.

DynoZoom board installation

Before doing this task, the carrier module must be removed.

1. On the K2 Summit system, use Embedded Security Manager and put the local computer in Update Mode.
2. Shutdown the K2 Summit system.
3. Disconnect cabling as necessary and remove the carrier module.

4. To install the DynoZoom board, assemble the carrier module as illustrated.



5. Install the carrier module and reconnect cabling on the K2 Solo 3G system.

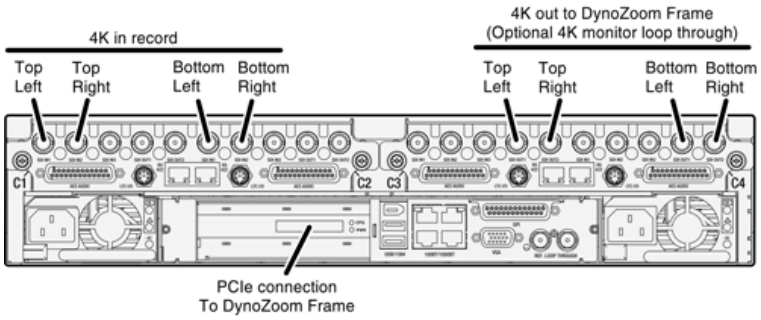
Next, make the PCIe connection between the DynoZoom board and the DynoZoom Frame. Make 4K in/out connections as well.

Cable K2 Summit system for DynoZoom

These cabling instructions apply to the following:

- K2 Summit 3G system with DynoZoom PCIe board.

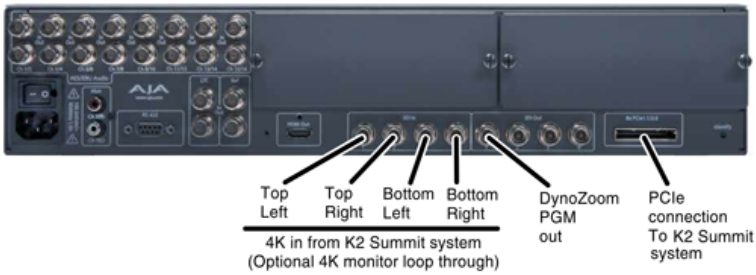
Refer to "K2 Summit Production Client Quick Start Guide" for additional cabling details.



Cable DynoZoom Frame

These cabling instructions apply to the following:

- DynoZoom Frame



Install DynoZoom software on a K2 Summit system

- On a K2 Solo 3G system that supports DynoZoom, the DynoZoom board in the K2 Summit system and the DynoZoom Frame must be connected via PCIe and the DynoZoom Frame must be powered on before the K2 Summit system is powered on.
- On the K2 Summit system, Embedded Security must be in Update Mode.

1. Power on the DynoZoom Frame, if you have not already done so.
2. Power on the K2 Summit system.
3. On the K2 Summit system, insert the USB Flash Drive you received with the upgrade kit.
4. On the USB Flash Drive, find `DynoZoom_x.x.x.msi`, which is the DynoZoom software installation file.
5. Copy the DynoZoom installation file to the K2 Summit system.
6. On the K2 Summit system, double-click `DynoZoom_x.x.x.msi`.

   The setup program launches to install the DynoZoom software.
7. Complete the setup wizard, accepting default settings.
8. Restart the K2 Summit system.
9. On the K2 Summit system, use Embedded Security Manager and leave the Update Mode.

   Embedded Security Manager now reports **Enabled**.

NOTE: Once DynoZoom software is installed, the DynoZoom Frame must be connected and powered on first whenever powering up the K2 Summit system.

Next, do final steps.

Final steps for DynoZoom upgrade

- On the K2 Summit system, Embedded Security must not be in Update Mode. Embedded Security Manager must report **Enabled**.

1. When the K2 Summit 3G system is fully configured, licensed, and operational, create a disk image and store it on the USB Recovery Flash Drive. Refer to the K2 product's service procedures.
2. Disconnect the USB Recovery Flash Drive and store it in the front bezel assembly.

The upgrade process is complete for the following upgrade kits:

- K2-DYNOZOOM-FK

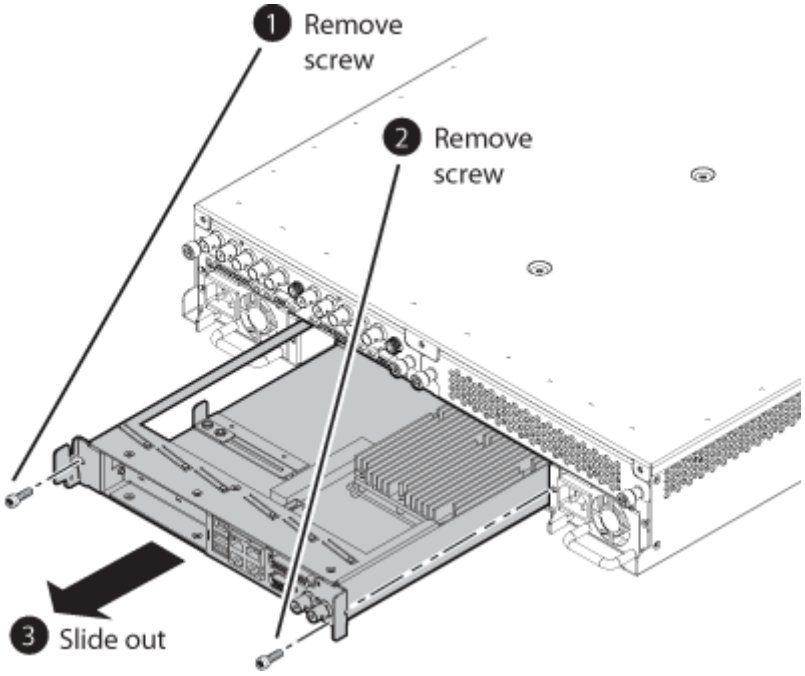
Refer to related topics in the "Using K2 Dyno S Replay Controller" section of the K2 Dyno Topic Library to configure and use the DynoZoom system.

K2 Summit system procedures

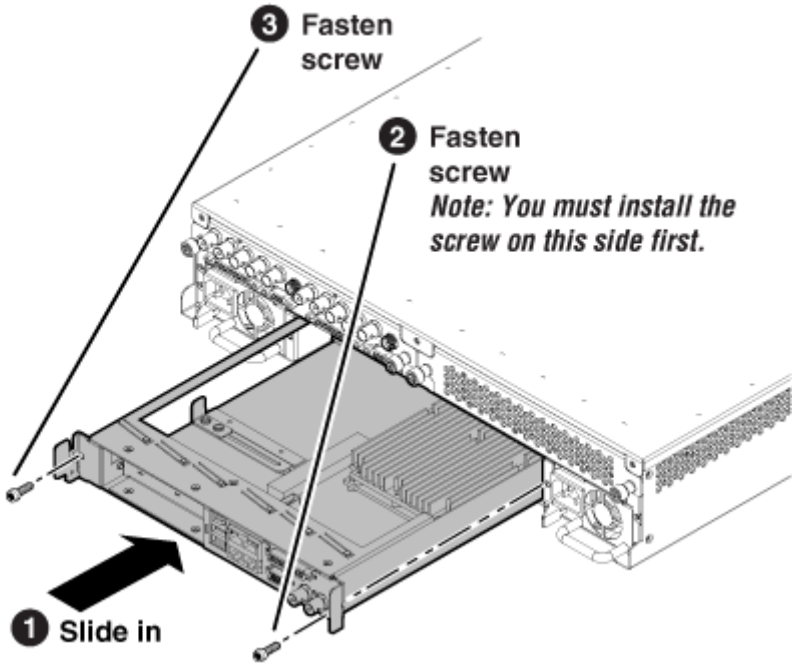
Refer to the following procedures as directed by the instructions for the Field Kit you are installing.

Carrier module removal

1. When removing the carrier module, access it from the rear panel. Remove as illustrated.

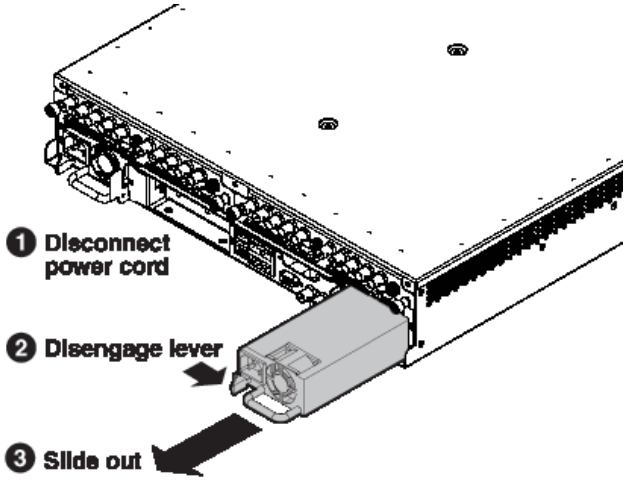


2. When replacing the carrier module, the screw attachment sequence is critical, as illustrated.



Power supply module removal

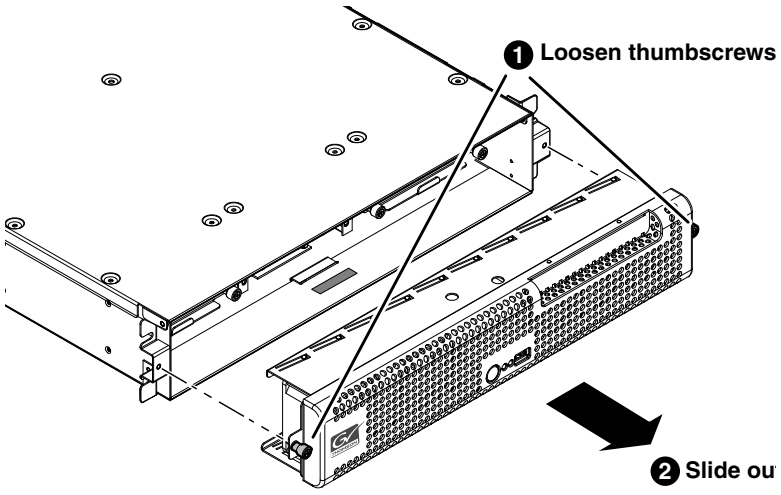
Access the power supply module from the rear panel. Remove as illustrated.



Front bezel assembly removal K2 Summit

You can remove the bezel assembly while the K2 Solo 3G system is operating. If you do so, make sure you replace it within three minutes to ensure that the correct operating temperature is maintained.

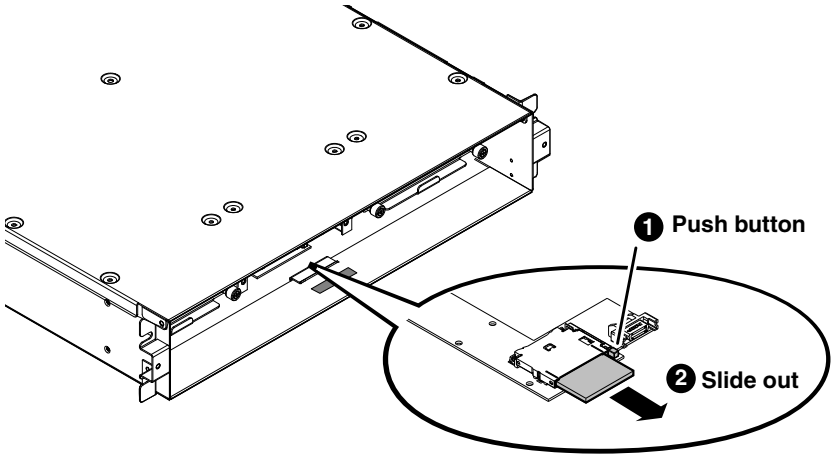
To remove the front bezel assembly, proceed as illustrated.



CompactFlash boot media removal K2 Summit

Before doing this task, remove the front bezel assembly.

To remove the boot media, proceed as illustrated.



You must use the CompactFlash boot media provided by Grass Valley. Do not use CompactFlash media procured elsewhere.

Deploy Embedded Security solution - One-time process

You must have a system system-specific recovery disk image of the computer on which you are doing the Embedded Security one-time process.

NOTE: A re-image of the computer might be necessary if the Embedded Security one-time process is done incorrectly. Follow instructions carefully.

This is a two-phase task:

1. Run a script on the local system to which you are deploying software.
2. Deploy software with SiteConfig.

NOTE: You must carefully read and verify that you have completed each step in the task. Do not assume the task is the same as other software install tasks with which you are familiar.

On the computers in your system that are running the Grass Valley Embedded Security solution, you must do a one-time initial deployment process, as instructed by this task. This task isolates the steps required for the one-time process. If you have sufficient knowledge of systems and upgrades, you can modify your software upgrade steps as necessary to do the one-time process at the same time as your other software upgrades, rather than as isolated steps. After you have done this one-time process, you can do future upgrades using the normal upgrade process.

This applies to the following:

- K2 Summit/Solo system
- All types/roles of K2 Media Server

- All types/roles of GV STRATUS server

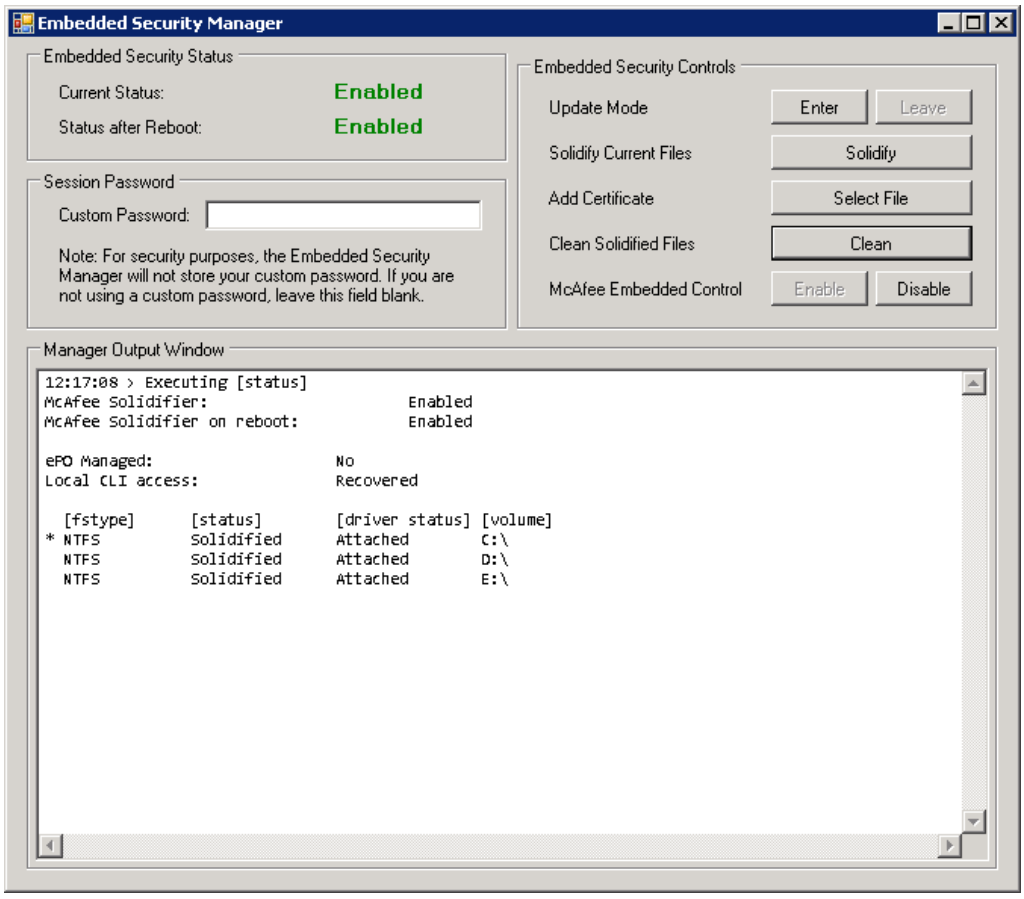
1. Determine the status of the Embedded Security solution on the computer. You can use SiteConfig check/view software to make this determination or on the local computer you can use the Programs and Features Control Panel to make this determination. Proceed as follows:
   - If the computer does not have **McAfee Solidifier**, which is a component of the Embedded Security solution, do not continue with these steps. The computer must already have the Embedded Security solution before the one-time process is applied.
   - If the computer has **McAfee Solidifier** at version 6.1.1.369, do not continue with these steps. That version indicates that the computer already has the one-time process applied, through either a software installation or a disk image process.
   - If the computer has **McAfee Solidifier** at a version lower than 6.1.1.369, continue with these steps.
2. Procure the McAfee script from the software download page on the Grass Valley website.
   The filename to download is *McAfee-6.1.1.zip*.
3. Unzip and copy the directory containing the McAfee script files to any location on the local computer.
4. Use Embedded Security Manager and put the local computer in Update Mode.
5. On the local computer, in the directory of McAfee script files that you downloaded from the Grass Valley website, run *UpdateMcAfee.cmd*.
6. Delete the directory of McAfee script files from the local computer.
7. In SiteConfig, do the following:
   a) Add the **GV Embedded Security Manager** role to the device.
   b) Add cab file as necessary to the device's deployment group so that the *GVEmbeddedSecurityManager* cab file is available for deployment.
   c) Do a **Check Software** operation on the device.
   d) Deploy software to the device.
8. Use Embedded Security Manager and leave the Update Mode.
   Embedded Security Manager now reports **Enabled**.
9. Do Windows updates on the local computer.
   You can now install Windows updates KB2859537 and KB2872339, which were previously not allowed on Grass Valley systems.

- For future Windows updates, it is no longer necessary to exclude KB2859537 and KB2872339.
- For future deployment of K2 and GV STRATUS software using SiteConfig, it is no longer necessary to put Embedded Security in Update Mode.

  NOTE: If not using SiteConfig, it can still be necessary to put Embedded Security in Update Mode. Refer to your product's software install/upgrade instructions.

Manage Embedded Security Update mode

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



   Interpret Current Status as follows:

   - **Enabled**: Embedded Security is enabled but is not in Update mode.
   - **Update**: Embedded Security is enabled and is in Update mode, ready for software installation.

2. Manage the Update mode as follows:

   - If Embedded Security is not in Update mode, click **Enter** to put it in Update mode.
   - If Embedded Security is already in Update mode, click **Leave** to take it out of Update mode.

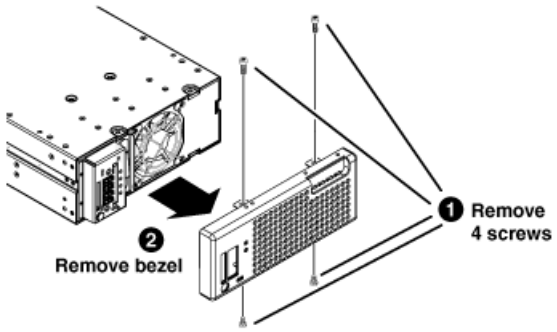
   A restart is not required after you change the Update mode.

K2 Solo Media Server procedures

Refer to the following procedures as directed by the instructions for the Field Kit you are installing.

Front bezel removal K2 Solo

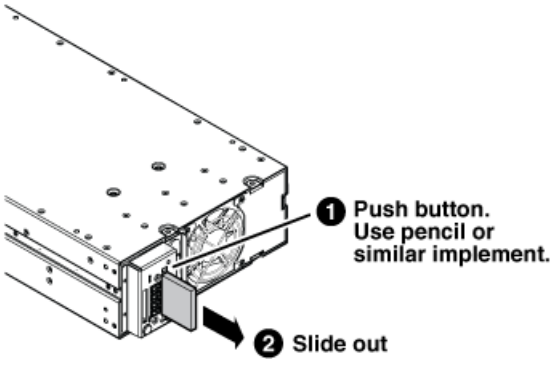
To remove the front bezel, proceed as illustrated.



⚠ ***CAUTION: Do not remove bezel while power is on. If powered, the fan can turn on with moving blades exposed.***

CompactFlash boot media removal K2 Solo

To remove the boot media, first remove the front bezel, then proceed as illustrated.



You must use the CompactFlash boot media provided by Grass Valley. Do not use CompactFlash media procured elsewhere.

Servicing the K2 Summit system

Product description

Overview description

The K2 Solo 3G system is a cost-effective media platform that incorporates IT and storage technologies. It delivers a networked solution to facilities for replay in sports, news, live, and live-to-tape applications, as well as ingest, playout, and media asset management. It is a comprehensive platform that provides a suite of user applications, system tools, and the largest range of third party interactivity in the industry.

Refer to the the "Configuring the K2 System" section of this Topic Library for other high-level descriptions of features, controls, applications, and subsystems.

K2 Summit 3G system features

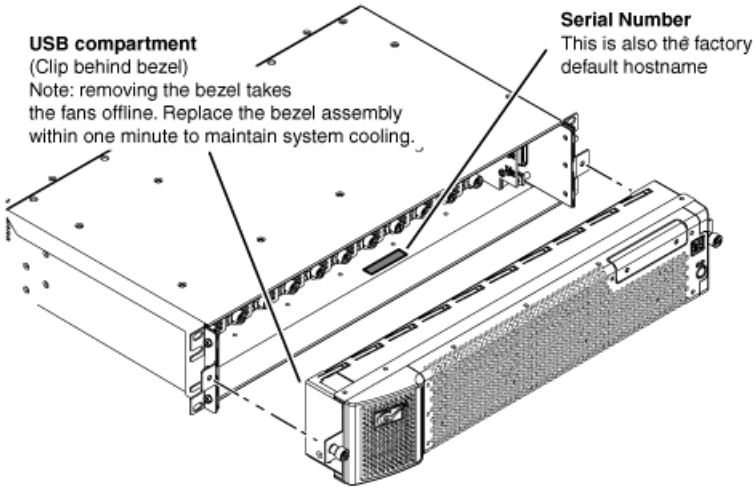
The following features apply to the K2 Summit 3G Production Client:

- Windows 7 64-bit embedded operating system.
- Embedded Security for protection against viruses and other unauthorized programs.
- Bidirectional channels (channel can be either an input channel or it can be an output channel).
- Two or four channels per chassis.
- SDI video inputs and outputs.
- AES/EBU or embedded audio inputs and outputs.
- Standard Definition (SD) video formats and High Definition (HD) video formats.
- Support for DV, MPEG-2, AVCHD/H.264, AVC-Intra, AVC - LongG, and Avid DNxHD. For details regarding licenses, hardware support, and video codec specifications, refer to related topics in the "Using K2 AppCenter" section of the K2 Topic Library.
- 3G codec module hosts codec option cards that are programmable for multiple formats and functions.
- Mixed format playback of SD or HD clips on the same timeline.
- Up/down/cross HD/SD conversion (e.g. SD and HD clips ingested, then played back as SD or HD clips) or as a different SD or HD format (e.g. 720p to 1080i).
- 4K, Super Slo-Mo, Multi-cam, and 3D/Video + Key features are available as part of the ChannelFlex Suite.
- 4K/UHD workflow and 4K/UHD Pan & Zoom using the GV DynoZoom software.
- High endurance SSD internal storage for 6-in/2-out configuration, 6x Super Slow Motion (SSM), and 4K/UHD workflow.
- VGA monitoring capability.
- Redundant power supply, cooling fans for reliability.
- 2.5 inch media storage drives.
- mSATA SSD system drive.
- Type IV CPU carrier module with 8 GB RAM.
- USB 3.0 interface for file exchange. (In K2 Summit 3G system only).
- Ability to create nested bins, i.e. sub-bins within bins.

- Freeze mode can be frame or field.
- Various video mix effects (e.g. dissolves between two video and audio tracks on the same channel, or fade thru matte color).
- Remote operation and configuration via AppCenter.
- Gigabit Ethernet.
- AMP, VDCP, and BVW remote control protocols supported.
- Remote control over RS-422 or Ethernet.
- Low-resolution proxy files created during record and live streaming from SDI In/out are available as part of the AppCenter Pro and Elite licenses.
- RAID media storage.
- Stand-alone internal storage, stand-alone external direct-connect storage, and external shared (SAN) storage.

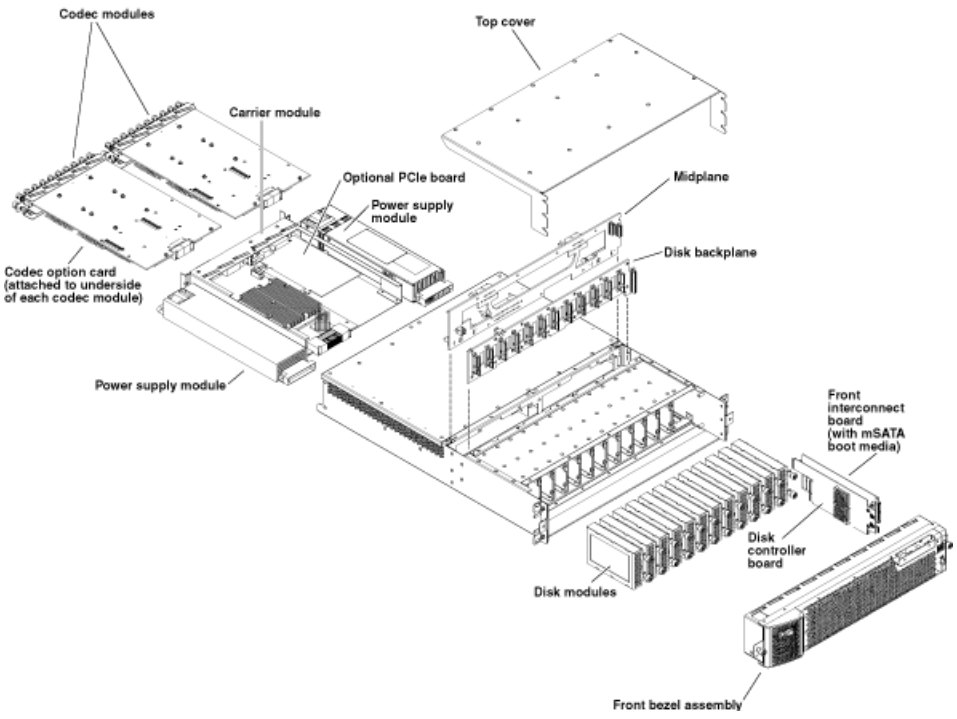
Product identification K2 Summit 3G

The K2 Summit 3G system has labels affixed to the chassis that provide product identification as illustrated:



K2 Summit 3G system orientation

The following illustration shows the location of Field Replaceable Units (FRUs) and other components in the K2 Summit 3G system.



FRU functional descriptions

K2 Solo 3G system Field Replaceable Units (FRUs) are described in this section.

Front bezel assembly

The front bezel assembly includes the bezel, fans, and fan status board. The assembly has four fans and provides cooling for the K2 Solo 3G system chassis. Air intake is from the front of the K2 Solo 3G system and outflow is through the rear. The assembly connects to the front interconnect board and is secured to the chassis by two thumbscrews.

Disk modules

There are slots for disk modules in the K2 Solo 3G system. The slots are located behind the front bezel assembly in the front of the chassis. Each slot can contain one disk module, and each module contains one hard drive. Depending on storage options, a K2 Solo 3G system can be fully populated, partially populated, or can contain no disk modules. Disk modules plug into the disk backplane board.

Data is written or “striped” across the disks in a continuous fashion, which makes the disks a “stripe group”. This stripe group appears as the V: drive to the Windows operating system.

The V: drive stores media. It also stores media file system, database, and configuration information. K2 Solo 3G systems with direct-connect storage or shared SAN storage do not contain disk modules, as the V: drive is on the external RAID storage devices.

When configured as RAID 1, you can remove and replace a disk module while the K2 Solo 3G system is operational.

mSATA boot media

The mSATA SSD boot media contains the system drive, also known as the C: drive. The C: drive contains application and operating system files. The mSATA media is hosted by the front interconnect board.

Power supply modules

The K2 Solo 3G system has redundant (two) power supplies. You should connect a power cable to each power supply, but both power supplies remain operational if only one cable is connected. The power supplies can be accessed from the rear of the unit. You can remove and replace a power supply while the K2 Solo 3G system is operational. Each power supply has a fan with automatic speed control and status LEDs that indicate current state and health. The power supply has protection for over voltage, over current, and short circuits. The power supply modules plug into the midplane board.

Codec module

The K2 Solo 3G system has slots for two codec modules. Each codec module hosts two media input/output channels. The codec modules are oriented horizontally across the rear of the K2 Solo 3G system chassis. They provide the majority of the K2 Solo 3G system's media-related input and output connectors on the rear panel. The codec modules plug into the midplane board.

A codec module can host a codec option card. The codec option card provides extended functionality to the channels hosted by the codec module.

Codec option card

There is one type of codec option card available for the K2 Solo 3G system. The codec module hosts the codec option card. The single codec option card provides functionality for both of the codec module's channels.

Disk controller board

The disk controller board provides the RAID functionality for the internal disks. It is mounted in the front of the unit. The disk controller board plugs into the disk backplane board and the midplane board. K2 Solo 3G systems with direct-connect storage or shared SAN storage do not contain a disk controller board, as RAID disks are in the external RAID storage devices.

Front interconnect board

The front interconnect board has the control and speed monitoring circuit for the fans and incorporates a PCIE to dual USB 3.0 controller circuit. It hosts the boot media, standby switch, Power LED and Service LED. The LEDs are driven by circuitry on the carrier module. The front interconnect board is mounted in the front of the unit and plugs into the midplane board.

Disk backplane unit

The disk backplane unit includes the disk backplane board. The disk backplane board provides the connections for the disk modules and hosts the disk status LEDs. It is mounted in the front center of the chassis. It plugs into the disk controller board. A power cable connects the midplane board and the disk backplane board. K2 Solo 3G system with direct-connect storage or shared SAN storage do not contain a disk backplane board, as RAID disks are in the external RAID storage devices.

Midplane board

The midplane board provides connections for the rear modules. The disk controller board and the front interconnect board also plug into the midplane board. It is mounted in the center of the unit. A power cable connects the midplane board and the disk backplane board, if present.

Carrier module

The carrier module provides the functionality typically associated with a motherboard in a PC. It hosts the CPU, one optional PCIe board, and provides rear panel connections for Gigabit Ethernet, USB, VGA, and IEEE 1394a (Firewire). The IEEE 1394a port is for debugging purposes only. It is not supported for customer use. Do not attempt to configure or otherwise use this port. The carrier module also provides a GPI connection and connections for reference. It plugs into the midplane board.

Optional PCIe board

An optional PCIe board, such as a Fibre Channel board or a DynoZoom board, is hosted by the carrier module.

System Overview

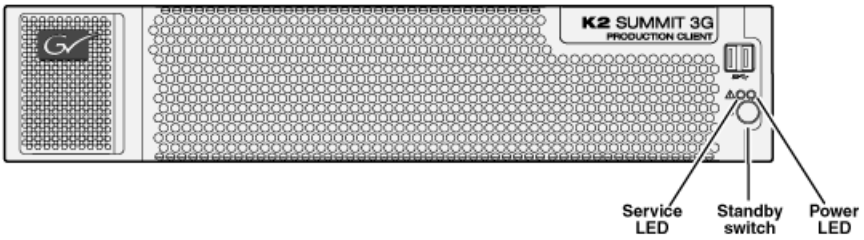
The K2 Solo 3G system is a PCIe bus-based Windows computer with extensive enhancements to provide the video disk recorder functionality. This section explains the major architectural blocks.

Status indicators

The following sections describe the visual and audible indicators that communicate the current operating status and system health of the K2 Solo 3G system.

Front panel indicators

The front bezel assembly must be installed for front panel LEDs to provide status.



Power LED

The Power LED indicates status as follows::

LED behavior	Status Condition
Off	The standby switch is set to Off and the K2 Solo 3G system is not operational.
Green steady on	The standby switch is set to On and the K2 Solo 3G system is either in the startup process or has completed the startup process and is operational.

⚠ ***WARNING: The power standby switch does not turn off power to the system. To turn power off both power supplies must be disconnected from the power source.***

Service LED

The following table explains the status conditions indicated by the different Service LED behaviors. If two or more status conditions occur simultaneously, the LED displays the behavior for the highest priority condition.

LED behavior	Status Condition	Priority
Flashing pattern alternating Yellow/Green/Red/Off twice a second	Identify — The K2 Solo 3G system is being directed to identify itself by NetCentral or some other application.	1
Solid Red	Global failure — The K2 Solo 3G system software has detected a critical error or failure that impacts record/play operations.	2
Solid Yellow	Warning — The K2 Solo 3G system software has detected a problem that requires attention but does not immediately impact record/play operations. For example, a fan or power supply has failed but its redundant partner is maintaining functionality.	3
Flashing Yellow pattern three times a second.	Drive failure — An internal RAID drive has failed. If RAID 1, the failure does not immediately impact record/play operations. The redundant partner RAID drive is maintaining functionality.	4
Flashing pattern alternating Yellow/Green once a second.	Drive rebuild — If RAID 1, an internal RAID drive is rebuilding.	5

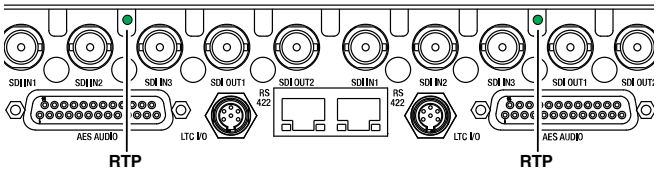
LED behavior	Status Condition	Priority
Off	Normal — The K2 Solo 3G system is healthy and operating normally.	5

Rear panel indicators

The following indicators are visible from the rear panel view.

Codec board indicator

Each channel has a green/red LED that indicates the status of the Real Time Processor (RTP).



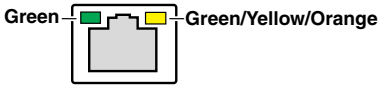
Codec board indicator codes

Interpret the RTP LED as follows:

LED behavior	Status condition
Green flashing at approximately 1 second intervals	RTP is up and connected to the host
Green flashing at greater than 1 second intervals	RTP is not connected to the host.
Red	RTP error condition. Real Time OS is not running.
Off	Real Time OS is not running.

LAN connector indicator codes

The motherboard has four RJ-45 LAN connectors that include integrated status LEDs. The LEDs are oriented as follows:



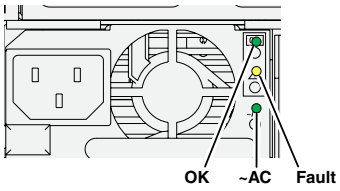
The meanings of the LED states are described in the following table:

LED	LED state	Status Condition
Green	Green On	The adapter is connected to a valid link partner
	Green flashing	Data activity
	Off	No link
Green/Yellow/Orange	Off	10 Mbps
	Green	100 Mbps
	Yellow	1000 Mbps
	Orange flashing	Identify

If a LAN connector is faulty, you must replace the carrier module.

Power supply indicators

Each power supply has LEDs that indicates status.



Interpret the power supply LEDs as follows:

LED	LED state	Status Condition
OK	Green On	The power supply is operating normally.
Fault	Yellow On	There is a power supply fault.
~AC	Green On	The electrical current available to the power supply meets power supply requirements. Input > 85 VAC.

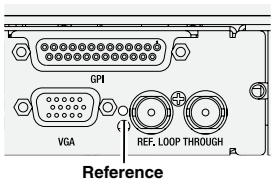
Another indicator of power supply operation is the audible fan noise. If a power cable is connected to either power supply, the fan should stay on continuously on both power supplies. This is the case even if the K2 Solo 3G system is shut down or restarting via the standby switch or the Windows operating system.

The Service LED on the front of the K2 Solo 3G system also indicates power supply status.

If the power source and the power cord are OK yet there is still a power supply problem, the status lights on the power supply indicate the problem.

Reference indicator

There is a small hole in the carrier module next to the “REF. LOOP THROUGH” BNC connectors.



Through this hole a LED is visible. When the LED is lit, the reference signal is present and locked.

Internal indicators

You must remove one or more modules to expose the following indicators for viewing.

Disk module indicators

You must remove the front bezel assembly to see these LEDs. Each disk module has LEDs that indicate status. The LEDs are located on the disk backplane. Flexible light pipes transmit the light so that it appears on the disk pillar next to the disk module. The following table explains the status conditions indicated by the different LED behaviors. If two or more status conditions occur simultaneously, the LED displays the behavior for the highest priority condition. Priority number 1 is the highest priority

LED behavior	Status Condition	Priority
Amber flashing pattern.	Identify — The drive is being directed to identify itself by Storage Utility or some other application.	1
Green flashing pattern twice a second.	Rebuild — The RAID controller has marked the drive as rebuilding.	3
Red ON solid.	Fault — The RAID controller has marked the drive as faulty.	3
Amber ON solid.	Offline — The drive is unbound.	3
Green flashing pattern ten times a second.	Normal drive activity — The drive is healthy and disk access is underway.	3
Green ON solid.	Normal drive activity — The drive is healthy and no disk access is currently underway.	3
OFF	No drive — Drive is not present or is not fully engaged in slot.	—

System beep codes

When you start up the K2 Solo 3G system by pressing the standby switch or by doing a Windows operating system restart, the CPU module might emit two short beeps. Otherwise, if there are no errors present, the K2 Solo 3G system does not emit any audible beeps.

When an error occurs during Power On Self Test (POST), the BIOS displays a POST code that describes the problem. The BIOS might also issue one or more beeps to signal the problem. This

indicates a serious error and it is likely that the carrier module must be replaced. Contact Grass Valley Support.

System Messages

About system messages

The following messages are displayed to indicate system status:

- Normal BIOS messages — These messages can be observed on a locally connected VGA monitor during normal startup processes.
- BIOS POST error messages — If there is a problem these messages are displayed on a locally connected VGA monitor. During the Power On Self Test (POST), the BIOS checks for problems and displays these messages.
- AppCenter startup messages — As AppCenter opens the system determines if health is adequate by checking critical subsystems. A dialog box is displayed that indicates progress and displays messages.
- Status bar and StatusPane messages — During normal operation AppCenter displays system status messages on the status bar. From the status bar you can open the StatusPane to see both current and previous messages. You can observe these messages in AppCenter on a locally connected VGA monitor or on a network connected control point PC.
- Storage Utility messages — While you are using Storage Utility, pop-up message boxes inform you of the current status of the storage system.

Critical system startup messages

The following messages appear in the AppCenter system startup message box as critical subsystems are checked during startup processes. If a critical failure is detected, the K2 Solo 3G system is rendered inoperable and the failure message appears.

Critical subsystem check messages	Failure messages
System Startup	Startup error
	Missing or bad hardware
	A real time processor is not functioning correctly
Checking hardware…	Hardware fault
Checking media disks…	One or more media disks failed to initialize
	Missing or bad hardware
	Missing or bad database
Checking file system…	No file system is running
Checking database…	Database fault
Checking real-time system status…	A real-time system failed to initialize
Updating configuration…	Failed to synchronize configurations

Critical subsystem check messages	Failure messages
Starting services…	Unable to communicate with <service name>

AppCenter startup errors

If you start AppCenter and the K2 Solo 3G system is not running, or your login information is not correct, you will see a Startup Error message.

The following table describes the two most common startup error messages.

Startup Error	Description
Log on failed	Your user name or password is not valid for this K2 Solo 3G system. Remember that the password is case sensitive. • Click **Ignore** to view the AppCenter channels. If working remotely, you will see the channels from the last-used channel suite. Or, • Click **Retry** to enter the login information again. Or, • Click Abort. If you are accessing AppCenter through a network-connected Control Point PC, **Abort** lets you try to create a new channel suite. If you are accessing AppCenter locally, it lets you exit to Windows. For assistance with your user name or password, consult your Windows administrator.
<K2 system>:<error>	The K2 Solo 3G system might be offline or have had difficulty with the start up checks. There are various reasons why AppCenter is having difficulty connecting to the K2 Solo 3G system; for example, the error might say there is no file system or that the K2 Solo 3G system has been taken offline for maintenance. • Verify that the host name or IP address is correct and see if you can correct the problem. • If working locally, reboot the K2 Solo 3G system. If working from a network-connected Control Point PC, select **System | Reconnect** from the AppCenter **System** menu.

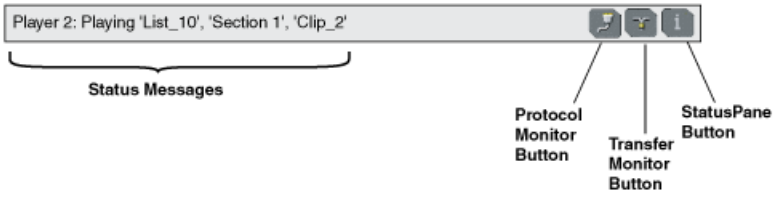
Viewing AppCenter system status messages

System status messages are displayed in the AppCenter status bar. There are two types of system status messages, as follows:

- Channel status messages — In normal operation, this type of message displays the current operating status of the selected channel.
- System error messages — If a problem develops with the system software or a hardware subsystem, this type of message is displayed for approximately 5 seconds. Afterward, the display returns to the channel status message and the error message is written to the status log file. When a message is written to the status log, a *Status Icon* indicates the severity of the message.

Status bar

System status messages appear in the AppCenter status bar, which is located across the bottom of the AppCenter window, and consists of a message area, several tool buttons, and a status icon. The button icons appear only when the related function is active. In the position of the StatusPane button, status icons appear.



The status bar displays information about the state of the delegated channel as well as low-level error messages. (High priority error messages are displayed in pop-up windows.)

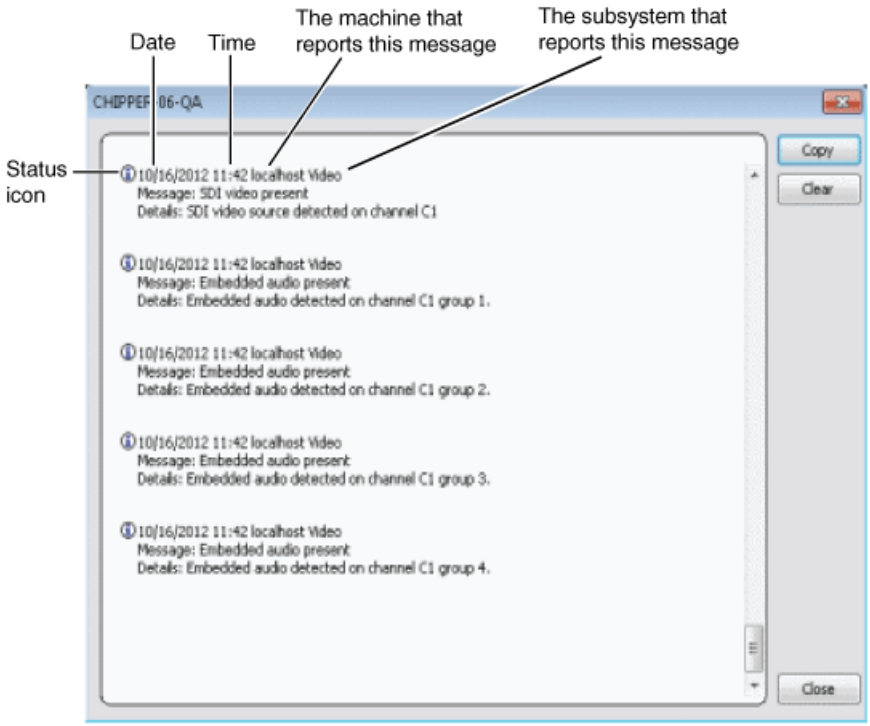
If you select a channel, a status message appears on the left-hand side of the status bar. If a potential error arises while an application is running in a channel, a status message flashes briefly on the left-hand side of the status bar, and an icon displays on the right-hand side. Double click on the icon to open the status pane to view a more detailed message about the channel's status.

The status icon changes depending on the status of the current status message.

Icon	Name	Description
	Information	A recent information message is present.
	Warning	There is at least one warning message, and no alert messages.
	Alert	There is at least one uncleared alert message.

Status pane

Current and previous system status messages can be viewed in the StatusPane. The system status pane also displays general information such as the video and audio settings on the channels. To open the StatusPane, click **Help | System Status**.



The StatusPane is used to view detailed system messages including status, warning, and error messages. System status messages provide status icons and a description of the status event reported by the message. If there is a problem, a corrective action is indicated. Use these messages along with troubleshooting problems to determine if a service procedure is necessary.

If you have a remote AppCenter Channel Suite with channels from multiple K2 systems, the messages from the different machines are combined in the StatusPane that you view from the Channel Suite. To help you determine which machine is generating a message, each message lists the machine name.

NOTE: If the Clear button is grayed out, you do not have the necessary privileges to perform this action, based on the type of user account with which you are currently logged on.

Copying StatusPane messages to the clip board

1. Select the message or messages in the StatusPane.
2. Click **Copy**.

After copying the message, it can be pasted using standard Windows techniques.

Clearing messages

Clearing messages from the StatusPane removes them from the logging database and the StatusPane. This also clears the state of the subsystem indicators so they no longer display the alert and warning symbols.

1. Open the StatusPane, then click **Clear**.
2. When a message prompts you to confirm, click **Yes**.

All messages are removed from the StatusPane and logging database.

Exporting log files

This topic describes how to export log files from the K2 Solo 3G system. The log files include the following:

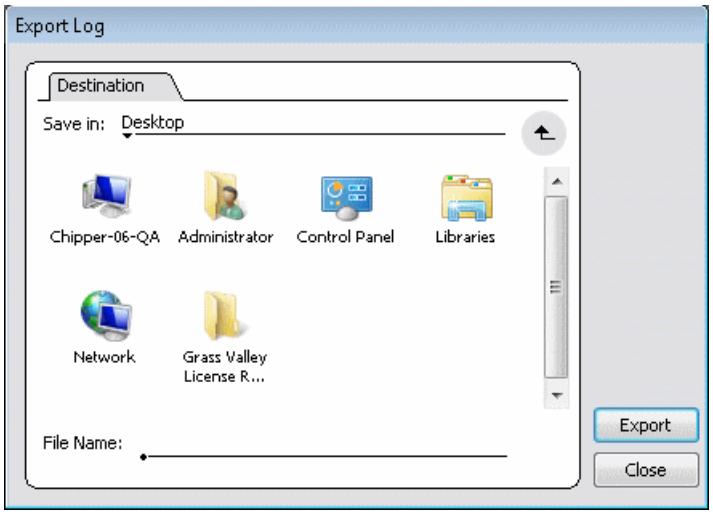
- All application and media database messages
- Version information
- Configuration file, from Configuration Manger

The exported files are combined in a ZIP file. The ZIP file can be sent to Grass Valley product support where they can analyze the logs to determine the operational status of your system.

NOTE: ExportLog does not export StatusPane messages. To capture StatusPane messages, you can copy StatusPane messages to the clip board.

1. Log in as Administrator.
2. Do one of the following to open the Export Log dialog box.
   - In AppCenter click **System | Export Log**.
   - From the Windows desktop, click **Start | All Programs | Grass Valley| Export logs**.
   - From the Windows desktop, click **Start | Run**, type `c:\profile\exportlog` in the Run dialog box, then click **OK**.

   The Export Log dialog box opens.



3. Browse to `C:\Logs` to save the log file.
4. Name the log file.
5. Click **Export**. A progress bar appears.
6. When the export process is complete, and message confirms success. Click **OK** and close the Export Log dialog box to continue.
7. Find the log file at the specified location.

Service procedures

Replacing a RAID 1 drive

If configured as RAID 1, you will repair the system by replacing the drive as soon as possible. You can replace a single RAID 1 drive while continuing media operations.

Always use the Storage Utility to physically identify the failed drive. Accidentally removing the wrong drive can destroy data. To identify a drive, in Storage Utility right-click the drive and select **Identify**. This causes the disk lights to flash. Refer to related topics in the "Configuring the K2 System" section of this Topic Library for Storage Utility procedures.

NOTE: Do not shut down. Keep the system powered on while replacing a drive.

Before removing the disk module, you should use Storage Utility to disable the disk.

To remove and insert a drive, refer to the mechanical procedure for disk module removal.

On inserting a RAID 1 replacement drive, if disk access (record/play operations) is underway, the RAID controller automatically starts rebuilding the drive. You can verify rebuild status by looking at the drive LED or by looking at the Service LED. If there is no media access currently underway, you can use Storage Utility to force-start the rebuild process.

You can also check disk status in the Storage Utility by selecting the disk module icon in the device tree. Status is reported in the right-hand pane. On completion, the disk drive status changes from Rebuilding to Online. You may need to refresh the Storage Utility display. You can also open the Progress dialog box, by clicking **View | Progress Report**.

Replacing a RAID 0 drive

If configured as RAID 0, when one drive fails, all media is lost. To replace a RAID 0 drive, do the following:

1. Unbind the LUN that has the failed drive.
2. Remove the failed drive from the K2 Solo 3G system chassis.
3. Insert the replacement drive in the K2 Solo 3G system chassis.
4. Restart the K2 Solo 3G system.
5. Using Storage Utility on the K2 Solo 3G system, bind disks as RAID 0.
6. Restart the K2 Solo 3G system.
7. Using Storage Utility on the K2 Solo 3G system, make a new file system.

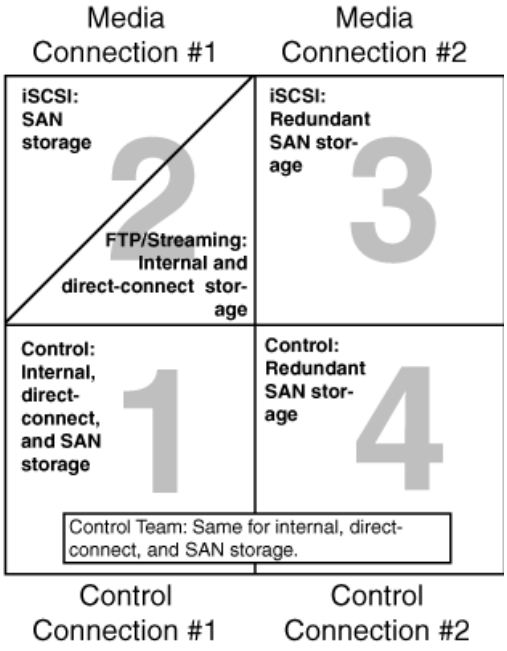
   Always use the Storage Utility to physically identify the failed drive. To identify a drive, in Storage Utility right-click the drive and select **Identify**. This causes the disk lights to flash.

   Refer to related topics in the "Configuring the K2 System" section of this Topic Library for Storage Utility procedures.

   To remove and insert a drive, refer to the mechanical procedure for disk module removal.

About networking

When you receive a K2 Solo 3G system from the factory, it has a specific network configuration, including a loopback adapter and two of the four Gigabit Ethernet ports configured as a teamed pair. The Gigabit Ethernet ports, as viewed when looking at the rear panel, are represented in the following illustration.



Restoring network configuration

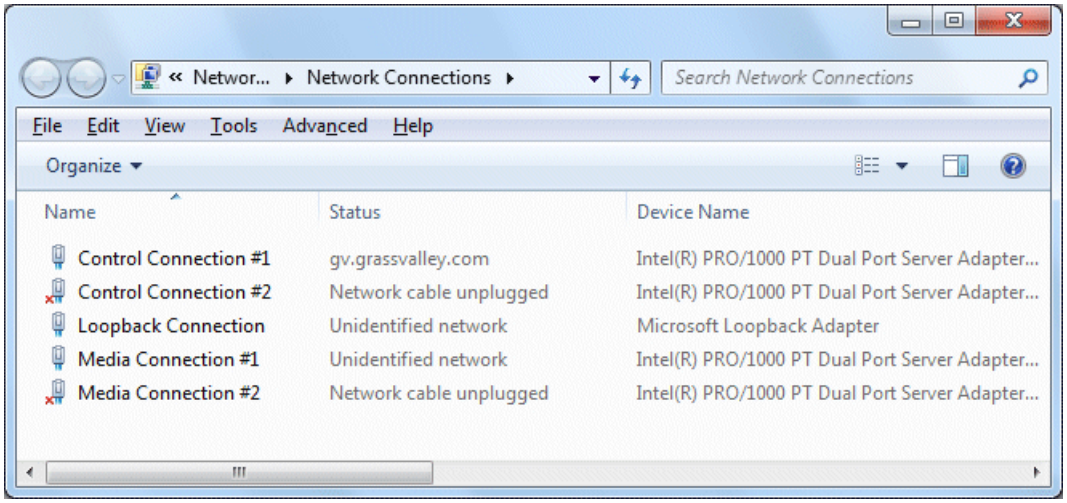
When you restore a system from its system specific image, network configuration is also restored to the factory default settings. This is the recommended method of restoring network configuration. However, if for some other reason you must configure network settings manually, use the tasks in this section to restore the default network configuration.

Create the Control Team

NOTE: Team control ports only. Do not team media ports.

1. Open Network Connections, if it is not already open.
   a) From the Windows **Start** menu, in the **Run** or the **Search programs and files** box, type `ncpa.cpl` and press **Enter**.

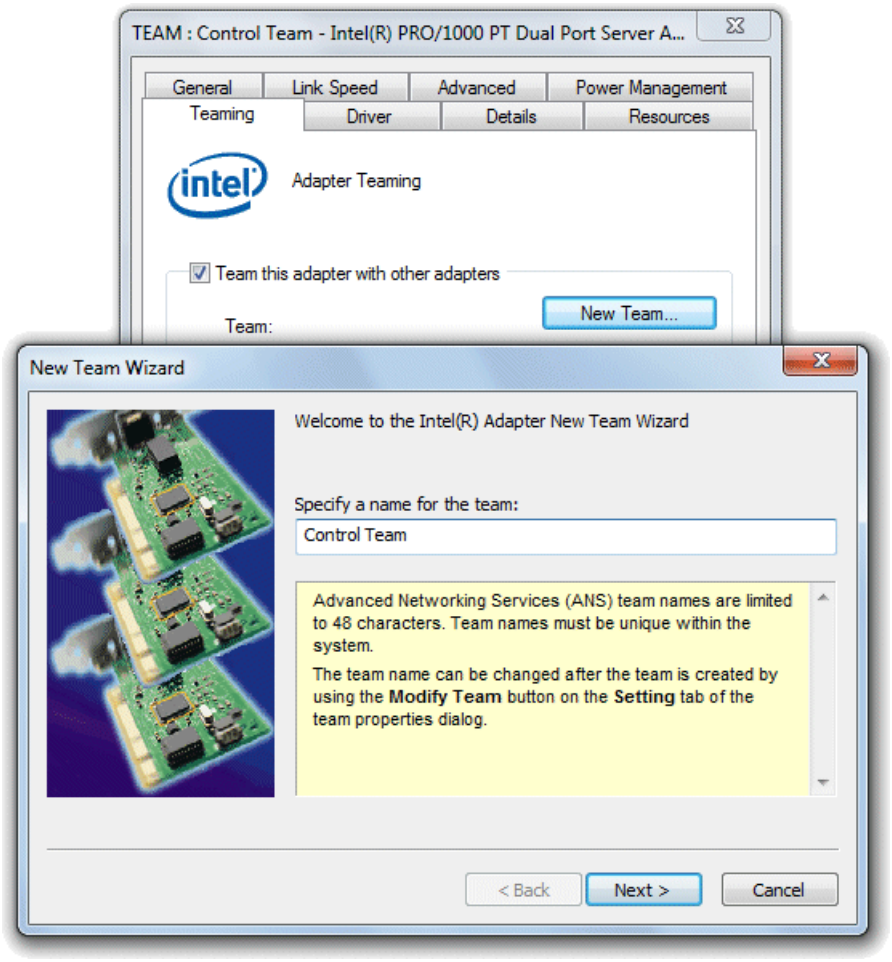
2. In Network Connections, view **Details** and identify the adapter name that maps to Control Connection #1 and the adapter name that maps to Control Connection #2.



3. Right-click the adapter name that maps to Control Connection #1.
4. Select **Properties**, then click **Configure**.

   The Properties dialog box opens.

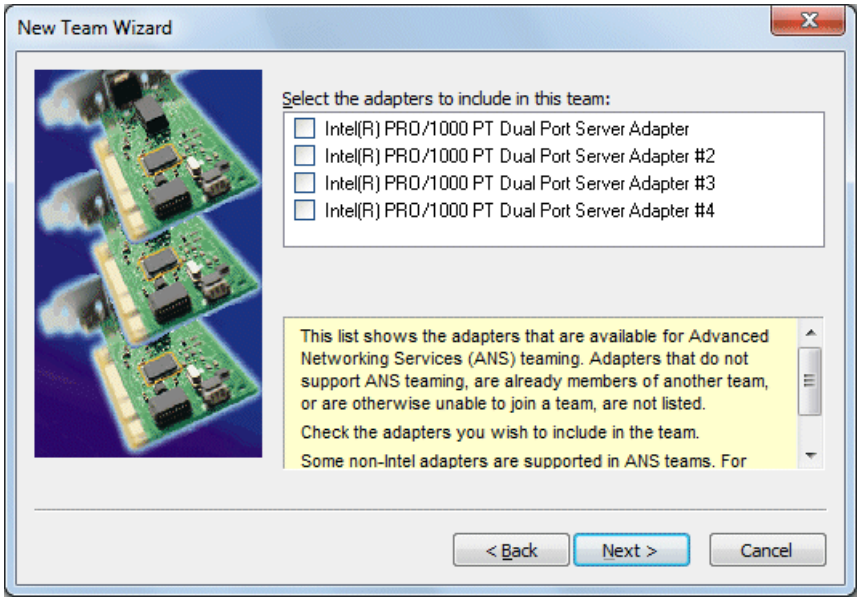
5. Select the **Teaming** tab.



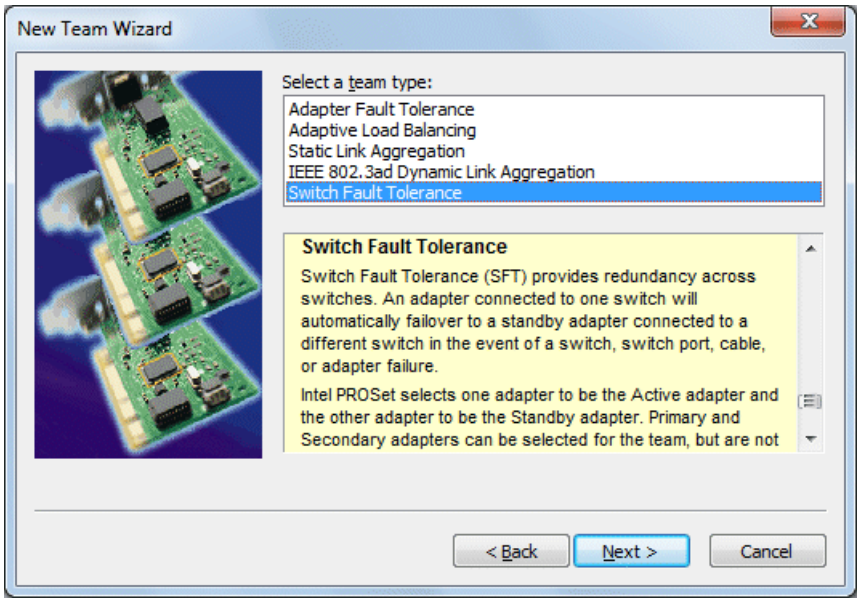
6. Select **Team this adapter with other adapters**, then click **New Team**. The New Team Wizard opens.

7. Enter Control Team.

   Click **Next**.



8. Select the check box for the adapter name that maps to Control Connection #1 and for the adapter name that maps to Control Connection #2. Click **Next**.



9. Select **Switch Fault Tolerance**. Click **Next**.
10. Click **Finish** and wait a few seconds for the adapters to be teamed.

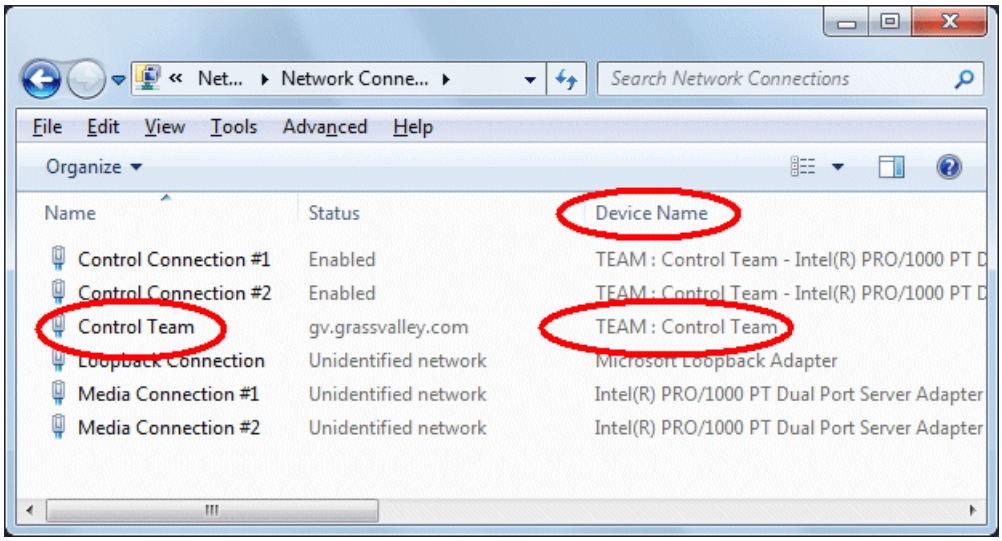
11. Open the Modify Team dialog box as follows:
    a) In **Device Manager | Network Adapters**, right-click **Control Team** and select **Properties**. The Properties dialog box opens.
    b) Select the **Settings** tab.
    c) Click **Modify Team**. A dialog box opens.
12. On the **Adapters** tab, do the following:
    a) Select the top entry, which is the adapter name that maps to Control Connection #1 and click **Set Primary**.
    b) Select the adapter name that maps to Control Connection #2 and click **Set Secondary**.
13. Click **OK** and **OK** and to close dialog boxes.
14. Restart the K2 Solo 3G system.

If continuing with network configuration, your next task is to name team and loopback.

Name team and loopback

- Adapters must be named
- The control team must be created

1. On the Windows desktop right-click **Start | Control Panel | Network and Sharing Center | Change adapter settings**. The Network Connections window opens.



2. For the Control Team and the loopback, select adapter names in the "Device Name" column and rename them as follows:
    a) Select the adapter name.
    b) Select **File | Rename** to enter rename mode.
    c) Type the name, as specified in the following table:

In the Device Name column, select this adapter name…	And rename it as follows:
TEAM : Control Team	Control Team

3. Do one of the following:
   - If you intend to use SiteConfig for device discovery and IP address configuration, you do not need to set an IP address for the Control Team at this time. You are done with this procedure.
   - If you are not using SiteConfig, set an IP address for the Control Team at this time. Use standard Windows procedures.

   NOTE: Do not set IP addresses for the two Media Connections.

If continuing with network configuration, your next task is to reorder adapters.

Reorder adapters

- Adapters must be named correctly
- The control team must be created
- The team and loopback must be named

1. Open Network Connections, if it is not already open.
   a) From the Windows **Start** menu, in the **Run** or the **Search programs and files** box, type `ncpa.cpl` and press **Enter**.

   The Network Connections window opens.
2. Select **Advanced**, then **Advanced Settings…**
3. On the **Adapters and Bindings** tab, depending on the K2 system storage, order adapters as follows:

Internal or direct-connect storage	Shared (SAN) storage
Loopback	Control Team
Control Team	Control Connection #1
Control Connection #1	Control Connection #2
Control Connection #2	Media Connection #1
Media Connection #1	Media Connection #2
Media Connection #2	Loopback
1394 Connection	1394 Connection

   If controlled by Dyno Production Assistant, refer to Dyno PA documentation for adapter order.
4. Click **OK** to close and accept the changes.
5. Close Network Connections.

Network configuration is complete.

Next, enhance network bandwidth.

Enhance network bandwidth

On K2 Summit/Solo systems with K2 system software 9.x, the on-board network adapters have a performance limitation that causes them to function at half the expected bandwidth. On most systems, there are no symptoms related to this limitation, as network traffic is below the limitation. Systems

using ShareFlex or having other requirements for high network bandwidth might be impacted to some degree. Symptoms include general network bandwidth restrictions, slow iSCSI I/O performance, slower than expected FTP traffic, and other slowness not caused by other factors.

Grass Valley requires that you remove the limitation and enhance the network performance. Once the limitation is removed, the change persists throughout normal software upgrades. However, if you reimage the K2 Summit/Solo system you must check and reapply the change if necessary.

To remove the limitation, disable "Large Send Offloads" on the network adapters and disable "CPU Power Technology" in the BIOS.

Refer to Grass Valley Knowledge Base Article *#000011688* for more information.

Disable Large Send Offloads

1. From the Windows operating **Start** menu, open **Control Panel**.
2. In **Control Panel**, open **Network and Sharing Center**.
3. In **Network and Sharing Center**, select **Change adapter settings**.
   Network Connections opens and displays network adapters, including the following:
   - Control Connection #1
   - Control Connection #2
   - Media Connection #1
   - Media Connection #2
4. For each Control Connection and each Media Connection, do the following:
   a) Right-click the connection and select **Properties**.
      The **Connection Properties** dialog box opens.
   b) In the **Connection Properties** dialog box, click **Configure**.
      The **Adapter Properties** dialog box opens.
   c) In the **Adapter Properties** dialog box, click the **Advanced** tab.
   d) On the Advanced tab, in the Settings list select **Large Send Offload v2 (IPv4)** and then in the Value drop-down list select **Disabled**.
   e) Click **OK** to save settings and close.
   f) Repeat these steps for each Control Connection and each Media Connection.

Next, disable CPU power technology.

Disable CPU Power Technology

1. Restart the K2 Summit/Solo system.
2. During the BIOS startup screen, press **F2** repeatedly until `Entering Setup...` appears.
   The BIOS screen opens.
3. On the BIOS screen, use arrow keys and select the **Advanced** tab.
4. On the Advanced tab select **CPU Core Configuration** and then press **Enter**.
   The CPU Core Configuration screen opens.

5. On the CPU Core Configuration screen, select **Power Technology** and then press **Enter**.
   A **Power Technology** dialog box opens.
6. In the **Power Technology** dialog box select **Disable** and then press **Enter**.
7. Press **F4** to save and exit.
   A **Save & Exit Setup** dialog box opens.
8. In the **Save & Exit Setup** dialog box, select **Yes** and then press **Enter**.
9. The K2 Summit/Solo system restarts.

Next, install the SiteConfig Discovery Agent.

Checking services

Depending on storage type (standalone or shared) of the K2 Solo 3G system, various services are turned off or on or set to different startup types. These services are automatically set by the K2 Solo 3G system software installation program and by the Status Server service whenever the K2 Solo 3G system starts up.

***NOTE: Do not manually change the way services run on a* K2 Solo 3G system.**

If you suspect that services have been tampered with or for any reason are not set correctly, you can check their current settings in the Windows Services Control Panel. The table below provides the settings for the services that are critical to a correctly operating K2 Solo 3G system.

Services on a standalone storage K2 Summit 3G system

When a standalone K2 Solo 3G system with internal storage or a K2 Solo 3G system with direct-connect storage is operating normally, in the Services control panel services appear as follows:

Table 50: Standalone storage K2 Summit 3G system services

Service	Status	Startup Type	Comments
CvfsPM[26]	Started	Automatic	—
Grass Valley AppService	Started	Automatic	Depends on Status Server service.
Grass Valley Extent Manager Service	Started	Manual	Used to consolidate unused space (extents) at the end of proxy clips on an SNFS file system. Does not apply to non-SNFS file systems.
Grass Valley FTP Daemon	Started	Manual	Started by Status Server service on standalone storage models.

[26] With SNFS version 3.5, this is the only service. Previous versions had StorNext File System service and StorNext File System RPC Port Mapper service.

Service	Status	Startup Type	Comments
Grass Valley Host File Service	Started	Automatic	—
Grass Valley HTTP File Server	Started	Manual	Provides access to live streaming configuration (SDP) files.
Grass Valley Import Service	—	Manual	This is the service that provides the functionality for a K2 capture service. It is the service that automatically creates the K2 clip from the media files in the watched folder (source directory) and puts the K2 clip in the K2 media storage (destination bin).
Grass Valley K2 Config	Started	Automatic	Not used on standalone storage K2 Summit/Solo system.
Grass Valley MegaRaid Server	—	Manual	—
Grass Valley MetaDataService	Started	Manual	—
Grass Valley RTS Config Service	Started	Manual	—
Grass Valley SabretoothWS	—	Manual	Allows Macintosh systems to remotely check out a license.
Grass Valley Storage Utility Host	Started	Automatic	—
Grass Valley System Status Server	Started	Automatic	At startup the Status Server service makes sure the following services are started: AMP TCP Service; AppService; FTP Daemon.
GV STRATUS Summit Services	Started	Automatic	Required if part of a GV STRATUS system.
Microsoft iSCSI Initiator Service	Started	Automatic	Not used on a standalone storage K2 Summit/Solo system.
ProductFrame Discovery Agent Service	Started	Automatic	—
Sabretooth License Server	Started	Manual	—

Service	Status	Startup Type	Comments
Sabretooth Protocol Service	—	Manual	—

Services on an shared storage K2 Summit 3G system

When a shared storage (SAN) K2 Solo 3G system is operating normally, in the Services control panel services appear as follows:

Table 51: Shared storage K2 Summit 3G system services

Service	Status	Startup Type	Comments
CvfsPM[27]	Started	Automatic	—
Grass Valley AppService	Started	Automatic	Depends on Status Server service.
Grass Valley Extent Manager Service	Started	Manual	Used to consolidate unused space (extents) at the end of proxy clips on an SNFS file system. Does not apply to non-SNFS file systems.
Grass Valley FTP Daemon	Started	Manual	Intentionally not started by Status Server service on shared storage models. Transfers go to K2 Media Server, not K2 Summit 3G system.
Grass Valley Host File Service	Started	Automatic	—
Grass Valley HTTP File Server	Started	Manual	Provides access to live streaming configuration (SDP) files.
Grass Valley K2 Config	Started	Automatic	Needed on shared storage K2 Summit 3G system.
Grass Valley MegaRaid Server	—	Manual	—
Grass Valley MetaDataService	Started	Manual	—
Grass Valley RTS Config Service	Started	Manual	—
Grass Valley SabretoothWS	—	Manual	Allows Macintosh systems to remotely check out a license.
Grass Valley Storage Utility Host	Started	Automatic	—
Grass Valley STRATUS K2 Configuration Service	Started	Automatic	Provides communication with K2Config. Required on any device configured by K2Config. Also provides communication with GV STRATUS configuration tools.

[27] With SNFS version 3.5, this is the only service. Previous versions had StorNext File System service and StorNext File System RPC Port Mapper service.

Service	Status	Startup Type	Comments
Grass Valley System Status Server	Started	Automatic	At startup the Status Server service makes sure the following services are started: AMP TCP Service; AppService; FTP Daemon.
Microsoft iSCSI Initiator Service	Started	Automatic	Needed on shared storage K2 Summit 3G system.
ProductFrame Discovery Agent Service	Started	Automatic	—
Sabretooth License Server	Started	Manual	—
Sabretooth Protocol Service	—	Manual	—

Checking pre-installed software

Software is pre-installed on K2 products when you receive them from the factory. This load of pre-installed software is referred to as the “golden drive”. The following list is an example of the software pre-installed. Check the "About This Release" section of the K2 Topic Library for the most up-to-date list with version information.

If you suspect that pre-installed software is not correct, use the recovery process to re-load the software. Do not attempt to un-install, install, or repair pre-installed software without guidance from your Grass Valley Support representative.

K2 Solo 3G system pre-installed software

- Intel Pro Software
- QuickTime
- Microsoft iSCSI Initiator
- MS XML
- .NET Framework
- MegaRAID — Do not use this utility on a K2 Solo 3G system. This utility is for use by qualified Grass Valley Service personnel only. When this utility is opened it scans the SCSI bus and interferes with record and play operations.
- J2SE Runtime Environment
- StorNext software
- Windows PowerShell
- Windows XP Embedded

Making CMOS settings

NOTE: This procedure is intended for use by Grass Valley Service personnel or under the direct supervision of Grass Valley Service personnel.

1. Connect keyboard, monitor, and mouse to the K2 Solo 3G system.
2. Restart the K2 Solo 3G system.

3. During the BIOS startup screen, watch the keyboard lights (capslock, numlock, etc.). When the lights flash, press **Delete** to enter Setup.
4. Press **F3** and then press **Enter**. This loads optimal default values for all the setup questions.
5. Press **F4** and then press **Enter** to save settings and restart.

Restoring disk controller configuration

Do this task when replacing the disk controller board.

This task can be used on any K2 Solo 3G system, but it is required on any system that has a Type II (ADLINK) CPU carrier module. This includes the first generation K2 Summit system, which can have a Type II CPU carrier module that was installed in the factory or that was upgraded in the field.

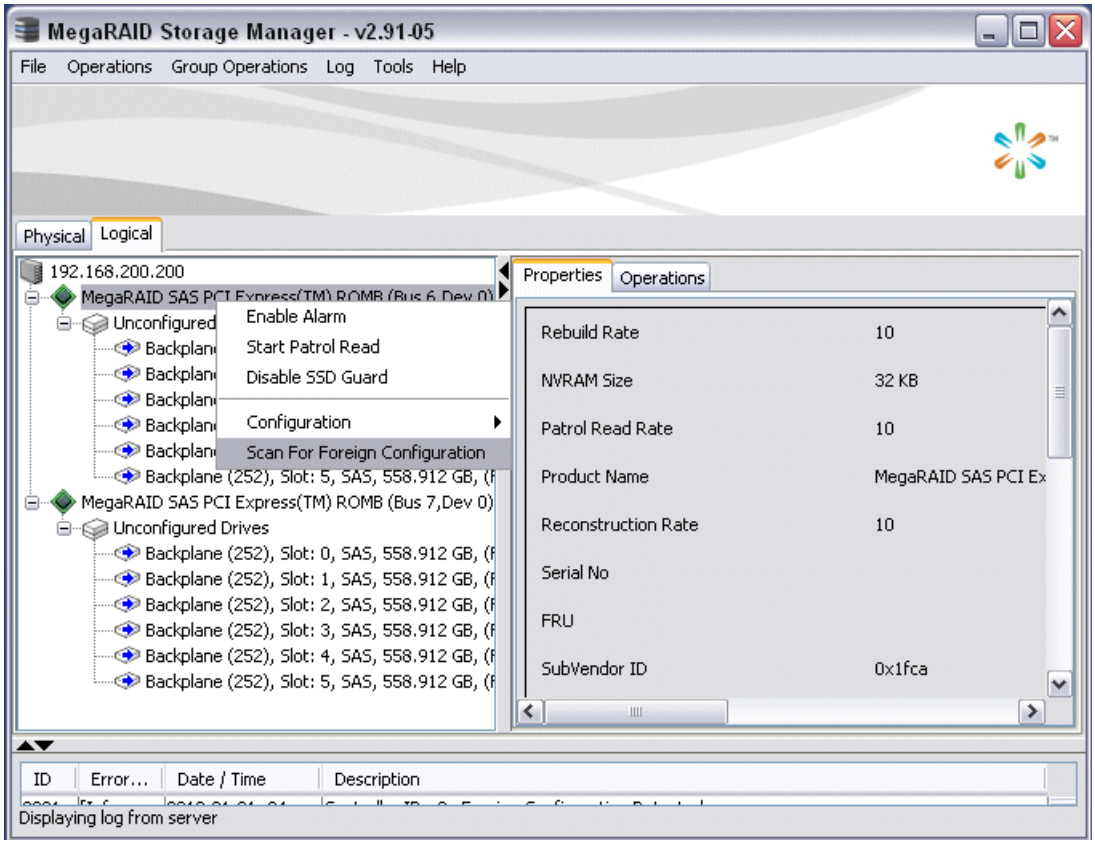
NOTE: This procedure is intended for use by Grass Valley Service personnel or under the direct supervision of Grass Valley Service personnel.

After you replace a disk controller board, you must import the configuration information from the existing disks. This allows the new board to see the LUNs as previously configured.

1. After replacing the disk controller board, power up the K2 Solo 3G system.

   Ignore SNFS messages that can open at any time during this procedure.
2. On the Windows desktop, open the **MegaRAID Storage Manager** icon.

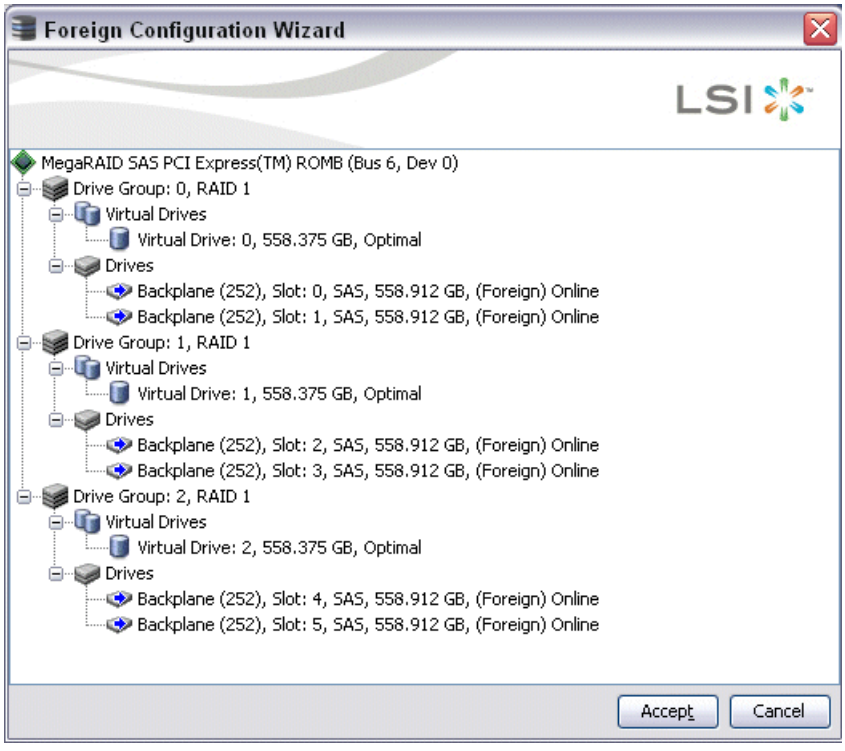
3. When prompted, enter administrator credentials.
   The MegaRAID Storage Manager main window opens.



4. In the MegaRAID Storage Manager main window tree-view, verify that drives are reported as "Unconfigured Drives".

5. In the tree-view, right-click the top controller and select **Scan For Foreign Configuration**.
   A Foreign Configuration Detected dialog box opens.

6. Make sure **Import** is selected and click **OK**.
   A Foreign Configuration Wizard opens.



7. Click **Accept**.
8. When prompted "...import?", click **Yes**.
9. When informed "...imported successfully", click **Yes**.

10. In the MegaRAID Storage Manager main window tree-view, verify that one controller reports configured drives and one controller reports unconfigured drives.
11. For the controller with unconfigured drives, repeat previous steps to import the foreign configuration.
12. When you have imported the foreign configuration for both controllers, click **File | Exit** to close MegaRAID Storage Manager.
13. Restart the K2 Solo 3G system.

Recovering the media database

This section provides topics about recovering the media database.

About the automatic database backup process

Every 15 minutes the K2 system checks to see if any media operations have changed the media database. If a change has occurred, the K2 system creates a backup file of the media database. The backup file is saved in the same directory as the media database using a rotating set of three file names. These files are named *media.db_bakX* where X is the number in the rotation. Each time a backup occurs, the oldest backup file is overwritten. If some condition renders one of the backup files un-writable, the backup file following that in the rotation is subsequently used for every backup until the condition is resolved.

Identifying a corrupt media database

The following symptoms could indicate a corrupt media database:

- On startup, the Grass Valley MetaDataService is unable to start. This is indicated in the Services control panel if the Grass Valley MetaDataService does not display as Started.
- The K2 log displays a "…file is encrypted or is not a database…" error.

As soon as you suspect a corrupt media database, stop all media access and take the K2 system offline.

Restoring the media database

1. Stop all media access and take the K2 system offline.
2. Navigate to the V:\media directory.
3. Make a copy of the media.db and media.db_bak* files and store them in a secure location.
4. Stop the Grass Valley MetaDataService as follows:

   For the standalone K2 system, use the Services control panel to stop the service.
5. Determine which backup file is the most recent good file by examining the file modification date on each backup file.
6. Rename the current *media.db* file (which is assumed to be corrupt) to another name, and rename the most recent good *media.db_bakX* file to *media.db*.
7. Restart the K2 system following normal procedures.
8. Confirm that the systems come up correctly with the restored database now in place.

9. Use Storage Utility **Clean Unreferenced Files** and **Clean Unreferenced Movies** to repair any inconsistencies between the contents of the database and the file system.

Using recovery images

This section provides topics about using recovery images.

About the recovery image process

An image of the K2 Solo 3G system system drive is provided with the product package. You can restore the K2 Solo 3G system from this image. This simplifies the process of rebuilding a system in a disaster recovery scenario.

NOTE: This process is not intended as a means to backup and restore media.

When you receive your K2 Solo 3G system new from the factory, you receive a system-specific image for that particular K2 Solo 3G system. This factory image is stored on a bootable USB Recovery Flash Drive. Also on the Recovery Flash Drive is the Acronis True Image software necessary to create and restore an image. You can find the Recovery Flash Drive in a holder in the front bezel assembly.

After your K2 Solo 3G system is installed, configured, and running in your system environment, you should create a new recovery image to capture settings changed from default. This "first birthday" image is the baseline recovery image for the K2 Solo 3G system in its life in your facility. There is enough space on the Recovery Flash Drive to store the first birthday image along with the factory image.

You should likewise create a new recovery image after completing any process that changes system software or data, such as a software upgrade. In this way you retain the ability to restore your K2 Solo 3G system to a recent "last known good" state.

NOTE: The recovery image process is an "off-line" process. Do not attempt this process while media access is underway.

The recovery image process that you should follow is summarized in the following steps.

- **At the K2 Solo 3G system first birthday…**

  Boot from the Recovery Flash Drive.

  Create a recovery image for the K2 Solo 3G system.

  Create a recovery image for the Control Point PC.

- **At milestones, such as software upgrades…**

  Boot from the Recovery Flash Drive.

  Create a recovery image for the K2 Solo 3G system.

- **If you need to restore the K2 Solo 3G system…**

  Boot from the Recovery Flash Drive.

  Read the image from the Recovery Flash Drive or from the location that you stored the image.

- **If you need to restore the Control Point PC…**

  Boot from the Recovery Flash drive.

  Read the image from the location that you stored the image.

Use the following procedures to implement the recovery image process as necessary.

Creating a recovery image

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

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

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

      A MS-DOS command window opens.

   c) When prompted with a list of options, type `2` to select the Acronis option and then press **Enter**.

   The Acronis program loads.
4. In the Acronis main window, click **Backup**.

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

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

      If a "…choose full backup mode…" message appears, click **OK**.
7. On the Backup Archive Location page, do the following:
   a) in the tree view select **Removable Disk (D:)** and enter the name of the image file you are creating.

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

      For example, if the hostname is MySystem1, in the File name field you enter `A:\MySystem1_20121027.tib`.

   b) Click **Next**.
8. On the Select Backup Mode page, select **Create a new full backup archive** and then click **Next**.
9. On the Backup Options page, do not change any settings. Click **Next**.

10. On the Archive Comment page, if desired, enter image comments such as the date, time, and software versions contained in the image you are creating. Click **Next**.
11. On the "…ready to proceed…" page, do the following:
    a) Verify that you are creating an image from the C: drive and writing to the D:\ drive, then click **Proceed**.

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

    The machine restarts automatically.
15. Remove the recovery media while the machine is shutting down.

Restoring from a system-specific recovery image

Use this task to restore a K2 Solo 3G system using an image made from that particular K2 Solo 3G system. If restoring from a generic factory default image, use the appropriate task.

Before restoring from a recovery image, make sure that the K2 Solo 3G system has access to the image from which you are restoring. This task provides instructions for accessing an image on the Recovery Flash Drive. If you access an image from a different location, such as a network connected drive or another connected USB drive, alter the steps in this task as appropriate.

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

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

      A MS-DOS command window opens.
   c) When prompted with a list of options, type `2` to select the Acronis option and then press **Enter**.

   The Acronis program loads.
4. In the Acronis main window, click **Recovery**.

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

   NOTE: Verify capacity to make sure you select the boot media card (CompactFlash or mSATA) and not a media drive. The boot media has a much smaller capacity and has an interface identified as "IDE (0) Primary Master".

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

    NOTE: Verify capacity to make sure you select the boot media card (CompactFlash or mSATA) and not a media drive. The boot media has a much smaller capacity and has an interface identified as "IDE (0) Primary Master".

14. On the Restored Partition Type page, select **Active** and then click **Next**.
15. Do one of the following:

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

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

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

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

    The machine restarts automatically.

23. Remove the recovery media while the machine is shutting down.
24. When prompted, enter the K2 Solo 3G system machine name.

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

    After start up, one or more device discovery windows can open. Allow processes to complete without interference. Refer to Release Notes for informaion on compatible driver versions. If a Fibre Channel card driver, ignore until instructed later in this process.

    At first start up after reimage, the system is in Embedded Security Update mode by default.

Next, check the adapter names and order. If adapter names and order are not as documented, restore network configuration.

Restoring to blank mSATA

This task is for a K2 Summit 3G system that has had its mSATA boot media replaced with a new blank mSATA card. This means the mSATA card has never been initialized and has never before contained a disk image.

You can use this task to restore from a system-specific image or from a generic image. This task provides instructions for accessing an image on the Recovery Flash Drive. If you access an image from a different location, such as a network connected drive or another connected USB drive, alter the steps in this task as appropriate. There can be multiple versions of the generic recovery disk image on the Recovery Flash Drive. Refer to related topics in the "About This Release" section of the K2 Topic Library to determine which version you should use.

NOTE: If restoring using a generic image, the* K2 Solo 3G system *is returned to its factory default condition. Passwords and other site-specific configurations are reset to factory defaults.

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

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

      A MS-DOS command window opens.

   c) When prompted with a list of options, type `2` to select the Acronis option and then press **Enter**.

   The Acronis program loads.
4. In the Acronis main window, click **Recovery**.

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

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

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

15. Do one of the following:
    - If the Restored Partition Size page does not appear. Skip ahead to the Next Selection page.
    - If the Restored Partition Size page appears. Continue with the next step.
16. On the Restored Partition Size page, do one of the following:
    - If **Free space after** reports 0 bytes, leave settings as they are. Click **Next**.
    - If **Free space after** does not report 0 bytes, increase **Partition size** until **Free space after** reports 0 bytes. Click **Next**.
17. On the Next Selection page, select **No, I do not** and then click **Next**.
18. On the Restoration Options page, do not make any selections. Click **Next**.
19. On the "…ready to proceed…" page, verify that you are restoring the correct image to the correct location. Click **Proceed**.
20. On the Operation Progress page, observe the progress report.
21. When a message appears indicating a successful recovery, click **OK**.
22. Click **Operations | Exit** to exit the Acronis True Image program.

    The machine restarts automatically.
23. Remove the recovery media while the machine is shutting down.
24. When prompted, enter the machine name.

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

    At first start up after reimage, the system is in Embedded Security Update mode by default.

Depending on whether you restored from a system-specific image or from a generic image, refer to the appropriate disk image recovery task for next steps.

About saving and restoring settings while reimaging

If you are reimaging a K2 Solo 3G system with a generic disk image, you can run scripts to save the media file system and other settings before the reimage, then restore the settings after the reimage. Setting are saved and restored as follows:

- Media file system (SNFS): You run scripts to save and restore these settings. After the settings are restored, on a standalone system you can access the media in the local media storage. On a SAN-attached system, K2Config settings are restored so you can access media on the shared media storage.
- SID, computer name, and network settings: You run the script to save settings to a text file, so you can manually reconfigure as desired after the reimage.

If the media file system and settings are valid (not corrupt) on the K2 Solo 3G system before the reimage, it is recommended that you use the save/restore scripts to save your media and settings, thus saving time in the reimage process. However, if the media file system or settings are corrupt and your purpose for reimaging is to remove the corruption, it is likely that you do not want to use the save/restore scripts.

Saving settings before generic reimage

1. If you are working on a K2 client SAN-attached system, record iSCSI bandwidth settings, so you can reconfigure after removing and readding to SAN.
2. Make sure you are logged in to the K2 Solo 3G system with administrator privileges.
3. Connect the USB Recovery Flash Drive to a USB port on the K2 Solo 3G system.
4. On the USB Recovery Flash Drive, navigate to the following location:

   `\tools\SaveRestoreScripts.`

   NOTE: Do not attempt to use the same Recovery Flash Drive on multiple systems.
5. Run the following and wait for the process to complete:

   `ssave.bat`

   This saves current settings onto the USB Recovery Flash Drive in the `\settings` directory.
6. Disconnect the USB Recovery Flash Drive.

Restoring from a generic image

This task can be used on a K2 Solo 3G system that needs to be restored to its factory default state. For example, if you neglected to make a first birthday image, you might need to use this procedure. If the image from which you are restoring was made from the specific machine, refer to the appropriate procedure.

This task provides instructions for accessing an image on the Recovery Flash Drive. If you access an image from a different location, such as a network connected drive or another connected USB drive, alter the steps in this task as appropriate. There can be multiple versions of the generic recovery disk image on the Recovery Flash Drive. Refer to related topics in the "About This Release" section of the K2 Topic Library to determine which version you should use.

NOTE: This procedure restores the* K2 Solo 3G system *to its factory default condition. Passwords and other site-specific configurations are reset to factory defaults.

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

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

      A MS-DOS command window opens.
   c) When prompted with a list of options, type `2` to select the Acronis option and then press **Enter**.

   The Acronis program loads.
4. In the Acronis main window, click **Recovery**.

   The Restore Data Wizard opens.
5. On the Welcome page, click **Next**.

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

   NOTE: Verify capacity to make sure you select the boot media card (CompactFlash or mSATA) and not a media drive. The boot media has a much smaller capacity and has an interface identified as "IDE (0) Primary Master".

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

    NOTE: Verify capacity to make sure you select the boot media card (CompactFlash or mSATA) and not a media drive. The boot media has a much smaller capacity and has an interface identified as "IDE (0) Primary Master".

14. On the Restored Partition Type page, select **Active** and then click **Next**.
15. Do one of the following:

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

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

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

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

    The machine restarts automatically.

23. Remove the recovery media while the machine is shutting down.
24. Upon startup, wait for initialization processes to complete. This can take several minutes, during which time USB keyboard/mouse input is not operational. The system might automatically restart. Do not attempt to shutdown or otherwise interfere with initialization processes.

25. When prompted, enter the K2 Solo 3G system machine name.

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

    After start up, one or more device discovery windows can open. Allow processes to complete without interference. Refer to Release Notes for informaion on compatible driver versions. If a Fibre Channel card driver, ignore until instructed later in this process.

    At first start up after reimage, the system is in Embedded Security Update mode by default.

Next, check the adapter names and order. If adapter names and order are not as documented, restore network configuration.

Restoring settings after generic reimage

Settings must be saved using *ssave.bat* before reimaging the K2 Solo 3G system, and the reimage (Acronis) process must be complete.

1. If you have not already done so, start up the K2 Solo 3G system and log on with administrator privileges.

   The administrator password is `adminGV!`.

2. Connect the USB Recovery Flash Drive to a USB port on the K2 Solo 3G system.
3. From the USB Recovery Flash Drive, run the following and wait for the process to complete:

   Tools\SaveRestoreScripts\srestore.bat

Next, do the following as appropriate to restore your K2 Solo 3G system. Refer to related topics in this document or as otherwise indicated.

1. Restore network configuration. If you saved settings with *ssave.bat*, refer to *C:\ipconfig.txt* for the complete listing of the network settings that the K2 Solo 3G system had before reimaging.
2. Enhance network bandwidth.
3. Install the SiteConfig Discovery Agent.
4. If you install software with SiteConfig, do the following:

   - Take Embedded Security out of Update mode.
   - Install SNFS software and K2 software using SiteConfig.
   - Restore SabreTooth licenses.

5. If you install software manually (without SiteConfig), do the following:

   - Install SNFS software and K2 software manually.
   - Take Embedded Security out of Update mode.
   - Restore SabreTooth licenses.

   If you saved/restored settings with *ssave.bat* and *srestore.bat*, SNFS uses the restored settings. Refer to related topics in the "About This Release" section of the K2 Topic Library.

6. If a K2 Solo 3G system with direct-connect storage or shared storage on a redundant K2 SAN, install MPIO software.
7. If a K2 Solo 3G system with a Fibre Channel card, install the Fibre Channel Card driver. Refer to related topics in "K2 Summit Production Client Service Manual".
8. If a K2 Summit SAN-attached system, on the K2 SAN's control point PC, use the K2Config application to add the K2 Solo 3G system back to the SAN
9. Check the Windows operating system clock, and if necessary, set it to the correct time.
10. Activate Windows within 30 days.

Installing the Discovery Agent on a K2 Summit system

If the device that you plan to manage with SiteConfig does not have a SiteConfig Discovery agent installed, use this topic to verify and, if necessary, manually install SiteConfig support software. Doing so allows SiteConfig to discover and manage the device. If the device has any version of the SiteConfig Discovery Agent currently installed, you should use SiteConfig to upgrade the Discovery Agent, rather than installing it manually.

1. On the device you plan to manage with SiteConfig, open the Windows Services Control Panel and look for the following required item:
   - ProductFrame Discovery Agent
2. Proceed as follows:
   - If you find the required items, no further steps are necessary. SiteConfig support software is installed.
   - If a required item is not present, navigate to your SiteConfig files. If you do not already have these files in convenient location, you can find them on the PC that hosts SiteConfig, in the SiteConfig install location. Then continue with next steps as appropriate.
3. To launch the program that installs the ProductFrame Discovery Agent Service do the following:
   a) Copy the `Discovery Agent Setup` directory to the device.
   b) In the directory, double-click the `DiscoveryAgentServiceSetup.msi` file.
   The setup program launches to install the SiteConfig Discovery Agent.
   c) Follow the setup wizard.
4. When presented with a list of device types, select one of the following as appropriate:
   - K2SummitSanClient
   - K2SummitStandaloneClient
5. Complete the setup wizard and restart the device.
   The restart is required after the installation.

Installing the ATTO Fibre Channel card driver

If the K2 Solo 3G system is on a redundant K2 SAN or is connected to direct-connect storage, MPIO software must be installed.

If your K2 Solo 3G system has the optional Fibre Channel card, the driver for the Fibre Channel card is not installed on the recovery image provided by Grass Valley for that K2 Solo 3G system. Therefore, after restoring the image, you must install the Fibre Channel card driver.

1. Open Device Manager.
2. Right-click on **K2 Summit Client** and select **Manage.**
3. Click **Device Manager**

4. Install the first Fibre Channel driver as follows:
   a) Right click on the upper Fibre Channel Controller and select **Update Driver…**
   b) On the Welcome page, select **No, not this time** and then click **Next**.
   c) Select **Install from a list or specific location** and then click **Next**.
   d) Browse to *C:\Profile\Drivers\ Atto 8Gb HBA Drivers\x86*.
   e) Click **OK**.
   f) Click **Next**.
   g) Click **Finish** when prompted.
   h) In the Found new hardware wizard that will open for the ATTO Phantom device, select **No, not this time**.
   i) Select **Install from a list or specific location** and then click **Next**.
   j) Browse to *C:\Profile\Drivers\ Atto 8Gb HBA Drivers* and select the *x86* directory if installing on a 32-bit computer or the *x64* directory if installing on a 64-bit computer.
   k) Click **OK** .
   l) Click **Next.**.
   m) Click **Finish** when prompted.
5. Repeat the process for the second Fibre Channel Controller as follows:
   a) Right-click on the remaining Fibre Channel Controller and select **Update Driver…**
   b) On the Welcome page, select **No, not this time** and then click **Next**.
   c) Select **Install from a list or specific location** and then click **Next**.
   d) Browse to *C:\Profile\Drivers\ Atto 8Gb HBA Drivers* and select the *x86* directory if installing on a 32-bit computer or the *x64* directory if installing on a 64-bit computer..
   e) Click **OK**.
   f) Click **Next**.
   g) Click **Finish** when prompted.
6. Verify that the two "ATTO" devices are now listed under the SCSI and RAID Controllers
7. Close the Device Manager and System windows

Using diagnostic tools

Use the following sections as necessary to identify problems.

Running Check Disk

If your K2 Solo 3G system has a critical system fault, you should run Check Disk to identify and remove any corrupted files.

1. Make sure the K2 Solo 3G system 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:

      ```
      ...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 Solo 3G system.

Running diagnostics for K2 Solo 3G system

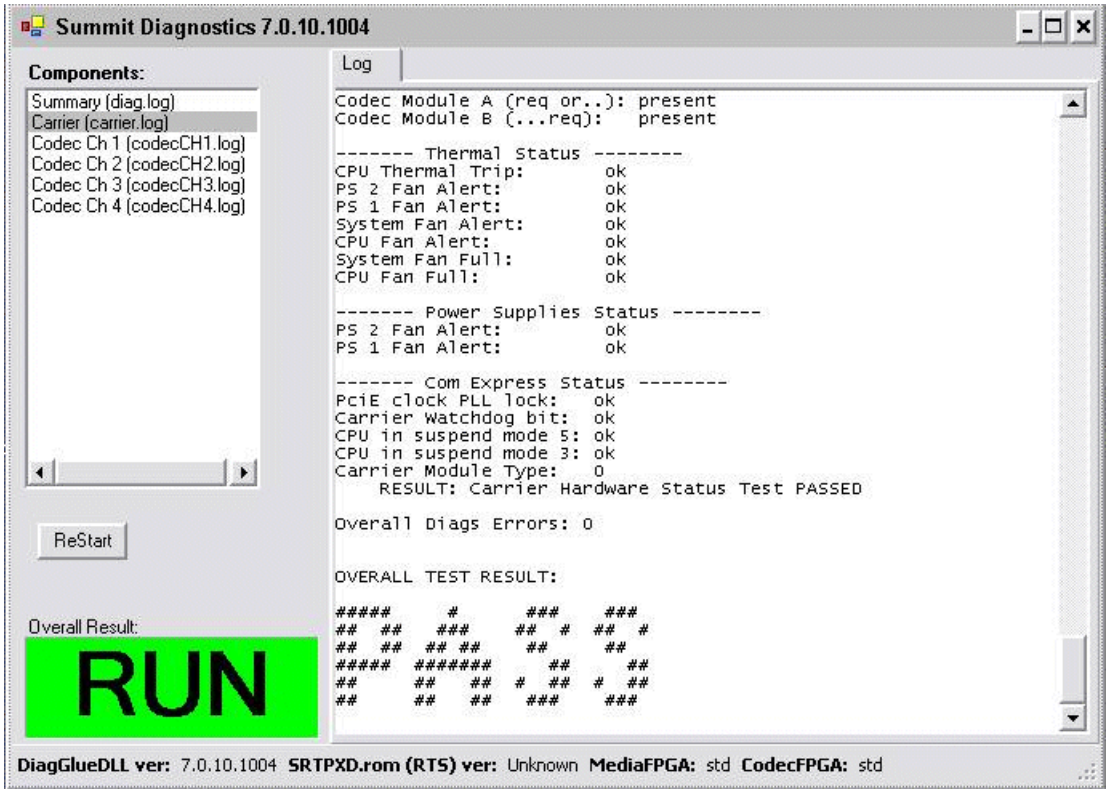
If you suspect a problem with K2 Solo 3G system hardware, you can run diagnostics and check for errors.

1. Make sure all media access is stopped on the K2 Solo 3G system. 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 Solo 3G system.

   You must restart before you can use the K2 Solo 3G system. Running diagnostics puts the real time processor and other services in a non-production state.

Troubleshooting problems

Step 1: Check configurations

Many times what appears to be a K2 Solo 3G system fault is actually an easy-to-fix configuration problem. Check settings in Configuration Manager and verify that the system is configured as you expect. Refer to related topics in the "Using K2 AppCenter" section of the K2 Topic Library and the "Configuring the K2 System" section of this Topic Library.

Step 2: Check connections and external equipment

Loose or improperly connected cables are the most likely source of problems for the system. A quick check of all the cable connections can easily solve these problems. Refer to related topics in the "Configuring the K2 System" section of this Topic Library for help with making connections. Check external equipment if you suspect a failure in a device connected to the K2 Solo 3G system.

Step 3: Check system status messages

While the K2 Solo 3G system is in operation, some problems are detected and reported in system status messages. To view system status messages, in AppCenter select **Help | System Status**.

When connecting to a K2 Solo 3G system from a control point PC using remote AppCenter, if there is an AppCenter system startup error, the error is reported during the connection attempt.

If the system status message indicates a problem, refer to related topics in "K2 Summit Production Client Service Manual".

NOTE: Do not use the MegaRAID utility on a* K2 Solo 3G system*. This utility is for use by qualified Grass Valley Service personnel only. When this utility is opened it scans the SCSI bus and interferes with record and play operations.

Step 4: Identify problems using the startup sequence

The startup sequence is your primary tool for identifying a K2 Solo 3G system fault. As the different levels of the K2 Solo 3G system system become operational in the startup process, the primary components of the system are checked. You can identify most problems by evaluating the messages and other indicators that occur during the startup sequence.

NOTE: This procedure assumes that the* K2 Solo 3G system *is not in Storage Utility's "offline" mode.

To identify problems using the startup sequence, do the following:

1. Connect mouse, keyboard, and monitor. You must observe the VGA screen and be able to interact with the system via keyboard and mouse to fully identify problems.
2. Restart the K2 Solo 3G system.

3. Once the startup sequence begins, observe the progression of behaviors as listed in the following table. These are the behaviors you should expect for a normally operating K2 Solo 3G system. If you observe behaviors other than those listed, refer to the indicated troubleshooting topics to identify problems.

   NOTE: You can press the Pause/Break key on the keyboard to keep startup text on the screen for longer viewing.

At about this time…	This behavior should occur…	If not, refer to the following:
—	Pressing the standby button starts the K2 Solo 3G system.	*Shutdown/restart problems* on page 876
0 seconds	Power on LED goes on and stays on.	*Power supply problems* on page 879
	Service LED stays off.	*Shutdown/restart problems* on page 876
	Front bezel assembly and processor fan start.	*Windows startup problems* on page 878
10 seconds	System BIOS screen appears.	*BIOS startup* on page 877
35 seconds	Grass Valley logo screen appears.	—
70 seconds	Windows logon screen appears.	*Windows startup* on page 877

Logon to Windows to continue the startup sequence.

After Windows logon:

At about this time…	This behavior should occur…	If not, refer to the following:
0 seconds	Grass Valley logo desktop appears.	*K2 Solo 3G system startup* on page 878
5 seconds	Service LED goes on for a few seconds, then off.	
20 seconds	Desktop icons, startbar, and AppCenter logon box appear.	*Windows startup* on page 877, *K2 Solo 3G system startup* on page 878

Logon to AppCenter to continue the startup sequence.

After AppCenter logon:

At about this time…	This behavior should occur…	If not, refer to the following:
0 seconds	System Startup messages appear.	*K2 Solo 3G system startup* on page 878

At about this time…	This behavior should occur…	If not, refer to the following:
Time varies. Between 30 seconds and 2 minutes.	All system components check out as OK and AppCenter opens. Media operations are functional.	*Operational problems* on page 881

Shutdown/restart problems

If the K2 Solo 3G system is inoperable due to an error it can affect the operation of the standby button. If pressing the standby button does not shut down the K2 Solo 3G system, press and hold the button for five seconds. This forces the K2 Solo 3G system to execute a hard power down. If that doesn't work or if after the hard power down the system does not boot, disconnect then reconnect the power cable(s).

The K2 Solo 3G system is set to attempt to boot from a USB drive first, before it boots from the boot media card. If you have a drive connected to a USB port that does not contain an appropriate operating system and you start up the K2 Solo 3G system, an error message is displayed and the boot up process halts.

Checking external equipment

This section provides troubleshooting procedures for external devices that connect to the K2 Solo 3G system. Before using these procedures, first check connections.

VGA display problems

Problem	Possible Causes	Corrective Actions
Screen turns on, but nothing from K2 Solo 3G system is displayed.	VGA connector or cable is not connected or is faulty.	Replace VGA monitor.
	K2 Solo 3G system system settings have been tampered with.	Restore default settings by restoring the system drive image from a recent backup image.

Keyboard and mouse problems

The keyboard and mouse are detected during BIOS startup. There should be a very brief message displayed indicating detection of input devices connected to USB ports

Problem	Possible Causes	Corrective Actions
The K2 Solo 3G system does not respond correctly when one or more of the keys on the keyboard are pressed or the mouse is used.	The keyboard or mouse is faulty.	Replace the keyboard or mouse.
	K2 Solo 3G system system settings have been tampered with.	Restore default settings by restoring the system drive image from a recent backup image.

Power connection sequence

The following table lists the sequence of behaviors you should expect to see and/or hear as you connect the first power cable to a normally operating K2 Solo 3G system. If you observe behaviors other than those listed, refer to related topics in "K2 Summit Production Client Service Manual" to investigate potential problems.

In this time…	On the K2 Solo 3G system front panel or chassis, look/listen for the following…	If not, refer to the following.
0 seconds	Power supply fans go on and stay on.	*Power supply problems* on page 879
	Power on LED goes on and stays on.	
	Drive busy LED goes on then off.	*Media disk problems* on page 883

This power connection sequence assumes that before power was removed, the K2 Solo 3G system was properly shut down from AppCenter, from the Windows operating system, or from the standby button. If the power was removed without a proper shutdown, when the first power cord is connected the K2 Solo 3G system might go directly to the startup sequence.

BIOS startup

A few seconds after startup, on the VGA monitor a screen displays BIOS information, with instructions about how to access settings. While this information is displayed, press the key on the keyboard as instructed to enter the BIOS settings pages. When the BIOS completes the Windows operating system begins to load.

If during the BIOS time a message appears that requires your input or if the K2 Solo 3G system does not progress to Windows startup, it indicates a problem at the motherboard level. To correct problems of this nature, contact Grass Valley Support.

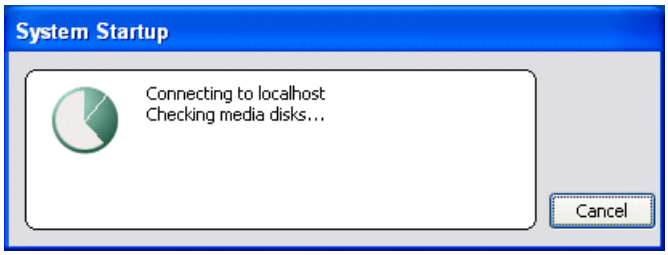
Windows startup

After the host startup processes complete the Windows operating system starts up. Normally the Windows operating system completes its processes automatically without the need to press keys or respond to messages. When the Windows startup is complete the Windows logon dialog box is displayed.

If the Windows startup screen does not proceed automatically or if a message appears that requires your input, it indicates a problem at the operating system level. If the problem cannot be corrected with a supported procedure (such as networking), the Windows operating system is not operating as it should. To correct problems of this nature, restore the system drive image.

K2 Solo 3G system startup

After the Windows operating system startup processes complete, you must log in to AppCenter to trigger K2 Solo 3G system startup processes to begin. The K2 Solo 3G system determines that system health is adequate by checking critical subsystems. Critical subsystems are those upon which the K2 Solo 3G system depends for core media functionality. Critical subsystem checks are displayed in the System Startup message box.



When all critical subsystem checks are successful, AppCenter opens. If a critical error occurs, a message appears and AppCenter does not open. You can check the list of the messages that can appear.

To correct problems revealed at system startup, use the indicated troubleshooting information from the following sections.

Windows startup problems

Problem	Possible Causes	Corrective Actions
A "Non-system disk. Press any key to restart" message appears.	A non-bootable USB drive is connected.	Remove the USB drive, then press any key to continue.
	The boot media is corrupted.	Restore from the USB Recovery Flash Drive.

Thermal problems

Problem	Possible Causes	Corrective Actions
The K2 Solo 3G system overheats. This can be accompanied by a StatusPane message indicating a temperature or fan problem.	Airflow is blocked. The fan module is not operating correctly.	Ensure adequate airflow around the K2 Solo 3G system. Inspect the fans in the front bezel assembly and its connections for proper operation. If the fans are not operating correctly, replace the front bezel assembly.

Codec board problems

Investigate the problem further as described in the following table. If the problem persists, contact Grass Valley Support.

Problem	Possible Causes	Corrective Actions
A system status message indicates a problem with the codec board.	The codec module is not connected properly or is faulty.	Check the codec board indicator (LED) on the rear panel. Visually inspect codec module. Make sure it is connected properly and there is no sign of physical damage. Restart the K2 Solo 3G system. If the problem persists, replace the codec module.

Power supply problems

Problem	Possible Causes	Corrective Actions
The K2 Solo 3G system will not power on or power fails while the K2 Solo 3G system is in operation. This can be accompanied by a StatusPane message indicating a power supply problem prior to the failure.	The power source is faulty.	Make sure your power source is reliable.
	A power cord is faulty.	Both power supplies run and the K2 Solo 3G system can operate with just one power cord connected. Connect one power cord at a time and test with a replacement cord.
	The K2 Solo 3G system is too hot. The built-in overtemperature protection can shut down the power supply.	Check for thermal problems. Cool the K2 Solo 3G system.
	The power supply is faulty. This is indicated if the front panel power indicator does not come on.	Replace the power supply.
Power supply "~AC" LED is amber	Over temperature due to air flow restriction.	Check for and remove any air flow blockage around the power supply.
	Over temperature due to power supply fan failure.	Visually inspect fan. Listen for fan noise. If faulty, replace power supply.

Problem	Possible Causes	Corrective Actions
	Over current, under voltage, over voltage. These conditions could be caused by a faulty FRU module.	Disengage all FRU modules, then re-engage one at time. If one module causes the amber LED to go on, replace the module. If both power supplies have the amber LED, disengage one, then the other. If doing so results in just one power supply having the amber LED, replace that power supply.

Video problems

For the corrective actions in this section, refer to related topics in the "Using K2 AppCenter" section of the K2 Topic Library for detailed instructions.

Problem	Possible Causes	Corrective Actions
The picture level modulates at a particular frequency.	There is distortion in the video input signal.	Check the video input signal for distortion. Compare with test color bars and audio test tone.
In stop mode the still-play video shows some motion jitter.	Two fields are displayed in still play mode.	Switch the still-play mode setting to Field.
The video displays erratically moving green lines.	K2 Solo 3G system is not locked to a video reference.	Lock the K2 Solo 3G system to a video reference.

Audio problems

For the corrective actions in this section, refer to related topics in the "Using K2 AppCenter" section of the K2 Topic Library for detailed instructions.

Problem	Possible Causes	Corrective Actions
No record audio.	Wrong audio input selected.	Select the correct audio input.
No embedded audio.	Video source does not have embedded audio.	Check your video source for embedded audio.
Playback audio output is distorted.	Audio input signal clipping caused by excessive audio input level.	Check for input audio clipping. Adjust the audio input trim. Adjust the Player audio level. Reduce the source audio input level.
Audio level is too low.	Audio level needs to be adjusted.	Adjust the Player or Recorder audio level. Increase the source audio input level.

Problem	Possible Causes	Corrective Actions
The audio level is not correct only when playing a particular clip.	The clip's audio level is out of adjustment.	Load the clip in Player and adjust its playback audio level.
Audio level meters do not display the correct reference level on connected equipment.	Incorrect audio reference level.	Select the correct audio reference level.
Audio meters do not appear in the AppCenter Monitor Pane.	The Monitor Pane configured to not display audio meters.	Configure the Channel Monitoring setting to display audio meters.

Timecode problems

For the corrective actions in this section, refer to related topics in the "Using K2 AppCenter" section of the K2 Topic Library for detailed instructions.

Problem	Possible Causes	Corrective Actions
Recorded timecode reads xx.xx.xx.xx.	During recording, the channel had no timecode source.	Check that you have the right record channel timecode source selected, verify that timecode is present in the source, and record the clip again. You can also stripe the timecode on an existing clip.
A clip shows no mark-in/mark-out timecode, the current timecode display shows XX:XX:XX:XX, or the last valid timecode is displayed.	The selected timecode source was missing or intermittent during recording.	

Operational problems

For the corrective actions in this section, refer to related topics in the "Using K2 AppCenter" section of the K2 Topic Library for detailed instructions.

Problem	Possible Causes	Corrective Actions
Moving video in AppCenter does not operate.	The K2 Solo 3G system is not licensed for AppCenter Pro.	Obtain an AppCenter Pro license.
	The VGA monitor resolution is less than 1024x768x32.	Configure VGA monitor resolution. The resolution must be at least 1024x768x32 to support live video.
	Another user is connected via Remote Desktop.	Restart AppCenter.
The K2 Solo 3G system is not operating as expected in relation to a setting displayed in Configuration Manager.	The setting was changed in Configuration Manager but not saved to the database.	Verify the setting you want in Configuration Manager and then select OK. When prompted to change the system settings, select Yes.

Problem	Possible Causes	Corrective Actions
AppCenter displays different buttons than those expected.	Assignable buttons have been changed.	Assign buttons to the interface as desired.
A clip does not play, even though other clips play on the same channel.	The clip does not match current K2 Solo 3G system settings or the clip is corrupt.	If the clip appears grayed-out it means it doesn't match current settings. Check the clip's properties and verify they are correct for the standard, compression, and other current settings. Compare properties with those of a clip that plays correctly. If properties are correct the clip is corrupt. Delete and re-record the clip.
	The K2 system is not licensed for the format of the clip.	Verify licensing.
A clip can not be edited.	The clip is locked.	Unlock the clip.
Can't rename a clip or modify mark-in/mark-out points	The clip loaded or playing is still being recorded. In this case, "Read-Only" is displayed in the StatusBar.	Wait until recording is complete.
Cannot load and play a list.	The list contains invalid clips.	Check format, licensing, and security setting of the clips in the list.
On setting mark-out, the subclip is automatically generated and ejected, and a new subclip name is loaded in the subclip pane.	Auto Subclip mode is enabled.	Disable Auto Subclip mode.
Can't change what information is displayed in the Monitor Pane for Playlist.	You are attempting to use Configuration Manager to change what information is displayed in Monitor Pane for Playlist.	Use the Playlist Options dialog instead.
Can't control a channel from AppCenter. Controls are disabled.	The channel is configured for control by a remote control protocol.	Set the control mode for limited local control.

System problems

For the corrective actions in this section, refer to related topics in the "Using K2 AppCenter" section of the K2 Topic Library for detailed instructions.

Problem	Possible Causes	Corrective Actions
One of the record channels does not record or video is jumpy.	The K2 Solo 3G system is configured for PAL, yet the video input is NTSC	Check the current setting for video standard. Verify that the video input signal is the correct standard.
A scheduled event, such as an automatic play or record event, does not occur at the proper time.	The time-of-day source for event scheduling is not accurate.	Verify the time-of-day source. Verify the source's time accuracy.

Storage problems

Use the following sections if you suspect problems with your K2 Solo 3G system's storage. Refer to related topics in the "Configuring the K2 System" section of this Topic Library for Storage Utility procedures.

Media File System problems

Problem	Possible Causes	Corrective Actions
One or more clips do not play or record correctly. This can be accompanied by a StatusPane message indicating a fault in the media file system.	The media database is out of sync with the media files or there is a corrupt media file. Also check the storage system for causes related to certain usage patterns.	1. If the problem is only associated with a specific clip or clips, delete the problem clips. If the problem persists, proceed with the next step. 2. Use Storage Utility and Check File System. If the file system fails the check process you must make a new file system. When you do so you lose all media.
During K2 Solo 3G system startup a "…no file system running…" message appears.	The file system is corrupt or disks are faulty/missing such that they are not part of a stripe group.	Use Storage Utility and Check File System. If the file system fails the check process you must make a new file system. When you do so you lose all media.

Media disk problems

On the Windows desktop open the "My Computer" for you K2 system and do a quick check of the drives. You should see C: and V: drives.

Problem	Possible Causes	Corrective Actions
No clips appear in the Clips pane. This may be accompanied by a startup message or a StatusPane message regarding media disks being unavailable.	A media disk is bad or there has been a hardware failure.	Open Storage Utility and identify faulty disks. Replace faulty disks.
The StatusPane message "Media disks getting full…" appears or a "FSS 'default(0)'" message appears.	The media disks are reaching maximum capacity.	In Recorder, select the Time Dome and choose **Available Storage**. If the Time Dome is filled it confirms that your K2 Solo 3G system is out of space. Make space on the media drives by doing the following: - Delete unused clips and empty the Recycled Bin.
When streaming to another K2 Solo 3G system the operation fails. In Transfer Monitor the streaming operation shows "Status:Error".	There is a network connection error or the media disks at the destination are reaching maximum capacity.	Check network connections and configuration. Check available storage on the destination K2 Solo 3G system. In Recorder, select the Time Dome and choose **Available Storage**. If the Time Dome is filled it confirms that the destination K2 Solo 3G system is out of space. Make space on the media drives by deleting unused clips and emptying the Recycle Bin.
System status message "File system…is fragmented".	Extended record/play activity has fragmented the disks.	Use the Storage Utility to check the file system.

Checking the storage system

The following section provides guidelines for investigating problem areas related to the storage system. Use this section if you have problems with media input and/or output that are intermittent or seem to be related to certain usage patterns.

Problem	Possible Causes	Corrective Actions
Symptoms can include black video recorded or at playout, frozen video, slow performance, or inconsistent media access. These symptoms can be accompanied by StatusPane messages regarding disk problems or overrun/underrun conditions for encoders, decoders, or timecode.	The following causes can occur on their own or in combination to produce the problem: • Disk oversubscription — This occurs when requests to the media disk exceed the disk's bandwidth capabilities. This generally occur in extreme cases when a combination of high-bandwidth operations are taking place, such as jog/shuttle, record/play on multiple channels, or streaming multiple clips. • High CPU activity in Windows — This occurs when activities on the Windows operating system over-tax the capabilities of the CPU. This commonly happens when unsupported software has been installed that competes with K2 Solo 3G system applications. Virus scanners and screen savers can cause this type of problem, since they can start automatically and consume system resources. • Encoder overrun — This occurs when an encoder is flooded with more data than it can process within its real-time requirements for recording. • Decoder underrun — This occurs when a decoder is starved for data and cannot deliver enough to satisfy real-time requirements for playout. • Disk faults — This occurs when a media disk is severely fragmented or has a bad blocks that interfere with some, but not all, media operations. For example, a particular clip can be written on a bad block, so the problem occurs only on that clip.	Try to re-create the problem. Identify all the interactions that affected the system and run all the same operations as when the error occurred. Record/play/stream the same clips. Investigate the functions that seem to push the system into the error state. If you determine that certain simultaneous operations cause the problem, re-order your workflow to avoid those situations. If you determine that the problem is only on certain clips, investigate disk faults.

Network, transfer, and streaming problems

Problem	Possible Causes	Corrective Actions
When importing or exporting (sending) between K2 Solo 3G systems a "…failed to connect…" message appears and the operation fails.	There is a problem with Windows networking or there is a mis-spelling with the host name as entered in Configuration Manager.	Check networking as follows: - Check basic Windows networking. Use Windows Explorer to test a basic copy operation to the machine to which you are trying to connect. If basic networking fails, use standard Windows procedures to troubleshoot and correct your network. - If the Windows network is working properly, in AppCenter select **System | Configuration | Remote** and verify that the name of the machine to which you are trying to connect is spelled correctly and has no extra spaces or characters.
	The K2 Solo 3G system to which you are trying to connect is not operating or the network is mis-configured.	Verify that the K2 Solo 3G system to which you are trying to connect is operational and that the network is configured correctly. Verify that the name of the K2 Solo 3G system is entered correctly in the Configuration Manager Hosts page. Refer to networking topics in the "Configuring the K2 System" section of this Topic Library.
A networked device does not appear in the "Import" and "Send to" dialog boxes, even though it is present on the Windows network.	The device is not entered as a host.	In AppCenter select **System | Configuration | Remote | Add** and enter the name of the machine to which you are trying to connect. Make sure it is spelled correctly and has no extra spaces or characters. Also check the hosts file. Refer to networking topics in the "Configuring the K2 System" section of this Topic Library.
	If a SAN K2 client, the client's K2 Media Server with role of FTP server is not operational.	Verify FTP server.

Problem	Possible Causes	Corrective Actions
Files do not appear in" Send To" or "Export" dialogs.	File names do not have proper extensions.	Rename files with proper extensions.

Also refer to the *UIM Instruction Manual* for more troubleshooting information.

Removing and replacing FRUs

Removing and replacing FRUs

Field Replaceable Units (FRUs) are modular hardware components that can be serviced without disturbing other components in the system.

The pictures in the following topics show how to disassemble. Unless otherwise documented, re-assembly is the reverse.

Unless otherwise indicated, you need only a Torx tool with T15 magnetic tip to remove and replace parts in the K2 Solo 3G system.

NOTE: Only Grass Valley components are supported. Do not attempt to use components procured from a different source.

NOTE: Do not discard any hardware unless specifically instructed to do so.

⚠ ***WARNING: To avoid serious injury from high currents, ensure that both power cords are disconnected prior to removing or replacing any parts.***

⚠ ***CAUTION: This system contains board-level components that must be protected from static discharge and physical shock. Wear a wrist strap grounded to the system chassis when handling system components.***

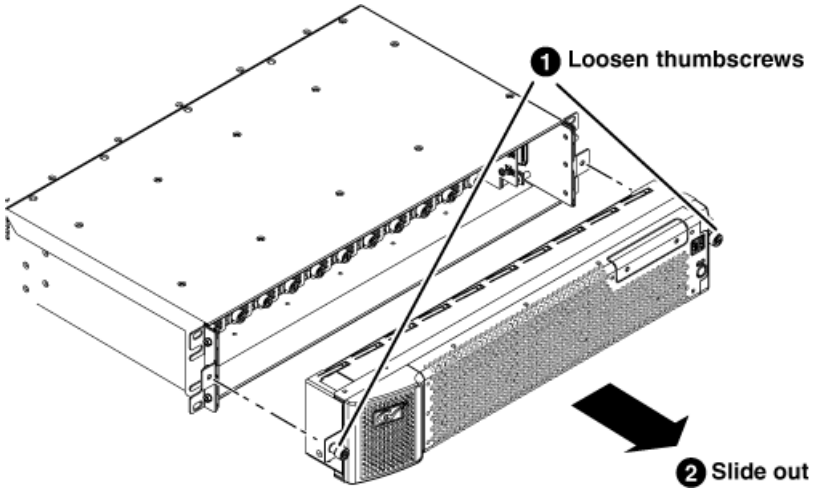
External Parts Removal

All the parts in this category can be removed and replaced without opening the K2 Solo 3G system cabinet.

Front bezel assembly removal

You can remove the bezel assembly while the K2 Solo 3G system is operating. If you do so, make sure you replace it within three minutes to ensure that the correct operating temperature is maintained.

1. To remove the front bezel assembly, proceed as illustrated.



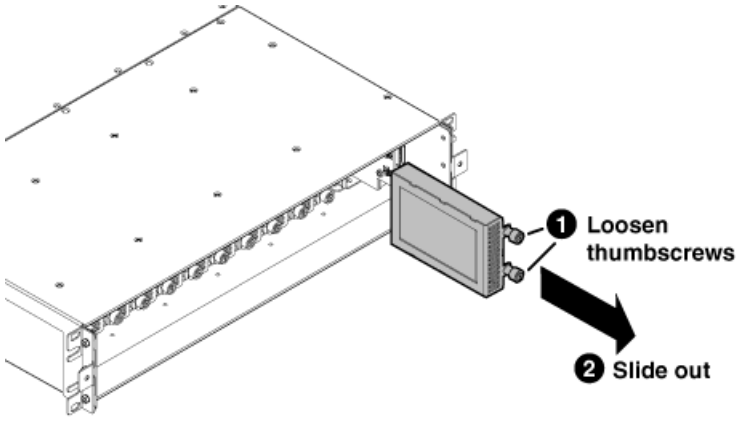
2. When installing, avoid pressing the standby switch and accidentally turning the system on or off.

Disk module removal

Before doing this task, do the following:

- Make sure you have identified the proper disk module. In some cases you must also perform operations with Storage Utility.
- Remove the front bezel assembly.

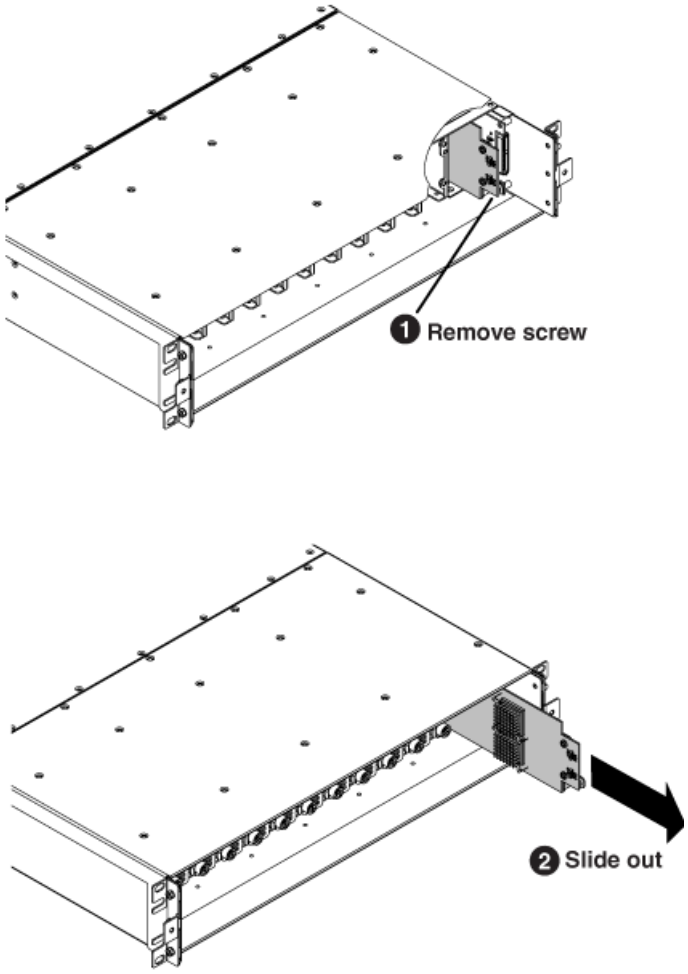
To remove a disk module, proceed as illustrated.



Disk controller board removal

Before doing this task, remove the front bezel assembly.

1. To remove the disk controller board, proceed as illustrated.



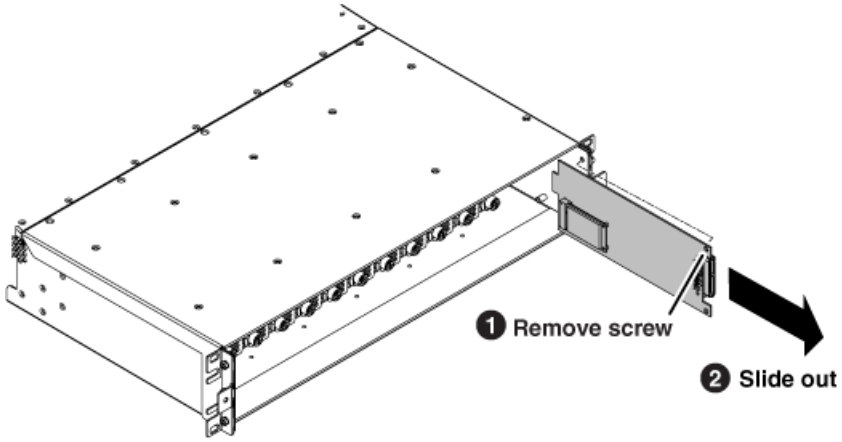
2. When installing, do the following:
   a) Make sure the board engages with the top and bottom guides.
   b) Make sure the board engages with the connectors on the disk backplane and midplane board.

After replacing the disk controller board on a K2 Summit 3G system or on any system that has a Type II (ADLINK) CPU carrier module, you must restore disk controller configuration. This includes the first generation K2 Summit system, which can have a Type II CPU carrier module that was installed in the factory or that was upgraded in the field.

Front interconnect board removal

Before doing this task, remove the front bezel assembly and disk controller board.

1. To remove the front interconnect board, proceed as illustrated.

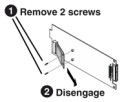


2. When installing, do the following:
   a) Make sure the board engages with the top and bottom guides.
   b) Make sure the board engages with the connector on the midplane board.

mSATA boot media removal

Before doing this task, remove the front bezel assembly, disk controller board, and front interconnect board.

1. To remove the boot media, work on the front interconnect board as illustrated.



   Use a #1 Phillips screwdriver to remove the screws.

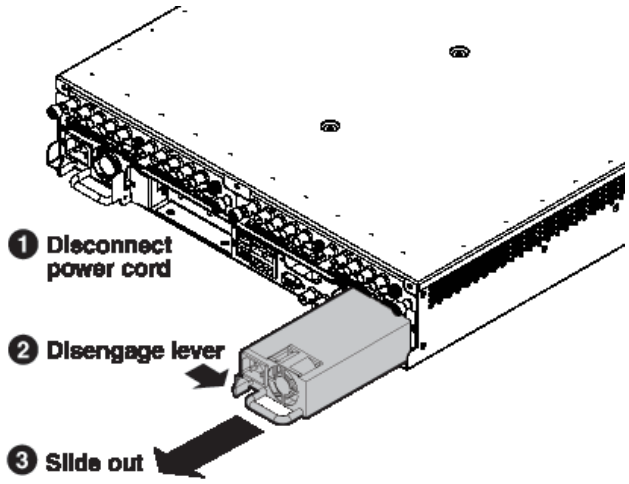
   The mounting mechanism is spring loaded and the mSATA media pops up when screws are removed.

   You must use the mSATA boot media provided by Grass Valley. Do not use media procured elsewhere.

2. When installing, hold down the mSATA media to align for fastening screws.

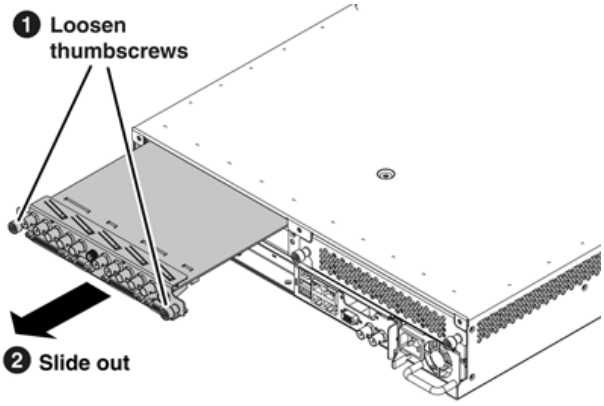
Power supply module removal

Access the power supply module from the rear panel. Remove as illustrated.



Codec module removal

Access the codec module from the rear panel. Remove as illustrated.



NOTE: With a firm grip on the metal (EMI) bracket, ensure the board is level and parallel to the card guides to avoid damage to the components on the edge opposite the rear panel.

⚠ ***CAUTION: Improper handling can damage components on the board. Do not allow the board to come in contact with the chassis sheet metal during removal or installation. The components on the edge opposite the rear panel are the most susceptible to damage.***

You must also remove any codec option (mezzanine) cards from the faulty codec module and install them on the replacement codec module.

After installing the replacement codec module, install the current version of K2 software. An over-install is all that is required. You do not need to first un-install the software. This ensures that the board is flashed with the proper version to be compatible with K2 software.

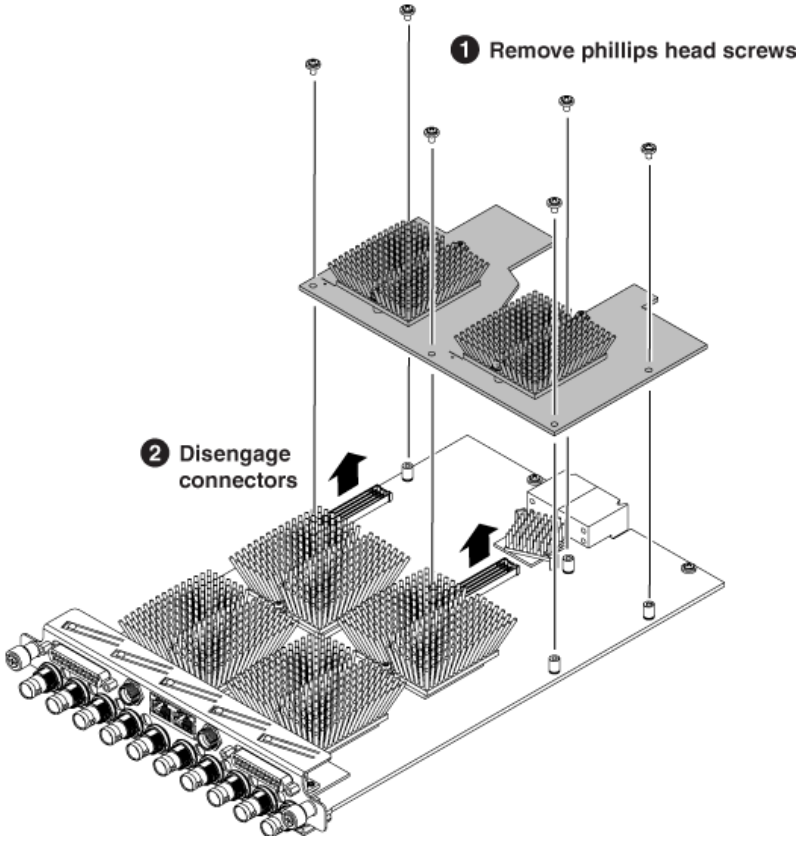
Related Topics

Compatible K2 systems hardware on page 1087

Codec option card removal

Before doing this task, remove the codec module.

To remove a codec option card from the codec module, proceed as illustrated.



Use a #1 Phillips screwdriver to remove the screws.

After installing the replacement card, install the current version of K2 software. An over-install is all that is required. You do not need to first un-install the software. This ensures that the card is flashed with the proper version to be compatible with K2 software.

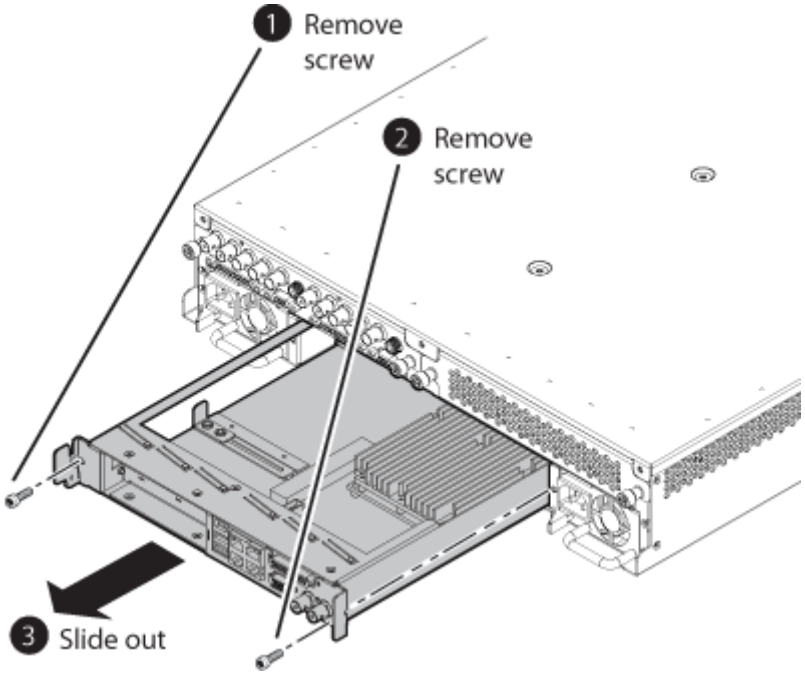
NOTE: Once a channel is operational with MPEG-2 or AVC-Intra, if you then remove the cards from the codec module you must also delete `C:/profile/config/config.xml`. Failure to do so causes errors in Configuration Manager.

Related Topics

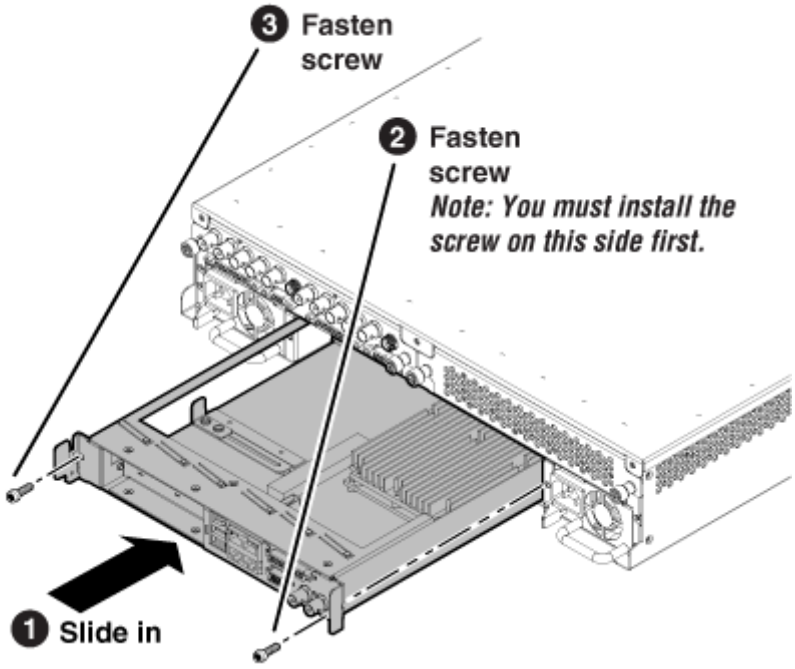
Compatible K2 systems hardware on page 1087

Carrier module removal

1. When removing the carrier module, access it from the rear panel. Remove as illustrated.



2. When replacing the carrier module, the screw attachment sequence is critical, as illustrated.

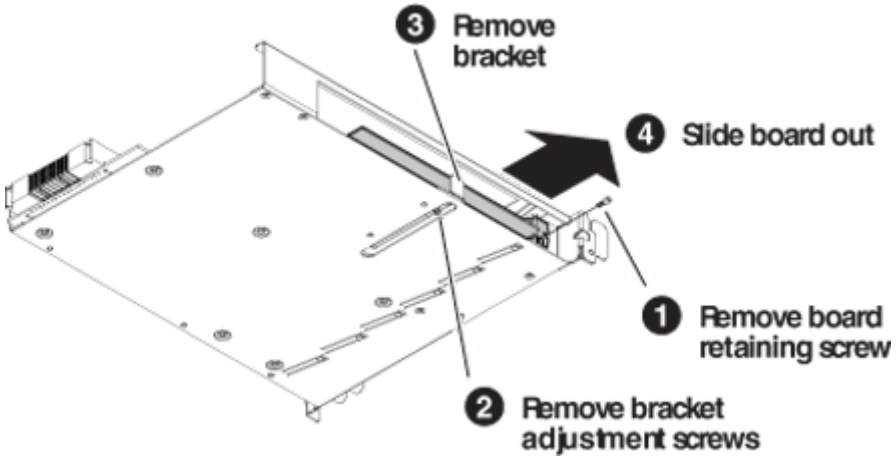


Optional PCIe board removal

Before doing this task, remove the carrier module.

This task applied to optional PCIe boards, such as a Fibre Channel board or a DynoZoom board.

To remove an optional PCIe board, disassemble the carrier module as illustrated.



Internal Parts Removal

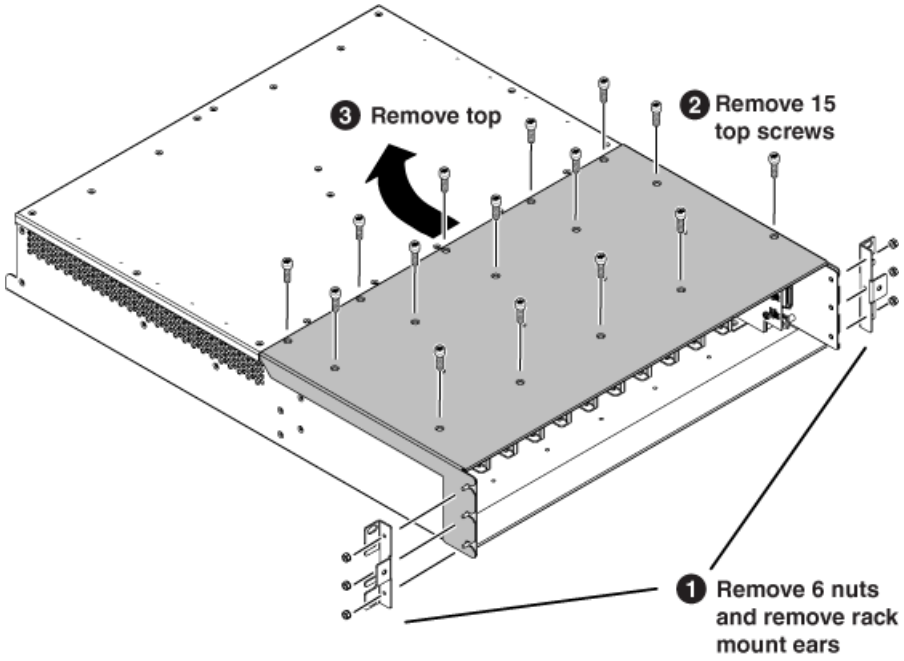
The sections that follow show how to remove internal parts from the K2 Solo 3G system.

⚠ ***CAUTION: To avoid possible damage to circuit boards and other sensitive parts, turn off the* K2 Solo 3G system *and disconnect both power cords before opening the top cover or removing any internal parts.***

Top cover removal

Before doing this task, remove the front bezel assembly.

To remove the top cover, proceed as illustrated.



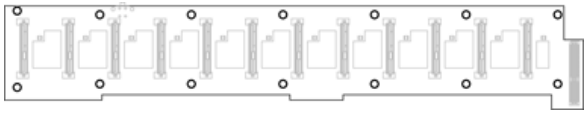
Use a #2 Phillips screw driver to remove the top screws.

Use a 1/4" nut driver to remove the rack mount ear nuts.

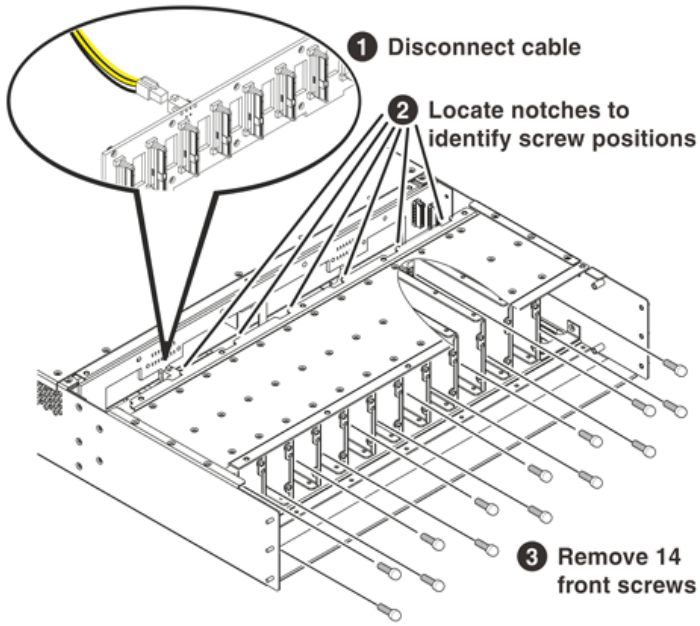
Disk backplane unit removal

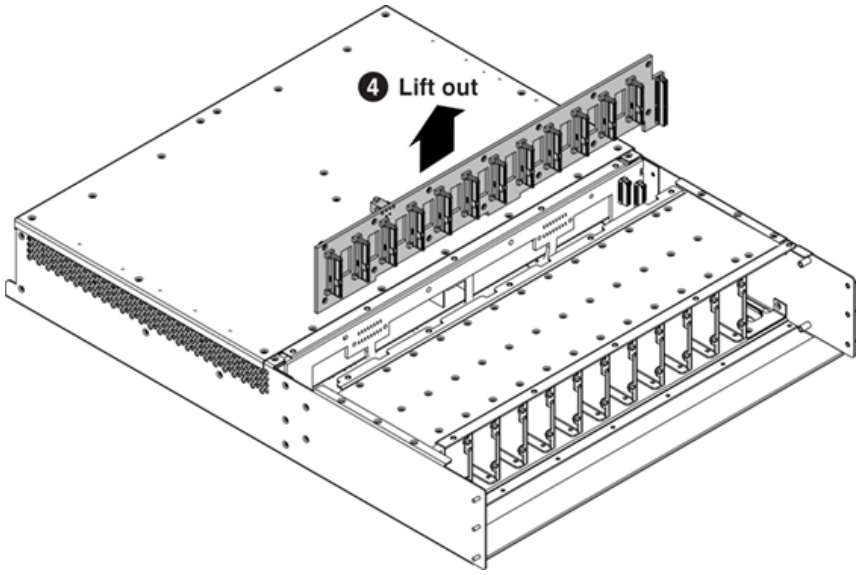
Before doing this task, remove the front bezel assembly, top cover, disk controller board, front interconnect board, and disk modules.

A screwdriver with a shaft at least 7 inches long is recommended. Use the following view of the disk backplane to help you locate screws.



To remove the disk backplane unit, proceed as illustrated.





Disk backplane unit installation

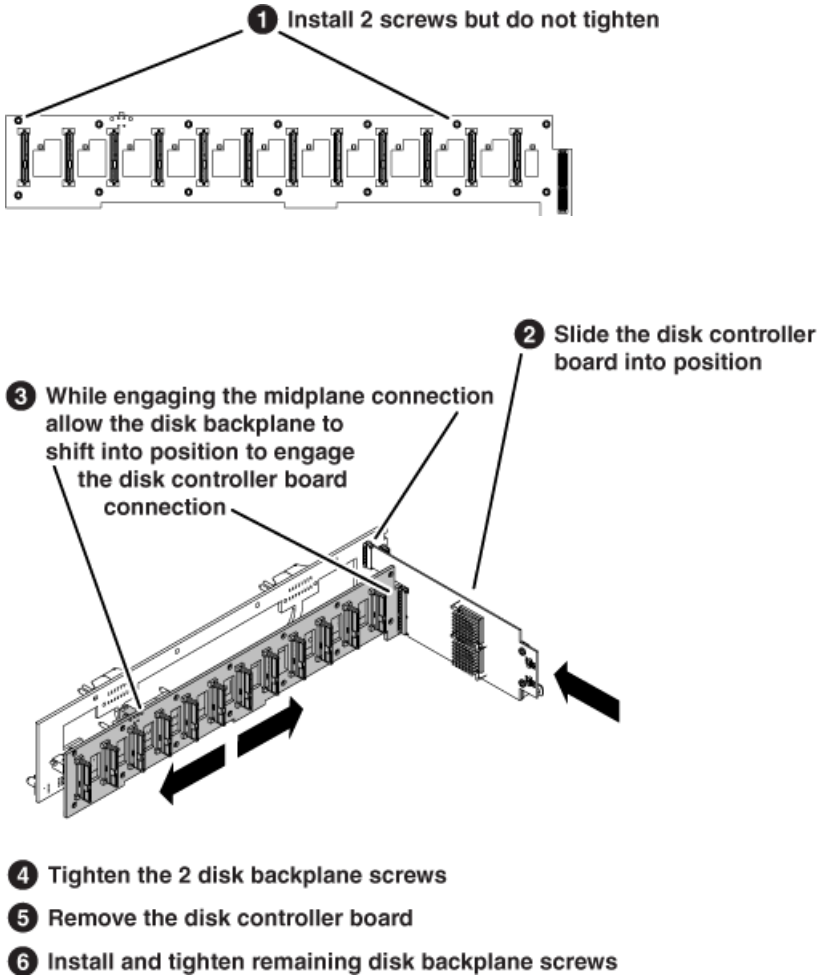
Before doing this task, install the midplane board, if it is not already installed.

Installation of the diskplane unit is the reverse of removal except as follows:

- When installing screws, use the disk controller board to index the position of the disk backplane unit.

Refer to the removal procedure for other installation steps.

Index the position of the disk backplane unit as illustrated.

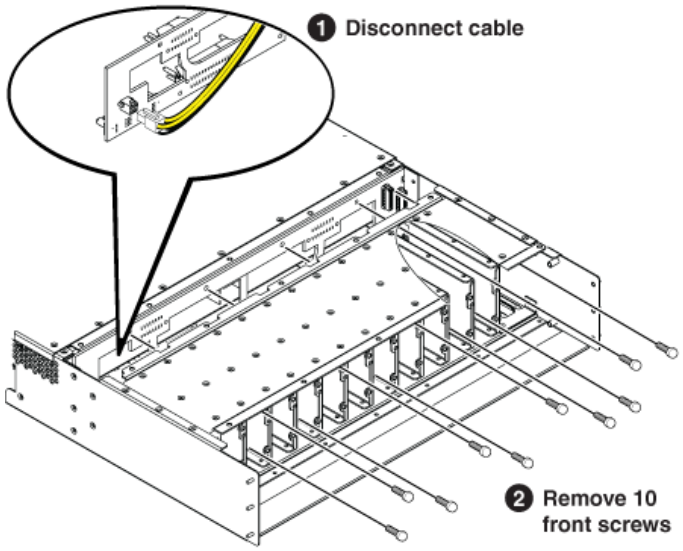


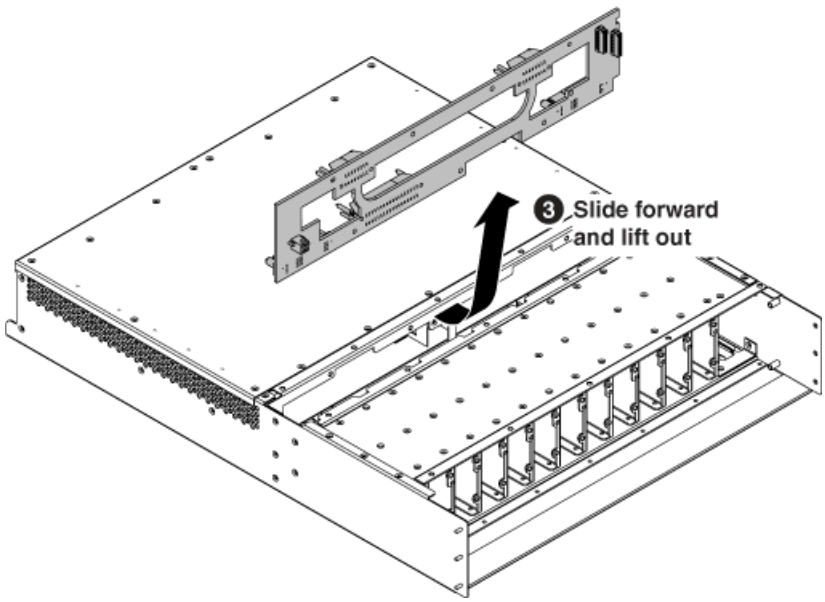
Midplane board removal

Before doing this task, remove the front bezel assembly, top cover, disk controller board, front interconnect board, disk modules, and disk backplane unit.

A screwdriver with a shaft at least 7 inches long is recommended. Use the following view of the midplane board to help you locate screws.

1. Disengage all rear FRU modules so that they are not connected to the midplane board.
2. To remove the midplane board, proceed as illustrated.





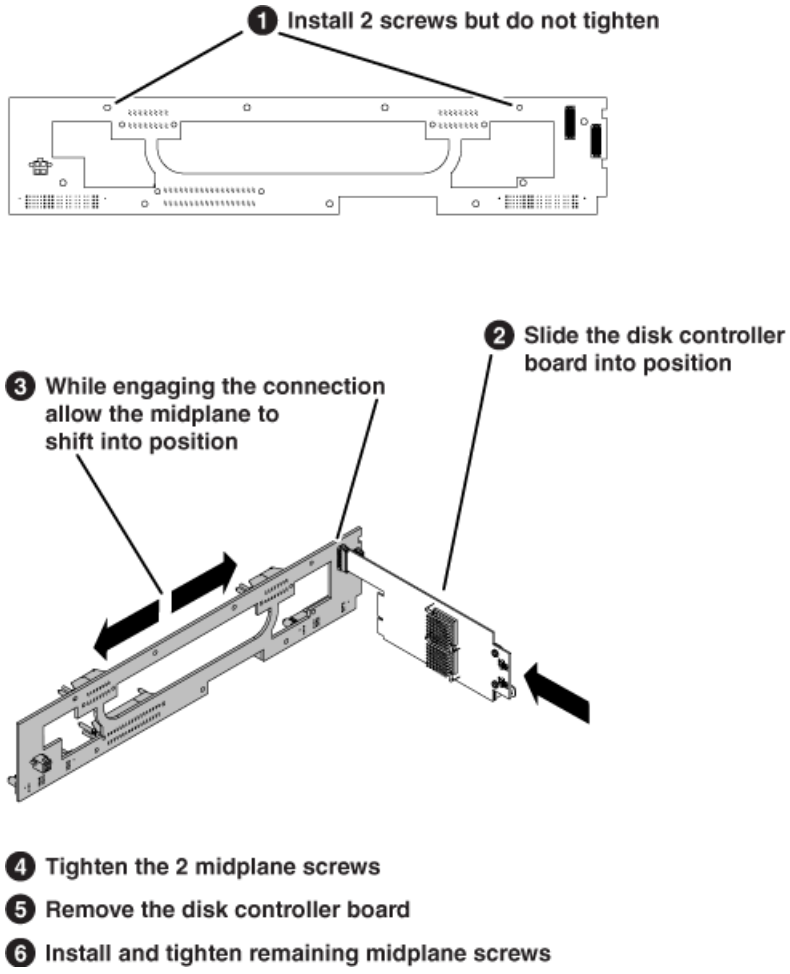
Midplane board installation

Installation of the midplane board is the reverse of removal except as follows:

- When installing screws, use the disk controller board to index the position of the midplane board.

Refer to the removal procedure for other installation steps.

Index the position of the midplane board as illustrated.



Servicing the K2 Solo system

Product description

Overview description

The K2™ Solo™ 3G system is a cost-effective media platform that incorporates IT and storage technologies. It delivers a networked solution to facilities for replay in sports, news, live, and live-to-tape applications, as well as ingest, playout, and media asset management. It is a comprehensive platform that provides a suite of user applications, system tools, and the largest range of third party interactivity in the industry.

Refer to the the "Configuring the K2 System" section of this Topic Library for other high-level descriptions of features, controls, applications, and subsystems.

K2 Solo 3G system features

The following features apply to the K2 Solo 3G Media Server:

- Windows 7 64-bit embedded operating system.
- Embedded Security for protection against viruses and other unauthorized programs.
- Bidirectional channels (channel can be either an input channel or it can be an output channel).
- Two channels per chassis.
- SDI video inputs and outputs.
- AES/EBU or embedded audio inputs and outputs.
- Standard Definition (SD) video formats and High Definition (HD) video formats.
- Support for DV, MPEG-2, AVCHD/H.264, AVC-Intra, AVC - LongG, and Avid DNxHD. For details regarding licenses, hardware support, and video codec specifications, refer to related topics in the "Using K2 AppCenter" section of the K2 Topic Library.
- 3G codec module. Codec option card not supported on K2 Solo 3G system.
- Mixed format playback of SD or HD clips on the same timeline.
- Up/down/cross HD/SD conversion (e.g. SD and HD clips ingested, then played back as SD or HD clips) or as a different SD or HD format (e.g. 720p to 1080i). Aspect ratios are adjusted.
- VGA monitoring capability.
- Compact Flash System drive.
- Type IV CPU carrier module with 8 GB RAM.
- USB 3.0 interface for file exchange.
- Ability to create nested bins, i.e. sub-bins within bins.
- Freeze mode can be frame or field.
- Various video mix effects (e.g. dissolves between two video and audio tracks on the same channel, or fade thru matte color).
- Remote operation and configuration via AppCenter.
- Gigabit Ethernet.
- AMP, VDCP, and BVW remote control protocols supported.
- Remote control over RS-422 or Ethernet.
- ExpressCard.

- Super Slo-Mo, Multi-cam, and 3D/Video + Key features are available as part of the ChannelFlex Suite.
- Low-resolution proxy files created during record and live streaming from SDI In/out are available as part of the AppCenter Pro and Elite licenses.
- Internal media storage.
- Support for Dyno S.

K2 Summit/Solo formats, models, licenses, and hardware support

Formats are supported as in the following tables.

Table 52: First-generation K2 Summit/Solo system

Formats	Compression	1x	Multi-Cam, 3D/Video + Key	3x Super Slo-Mo	4K
SD	DV	Encode/decode	Encode/decode	Not supported.	Not supported.
	MPEG-2	Decode is standard. Encode requires codec option card.	Decode is standard. Encode requires codec option card.	Not supported.	Not supported.
	AVCHD	Not supported.	Not supported.	Not supported.	Not supported.
1080i/720p	DV	Encode/decode. Requires HD license.	Encode/decode. Requires HD license.	Encode/decode. Requires HD license.	Not supported.
	MPEG-2	Decode is standard. Encode requires codec option card. Requires HD license.	Decode is standard. Encode requires codec option card. Requires HD license.	Not supported.	Not supported.
	AVC-Intra	Encode/decode. Requires codec option card. Requires HD license.	Encode/decode. Requires codec option card. Requires HD license.	Not supported.	Not supported.
	AVCHD	Not supported	Not supported	Not supported	Not supported.
	AVC - LongG	Not supported	Not supported	Not supported	Not supported.
	Avid DNxHD	Not supported	Not supported	Not supported	Not supported.
1080p	AVC-Intra Class 100	Not supported	Not supported	Not supported	Not supported.

To add support for additional formats, contact your Grass Valley representative for upgrade information.

Table 53: K2 Summit 3G system

Formats	Compression	1x	3x Super Slo-Mo, Multi-Cam, 3D/Video + Key	6x Super Slo-Mo	4K
SD	DV	Encode/decode	Encode/decode	Not supported.	Not supported.
	MPEG-2	Encode/decode	Encode/decode. Requires codec option card.	Not supported.	Not supported.
	AVCHD/H.264	Decode only. Requires AVC license.	Not supported	Not supported	Not supported.
1080i/720p	DV	Encode/decode. HD license is required.	Encode/decode. HD license is required.	Encode/decode. Requires codec option card, plus HD and 6xSSM licenses. Requires K2 Summit 3G chassis with 2.5” hard drives for one channel or high endurance solid state drives for full features with two channels.	Not supported.
	MPEG-2	Encode/decode. HD license is required.	Encode/decode. Requires codec option card. HD license is required.	Not supported.	Not supported.

Formats	Compression	1x	3x Super Slo-Mo, Multi-Cam, 3D/Video + Key	6x Super Slo-Mo	4K
	AVC-Intra	Encode/decode. Requires HD and AVC licenses.	Encode/decode. Requires HD and AVC licenses.	Encode/decode. Requires codec option card, plus HD, 6xSSM and AVC licenses. Requires K2 Summit 3G chassis with 2.5” hard drives for one channel or high endurance solid state drives for full features with two channels.	Not supported.
	AVCHD/H.264	Decode only. Requires HD and AVC licenses.	Not supported	Not supported	Not supported.
	AVC - LongG	Decode only. Requires HD and AVC licenses.	Not supported	Not supported	Not supported.
	Avid DNxHD	Encode/decode. Requires HD and DNxHD licenses.	Encode/decode. Requires HD and DNxHD licenses.	Not supported	Not supported.
1080p	AVC-Intra Class 100	Encode/decode. Requires HD, 3G and AVC licenses.	Encode/decode. Requires codec option card, plus HD, 3G and AVC licenses.	Not supported	Encode/decode. Requires codec option cards and high endurance solid state drives. Requires HD, 3G, 4K and AVC licenses.

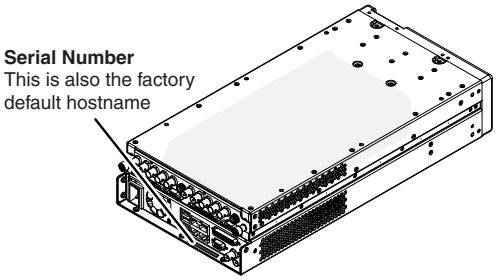
Table 54: K2 Solo 3G system

Formats	Compression	1x	Multi-Cam, 3D/Video + Key	3x Super Slo-Mo	4K
SD	DV	Encode/decode	Encode/decode	Not supported.	Not supported.

Formats	Compression	1x	Multi-Cam, 3D/Video + Key	3x Super Slo-Mo	4K
	MPEG-2	Encode/decode	Not supported	Not supported	Not supported.
	AVCHD/H.264	Decode only. Requires AVC license.	Not supported	Not supported	Not supported.
1080i/720p	DV	Encode/decode. HD license is required.	Encode/decode. HD license is required.	Encode/decode. HD license is required.	Not supported.
	MPEG-2	Encode/decode. HD license is required.	Not supported	Not supported	Not supported.
	AVC-Intra	Encode/decode. Requires HD and AVC licenses.	Encode/decode. Requires HD and AVC licenses.	Encode/decode. Requires HD and AVC licenses.	Not supported.
	AVCHD/H.264	Decode only. Requires HD and AVC licenses.	Not supported	Not supported	Not supported.
	AVC - LongG	Decode only. Requires HD and AVC licenses.	Not supported	Not supported	Not supported.
	Avid DNxHD	Encode/decode. Requires HD and DNxHD licenses.	Encode/decode. Requires HD and DNxHD licenses.	Encode/decode. Requires HD and DNxHD licenses.	Not supported.
1080p	AVC-Intra Class 100	Encode/decode. Requires HD and 3G licenses.	Not supported	Not supported	Not supported.

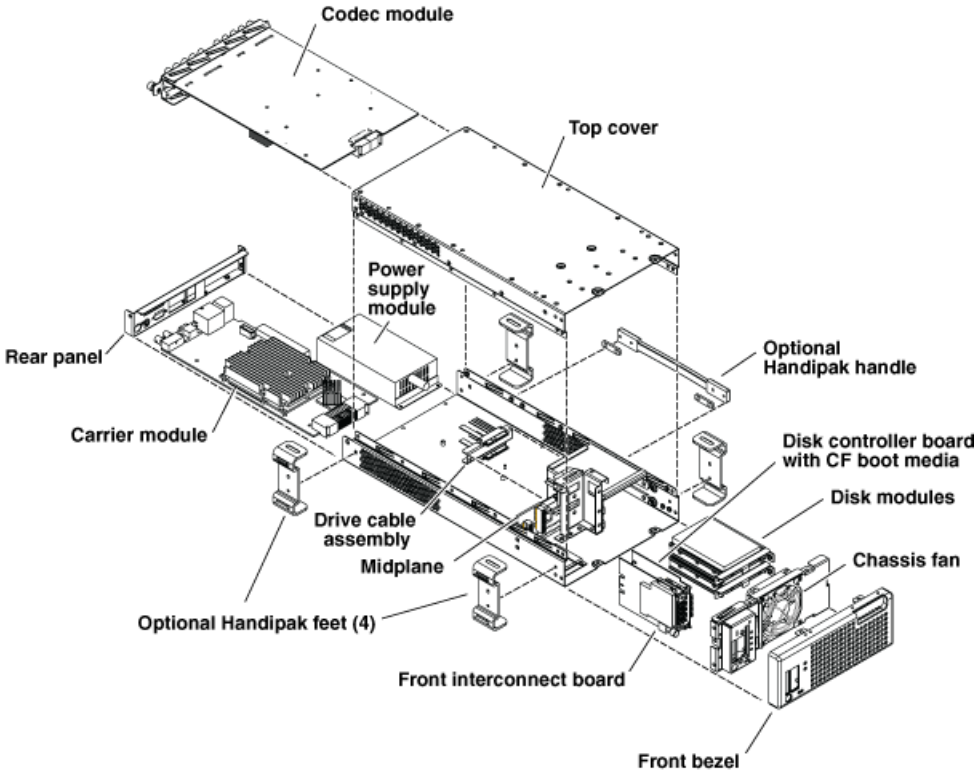
Product identification K2 Solo

K2 Solo 3G system have labels affixed to the chassis that provide product identification as illustrated:



K2 Solo 3G system orientation

The following illustration shows the location of Field Replaceable Units (FRUs) and other components in the K2 Solo 3G system.



FRU functional descriptions

K2 Solo 3G system Field Replaceable Units (FRUs) are described in this section.

Chassis fan

The chassis fan is mounted in the fan bracket. It provides cooling to the unit. It is mounted in the front of the unit, behind the front bezel.

Disk modules

There are slots for disk modules in the K2 Solo 3G system. The slots are located behind the front bezel assembly in the front of the chassis. Each slot can contain one disk module, and each module contains one hard drive. A K2 Solo 3G system contains 2 disk modules. Disk modules plug into the drive cable assembly.

Data is written or "striped" across the disks in a continuous fashion, which makes the disks a "stripe group". This stripe group appears as the V: drive to the Windows operating system. The V: drive stores media. It also stores media file system, database, and configuration information.

Disks are configured as RAID 0, so you can not remove and replace a disk module while the K2 Solo Media Server is operational. If a disk fails, you lose all media.

CompactFlash boot media

The CompactFlash boot media contains the system drive, also known as the C: drive. The C: drive contains application and operating system files. The CompactFlash media is hosted by the front interconnect board.

Power supply module

The K2 Solo 3G system has one power supply. You can not remove and replace the power supply while the K2 Solo 3G system is operational. The power supply has a fan with automatic speed control. The power supply has protection for over voltage, over current, and short circuits.

Codec module

The K2 Solo 3G Media Server has one codec module. The codec module hosts two media input/output channels. The codec module is oriented horizontally across the rear of the K2 Solo 3G Media Server chassis. It provides the majority of the K2 Solo 3G Media Server's media-related input and output connectors on the rear panel. The codec module plugs into the midplane board.

The K2 Solo 3G Media Server does not support a codec option card on the codec module.

Disk controller board

The disk controller board provides the RAID functionality for the internal disks and reports the status of the chassis fans. It controls status LEDs and the front bezel Power and Service LEDs. It hosts the CompactFlash boot media. It is mounted in the front of the unit and plugs into the midplane board.

Front interconnect board

The front interconnect board provides front interface functionality. It hosts the front USB ports, the Express Card, and the standby switch. It is mounted in the front of the unit and plugs into the midplane board.

Midplane board

The midplane board provides connections for the rear modules. The disk controller board and the front interconnect board also plug into the midplane board. It is mounted in the center of the unit.

Carrier module

The carrier module provides the functionality typically associated with a motherboard in a PC. It hosts the CPU, one optional PCIe board, and provides rear panel connections for Gigabit Ethernet, USB, VGA, and IEEE 1394a (Firewire). The IEEE 1394a port is for debugging purposes only. It is not supported for customer use. Do not attempt to configure or otherwise use this port. The carrier module also provides a GPI connection and connections for reference.

Drive cable assembly

The drive cable assembly includes the disk cables and a bracket for mounting drive connectors in the chassis.

System Overview

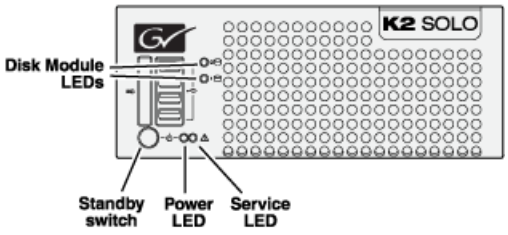
The K2 Solo 3G system is a PCIe bus-based Windows computer with extensive enhancements to provide the video disk recorder functionality. This section explains the major architectural blocks.

Status indicators

The following sections describe the visual and audible indicators that communicate the current operating status and system health of the K2 Solo 3G system.

Front panel indicators

The following indicators are visible from the front panel view.



Power LED

The Power LED indicates status as follows::

LED behavior	Status Condition
Off	The standby switch is set to Off and the K2 Solo 3G system is not operational.
Green steady on	The standby switch is set to On and the K2 Solo 3G system is either in the startup process or has completed the startup process and is operational.

⚠ ***WARNING: The power standby switch does not turn off power to the system. To turn power off both power supplies must be disconnected from the power source.***

Service LED

The following table explains the status conditions indicated by the different Service LED behaviors. If two or more status conditions occur simultaneously, the LED displays the behavior for the highest priority condition.

LED behavior	Status Condition	Priority
Flashing pattern alternating Yellow/Green/Red/Off twice a second	Identify — The K2 Solo 3G system is being directed to identify itself by NetCentral or some other application.	1
Solid Red	Global failure — The K2 Solo 3G system software has detected a critical error or failure that impacts record/play operations.	2
Solid Yellow	Warning — The K2 Solo 3G system software has detected a problem that requires attention but does not immediately impact record/play operations. For example, a fan or power supply has failed but its redundant partner is maintaining functionality.	3
Flashing Yellow pattern three times a second.	Drive failure — An internal RAID drive has failed. If RAID 1, the failure does not immediately impact record/play operations. The redundant partner RAID drive is maintaining functionality.	4
Flashing pattern alternating Yellow/Green once a second.	Drive rebuild — If RAID 1, an internal RAID drive is rebuilding.	5
Off	Normal — The K2 Solo 3G system is healthy and operating normally.	5

Disk module LEDs

Each disk module has an LED that indicates status. The LEDs are located on the front bezel. The following table explains the status conditions indicated by the different LED behaviors. If two or more status conditions occur simultaneously, the LED displays the behavior for the highest priority condition. Priority number 1 is the highest priority.

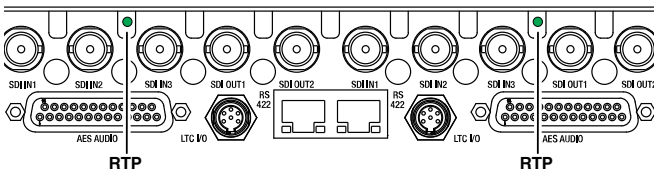
LED behavior	Status Condition	Priority
Amber flashing pattern	Identify — The drive is being directed to identify itself by Storage Utility or some other application.	1
Green flashing pattern twice a second.	Rebuild — The RAID controller has marked the drive as rebuilding.	3
Red ON solid	Fault — The RAID controller has marked the drive as faulty.	3
Amber ON solid	Offline — The drive is unbound.	3
Green flashing pattern ten times a second.	Normal drive activity — The drive is healthy and disk access is underway.	3
Green ON solid	Normal drive activity — The drive is healthy and no disk access is currently underway.	3
Off	No drive — Drive is not present or is not fully engaged in slot.	—

Rear panel indicators

The following indicators are visible from the rear panel view.

Codec board indicator

Each channel has a green/red LED that indicates the status of the Real Time Processor (RTP).



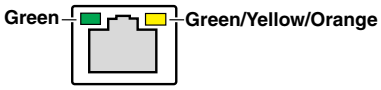
Codec board indicator codes

Interpret the RTP LED as follows:

LED behavior	Status condition
Green flashing at approximately 1 second intervals	RTP is up and connected to the host
Green flashing at greater than 1 second intervals	RTP is not connected to the host.
Red	RTP error condition. Real Time OS is not running.
Off	Real Time OS is not running.

LAN connector indicator codes

The motherboard has four RJ-45 LAN connectors that include integrated status LEDs. The LEDs are oriented as follows:



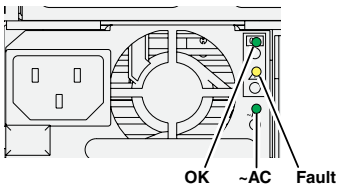
The meanings of the LED states are described in the following table:

LED	LED state	Status Condition
Green	Green On	The adapter is connected to a valid link partner
	Green flashing	Data activity
	Off	No link
Green/Yellow/Orange	Off	10 Mbps
	Green	100 Mbps
	Yellow	1000 Mbps
	Orange flashing	Identify

If a LAN connector is faulty, you must replace the carrier module.

Power supply indicators

Each power supply has LEDs that indicates status.



Interpret the power supply LEDs as follows:

LED	LED state	Status Condition
OK	Green On	The power supply is operating normally.
Fault	Yellow On	There is a power supply fault.
~AC	Green On	The electrical current available to the power supply meets power supply requirements. Input > 85 VAC.

Another indicator of power supply operation is the audible fan noise. If a power cable is connected to either power supply, the fan should stay on continuously on both power supplies. This is the case

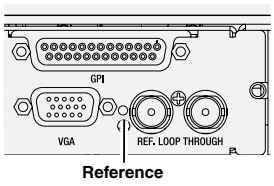
even if the K2 Solo 3G system is shut down or restarting via the standby switch or the Windows operating system.

The Service LED on the front of the K2 Solo 3G system also indicates power supply status.

If the power source and the power cord are OK yet there is still a power supply problem, the status lights on the power supply indicate the problem.

Reference indicator

There is a small hole in the carrier module next to the "REF. LOOP THROUGH" BNC connectors.



Through this hole a LED is visible. When the LED is lit, the reference signal is present and locked.

System beep codes

When you start up the K2 Solo 3G system by pressing the standby switch or by doing a Windows operating system restart, the CPU module might emit two short beeps. Otherwise, if there are no errors present, the K2 Solo 3G system does not emit any audible beeps.

When an error occurs during Power On Self Test (POST), the BIOS displays a POST code that describes the problem. The BIOS might also issue one or more beeps to signal the problem. This indicates a serious error and it is likely that the carrier module must be replaced. Contact Grass Valley Support.

System Messages

About system messages

The following messages are displayed to indicate system status:

- Normal BIOS messages — These messages can be observed on a locally connected VGA monitor during normal startup processes.
- BIOS POST error messages — If there is a problem these messages are displayed on a locally connected VGA monitor. During the Power On Self Test (POST), the BIOS checks for problems and displays these messages.
- AppCenter startup messages — As AppCenter opens the system determines if health is adequate by checking critical subsystems. A dialog box is displayed that indicates progress and displays messages.

- Status bar and StatusPane messages — During normal operation AppCenter displays system status messages on the status bar. From the status bar you can open the StatusPane to see both current and previous messages. You can observe these messages in AppCenter on a locally connected VGA monitor or on a network connected control point PC.
- Storage Utility messages — While you are using Storage Utility, pop-up message boxes inform you of the current status of the storage system.

Critical system startup messages

The following messages appear in the AppCenter system startup message box as critical subsystems are checked during startup processes. If a critical failure is detected, the K2 Solo 3G system is rendered inoperable and the failure message appears.

Critical subsystem check messages	Failure messages
System Startup	Startup error
	Missing or bad hardware
	A real time processor is not functioning correctly
Checking hardware…	Hardware fault
Checking media disks…	One or more media disks failed to initialize
	Missing or bad hardware
	Missing or bad database
Checking file system…	No file system is running
Checking database…	Database fault
Checking real-time system status…	A real-time system failed to initialize
Updating configuration…	Failed to synchronize configurations
Starting services…	Unable to communicate with <service name>

AppCenter startup errors

If you start AppCenter and the K2 Solo 3G system is not running, or your login information is not correct, you will see a Startup Error message.

The following table describes the two most common startup error messages.

Startup Error	Description
Log on failed	Your user name or password is not valid for this K2 Solo 3G system. Remember that the password is case sensitive. • Click **Ignore** to view the AppCenter channels. If working remotely, you will see the channels from the last-used channel suite. Or, • Click **Retry** to enter the login information again. Or, • Click Abort. If you are accessing AppCenter through a network-connected Control Point PC, **Abort** lets you try to create a new channel suite. If you are accessing AppCenter locally, it lets you exit to Windows. For assistance with your user name or password, consult your Windows administrator.
<K2 system>:<error>	The K2 Solo 3G system might be offline or have had difficulty with the start up checks. There are various reasons why AppCenter is having difficulty connecting to the K2 Solo 3G system; for example, the error might say there is no file system or that the K2 Solo 3G system has been taken offline for maintenance. • Verify that the host name or IP address is correct and see if you can correct the problem. • If working locally, reboot the K2 Solo 3G system. If working from a network-connected Control Point PC, select **System | Reconnect** from the AppCenter **System** menu.

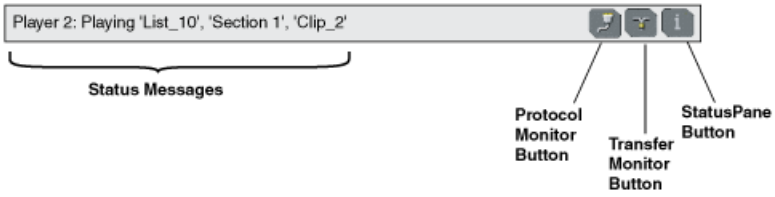
Viewing AppCenter system status messages

System status messages are displayed in the AppCenter status bar. There are two types of system status messages, as follows:

- Channel status messages — In normal operation, this type of message displays the current operating status of the selected channel.
- System error messages — If a problem develops with the system software or a hardware subsystem, this type of message is displayed for approximately 5 seconds. Afterward, the display returns to the channel status message and the error message is written to the status log file. When a message is written to the status log, a *Status Icon* indicates the severity of the message.

Status bar

System status messages appear in the AppCenter status bar, which is located across the bottom of the AppCenter window, and consists of a message area, several tool buttons, and a status icon. The button icons appear only when the related function is active. In the position of the StatusPane button, status icons appear.



The status bar displays information about the state of the delegated channel as well as low-level error messages. (High priority error messages are displayed in pop-up windows.)

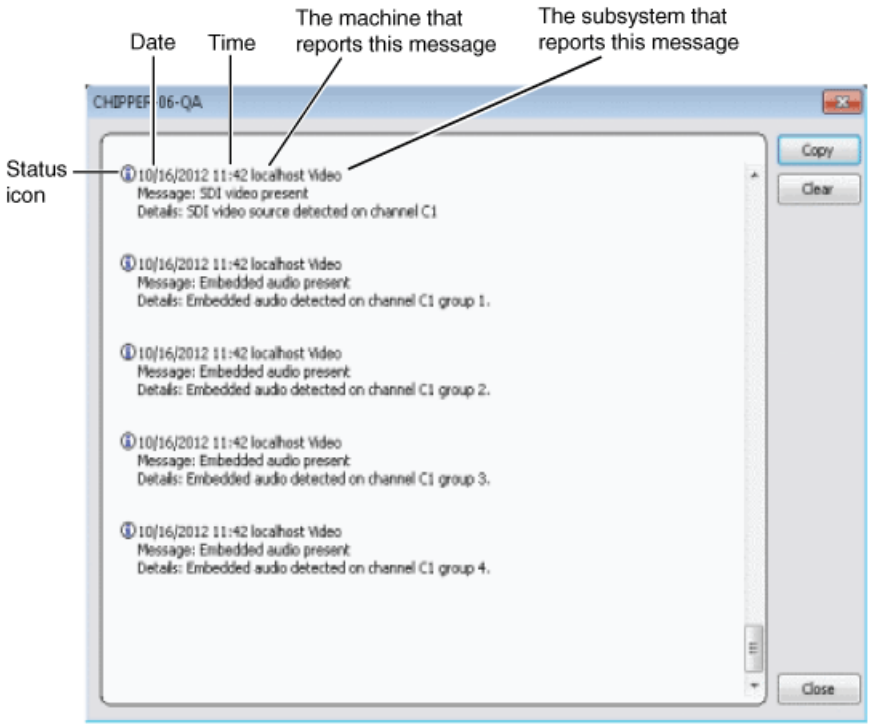
If you select a channel, a status message appears on the left-hand side of the status bar. If a potential error arises while an application is running in a channel, a status message flashes briefly on the left-hand side of the status bar, and an icon displays on the right-hand side. Double click on the icon to open the status pane to view a more detailed message about the channel's status.

The status icon changes depending on the status of the current status message.

Icon	Name	Description
	Information	A recent information message is present.
	Warning	There is at least one warning message, and no alert messages.
	Alert	There is at least one uncleared alert message.

Status pane

Current and previous system status messages can be viewed in the StatusPane. The system status pane also displays general information such as the video and audio settings on the channels. To open the StatusPane, click **Help | System Status**.



The StatusPane is used to view detailed system messages including status, warning, and error messages. System status messages provide status icons and a description of the status event reported by the message. If there is a problem, a corrective action is indicated. Use these messages along with troubleshooting problems to determine if a service procedure is necessary.

If you have a remote AppCenter Channel Suite with channels from multiple K2 systems, the messages from the different machines are combined in the StatusPane that you view from the Channel Suite. To help you determine which machine is generating a message, each message lists the machine name.

NOTE: If the Clear button is grayed out, you do not have the necessary privileges to perform this action, based on the type of user account with which you are currently logged on.

Copying StatusPane messages to the clip board

1. Select the message or messages in the StatusPane.
2. Click **Copy**.

After copying the message, it can be pasted using standard Windows techniques.

Clearing messages

Clearing messages from the StatusPane removes them from the logging database and the StatusPane. This also clears the state of the subsystem indicators so they no longer display the alert and warning symbols.

1. Open the StatusPane, then click **Clear**.
2. When a message prompts you to confirm, click **Yes**.

All messages are removed from the StatusPane and logging database.

Exporting log files

This topic describes how to export log files from the K2 Solo 3G system. The log files include the following:

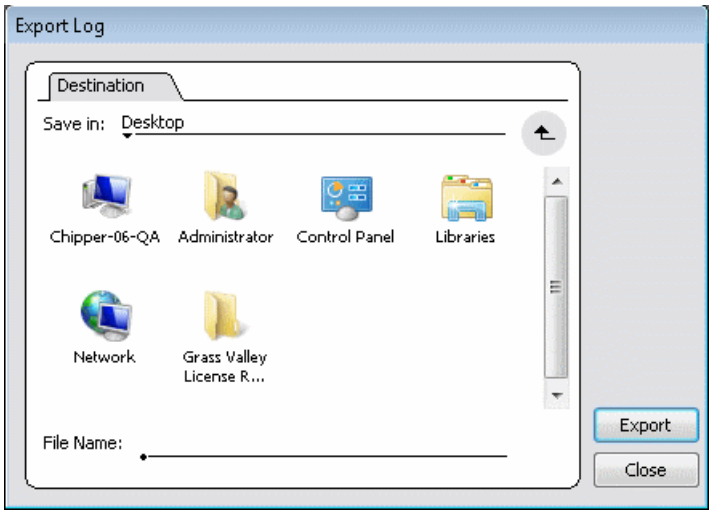
- All application and media database messages
- Version information
- Configuration file, from Configuration Manger

The exported files are combined in a ZIP file. The ZIP file can be sent to Grass Valley product support where they can analyze the logs to determine the operational status of your system.

NOTE: ExportLog does not export StatusPane messages. To capture StatusPane messages, you can copy StatusPane messages to the clip board.

1. Log in as Administrator.
2. Do one of the following to open the Export Log dialog box.
   - In AppCenter click **System | Export Log**.
   - From the Windows desktop, click **Start | All Programs | Grass Valley| Export logs**.
   - From the Windows desktop, click **Start | Run**, type `c:\profile\exportlog` in the Run dialog box, then click **OK**.

   The Export Log dialog box opens.



3. Browse to `C:\Logs` to save the log file.
4. Name the log file.
5. Click **Export**. A progress bar appears.
6. When the export process is complete, and message confirms success. Click **OK** and close the Export Log dialog box to continue.
7. Find the log file at the specified location.

Service procedures

Embedded Security modes and policies

The Embedded Security solution protects against viruses and other unauthorized programs on the following Grass Valley systems:

- K2 Summit/Solo system
- All types/roles of K2 Media Server
- All types/roles of GV STRATUS server

Embedded Security prevents any unauthorized programs from running on the system. It contains a whitelist of programs that are authorized to run. Whenever a program attempts to run, it is checked against the whitelist. If the program is not on the whitelist, Embedded Security blocks the program from running. SiteConfig, and any software deployed by SiteConfig, is on the whitelist, so you do not need to manage Embedded Security in any way when using SiteConfig to deploy software. All versions of SiteConfig are compatible with Embedded Security.

When installing software manually (without SiteConfig) it might be necessary to manage Embedded Security. When necessary, you can put Embedded Security in Update mode. This mode allows you to manually install software that is not on the whitelist. Do not confuse Update mode with the idea that Embedded Security is "disabled". When in Update mode, Embedded Security is still active. While in Update mode, Embedded Security keeps track of any software you run or install and adds it to the whitelist. When you are done installing software and any required restarts, you must take Embedded Security out of Update mode so that it can protect the system. For software that requires a restart after installation, such as K2 system software and SNFS media file system software, Embedded Security must remain in Update mode until after the restart is complete.

No system restarts are required for entering or leaving Update mode, and a restart does not change the Update mode status. If in Update mode before a restart, the system remains in Update mode after a restart. You use the Embedded Security Manager to enter and leave Update mode.

The following policies apply to the Embedded Security:

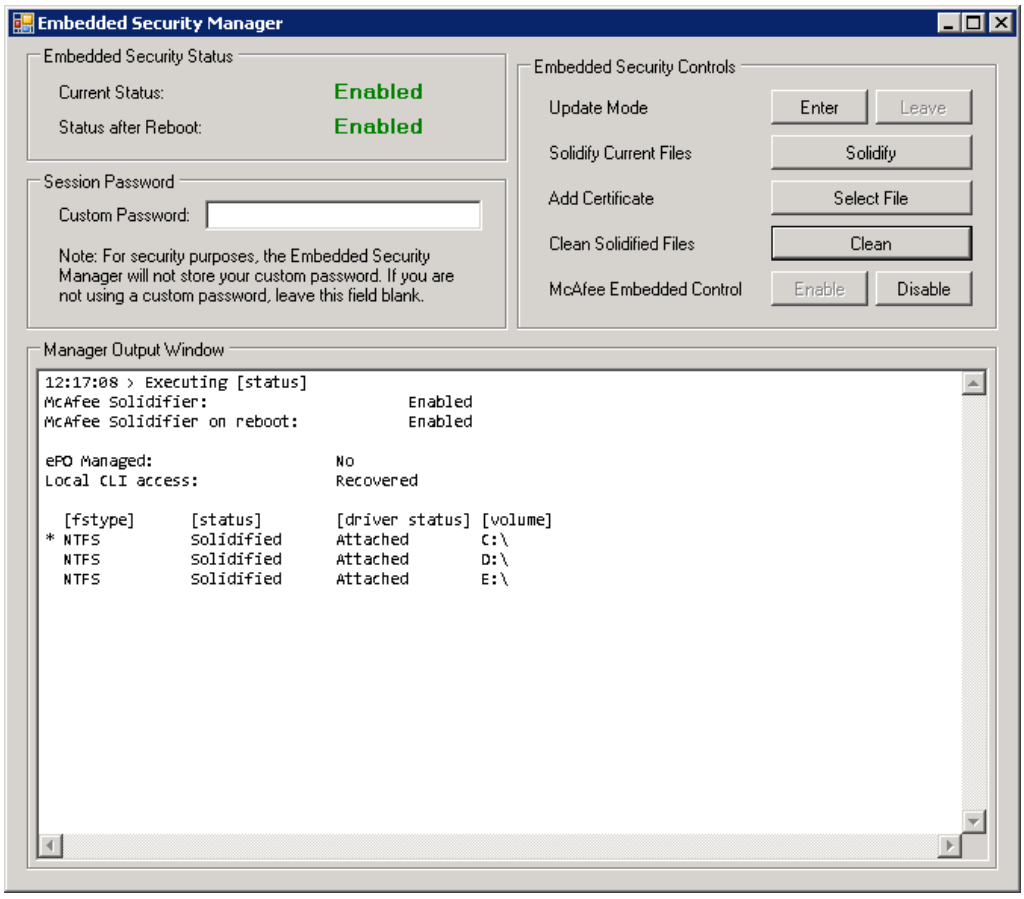
- Use Update mode only as instructed by Grass Valley product documentation or as directed by Grass Valley Support. Do not do any other operations with Embedded Security Manager, unless under the direct supervision of Grass Valley Support.
- Do not keep Embedded Security in Update mode long-term, as Embedded Security does extra processing while in Update mode and eventually problems arise when attempting to run software.
- Make sure that Embedded Security is not in Update mode when using SiteConfig to install software. Update mode interferes with SiteConfig's automatic management of Embedded Security and causes problems running the software installed.
- Leave Embedded Security enabled for normal operation of your Grass Valley system. Do not disable Embedded Security except as instructed by Grass Valley product documentation or as directed by Grass Valley Support. Enabling and disabling Embedded Security requires a restart.

- Do not install any programs or modify any operating system settings unless approved by Grass Valley. By design, Embedded Security prevents any programs from being installed or from running that are not present when you receive the system new from Grass Valley. These Grass Valley systems are not general purpose Windows workstations. The applications and configuration have been specifically optimized on each system for its intended use as part of the Grass Valley system.
- While Embedded Security is the key anti-virus component on these systems, you should still follow the Grass Valley anti-virus scan policy and scan all the devices in your Grass Valley system to ensure viruses are not propagated between machines.

Embedded Security is part of the K2 Solo 3G system generic disk image and the K2 Media Server generic disk image compatible with K2 software version 9.0 or higher. Both K2 Media Servers and GV STRATUS servers use the same generic disk image, so GV STRATUS servers inherit the Embedded Security solution. On K2 Solo 3G systems, the Embedded Security solution introduced with K2 software version 9.0 replaces the write filter from previous versions.

Manage Embedded Security Update mode

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



   Interpret Current Status as follows:

   - **Enabled**: Embedded Security is enabled but is not in Update mode.
   - **Update**: Embedded Security is enabled and is in Update mode, ready for software installation.

2. Manage the Update mode as follows:

   - If Embedded Security is not in Update mode, click **Enter** to put it in Update mode.
   - If Embedded Security is already in Update mode, click **Leave** to take it out of Update mode.

   A restart is not required after you change the Update mode.

Replacing a RAID 0 drive

A K2 Solo Media Server's disk modules are configured as RAID 0, so when one drive fails, all media is lost. To replace a RAID 0 drive, do the following:

1. Unbind the LUN that has the failed drive.
2. Remove the failed drive from the K2 Solo 3G system chassis.

3. Insert the replacement drive in the K2 Solo 3G system chassis.
4. Restart the K2 Solo 3G system.
5. Using Storage Utility on the K2 Solo 3G system, bind disks as RAID 0.
6. Restart the K2 Solo 3G system.
7. Using Storage Utility on the K2 Solo 3G system, make a new file system.

   Restart as prompted.

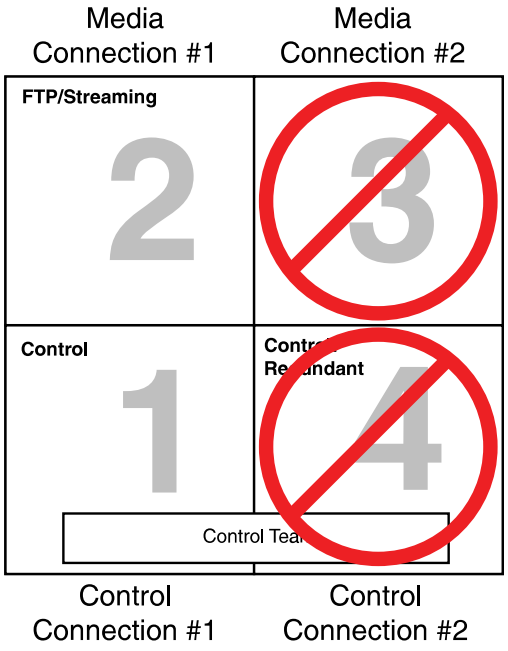
Always use the Storage Utility to physically identify the failed drive. To identify a drive, in Storage Utility right-click the drive and select **Identify**. This causes the disk lights to flash.

Refer to related topics in the "Configuring the K2 System" section of this Topic Library for Storage Utility procedures.

To remove and insert a drive, refer to the mechanical procedure for disk module removal.

About networking

When you receive a K2 Solo 3G system from the factory, it has a specific network configuration, including a loopback adapter and two of the four Gigabit Ethernet ports configured as a teamed pair. The Gigabit Ethernet ports, as viewed when looking at the rear panel, are represented in the following illustration.



Restoring network configuration

When you restore a system from its system specific image, network configuration is also restored to the factory default settings. This is the recommended method of restoring network configuration.

However, if for some other reason you must configure network settings manually, use the tasks in this section to restore the default network configuration.

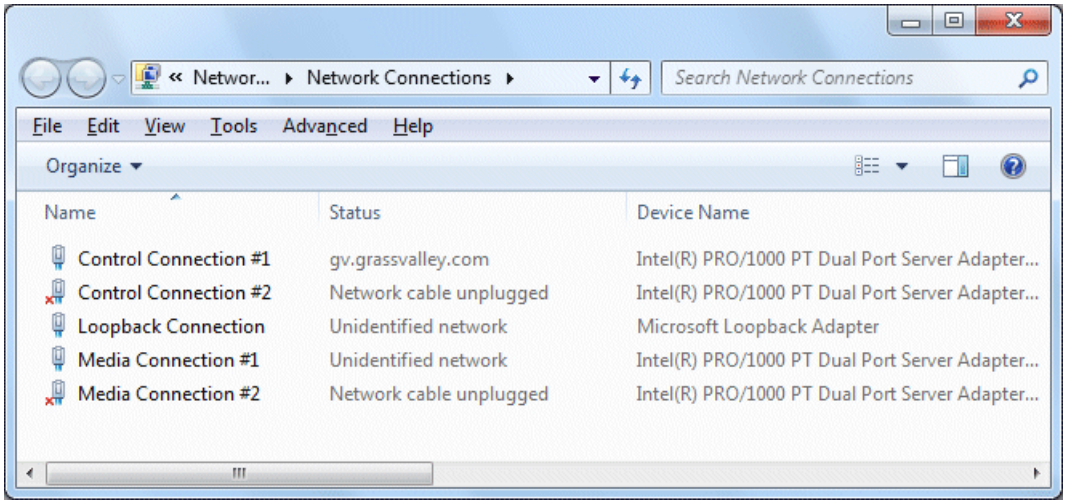
Create the Control Team

Before beginning this task, make sure of the following:

- Adapters are named

NOTE: Team control ports only. Do not team media ports.

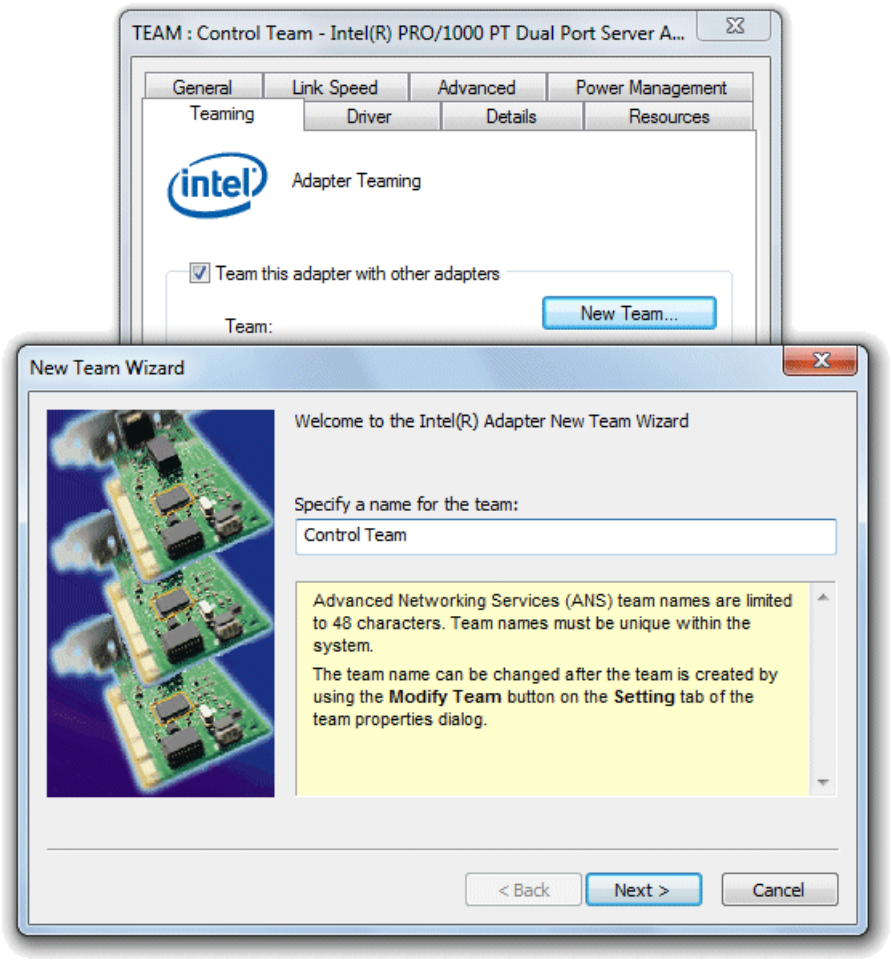
1. If K2 software is installed, disable the write filter, if it is not already disabled.
2. Open Network Connections, if it is not already open.
   a) From the Windows **Start** menu, in the **Run** or the **Search programs and files** box, type `ncpa.cpl` and press **Enter**.
3. In Network Connections, view **Details** and identify the adapter name that maps to Control Connection #1 and the adapter name that maps to Control Connection #2.



4. Right-click the adapter name that maps to Control Connection #1.
5. Select **Properties**, then click **Configure**.

   The Properties dialog box opens.

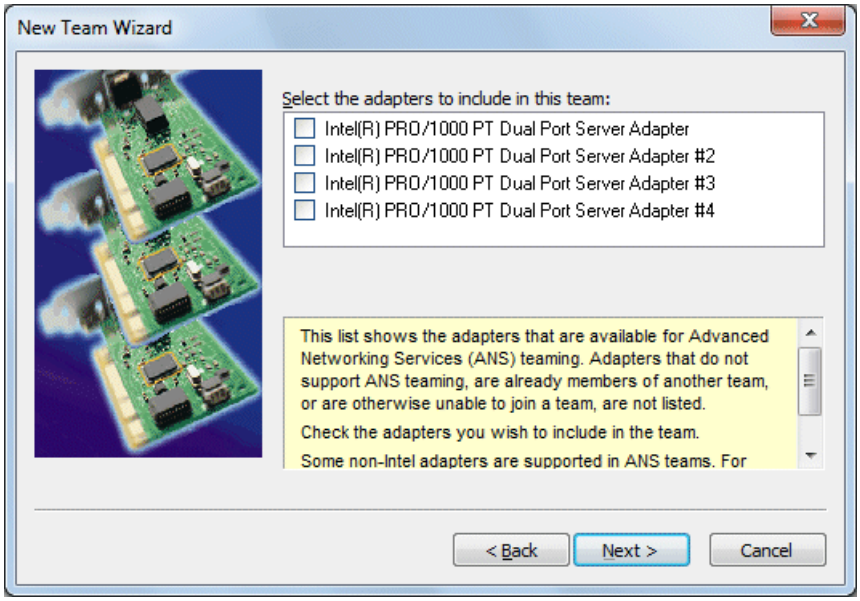
6. Select the **Teaming** tab.



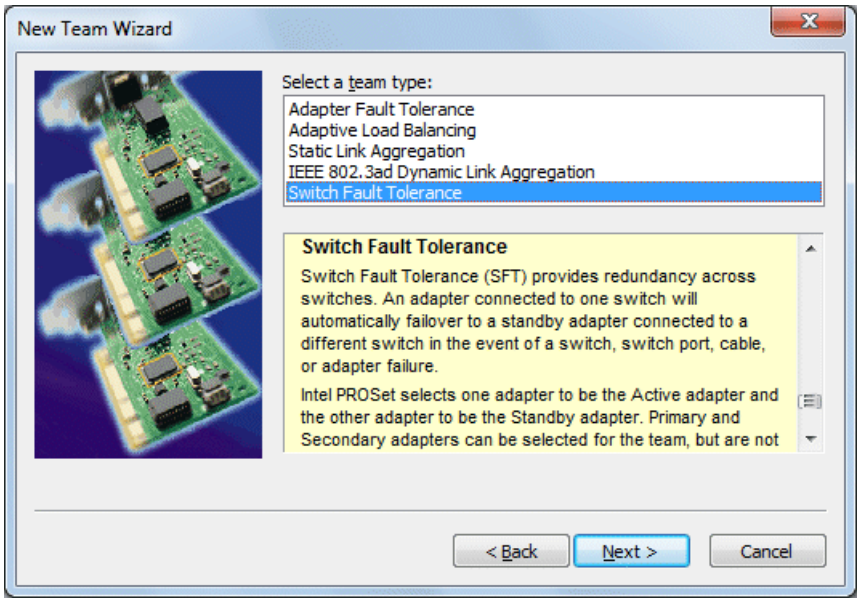
7. Select **Team this adapter with other adapters**, then click **New Team**. The New Team Wizard opens.

8. Enter Control Team.

   Click **Next**.



9. Select the check box for the adapter name that maps to Control Connection #1 and for the adapter name that maps to Control Connection #2. Click **Next**.



10. Select **Switch Fault Tolerance**. Click **Next**.
11. Click **Finish** and wait a few seconds for the adapters to be teamed.

12. Open the Modify Team dialog box as follows:
    a) In **Device Manager | Network Adapters**, right-click **Control Team** and select **Properties**. The Properties dialog box opens.
    b) Select the **Settings** tab.
    c) Click **Modify Team**. A dialog box opens.
13. On the **Adapters** tab, do the following:
    a) Select the top entry, which is the adapter name that maps to Control Connection #1 and click **Set Primary**.
    b) Select the adapter name that maps to Control Connection #2 and click **Set Secondary**.
14. Click **OK** and **OK** and to close dialog boxes.
15. Restart the K2 Solo 3G system.

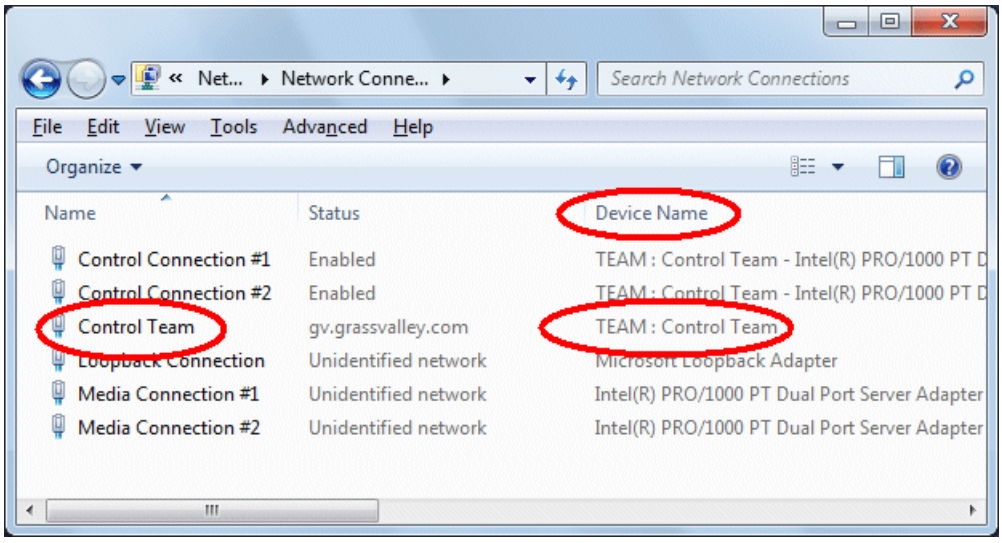
Next, proceed as follows:

- If network configuration is complete, enable the write filter.
- If continuing with network configuration, your next task is to name team and loopback.

Name team and loopback

- Adapters must be named
- The control team must be created

1. If K2 software is installed, disable the write filter, if it is not already disabled.
2. On the Windows desktop right-click **Start | Control Panel | Network and Sharing Center | Change adapter settings**. The Network Connections window opens.



3. For the Control Team and the loopback, select adapter names in the "Device Name" column and rename them as follows:
   a) Select the adapter name.
   b) Select **File | Rename** to enter rename mode.
   c) Type the name, as specified in the following table:

In the Device Name column, select this adapter name…	And rename it as follows:
TEAM : Control Team	Control Team

4. Do one of the following:
   - If you intend to use SiteConfig for device discovery and IP address configuration, you do not need to set an IP address for the Control Team at this time. You are done with this procedure.
   - If you are not using SiteConfig, set an IP address for the Control Team at this time. Use standard Windows procedures.

   NOTE: Do not set IP addresses for the two Media Connections.

Next, proceed as follows:

- If network configuration is complete, enable the write filter.
- If continuing with network configuration, your next task is to reorder adapters.

Reorder adapters

- Adapters must be named correctly
- The control team must be created
- The team and loopback must be named

1. If K2 software is installed, disable the write filter, if it is not already disabled.
2. Open Network Connections, if it is not already open.
   a) From the Windows **Start** menu, in the **Run** or the **Search programs and files** box, type `ncpa.cpl` and press **Enter**.

   The Network Connections window opens.
3. Select **Advanced**, then **Advanced Settings…**

4. On the **Adapters and Bindings** tab, depending on the K2 system storage, order adapters as follows:

Internal or direct-connect storage	Shared (SAN) storage
Loopback	Control Team
Control Team	Control Connection #1
Control Connection #1	Control Connection #2
Control Connection #2	Media Connection #1
Media Connection #1	Media Connection #2
Media Connection #2	Loopback
1394 Connection	1394 Connection

   If controlled by Dyno Production Assistant, refer to Dyno PA documentation for adapter order.

5. Click **OK** to close and accept the changes.
6. Close Network Connections.

Enable the write filter. Network configuration is complete.

Next, enhance network bandwidth.

Enhance network bandwidth

On K2 Summit/Solo systems with K2 system software 9.x, the on-board network adapters have a performance limitation that causes them to function at half the expected bandwidth. On most systems, there are no symptoms related to this limitation, as network traffic is below the limitation. Systems using ShareFlex or having other requirements for high network bandwidth might be impacted to some degree. Symptoms include general network bandwidth restrictions, slow iSCSI I/O performance, slower than expected FTP traffic, and other slowness not caused by other factors.

Grass Valley requires that you remove the limitation and enhance the network performance. Once the limitation is removed, the change persists throughout normal software upgrades. However, if you reimage the K2 Summit/Solo system you must check and reapply the change if necessary.

To remove the limitation, disable "Large Send Offloads" on the network adapters and disable "CPU Power Technology" in the BIOS.

Refer to Grass Valley Knowledge Base Article *#000011688* for more information.

Disable Large Send Offloads

1. From the Windows operating **Start** menu, open **Control Panel**.
2. In **Control Panel**, open **Network and Sharing Center**.

3. In **Network and Sharing Center**, select **Change adapter settings**.
   Network Connections opens and displays network adapters, including the following:
   - Control Connection #1
   - Control Connection #2
   - Media Connection #1
   - Media Connection #2
4. For each Control Connection and each Media Connection, do the following:
   a) Right-click the connection and select **Properties**.
      The **Connection Properties** dialog box opens.
   b) In the **Connection Properties** dialog box, click **Configure**.
      The **Adapter Properties** dialog box opens.
   c) In the **Adapter Properties** dialog box, click the **Advanced** tab.
   d) On the Advanced tab, in the Settings list select **Large Send Offload v2 (IPv4)** and then in the Value drop-down list select **Disabled**.
   e) Click **OK** to save settings and close.
   f) Repeat these steps for each Control Connection and each Media Connection.

Next, disable CPU power technology.

Disable CPU Power Technology

1. Restart the K2 Summit/Solo system.
2. During the BIOS startup screen, press **F2** repeatedly until `Entering Setup...` appears.
   The BIOS screen opens.
3. On the BIOS screen, use arrow keys and select the **Advanced** tab.
4. On the Advanced tab select **CPU Core Configuration** and then press **Enter**.
   The CPU Core Configuration screen opens.
5. On the CPU Core Configuration screen, select **Power Technology** and then press **Enter**.
   A **Power Technology** dialog box opens.
6. In the **Power Technology** dialog box select **Disable** and then press **Enter**.
7. Press **F4** to save and exit.
   A **Save & Exit Setup** dialog box opens.
8. In the **Save & Exit Setup** dialog box, select **Yes** and then press **Enter**.
9. The K2 Summit/Solo system restarts.

Next, install the SiteConfig Discovery Agent.

Checking services

Depending on storage type (standalone or shared) of the K2 Solo 3G system, various services are turned off or on or set to different startup types. These services are automatically set by the K2 Solo 3G system software installation program and by the Status Server service whenever the K2 Solo 3G system starts up.

***NOTE: Do not manually change the way services run on a* K2 Solo 3G system.**

If you suspect that services have been tampered with or for any reason are not set correctly, you can check their current settings in the Windows Services Control Panel. The table below provides the settings for the services that are critical to a correctly operating K2 Solo 3G system.

Services on a standalone storage K2 Summit 3G system

When a standalone K2 Solo 3G system with internal storage or a K2 Solo 3G system with direct-connect storage is operating normally, in the Services control panel services appear as follows:

Table 55: Standalone storage K2 Summit 3G system services

Service	Status	Startup Type	Comments
CvfsPM[28]	Started	Automatic	—
Grass Valley AppService	Started	Automatic	Depends on Status Server service.
Grass Valley Extent Manager Service	Started	Manual	Used to consolidate unused space (extents) at the end of proxy clips on an SNFS file system. Does not apply to non-SNFS file systems.
Grass Valley FTP Daemon	Started	Manual	Started by Status Server service on standalone storage models.
Grass Valley Host File Service	Started	Automatic	—
Grass Valley HTTP File Server	Started	Manual	Provides access to live streaming configuration (SDP) files.
Grass Valley Import Service	—	Manual	This is the service that provides the functionality for a K2 capture service. It is the service that automatically creates the K2 clip from the media files in the watched folder (source directory) and puts the K2 clip in the K2 media storage (destination bin).
Grass Valley K2 Config	Started	Automatic	Not used on standalone storage K2 Summit/Solo system.

[28] With SNFS version 3.5, this is the only service. Previous versions had StorNext File System service and StorNext File System RPC Port Mapper service.

Service	Status	Startup Type	Comments
Grass Valley MegaRaid Server	—	Manual	—
Grass Valley MetaDataService	Started	Manual	—
Grass Valley RTS Config Service	Started	Manual	—
Grass Valley SabretoothWS	—	Manual	Allows Macintosh systems to remotely check out a license.
Grass Valley Storage Utility Host	Started	Automatic	—
Grass Valley System Status Server	Started	Automatic	At startup the Status Server service makes sure the following services are started: AMP TCP Service; AppService; FTP Daemon.
GV STRATUS Summit Services	Started	Automatic	Required if part of a GV STRATUS system.
Microsoft iSCSI Initiator Service	Started	Automatic	Not used on a standalone storage K2 Summit/Solo system.
ProductFrame Discovery Agent Service	Started	Automatic	—
Sabretooth License Server	Started	Manual	—
Sabretooth Protocol Service	—	Manual	—

Checking pre-installed software

Software is pre-installed on K2 products when you receive them from the factory. This load of pre-installed software is referred to as the “golden drive”. The following list is an example of the software pre-installed. Check the "About This Release" section of the K2 Topic Library for the most up-to-date list with version information.

If you suspect that pre-installed software is not correct, use the recovery process to re-load the software. Do not attempt to un-install, install, or repair pre-installed software without guidance from your Grass Valley Support representative.

K2 Solo 3G system pre-installed software

- Intel Pro Software
- QuickTime
- Microsoft iSCSI Initiator

- MS XML
- .NET Framework
- MegaRAID — Do not use this utility on a K2 Solo 3G system. This utility is for use by qualified Grass Valley Service personnel only. When this utility is opened it scans the SCSI bus and interferes with record and play operations.
- J2SE Runtime Environment
- StorNext software
- Windows PowerShell
- Windows XP Embedded

Making CMOS settings

NOTE: This procedure is intended for use by Grass Valley Service personnel or under the direct supervision of Grass Valley Service personnel.

1. Connect keyboard, monitor, and mouse to the K2 Solo 3G system.
2. Restart the K2 Solo 3G system.
3. During the BIOS startup screen, watch the keyboard lights (capslock, numlock, etc.). When the lights flash, press **Delete** to enter Setup.
4. Press **F3** and then press **Enter**. This loads optimal default values for all the setup questions.
5. Press **F4** and then press **Enter** to save settings and restart.

Restoring disk controller configuration

Do this task when replacing the disk controller board.

This task can be used on any K2 Solo 3G system, but it is required on any system that has a Type II (ADLINK) CPU carrier module. This includes the first generation K2 Summit system, which can have a Type II CPU carrier module that was installed in the factory or that was upgraded in the field.

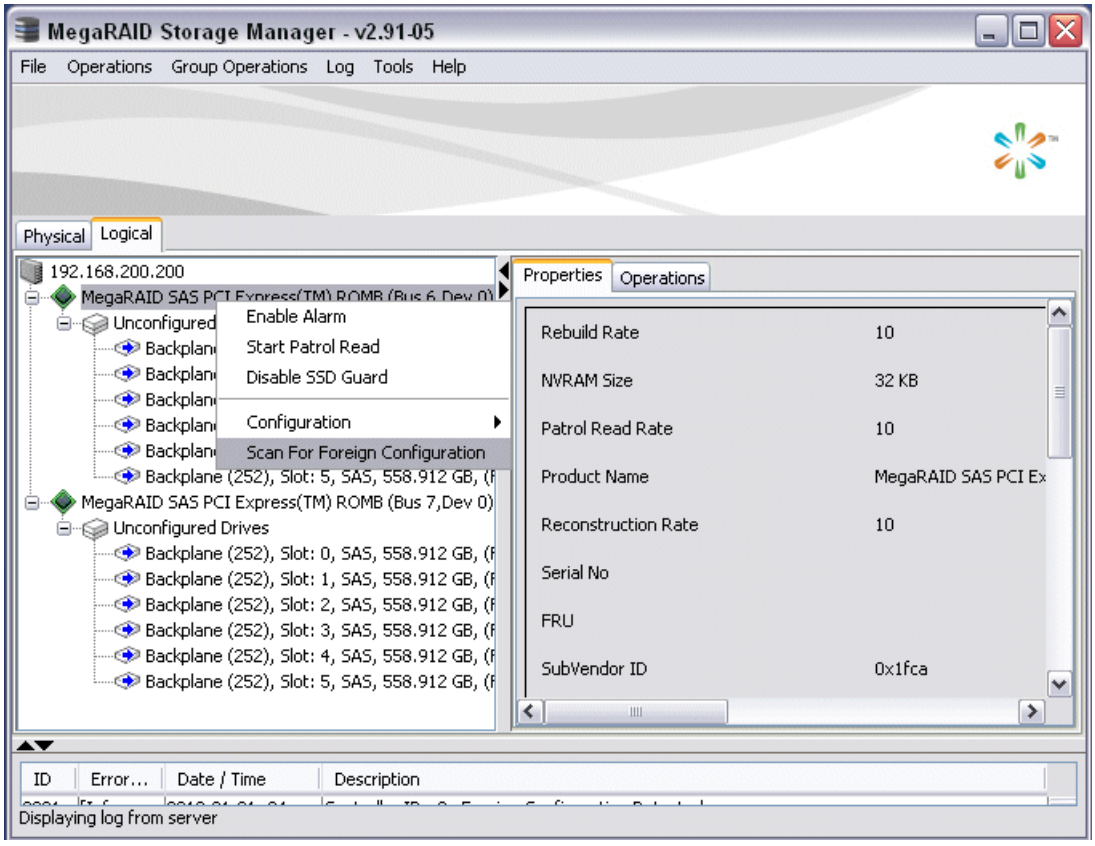
NOTE: This procedure is intended for use by Grass Valley Service personnel or under the direct supervision of Grass Valley Service personnel.

After you replace a disk controller board, you must import the configuration information from the existing disks. This allows the new board to see the LUNs as previously configured.

1. After replacing the disk controller board, power up the K2 Solo 3G system.

   Ignore SNFS messages that can open at any time during this procedure.
2. On the Windows desktop, open the **MegaRAID Storage Manager** icon.

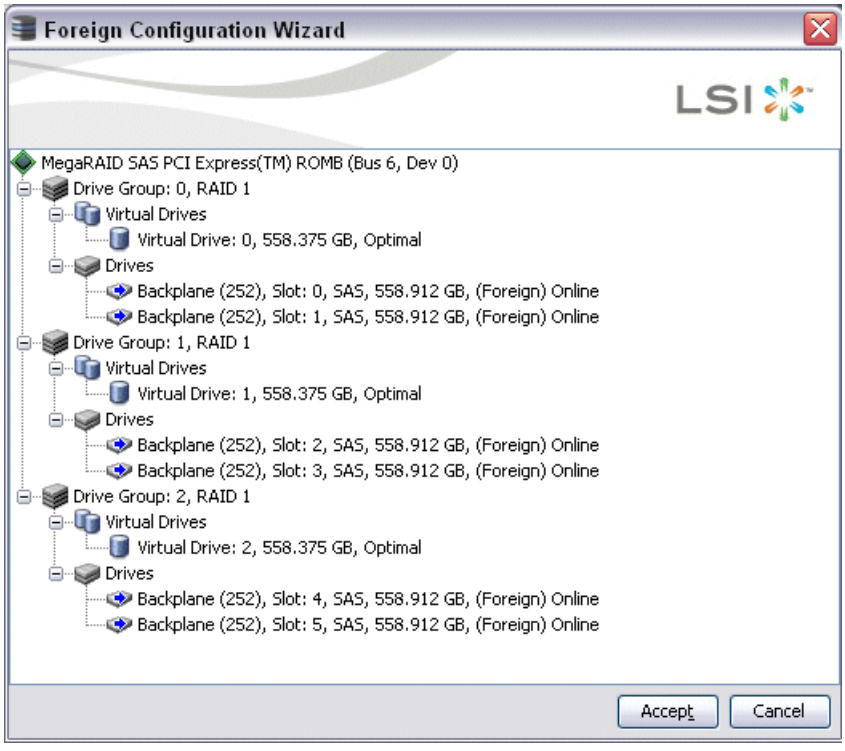
3. When prompted, enter administrator credentials.
   The MegaRAID Storage Manager main window opens.



4. In the MegaRAID Storage Manager main window tree-view, verify that drives are reported as "Unconfigured Drives".

5. In the tree-view, right-click the top controller and select **Scan For Foreign Configuration**.
   A Foreign Configuration Detected dialog box opens.

6. Make sure **Import** is selected and click **OK**.
   A Foreign Configuration Wizard opens.



7. Click **Accept**.
8. When prompted "...import?", click **Yes**.
9. When informed "...imported successfully", click **Yes**.

10. In the MegaRAID Storage Manager main window tree-view, verify that one controller reports configured drives and one controller reports unconfigured drives.
11. For the controller with unconfigured drives, repeat previous steps to import the foreign configuration.
12. When you have imported the foreign configuration for both controllers, click **File | Exit** to close MegaRAID Storage Manager.
13. Restart the K2 Solo 3G system.

Recovering the media database

This section provides topics about recovering the media database.

About the automatic database backup process

Every 15 minutes the K2 system checks to see if any media operations have changed the media database. If a change has occurred, the K2 system creates a backup file of the media database. The backup file is saved in the same directory as the media database using a rotating set of three file names. These files are named *media.db_bakX* where X is the number in the rotation. Each time a backup occurs, the oldest backup file is overwritten. If some condition renders one of the backup files un-writable, the backup file following that in the rotation is subsequently used for every backup until the condition is resolved.

Identifying a corrupt media database

The following symptoms could indicate a corrupt media database:

- On startup, the Grass Valley MetaDataService is unable to start. This is indicated in the Services control panel if the Grass Valley MetaDataService does not display as Started.
- The K2 log displays a "…file is encrypted or is not a database…" error.

As soon as you suspect a corrupt media database, stop all media access and take the K2 system offline.

Restoring the media database

1. Stop all media access and take the K2 system offline.
2. Navigate to the V:\media directory.
3. Make a copy of the media.db and media.db_bak* files and store them in a secure location.
4. Stop the Grass Valley MetaDataService as follows:

   For the standalone K2 system, use the Services control panel to stop the service.
5. Determine which backup file is the most recent good file by examining the file modification date on each backup file.
6. Rename the current *media.db* file (which is assumed to be corrupt) to another name, and rename the most recent good *media.db_bakX* file to *media.db*.
7. Restart the K2 system following normal procedures.
8. Confirm that the systems come up correctly with the restored database now in place.

9. Use Storage Utility **Clean Unreferenced Files** and **Clean Unreferenced Movies** to repair any inconsistencies between the contents of the database and the file system.

Using recovery images

This section provides topics about using recovery images.

About the recovery image process

An image of the K2 Solo 3G system system drive is provided with the product package. You can restore the K2 Solo 3G system from this image. This simplifies the process of rebuilding a system in a disaster recovery scenario.

NOTE: This process is not intended as a means to backup and restore media.

When you receive your K2 Solo 3G system new from the factory, you receive a system-specific image for that particular K2 Solo 3G system. This factory image is stored on a bootable USB Recovery Flash Drive. Also on the Recovery Flash Drive is the Acronis True Image software necessary to create and restore an image. You can find the Recovery Flash Drive in a holder in the front bezel assembly.

After your K2 Solo 3G system is installed, configured, and running in your system environment, you should create a new recovery image to capture settings changed from default. This "first birthday" image is the baseline recovery image for the K2 Solo 3G system in its life in your facility. There is enough space on the Recovery Flash Drive to store the first birthday image along with the factory image.

You should likewise create a new recovery image after completing any process that changes system software or data, such as a software upgrade. In this way you retain the ability to restore your K2 Solo 3G system to a recent "last known good" state.

NOTE: The recovery image process is an "off-line" process. Do not attempt this process while media access is underway.

The recovery image process that you should follow is summarized in the following steps.

- **At the K2 Solo 3G system first birthday…**

  Boot from the Recovery Flash Drive.

  Create a recovery image for the K2 Solo 3G system.

  Create a recovery image for the Control Point PC.

- **At milestones, such as software upgrades…**

  Boot from the Recovery Flash Drive.

  Create a recovery image for the K2 Solo 3G system.

- **If you need to restore the K2 Solo 3G system…**

  Boot from the Recovery Flash Drive.

  Read the image from the Recovery Flash Drive or from the location that you stored the image.

- **If you need to restore the Control Point PC…**

  Boot from the Recovery Flash drive.

  Read the image from the location that you stored the image.

Use the following procedures to implement the recovery image process as necessary.

Creating a recovery image

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

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

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

      A MS-DOS command window opens.

   c) When prompted with a list of options, type `2` to select the Acronis option and then press **Enter**.

   The Acronis program loads.
4. In the Acronis main window, click **Backup**.

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

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

      If a "…choose full backup mode…" message appears, click **OK**.
7. On the Backup Archive Location page, do the following:
   a) in the tree view select **Removable Disk (D:)** and enter the name of the image file you are creating.

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

      For example, if the hostname is MySystem1, in the File name field you enter `A:\MySystem1_20121027.tib`.

   b) Click **Next**.
8. On the Select Backup Mode page, select **Create a new full backup archive** and then click **Next**.
9. On the Backup Options page, do not change any settings. Click **Next**.

10. On the Archive Comment page, if desired, enter image comments such as the date, time, and software versions contained in the image you are creating. Click **Next**.
11. On the "…ready to proceed…" page, do the following:
    a) Verify that you are creating an image from the C: drive and writing to the D:\ drive, then click **Proceed**.

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

    The machine restarts automatically.
15. Remove the recovery media while the machine is shutting down.

Restoring from a system-specific recovery image

Use this task to restore a K2 Solo 3G system using an image made from that particular K2 Solo 3G system. If restoring from a generic factory default image, use the appropriate task.

Before restoring from a recovery image, make sure that the K2 Solo 3G system has access to the image from which you are restoring. This task provides instructions for accessing an image on the Recovery Flash Drive. If you access an image from a different location, such as a network connected drive or another connected USB drive, alter the steps in this task as appropriate.

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

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

      A MS-DOS command window opens.
   c) When prompted with a list of options, type `2` to select the Acronis option and then press **Enter**.

   The Acronis program loads.
4. In the Acronis main window, click **Recovery**.

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

   NOTE: Verify capacity to make sure you select the boot media card (CompactFlash or mSATA) and not a media drive. The boot media has a much smaller capacity and has an interface identified as "IDE (0) Primary Master".

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

    NOTE: Verify capacity to make sure you select the boot media card (CompactFlash or mSATA) and not a media drive. The boot media has a much smaller capacity and has an interface identified as "IDE (0) Primary Master".

14. On the Restored Partition Type page, select **Active** and then click **Next**.
15. Do one of the following:

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

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

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

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

    The machine restarts automatically.

23. Remove the recovery media while the machine is shutting down.
24. When prompted, enter the K2 Solo 3G system machine name.

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

    After start up, one or more device discovery windows can open. Allow processes to complete without interference. Refer to Release Notes for informaion on compatible driver versions. If a Fibre Channel card driver, ignore until instructed later in this process.

    At first start up after reimage, the system is in Embedded Security Update mode by default.

Next, check the adapter names and order. If adapter names and order are not as documented, restore network configuration.

About saving and restoring settings while reimaging

If you are reimaging a K2 Solo 3G system with a generic disk image, you can run scripts to save the media file system and other settings before the reimage, then restore the settings after the reimage. Setting are saved and restored as follows:

- Media file system (SNFS): You run scripts to save and restore these settings. After the settings are restored, on a standalone system you can access the media in the local media storage. On a SAN-attached system, K2Config settings are restored so you can access media on the shared media storage.
- SID, computer name, and network settings: You run the script to save settings to a text file, so you can manually reconfigure as desired after the reimage.

If the media file system and settings are valid (not corrupt) on the K2 Solo 3G system before the reimage, it is recommended that you use the save/restore scripts to save your media and settings, thus saving time in the reimage process. However, if the media file system or settings are corrupt and your purpose for reimaging is to remove the corruption, it is likely that you do not want to use the save/restore scripts.

Saving settings before generic reimage

1. If you are working on a K2 client SAN-attached system, record iSCSI bandwidth settings, so you can reconfigure after removing and readding to SAN.
2. Make sure you are logged in to the K2 Solo 3G system with administrator privileges.
3. Connect the USB Recovery Flash Drive to a USB port on the K2 Solo 3G system.
4. On the USB Recovery Flash Drive, navigate to the following location:

   `\tools\SaveRestoreScripts.`

   NOTE: Do not attempt to use the same Recovery Flash Drive on multiple systems.
5. Run the following and wait for the process to complete:

   `ssave.bat`

   This saves current settings onto the USB Recovery Flash Drive in the `\settings` directory.
6. Disconnect the USB Recovery Flash Drive.

Restoring from a generic image

This task can be used on a K2 Solo 3G system that needs to be restored to its factory default state. For example, if you neglected to make a first birthday image, you might need to use this procedure. If the image from which you are restoring was made from the specific machine, refer to the appropriate procedure.

This task provides instructions for accessing an image on the Recovery Flash Drive. If you access an image from a different location, such as a network connected drive or another connected USB drive, alter the steps in this task as appropriate. There can be multiple versions of the generic recovery disk image on the Recovery Flash Drive. Refer to related topics in the "About This Release" section of the K2 Topic Library to determine which version you should use.

NOTE: This procedure restores the* K2 Solo 3G system *to its factory default condition. Passwords and other site-specific configurations are reset to factory defaults.

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

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

      A MS-DOS command window opens.

   c) When prompted with a list of options, type `2` to select the Acronis option and then press **Enter**.

   The Acronis program loads.
4. In the Acronis main window, click **Recovery**.

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

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

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

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

16. On the Restored Partition Size page, do one of the following:
    - If **Free space after** reports 0 bytes, leave settings as they are. Click **Next**.
    - If **Free space after** does not report 0 bytes, increase **Partition size** until **Free space after** reports 0 bytes. Click **Next**.
17. On the Next Selection page, select **No, I do not** and then click **Next**.
18. On the Restoration Options page, do not make any selections. Click **Next**.
19. On the "…ready to proceed…" page, verify that you are restoring the correct image to the correct location. Click **Proceed**.
20. On the Operation Progress page, observe the progress report.
21. When a message appears indicating a successful recovery, click **OK**.
22. Click **Operations | Exit** to exit the Acronis True Image program.

    The machine restarts automatically.
23. Remove the recovery media while the machine is shutting down.
24. Upon startup, wait for initialization processes to complete. This can take several minutes, during which time USB keyboard/mouse input is not operational. The system might automatically restart. Do not attempt to shutdown or otherwise interfere with initialization processes.
25. When prompted, enter the K2 Solo 3G system machine name.

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

    After start up, one or more device discovery windows can open. Allow processes to complete without interference. Refer to Release Notes for informaion on compatible driver versions. If a Fibre Channel card driver, ignore until instructed later in this process.

    At first start up after reimage, the system is in Embedded Security Update mode by default.

Next, check the adapter names and order. If adapter names and order are not as documented, restore network configuration.

Restoring settings after generic reimage

Settings must be saved using *ssave.bat* before reimaging the K2 Solo 3G system, and the reimage (Acronis) process must be complete.

1. If you have not already done so, start up the K2 Solo 3G system and log on with administrator privileges.

   The administrator password is `adminGV!`.
2. Connect the USB Recovery Flash Drive to a USB port on the K2 Solo 3G system.
3. From the USB Recovery Flash Drive, run the following and wait for the process to complete:

   Tools\SaveRestoreScripts\srestore.bat

Next, do the following as appropriate to restore your K2 Solo 3G system. Refer to related topics in this document or as otherwise indicated.

1. Restore network configuration. If you saved settings with *ssave.bat*, refer to *C:\ipconfig.txt* for the complete listing of the network settings that the K2 Solo 3G system had before reimaging.
2. Enhance network bandwidth.
3. Install the SiteConfig Discovery Agent.

4. If you install software with SiteConfig, do the following:
   - Take Embedded Security out of Update mode.
   - Install SNFS software and K2 software using SiteConfig.
   - Restore SabreTooth licenses.
5. If you install software manually (without SiteConfig), do the following:
   - Install SNFS software and K2 software manually.
   - Restore SabreTooth licenses.

   If you saved/restored settings with `ssave.bat` and `srestore.bat`, SNFS uses the restored settings. Refer to related topics in the "About This Release" section of the K2 Topic Library.
6. Check the Windows operating system clock, and if necessary, set it to the correct time.
7. Activate Windows within 30 days.

Installing the Discovery Agent on a K2 Solo system

If the device that you plan to manage with SiteConfig does not have a SiteConfig Discovery agent installed, use this topic to verify and, if necessary, manually install SiteConfig support software. Doing so allows SiteConfig to discover and manage the device. If the device has any version of the SiteConfig Discovery Agent currently installed, you should use SiteConfig to upgrade the Discovery Agent, rather than installing it manually.

1. On the device you plan to manage with SiteConfig, open the Windows Services Control Panel and look for the following required item:
   - ProductFrame Discovery Agent
2. Proceed as follows:
   - If you find the required items, no further steps are necessary. SiteConfig support software is installed.
   - If a required item is not present, navigate to your SiteConfig files. If you do not already have these files in convenient location, you can find them on the PC that hosts SiteConfig, in the SiteConfig install location. Then continue with next steps as appropriate.
3. To launch the program that installs the ProductFrame Discovery Agent Service do the following:
   a) Copy the `Discovery Agent Setup` directory to the device.
   b) In the directory, double-click the `DiscoveryAgentServiceSetup.msi` file.

      The setup program launches to install the SiteConfig Discovery Agent.
   c) Follow the setup wizard.
4. When presented with a list of device types, select the following:
   - K2SoloStandaloneClient
5. Complete the setup wizard and restart the device.

   The restart is required after the installation.

Using diagnostic tools

Use the following sections as necessary to identify problems.

Running Check Disk

If your K2 Solo 3G system has a critical system fault, you should run Check Disk to identify and remove any corrupted files.

1. Make sure the K2 Solo 3G system 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:

      ```
      ...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 Solo 3G system.

Running diagnostics for K2 Solo 3G system

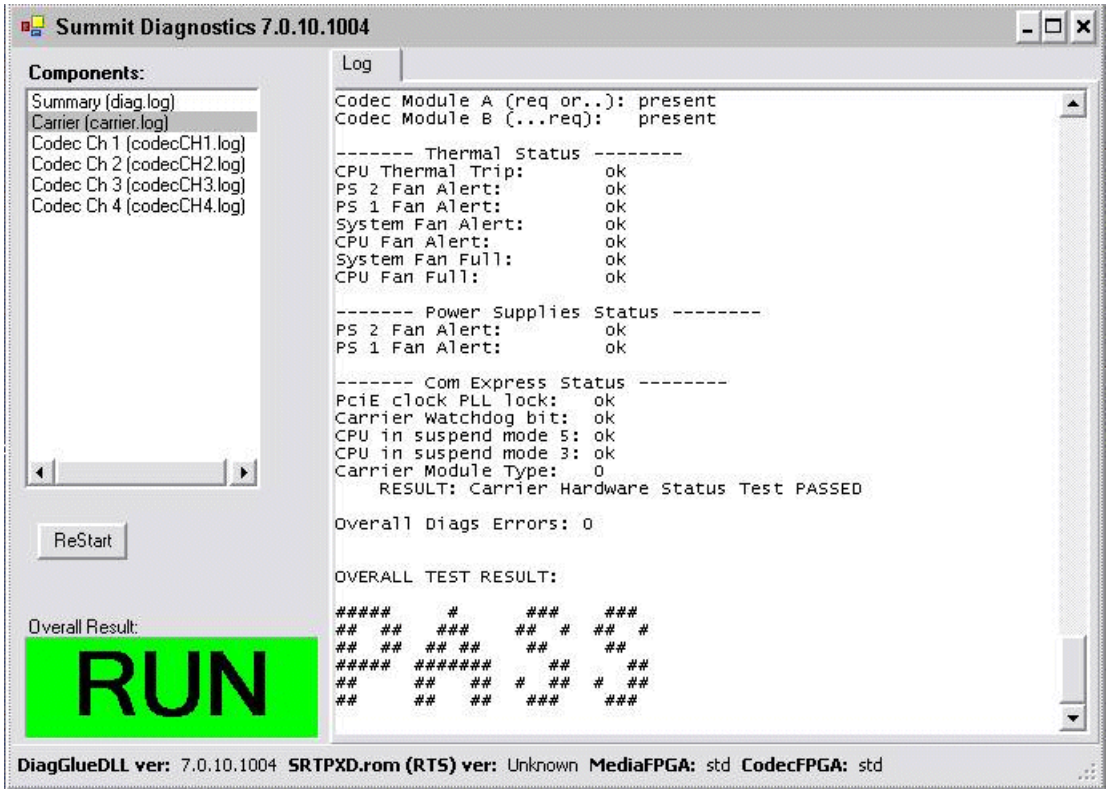
If you suspect a problem with K2 Solo 3G system hardware, you can run diagnostics and check for errors.

1. Make sure all media access is stopped on the K2 Solo 3G system. 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 Solo 3G system.

   You must restart before you can use the K2 Solo 3G system. Running diagnostics puts the real time processor and other services in a non-production state.

Troubleshooting problems

Step 1: Check configurations

Many times what appears to be a K2 Solo 3G system fault is actually an easy-to-fix configuration problem. Check settings in Configuration Manager and verify that the system is configured as you expect. Refer to related topics in the "Using K2 AppCenter" section of the K2 Topic Library and the "Configuring the K2 System" section of this Topic Library.

Step 2: Check connections and external equipment

Loose or improperly connected cables are the most likely source of problems for the system. A quick check of all the cable connections can easily solve these problems. Refer to related topics in the "Configuring the K2 System" section of this Topic Library for help with making connections. Check external equipment if you suspect a failure in a device connected to the K2 Solo 3G system.

Step 3: Check system status messages

While the K2 Solo 3G system is in operation, some problems are detected and reported in system status messages. To view system status messages, in AppCenter select **Help | System Status**.

When connecting to a K2 Solo 3G system from a control point PC using remote AppCenter, if there is an AppCenter system startup error, the error is reported during the connection attempt.

If the system status message indicates a problem, refer to related topics in "K2 Summit Production Client Service Manual".

NOTE: Do not use the MegaRAID utility on a* K2 Solo 3G system*. This utility is for use by qualified Grass Valley Service personnel only. When this utility is opened it scans the SCSI bus and interferes with record and play operations.

Step 4: Identify problems using the startup sequence

The startup sequence is your primary tool for identifying a K2 Solo 3G system fault. As the different levels of the K2 Solo 3G system system become operational in the startup process, the primary components of the system are checked. You can identify most problems by evaluating the messages and other indicators that occur during the startup sequence.

NOTE: This procedure assumes that the* K2 Solo 3G system *is not in Storage Utility's "offline" mode.

To identify problems using the startup sequence, do the following:

1. Connect mouse, keyboard, and monitor. You must observe the VGA screen and be able to interact with the system via keyboard and mouse to fully identify problems.
2. Restart the K2 Solo 3G system.

3. Once the startup sequence begins, observe the progression of behaviors as listed in the following table. These are the behaviors you should expect for a normally operating K2 Solo 3G system. If you observe behaviors other than those listed, refer to the indicated troubleshooting topics to identify problems.

   NOTE: You can press the Pause/Break key on the keyboard to keep startup text on the screen for longer viewing.

At about this time…	This behavior should occur…	If not, refer to the following:
—	Pressing the standby button starts the K2 Solo 3G system.	*Shutdown/restart problems* on page 876
0 seconds	Power on LED goes on and stays on.	*Power supply problems* on page 879
	Service LED stays off.	*Shutdown/restart problems* on page 876
	Front bezel assembly and processor fan start.	*Windows startup problems* on page 878
10 seconds	System BIOS screen appears.	*BIOS startup* on page 877
35 seconds	Grass Valley logo screen appears.	—
70 seconds	Windows logon screen appears.	*Windows startup* on page 877

Logon to Windows to continue the startup sequence.

After Windows logon:

At about this time…	This behavior should occur…	If not, refer to the following:
0 seconds	Grass Valley logo desktop appears.	*K2 Solo 3G system startup* on page 878
5 seconds	Service LED goes on for a few seconds, then off.	
20 seconds	Desktop icons, startbar, and AppCenter logon box appear.	*Windows startup* on page 877, *K2 Solo 3G system startup* on page 878

Logon to AppCenter to continue the startup sequence.

After AppCenter logon:

At about this time…	This behavior should occur…	If not, refer to the following:
0 seconds	System Startup messages appear.	*K2 Solo 3G system startup* on page 878

At about this time…	This behavior should occur…	If not, refer to the following:
Time varies. Between 30 seconds and 2 minutes.	All system components check out as OK and AppCenter opens. Media operations are functional.	*Operational problems* on page 881

Shutdown/restart problems

If the K2 Solo 3G system is inoperable due to an error it can affect the operation of the standby button. If pressing the standby button does not shut down the K2 Solo 3G system, press and hold the button for five seconds. This forces the K2 Solo 3G system to execute a hard power down. If that doesn't work or if after the hard power down the system does not boot, disconnect then reconnect the power cable(s).

The K2 Solo 3G system is set to attempt to boot from a USB drive first, before it boots from the boot media card. If you have a drive connected to a USB port that does not contain an appropriate operating system and you start up the K2 Solo 3G system, an error message is displayed and the boot up process halts.

Checking external equipment

This section provides troubleshooting procedures for external devices that connect to the K2 Solo 3G system. Before using these procedures, first check connections.

VGA display problems

Problem	Possible Causes	Corrective Actions
Screen turns on, but nothing from K2 Solo 3G system is displayed.	VGA connector or cable is not connected or is faulty.	Replace VGA monitor.
	K2 Solo 3G system system settings have been tampered with.	Restore default settings by restoring the system drive image from a recent backup image.

Keyboard and mouse problems

The keyboard and mouse are detected during BIOS startup. There should be a very brief message displayed indicating detection of input devices connected to USB ports

Problem	Possible Causes	Corrective Actions
The K2 Solo 3G system does not respond correctly when one or more of the keys on the keyboard are pressed or the mouse is used.	The keyboard or mouse is faulty.	Replace the keyboard or mouse.
	K2 Solo 3G system system settings have been tampered with.	Restore default settings by restoring the system drive image from a recent backup image.

Power connection sequence

The following table lists the sequence of behaviors you should expect to see and/or hear as you connect the first power cable to a normally operating K2 Solo 3G system. If you observe behaviors other than those listed, refer to related topics in "K2 Summit Production Client Service Manual" to investigate potential problems.

In this time…	On the K2 Solo 3G system front panel or chassis, look/listen for the following…	If not, refer to the following.
0 seconds	Power supply fans go on and stay on.	*Power supply problems* on page 879
	Power on LED goes on and stays on.	
	Drive busy LED goes on then off.	*Media disk problems* on page 883

This power connection sequence assumes that before power was removed, the K2 Solo 3G system was properly shut down from AppCenter, from the Windows operating system, or from the standby button. If the power was removed without a proper shutdown, when the first power cord is connected the K2 Solo 3G system might go directly to the startup sequence.

BIOS startup

A few seconds after startup, on the VGA monitor a screen displays BIOS information, with instructions about how to access settings. While this information is displayed, press the key on the keyboard as instructed to enter the BIOS settings pages. When the BIOS completes the Windows operating system begins to load.

If during the BIOS time a message appears that requires your input or if the K2 Solo 3G system does not progress to Windows startup, it indicates a problem at the motherboard level. To correct problems of this nature, contact Grass Valley Support.

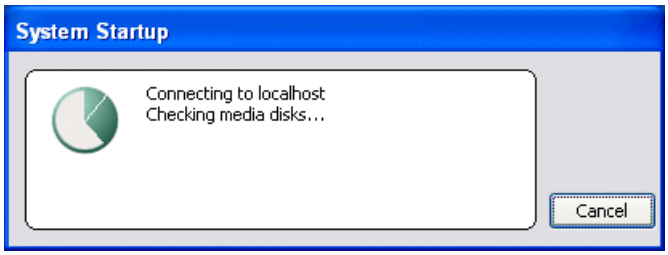
Windows startup

After the host startup processes complete the Windows operating system starts up. Normally the Windows operating system completes its processes automatically without the need to press keys or respond to messages. When the Windows startup is complete the Windows logon dialog box is displayed.

If the Windows startup screen does not proceed automatically or if a message appears that requires your input, it indicates a problem at the operating system level. If the problem cannot be corrected with a supported procedure (such as networking), the Windows operating system is not operating as it should. To correct problems of this nature, restore the system drive image.

K2 Solo 3G system startup

After the Windows operating system startup processes complete, you must log in to AppCenter to trigger K2 Solo 3G system startup processes to begin. The K2 Solo 3G system determines that system health is adequate by checking critical subsystems. Critical subsystems are those upon which the K2 Solo 3G system depends for core media functionality. Critical subsystem checks are displayed in the System Startup message box.



When all critical subsystem checks are successful, AppCenter opens. If a critical error occurs, a message appears and AppCenter does not open. You can check the list of the messages that can appear.

To correct problems revealed at system startup, use the indicated troubleshooting information from the following sections.

Windows startup problems

Problem	Possible Causes	Corrective Actions
A "Non-system disk. Press any key to restart" message appears.	A non-bootable USB drive is connected.	Remove the USB drive, then press any key to continue.
	The boot media is corrupted.	Restore from the USB Recovery Flash Drive.

Thermal problems

Problem	Possible Causes	Corrective Actions
The K2 Solo 3G system overheats. This can be accompanied by a StatusPane message indicating a temperature or fan problem.	Airflow is blocked. The fan module is not operating correctly.	Ensure adequate airflow around the K2 Solo 3G system. Inspect the fans in the front bezel assembly and its connections for proper operation. If the fans are not operating correctly, replace the front bezel assembly.

Codec board problems

Investigate the problem further as described in the following table. If the problem persists, contact Grass Valley Support.

Problem	Possible Causes	Corrective Actions
A system status message indicates a problem with the codec board.	The codec module is not connected properly or is faulty.	Check the codec board indicator (LED) on the rear panel. Visually inspect codec module. Make sure it is connected properly and there is no sign of physical damage. Restart the K2 Solo 3G system. If the problem persists, replace the codec module.

Power supply problems

Problem	Possible Causes	Corrective Actions
The K2 Solo 3G system will not power on or power fails while the K2 Solo 3G system is in operation. This can be accompanied by a StatusPane message indicating a power supply problem prior to the failure.	The power source is faulty.	Make sure your power source is reliable.
	A power cord is faulty.	Both power supplies run and the K2 Solo 3G system can operate with just one power cord connected. Connect one power cord at a time and test with a replacement cord.
	The K2 Solo 3G system is too hot. The built-in overtemperature protection can shut down the power supply.	Check for thermal problems. Cool the K2 Solo 3G system.
	The power supply is faulty. This is indicated if the front panel power indicator does not come on.	Replace the power supply.
Power supply "~AC" LED is amber	Over temperature due to air flow restriction.	Check for and remove any air flow blockage around the power supply.
	Over temperature due to power supply fan failure.	Visually inspect fan. Listen for fan noise. If faulty, replace power supply.

Problem	Possible Causes	Corrective Actions
	Over current, under voltage, over voltage. These conditions could be caused by a faulty FRU module.	Disengage all FRU modules, then re-engage one at time. If one module causes the amber LED to go on, replace the module. If both power supplies have the amber LED, disengage one, then the other. If doing so results in just one power supply having the amber LED, replace that power supply.

Video problems

For the corrective actions in this section, refer to related topics in the "Using K2 AppCenter" section of the K2 Topic Library for detailed instructions.

Problem	Possible Causes	Corrective Actions
The picture level modulates at a particular frequency.	There is distortion in the video input signal.	Check the video input signal for distortion. Compare with test color bars and audio test tone.
In stop mode the still-play video shows some motion jitter.	Two fields are displayed in still play mode.	Switch the still-play mode setting to Field.
The video displays erratically moving green lines.	K2 Solo 3G system is not locked to a video reference.	Lock the K2 Solo 3G system to a video reference.

Audio problems

For the corrective actions in this section, refer to related topics in the "Using K2 AppCenter" section of the K2 Topic Library for detailed instructions.

Problem	Possible Causes	Corrective Actions
No record audio.	Wrong audio input selected.	Select the correct audio input.
No embedded audio.	Video source does not have embedded audio.	Check your video source for embedded audio.
Playback audio output is distorted.	Audio input signal clipping caused by excessive audio input level.	Check for input audio clipping. Adjust the audio input trim. Adjust the Player audio level. Reduce the source audio input level.
Audio level is too low.	Audio level needs to be adjusted.	Adjust the Player or Recorder audio level. Increase the source audio input level.

Problem	Possible Causes	Corrective Actions
The audio level is not correct only when playing a particular clip.	The clip's audio level is out of adjustment.	Load the clip in Player and adjust its playback audio level.
Audio level meters do not display the correct reference level on connected equipment.	Incorrect audio reference level.	Select the correct audio reference level.
Audio meters do not appear in the AppCenter Monitor Pane.	The Monitor Pane configured to not display audio meters.	Configure the Channel Monitoring setting to display audio meters.

Timecode problems

For the corrective actions in this section, refer to related topics in the "Using K2 AppCenter" section of the K2 Topic Library for detailed instructions.

Problem	Possible Causes	Corrective Actions
Recorded timecode reads xx.xx.xx.xx.	During recording, the channel had no timecode source.	Check that you have the right record channel timecode source selected, verify that timecode is present in the source, and record the clip again. You can also stripe the timecode on an existing clip.
A clip shows no mark-in/mark-out timecode, the current timecode display shows XX:XX:XX:XX, or the last valid timecode is displayed.	The selected timecode source was missing or intermittent during recording.	

Operational problems

For the corrective actions in this section, refer to related topics in the "Using K2 AppCenter" section of the K2 Topic Library for detailed instructions.

Problem	Possible Causes	Corrective Actions
Moving video in AppCenter does not operate.	The K2 Solo 3G system is not licensed for AppCenter Pro.	Obtain an AppCenter Pro license.
	The VGA monitor resolution is less than 1024x768x32.	Configure VGA monitor resolution. The resolution must be at least 1024x768x32 to support live video.
	Another user is connected via Remote Desktop.	Restart AppCenter.
The K2 Solo 3G system is not operating as expected in relation to a setting displayed in Configuration Manager.	The setting was changed in Configuration Manager but not saved to the database.	Verify the setting you want in Configuration Manager and then select OK. When prompted to change the system settings, select Yes.

Problem	Possible Causes	Corrective Actions
AppCenter displays different buttons than those expected.	Assignable buttons have been changed.	Assign buttons to the interface as desired.
A clip does not play, even though other clips play on the same channel.	The clip does not match current K2 Solo 3G system settings or the clip is corrupt.	If the clip appears grayed-out it means it doesn't match current settings. Check the clip's properties and verify they are correct for the standard, compression, and other current settings. Compare properties with those of a clip that plays correctly. If properties are correct the clip is corrupt. Delete and re-record the clip.
	The K2 system is not licensed for the format of the clip.	Verify licensing.
A clip can not be edited.	The clip is locked.	Unlock the clip.
Can't rename a clip or modify mark-in/mark-out points	The clip loaded or playing is still being recorded. In this case, "Read-Only" is displayed in the StatusBar.	Wait until recording is complete.
Cannot load and play a list.	The list contains invalid clips.	Check format, licensing, and security setting of the clips in the list.
On setting mark-out, the subclip is automatically generated and ejected, and a new subclip name is loaded in the subclip pane.	Auto Subclip mode is enabled.	Disable Auto Subclip mode.
Can't change what information is displayed in the Monitor Pane for Playlist.	You are attempting to use Configuration Manager to change what information is displayed in Monitor Pane for Playlist.	Use the Playlist Options dialog instead.
Can't control a channel from AppCenter. Controls are disabled.	The channel is configured for control by a remote control protocol.	Set the control mode for limited local control.

System problems

For the corrective actions in this section, refer to related topics in the "Using K2 AppCenter" section of the K2 Topic Library for detailed instructions.

Problem	Possible Causes	Corrective Actions
One of the record channels does not record or video is jumpy.	The K2 Solo 3G system is configured for PAL, yet the video input is NTSC	Check the current setting for video standard. Verify that the video input signal is the correct standard.
A scheduled event, such as an automatic play or record event, does not occur at the proper time.	The time-of-day source for event scheduling is not accurate.	Verify the time-of-day source. Verify the source's time accuracy.

Storage problems

Use the following sections if you suspect problems with your K2 Solo 3G system's storage. Refer to related topics in the "Configuring the K2 System" section of this Topic Library for Storage Utility procedures.

Media File System problems

Problem	Possible Causes	Corrective Actions
One or more clips do not play or record correctly. This can be accompanied by a StatusPane message indicating a fault in the media file system.	The media database is out of sync with the media files or there is a corrupt media file. Also check the storage system for causes related to certain usage patterns.	1. If the problem is only associated with a specific clip or clips, delete the problem clips. If the problem persists, proceed with the next step. 2. Use Storage Utility and Check File System. If the file system fails the check process you must make a new file system. When you do so you lose all media.
During K2 Solo 3G system startup a "…no file system running…" message appears.	The file system is corrupt or disks are faulty/missing such that they are not part of a stripe group.	Use Storage Utility and Check File System. If the file system fails the check process you must make a new file system. When you do so you lose all media.

Media disk problems

On the Windows desktop open the "My Computer" for you K2 system and do a quick check of the drives. You should see C: and V: drives.

Problem	Possible Causes	Corrective Actions
No clips appear in the Clips pane. This may be accompanied by a startup message or a StatusPane message regarding media disks being unavailable.	A media disk is bad or there has been a hardware failure.	Open Storage Utility and identify faulty disks. Replace faulty disks.
The StatusPane message "Media disks getting full…" appears or a "FSS 'default(0)'" message appears.	The media disks are reaching maximum capacity.	In Recorder, select the Time Dome and choose **Available Storage**. If the Time Dome is filled it confirms that your K2 Solo 3G system is out of space. Make space on the media drives by doing the following: - Delete unused clips and empty the Recycled Bin.
When streaming to another K2 Solo 3G system the operation fails. In Transfer Monitor the streaming operation shows "Status:Error".	There is a network connection error or the media disks at the destination are reaching maximum capacity.	Check network connections and configuration. Check available storage on the destination K2 Solo 3G system. In Recorder, select the Time Dome and choose **Available Storage**. If the Time Dome is filled it confirms that the destination K2 Solo 3G system is out of space. Make space on the media drives by deleting unused clips and emptying the Recycle Bin.
System status message "File system…is fragmented".	Extended record/play activity has fragmented the disks.	Use the Storage Utility to check the file system.

Checking the storage system

The following section provides guidelines for investigating problem areas related to the storage system. Use this section if you have problems with media input and/or output that are intermittent or seem to be related to certain usage patterns.

Problem	Possible Causes	Corrective Actions
Symptoms can include black video recorded or at playout, frozen video, slow performance, or inconsistent media access. These symptoms can be accompanied by StatusPane messages regarding disk problems or overrun/underrun conditions for encoders, decoders, or timecode.	The following causes can occur on their own or in combination to produce the problem: • Disk oversubscription — This occurs when requests to the media disk exceed the disk's bandwidth capabilities. This generally occur in extreme cases when a combination of high-bandwidth operations are taking place, such as jog/shuttle, record/play on multiple channels, or streaming multiple clips. • High CPU activity in Windows — This occurs when activities on the Windows operating system over-tax the capabilities of the CPU. This commonly happens when unsupported software has been installed that competes with K2 Solo 3G system applications. Virus scanners and screen savers can cause this type of problem, since they can start automatically and consume system resources. • Encoder overrun — This occurs when an encoder is flooded with more data than it can process within its real-time requirements for recording. • Decoder underrun — This occurs when a decoder is starved for data and cannot deliver enough to satisfy real-time requirements for playout. • Disk faults — This occurs when a media disk is severely fragmented or has a bad blocks that interfere with some, but not all, media operations. For example, a particular clip can be written on a bad block, so the problem occurs only on that clip.	Try to re-create the problem. Identify all the interactions that affected the system and run all the same operations as when the error occurred. Record/play/stream the same clips. Investigate the functions that seem to push the system into the error state. If you determine that certain simultaneous operations cause the problem, re-order your workflow to avoid those situations. If you determine that the problem is only on certain clips, investigate disk faults.

Network, transfer, and streaming problems

Problem	Possible Causes	Corrective Actions
When importing or exporting (sending) between K2 Solo 3G systems a "…failed to connect…" message appears and the operation fails.	There is a problem with Windows networking or there is a mis-spelling with the host name as entered in Configuration Manager.	Check networking as follows: - Check basic Windows networking. Use Windows Explorer to test a basic copy operation to the machine to which you are trying to connect. If basic networking fails, use standard Windows procedures to troubleshoot and correct your network. - If the Windows network is working properly, in AppCenter select **System | Configuration | Remote** and verify that the name of the machine to which you are trying to connect is spelled correctly and has no extra spaces or characters.
	The K2 Solo 3G system to which you are trying to connect is not operating or the network is mis-configured.	Verify that the K2 Solo 3G system to which you are trying to connect is operational and that the network is configured correctly. Verify that the name of the K2 Solo 3G system is entered correctly in the Configuration Manager Hosts page. Refer to networking topics in the "Configuring the K2 System" section of this Topic Library.
A networked device does not appear in the "Import" and "Send to" dialog boxes, even though it is present on the Windows network.	The device is not entered as a host.	In AppCenter select **System | Configuration | Remote | Add** and enter the name of the machine to which you are trying to connect. Make sure it is spelled correctly and has no extra spaces or characters. Also check the hosts file. Refer to networking topics in the "Configuring the K2 System" section of this Topic Library.
	If a SAN K2 client, the client's K2 Media Server with role of FTP server is not operational.	Verify FTP server.

Problem	Possible Causes	Corrective Actions
Files do not appear in" Send To" or "Export" dialogs.	File names do not have proper extensions.	Rename files with proper extensions.

Also refer to the *UIM Instruction Manual* for more troubleshooting information.

Removing and replacing FRUs

Removing and replacing FRUs

Field Replaceable Units (FRUs) are modular hardware components that can be serviced without disturbing other components in the system.

The pictures in the following topics show how to disassemble. Unless otherwise documented, re-assembly is the reverse.

To complete all FRU procedures, the following tools are required:

- Torx tool with T15 magnetic tip. This is the only tool needed for most FRU procedures. If additional tools are required, they are listed with the FRU procedure.
- #1 Phillips screwdriver
- #2 Phillips screwdriver
- 3/16" nut driver
- 1/4" nut driver
- Side cutters

NOTE: Only Grass Valley components are supported. Do not attempt to use components procured from a different source.

NOTE: Do not discard any hardware unless specifically instructed to do so.

⚠ ***WARNING: To avoid serious injury from high currents, ensure that both power cords are disconnected prior to removing or replacing any parts.***

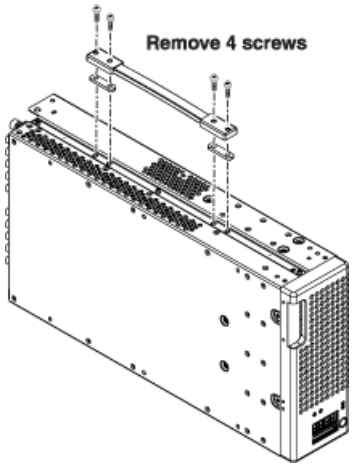
⚠ ***CAUTION: This system contains board-level components that must be protected from static discharge and physical shock. Wear a wrist strap grounded to the system chassis when handling system components.***

External Parts Removal

All the parts in this category can be removed and replaced without opening the K2 Solo 3G system cabinet.

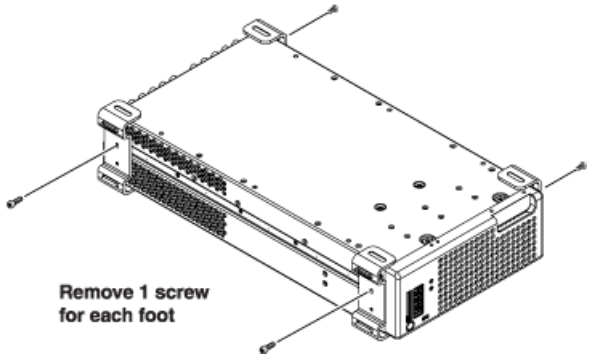
Handipak handle removal

Remove the optional Handipak handle as illustrated.



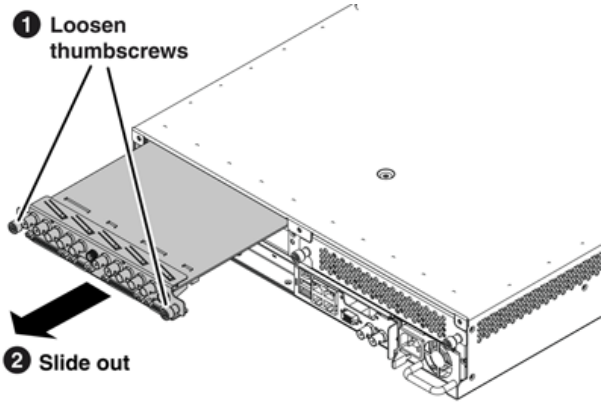
Handipak feet removal

Remove one or more of the optional Handipak feet as illustrated.



Codec module removal

Access the codec module from the rear panel. Remove as illustrated.



NOTE: With a firm grip on the metal (EMI) bracket, ensure the board is level and parallel to the card guides to avoid damage to the components on the edge opposite the rear panel.

⚠ ***CAUTION: Improper handling can damage components on the board. Do not allow the board to come in contact with the chassis sheet metal during removal or installation. The components on the edge opposite the rear panel are the most susceptible to damage.***

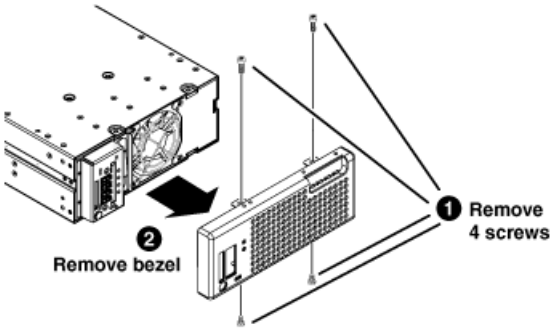
Before installing, inspect the codec module chamber and make sure no cables are protruding into the path of the codec module.

You must also remove any codec option (mezzanine) cards from the faulty codec module and install them on the replacement codec module.

After installing the replacement codec module, install the current version of K2 software. An over-install is all that is required. You do not need to first un-install the software. This ensures that the board is flashed with the proper version to be compatible with K2 software.

Front bezel removal K2 Solo

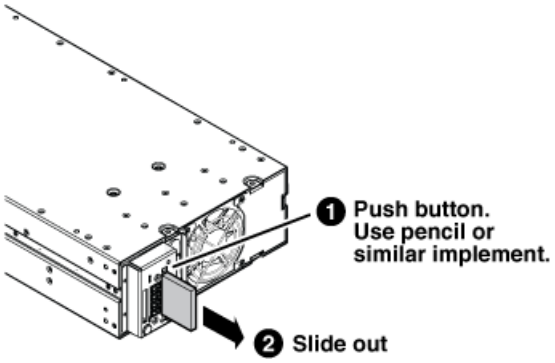
To remove the front bezel, proceed as illustrated.



⚠ ***CAUTION: Do not remove bezel while power is on. If powered, the fan can turn on with moving blades exposed.***

CompactFlash boot media removal K2 Solo

To remove the boot media, first remove the front bezel, then proceed as illustrated.



You must use the CompactFlash boot media provided by Grass Valley. Do not use CompactFlash media procured elsewhere.

Fan assembly removal

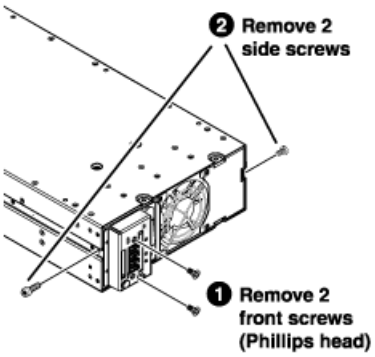
Additional tools needed:

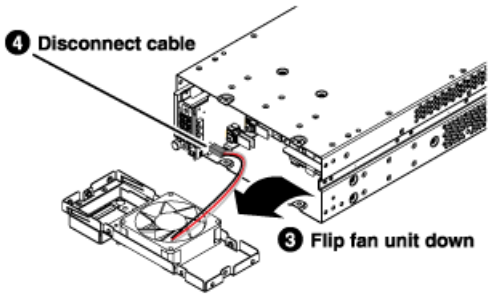
- #2 Phillips screwdriver

Before doing this task, do the following:

- Remove the front bezel.

To remove the fan assembly, proceed as illustrated.





⚠ ***CAUTION: Do not remove fan assembly while power is on. The standby button is frequently bumped during this procedure and if powered, circuits and fans are activated, which can cause damage.***

Fan removal

Additional tools needed:

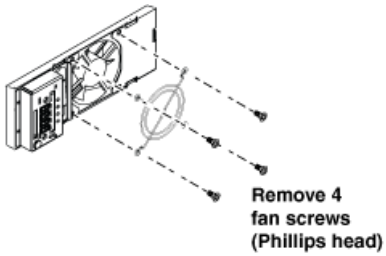
- #2 Phillips screwdriver

Before doing this task, do the following:

- Remove the front bezel.

- Remove the fan assembly.

  To remove the fan, proceed as illustrated.

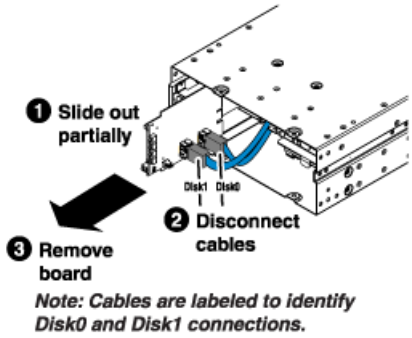


Disk controller board removal

Before doing this task, do the following:

- Remove the front bezel.
- Remove the fan assembly.

To remove the disk controller board, proceed as illustrated.



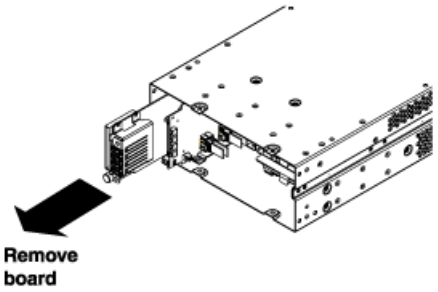
Front interconnect board removal

Before doing this task, do the following:

- Remove the front bezel.

- Remove the fan assembly.

  To remove the front interconnect board, proceed as illustrated.



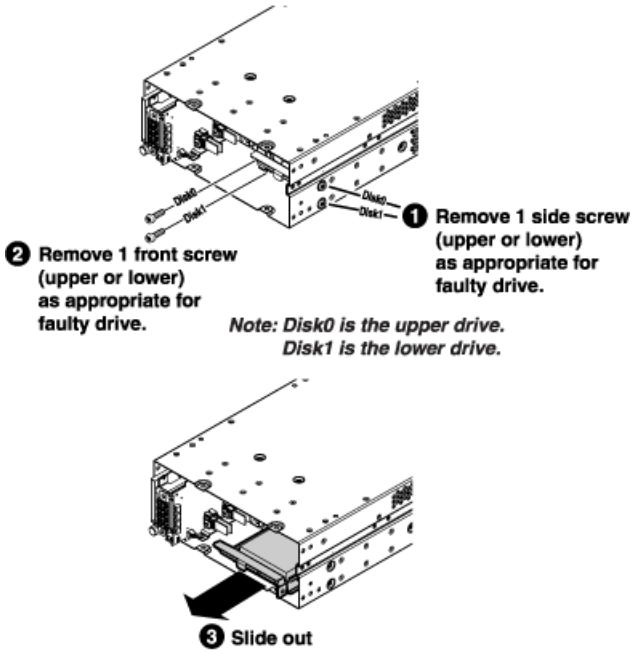
Disk module removal

Before doing this task, do the following:

- Make sure you have identified the proper disk module. In some cases you must also perform operations with Storage Utility.
- Remove the front bezel.

- Remove the fan assembly.

  To remove a disk module, proceed as illustrated.



Internal Parts Removal

The sections that follow show how to remove internal parts from the K2 Solo 3G system.

⚠ ***CAUTION: To avoid possible damage to circuit boards and other sensitive parts, turn off the* K2 Solo 3G system *and disconnect both power cords before opening the top cover or removing any internal parts.***

Top cover removal

Before doing this task, do the following:

- Remove the front bezel.
- Remove the fan assembly.
- Remove the disk controller board.

- Remove the front interconnect board.

To remove the top cover, proceed as illustrated:

Unfasten and disconnect cables

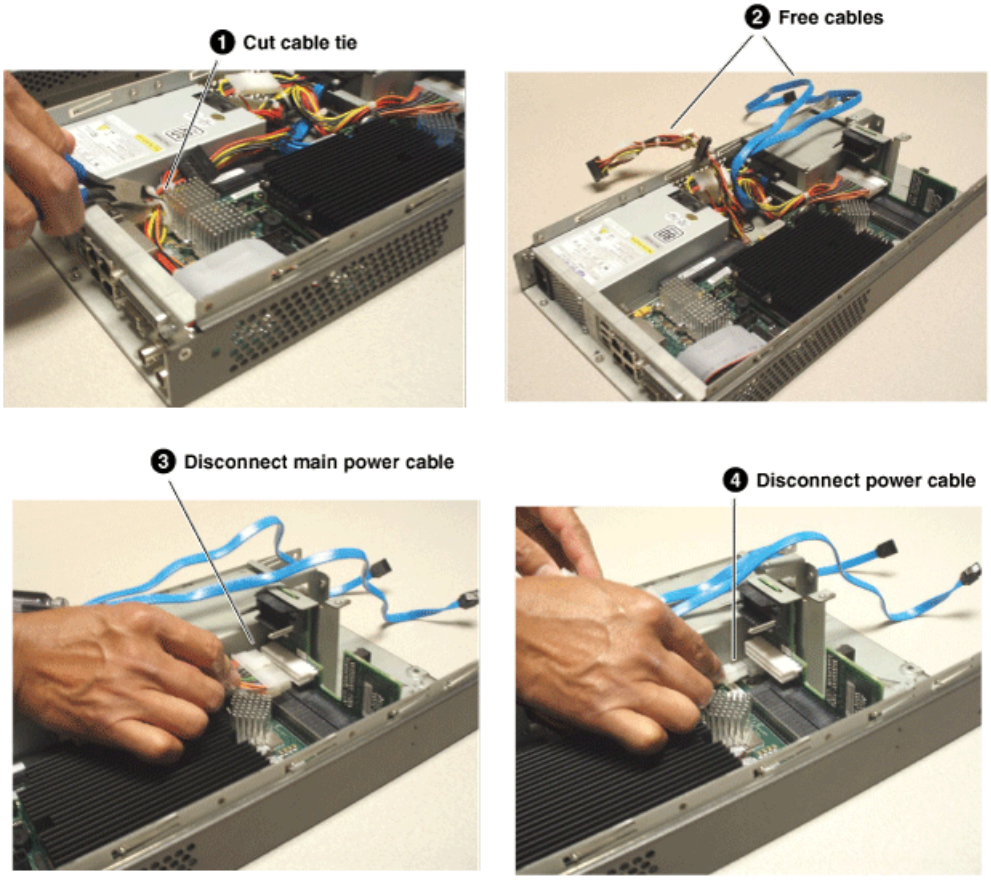
Additional tools needed:

- Side cutters

Before doing this task, do the following:

- Remove the top cover.

  To remove any of the internal FRUs you must cut cable ties, free cables, and disconnect cables as shown.



Remove rear panel

Additional tools needed:

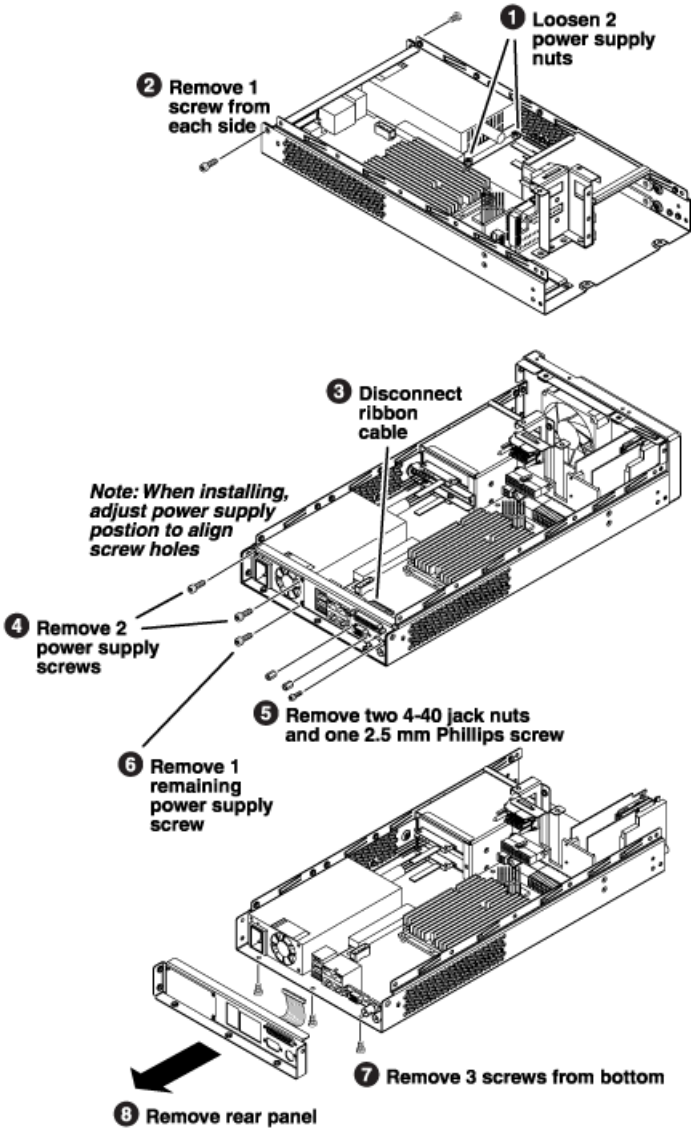
- #1 Phillips screwdriver
- #2 Phillips screwdriver

- 3/16” nutdriver
- 1/4” nutdriver

Before doing this task, do the following:

- Remove the top cover.
- Unfasten/disconnect cables.

Remove the rear panel as illustrated.



Carrier module removal

Before doing this task, do the following:

- Remove the top cover.
- Unfasten/disconnect cables.

- Remove the rear panel.

To remove the carrier module, proceed as illustrated.

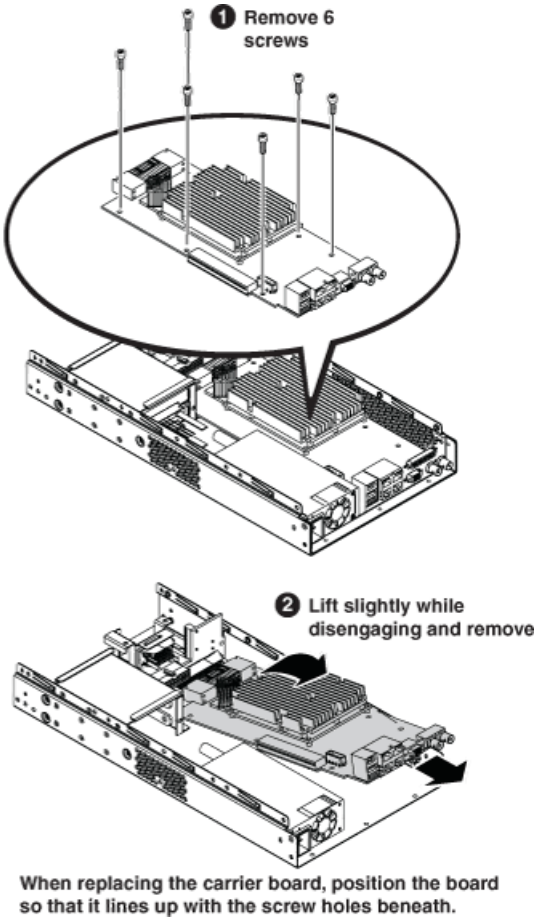
Caution: Improper handling can damage components on the board.

Maintain clearance between board and standoffs on chassis bottom.

Do not allow the board to come in contact with the standoffs or chassis sheet metal during removal or installation.

Do not slide board.

The components on the bottom are the most susceptible to damage.



Power supply removal

Additional tool needed:

- 1/4” nutdriver

Before doing this task, do the following:

- Remove the top cover.
- Unfasten/disconnect cables.
- Remove the rear panel.

- Remove the carrier board.

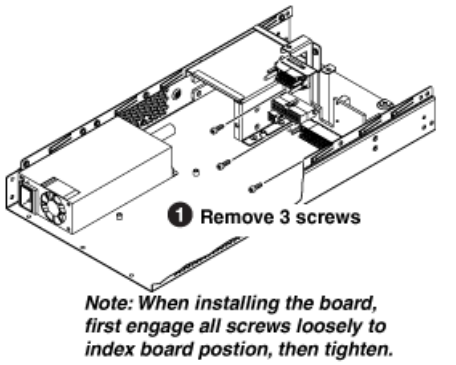
To remove the power supply proceed as illustrated.

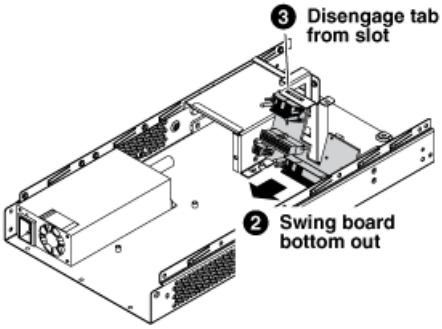
Midplane board removal

Before doing this task, do the following:

- Remove the top cover.
- Unfasten/disconnect cables.
- Remove the rear panel.
- Remove the carrier board.

To remove the midplane board proceed as illustrated.





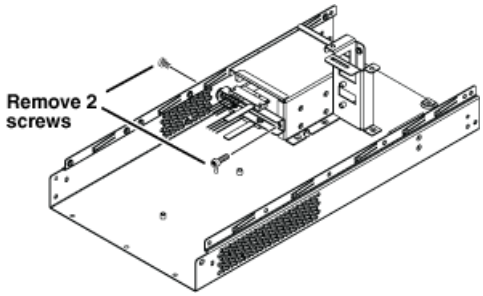
Drive cable assembly removal

Before doing this task, do the following:

- Remove the top cover.
- Unfasten/disconnect cables.
- Remove the rear panel.
- Remove the carrier board.

- Remove the power supply.

  To remove the drive cable assembly proceed as illustrated.



Installing components and dressing cables

Materials needed:

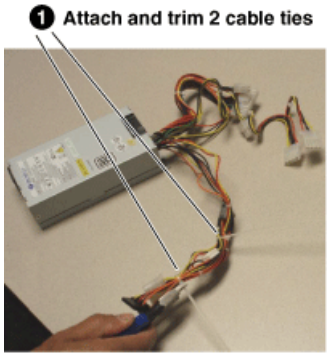
- Cable ties, as provided in FRU kit.

When installing internal components, follow the steps below, especially for cable routing and dressing.

NOTE: Take care with cable dressing, as cables must be trapped in the lower chassis to maintain clearance for codec module removal and installation. Incorrectly dressed cables can damage the codec module.

When following the steps below, also refer to removal procedures earlier in this section, with re-assembly being the reverse of the removal procedure.

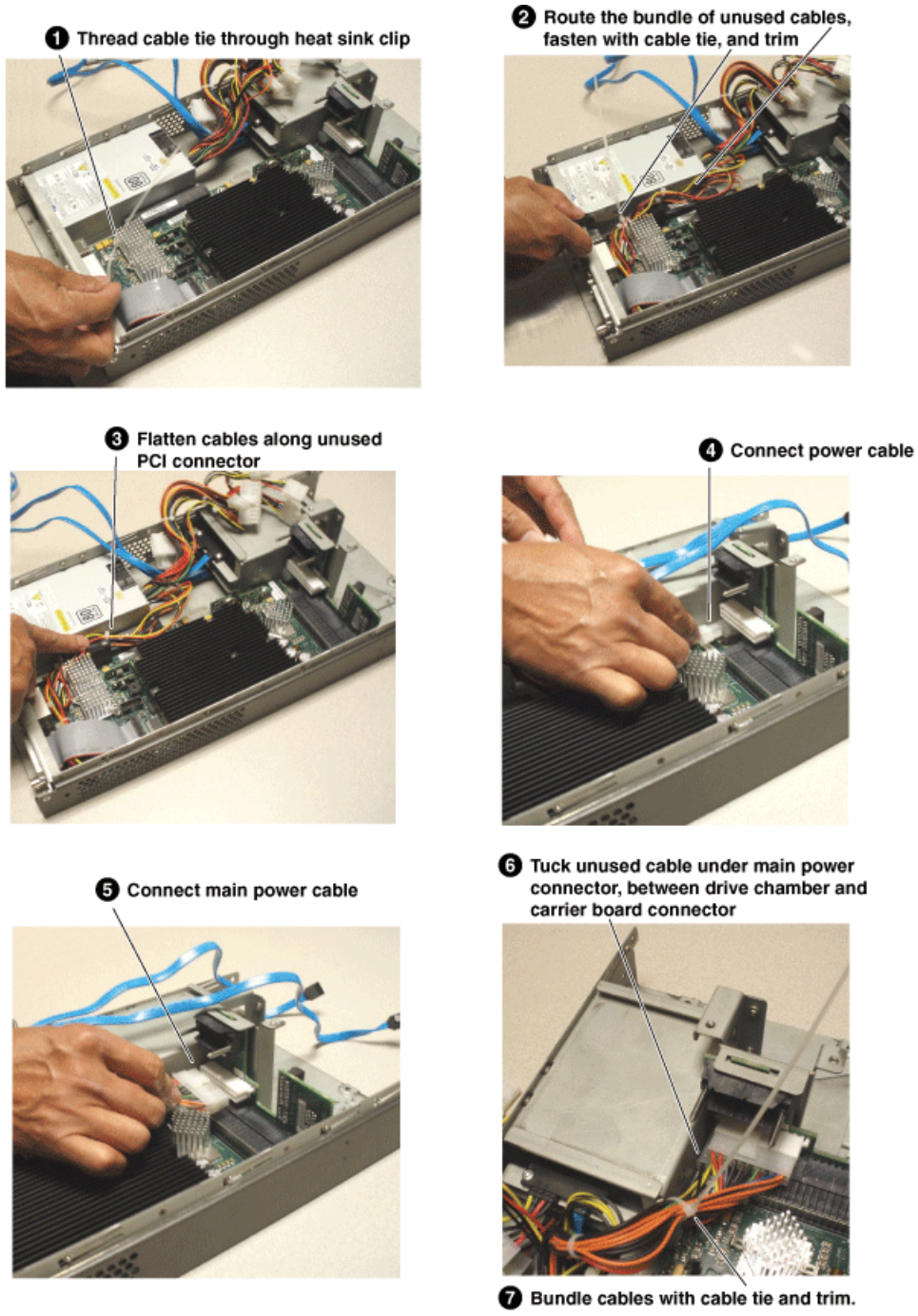
1. If replacing a midplane board, install it in the chassis.
2. If replacing a power supply, pre-dress unused cables as illustrated:

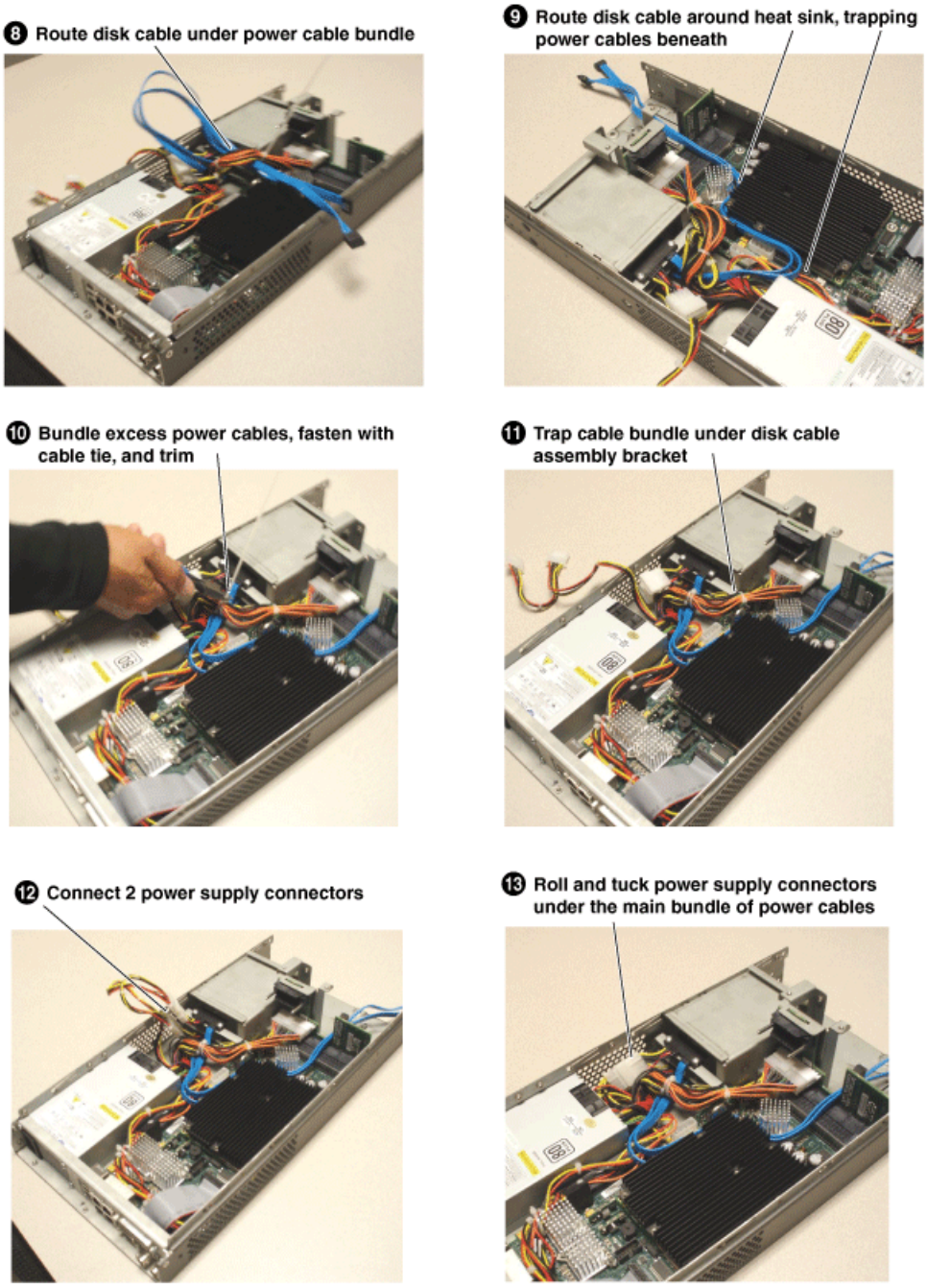


NOTE: Use the faulty power supply that you removed as a model for cable dressing.

3. If replacing a power supply, install it in the chassis.
4. Install the carrier module.
5. Install the rear panel.

6. Dress and connect cables as illustrated.





7. When cable dressing is complete, make sure that no cables protrude above the level of the drive chamber top.
8. Install the top cover.

Installing K2 Avid Connect

What's new in K2-AvidTM/AMA

About K2/Avid Transfer Manager and Avid Media Access

K2/Avid Transfer Manager is Grass Valley's push and pull plug-in application that allows you to push and pull files stored on a K2 system to and from an Avid editor or shared-storage device.

It provides a seamless interface between GV STRATUS and K2 servers and Avid standalone and shared-storage environments. The K2 system enhances the Avid Workgroup solution in several ways:

- Provide a fast and reliable server for ingest and playout; once a story or a promo created using the Avid editor, you can send it to a K2 system for immediate playout.
- Seamless Avid Interplay nonlinear workflow engine; you can begin playout while the file is being streamed from your editor to a server.,
- Additional features to accelerate your workflow that lets you access a file while it's being transferred.
- A mirror option that lets you save to two servers (main and backup) in one operation.
- Ability to simultaneously transfer up to four files between the K2 and editing environments.

With GV AMA (Avid Media Access) plug-in for Media Composer and NewsCutter, you can access GV file-based media directly on the K2 Summit system media volume `V:`. It allows fast editing since you are not required to import the files before the media can be used.

What's new in version 7.0.0.163

Build 7.0.0.163

1. Fixed DE7096 - AMA linked clips that are under construction should show up with the In Progress Icon in Media Composer. This fails if the under construction clip has a Mark-In greater than zero.
2. Build for GV STRATUS version 3.0.
3. Build for Media Composer version 6.5.2 and 7.0.2.
4. Build for Interplay engine version 2.7.5.

Changes and features in previous releases

The following sections describe changes and features in past releases.

Build 7.0.0.162

1. Build for GV STRATUS version 3.0.
2. Build for Media Composer version 6.5.2 and 7.0.2.
3. Build for Interplay engine version 2.7.5.

Build 7.0.0.161

1. Build for GV STRATUS version 2.8.
2. Build for Media Composer version 6.5.2 and 7.0.2.
3. Build for Interplay engine version 2.7.5.

Build 7.0.0.150

1. Build for Interplay transfer engine 2.6 and 2.7 and AMA plugins build with AMA_SDK_3.1_2660.
2. Added new configuration utilities, TServerconfig and IngestConfig.

Build 7.0.0.149

1. Build for Interplay transfer engine 2.6 and 2.7 and AMA plugins build with AMA_SDK_3.1_2660.
2. Increased the ping timeout in AMA K2ConnectionHelper to 300ms, therefore avoiding devices erroneously getting declared offline.
3. Rolled the MVP and MSP PluginMinorVersion to 3.
4. Fixed XmlParser, now validates data before attempting string copy, preventing Media Composer from vaporising.

Build 7.0.0.148

1. Build for Interplay transfer engine 2.6 and 2.7 and AMA plugins build with AMA_SDK_3.0_2555.
2. Added Support for GV STRATUS metadata to the AMA MVP plugin.
3. Rolled the MVP and MSP PluginMinorVersion to 2.
4. Increased the DEFAULT_RCVBUF_SIZE and DEFAULT_SNDBUF_SIZE to (1024*1024)*2 to push the transfer speeds to around 85 to 100MB/sec. If the registry key is already set, then, this must be removed first.

Build 7.0.0.147

1. Build for Interplay transfer engine 2.6 and 2.7 and AMA plugins build with AMA_SDK_3.0_2555.
2. Updated install script to correctly register and unregister dlls.

Build 7.0.0.146

1. Build for Interplay transfer engine 2.6 and 2.7 and AMA plugins build with AMA_SDK_3.0_2555.
2. Added Support for GV STRATUS metadata to the GvgK2Setup.dll.
3. Added Support for GV STRATUS metadata to the AMA MSP plugin.
4. Fixed ncbug00076294: At Random transfer (SEND to PLAY BACK) aborts midstream.

5. User can now select the colour of the locators when ingesting asset via the DHM. This is done via the registry at *Software\\Grass Valley Group\\Applications\\K2-AvidTM\\SETUP* value LocatorColour. Set the values to:
   - 0 = Red
   - 1=Green
   - 2=Blue
   - 3=Magenta
   - 4=Cyan
   - 5=Yellow
   - 6=White
   - 7=Black

Build 7.0.0.145

1. Build for Interplay transfer engine 2.6 and 2.7.
2. Fixed ncbug00076584: Increased the GXF parser buffer size to handle the large MPEG frames produced by long GOP recording 50Mbit records.
3. Added support for AMA chase editing.

Build 7.0.0.144

- Build for Interplay transfer engine 2.6 and 2.7.

Build 7.0.0.143

- Build for Interplay transfer engine 2.5.

Build 7.0.0.142

- Special Build for Interplay transfer engine 2.2.

Build 7.0.0.141

1. Build for Interplay transfer engine 2.5.
2. Fixed ncbug00075587: Transfers of programs which includes empty audio tracks to Avid MC has audio distortion on the filler tracks. Added Audio fill for 24 bit audio and corrected for progressive formats.
3. Fixed ncbug00074984: Transfer from Avid Media Composer to K2 Summit system fails if part of the Sequence does not have video track. Added DNxHD and AVCi fill fame support. Corrected AVCi fill frame size.

Build 7.0.0.140

1. Build for Interplay transfer engine 2.5.
2. Fixed ncbug00075794: Audio corrupted for Avid sequence transferred to K2 Summit system.
3. Fixed ncbug00075795: Need change the default password for Avid TServer/DHM Ok.
4. Fixed ncbug00075603: K2Avid Explorer hangs if one of the K2 Summit system is rebooted and shutdown.

5. Fixed ncbug00075831: K2Avid Explorer hangs whenever I click on a bin of a K2 Summit system that has just shutdown.
6. Fixed ncbug00075623: K2 AvidExplorer errors during K2 Summit system boot up.

Build 7.0.0.139

1. Build for Interplay transfer engine 2.5.
2. Fixed ncbug00075824: Second round of fixes with the correct path.

Build 7.0.0.138

1. Build for Interplay transfer engine 2.5.
2. Fixed ncbug00075822: Software license agreement for K2 DHM/Ingest/Tserver installation needs to be updated (get rid of Thomson). Changed the Email address from *K2license@thomson.net* to *K2License@grassvalley.com* in the *K2-AvidTm.ini* to be used for License requests wizard.
3. Fixed ncbug00075824: K2-AvidTMLicense request wizard does not launch. Unable to locate *wizard.hta.*. Updated the path used by install shield.
4. Fixed ncbug00075785: Updated the license cutter to create licenses named K2-AvidTM instead of k2-DHM and updated the *TemporaryLicense.txt* to include K2-AVIDTM Evaluation license instead of SERVER-SOFTWARE-TEMPORARY. Updated the receiver and dhm dll to work with both k2-DHM and K2-AVIDTM.

Build 7.0.0.137

1. Build for Interplay transfer engine 2.5.
2. Fixed ncbug00075811: Newer version of Sabretooth license manager should be used for Avid DHM PC.

Build 7.0.0.135

- Fixed ncbug00075587 — Filler tracks had random noise. Problem caused by filler audio frame was not initialised to zero. Fixed by memset(pc,0,sizeof(char)*nSize).

Build 7.0.0.134

1. Fixed ncbug00075461 — AvidTServer install had the option show the install log at the end, but it doesn't work. Disabled the "Show the Windows Installer log check box" from the SetupCompleteSuccess dialogbox.
2. Fixed ncbug00075397 — Unable to transfer List or Program from K2 Summit system to Avid.Failures to transfer Lists are caused by additional video frames transferred for transition's. There is no way to handle this on the Avid side. So to address this, any attempt to transfer a list is now rejected.
3. Fixed ncbug00075137 — Sighting: K2 Avid Explorer had an unhandled exception.Added better exception handling and check to guard against accessing null objects.
4. Fixed ncbug00075398 — K2AvidExplorer crashes when user clicks on a bin that no longer exists. Fixed additional issues where bin would not update or wrong bin would be deleted.
5. Fixed ncbug00075399 — Audio misalignment (out of sync with video) on Programs transferred from K2 Summit system to Avid MediaComposer. Added code to correct the Audio sample used when dealing with Programs (sequences).
6. Fixed ncbug00075401 — Logviewer throws an error from K2AvidExplorer whenever the clip name is changed while it is still being recorded.

7. Fixed ncbug00074988 — Transfer of subclips from K2 Summit system to Avid Media Composer sometimes fail. This should be addressed by the fix in ncbug00075399.

Build 7.0.0.133

1. Fixed ncbug00075359 — Send to playback: Drop Frame time code does not drop frames.
2. Fixed ncbug00075439 — Send to playback: Media files are dumped in the Interplay transfer engine folder.

Build 7.0.0.132

- Final fix for Bottom field versus top field issue with DNxHD content.

Build 7.0.0.131

- Fixed Bottom field versus top field issue with DNxHD content.

Build 7.0.0.130

- Added new configurations utility to ease the configuration of the K2-AvidTM.

Build 7.0.0.129

1. First build to support Media Composer version 6.0.1 and Interplay engine 5.0.1.
2. Added support for DNxHD.
3. Changed the Tserver dependencies so it can be installed on the FSM.

Build 7.0.0.112

With the introduction of build 7.0.0.112 and Avid Interplay 2.2.1.1, K2-AvidTM now supports the following:

1. 16 channels of audio.
2. AVC-I ingest and Send to playback. 1080i & 720P, 50Mbit or 100Mbit.
3. Ingest of XDCAM.
4. MetaData can be displayed in Avid editor bin view.
5. Basic sorting on Colum view in K2-Avid Explorer.
6. K2-Avid Explorer no longer allows assets to be deleted or renamed.

Reference to system compatibility

Software version versus Avid Operating System support

Software Version	Windows NT4.0	Windows XP	WIN 7 32 bit	WIN 7 64 bit
7.0.0.104	Yes	Yes	No	No

Software Version	Windows NT4.0	Windows XP	WIN 7 32 bit	WIN 7 64 bit
7.0.0.105	Yes	Yes	No	No
7.0.0.112	No	Yes	Yes	Yes
7.0.0.129	No	No	No	Yes
7.0.0.130	No	No	No	Yes
7.0.0.131	No	No	No	Yes
7.0.0.132	No	No	No	Yes
7.0.0.133	No	No	No	Yes
7.0.0.134	No	No	No	Yes
7.0.0.135	No	No	No	Yes
7.0.0.136	No	No	No	Yes
7.0.0.137	No	No	No	Yes
7.0.0.138	No	No	No	Yes
7.0.0.139	No	No	No	Yes
7.0.0.140	No	No	No	Yes
7.0.0.141	No	No	No	Yes
7.0.0.142	No	No	Yes	No
7.0.0.143	No	No	No	Yes
7.0.0.144	No	No	No	Yes
7.0.0.145	No	No	No	Yes
7.0.0.146	No	No	No	Yes
7.0.0.147	No	No	No	Yes
7.0.0.148	No	No	No	Yes
7.0.0.149	No	No	No	Yes
7.0.0.150	No	No	No	Yes
7.0.0.161	No	No	No	Yes
7.0.0.162	No	No	No	Yes
7.0.0.163	No	No	No	Yes

Microsoft Windows Operating System supported by Profile and K2 Summit system

Software Version	Profile PVS series	K2 Series	K2 Summit/Solo system	K2 Summit 3G/Solo 3G system
Windows NT4.0	Yes	No	No	No
Windows XP	Yes	Yes	Yes	Yes
WIN 7 32 bit	No	Yes	Yes	Yes
WIN 7 64 bit	No	Yes	Yes	Yes

K2-AvidTM Software Version and Avid version matrix

Software Version	Interplay Transfer engine	NewsCutter	Media Composer
7.0.0.104	1.6.2 & 1.6.4	7.5.9	3.5.9
7.0.0.105	2.1	8.x	4.x
7.0.0.112	2.2.1.4	9.x	5.x
7.0.0.126	2.2.1.4	9.x	5.x
7.0.0.127	2.3.0.3	9.5.3	5.5.3
7.0.0.128	2.4.0.2	9.5.3	5.5.3
7.0.0.129	2.5.0.3	10.0.3	6.0.3
7.0.0.130	2.5.0.3	10.0.3	6.0.3
7.0.0.131	2.5.0.3	10.0.3	6.0.3
7.0.0.132	2.5.0.3	10.0.3	6.0.3
7.0.0.133	2.5.0.3	10.0.3	6.0.3
7.0.0.134	2.5.0.3	10.0.3	6.0.3
7.0.0.135	2.5.0.3	10.0.3	6.0.3
7.0.0.136	2.5.0.3	10.0.3	6.0.3
7.0.0.137	2.5.0.3	10.0.3	6.0.3
7.0.0.138	2.5.0.3	10.0.3	6.0.3
7.0.0.139	2.5.0.3	10.0.3	6.0.3
7.0.0.140	2.5.0.3	10.0.3	6.0.3
7.0.0.141	2.5.0.3	10.0.3	6.0.3
7.0.0.142	2.2.1.4	9.0.4	5.0.4
7.0.0.143	2.7.0.2	10.5.2	6.5.2

Software Version	Interplay Transfer engine	NewsCutter	Media Composer
7.0.0.144	2.7.0.2	10.5.2	6.5.2
7.0.0.145	2.7.0.2	10.5.2	6.5.2
7.0.0.146	2.7.0.2	10.5.2	6.5.2
7.0.0.147	2.7.0.2	10.5.2	6.5.2
7.0.0.148	2.7.0.2	10.5.2	6.5.2
7.0.0.149	2.7.0.2	10.5.2	6.5.2
7.0.0.150	2.7.0.2	10.5.2	6.5.2
7.0.0.161	2.7.0.2	10.5.2 & 11.0.2	6.5.2 & 7.0.2
7.0.0.162	2.7.0.2	10.5.2 & 11.0.2	6.5.2 & 7.0.2
7.0.0.163	2.7.0.2	10.5.2 & 11.0.2	6.5.2 & 7.0.2

K2-AvidTM Software Version and Video server version matrix

Software Version	Profile PVS series	K2 series	K2 Summit system	K2 Summit/Solo system	Notes
7.0.0.104	5.4.9.1328	3.3.2.1412	7.3.8.1432	7.3.8.1432	
7.0.0.105	5.4.9.1328	3.3.2.1412	7.3.8.1432	7.3.8.1432	
7.0.0.112	No support	3.3.2.1412	7.3.8.1432	7.3.8.1432	
7.0.0.126	No support	3.3.2.1412	9.x	9.x	DNxHD not supported.
7.0.0.127	No support	3.3.2.1412	9.x	9.x	DNxHD not supported.
7.0.0.128	No support	3.3.2.1412	9.x	9.x	DNxHD not supported.
7.0.0.129	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.130	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.131	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.132	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.133	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.

Software Version	Profile PVS series	K2 series	K2 Summit system	K2 Summit/Solo system	Notes
7.0.0.134	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.135	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.136	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.137	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.138	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.139	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.140	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.141	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.142	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.144	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.145	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.146	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.147	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.148	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.149	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.150	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.161	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.162	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.
7.0.0.163	No support	3.3.2.1412	9.x	9.x	DNxHD use 3G hardware.

Supported compression formats

K2-AvidTM Build 7.0.0.104 supports

Compression formats Supported on PVS1100 with software build 5.4.9.1328

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
DVCAM	Yes	Yes	Yes	Yes	8	Yes	Yes	No
DVCPRO25	Yes	Yes	Yes	Yes	8	Yes	Yes	No
DVCPRO50	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 30 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 40 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 50 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No

NOTE: For PVS, ingest & Send to playback are only supported if Windows XP operating system are used on the Avid editor and transfer manager.

Compression formats Supported on K2 with software build 3.3.2.1412

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
DVCAM	Yes	Yes	Yes	Yes	8	Yes	Yes	No
DVCPRO25	Yes	Yes	Yes	Yes	8	Yes	Yes	No
DVCPRO50	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 30 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 40 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 50 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No

Compression formats Supported on K2 Summit/Solo system with software build 7.3.8.1432

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
DVCAM	Yes	Yes	Yes	Yes	8	Yes	Yes	No
DVCPRO25	Yes	Yes	Yes	Yes	8	Yes	Yes	No
DVCPRO50	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 30 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 40 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 50 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
DV100 1080I	Yes	Yes	Yes	Yes	8	Yes	Yes	No

K2-AvidTM Build 7.0.0.105 supports Interplay 2.1

Compression formats Supported on PVS1100 with software build 5.4.9.1328

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
DVCAM	Yes	Yes	Yes	Yes	8	Yes	Yes	No
DVCPRO25	Yes	Yes	Yes	Yes	8	Yes	Yes	No
DVCPRO50	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 30 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 40 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 50 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No

NOTE: For PVS, ingest & Send to playback are only supported if Windows XP operating system are used on the Avid editor and transfer manager.

Compression formats Supported on K2 with software build 3.3.2.1412

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
DVCAM	Yes	Yes	Yes	Yes	8	Yes	Yes	No
DVCPRO25	Yes	Yes	Yes	Yes	8	Yes	Yes	No
DVCPRO50	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 30 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 40 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 50 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No

Compression formats Supported on K2 Summit/Solo system with software build 7.3.8.1432

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
DVCAM	Yes	Yes	Yes	Yes	8	Yes	Yes	No
DVCPRO25	Yes	Yes	Yes	Yes	8	Yes	Yes	No
DVCPRO50	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 30 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No
D10 40 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
D10 50 Mb.	Yes	Yes	Yes	Yes	8	Yes	Yes	No
DV100 1080I	Yes	Yes	Yes	Yes	8	Yes	Yes	No

K2-AvidTM Build 7.0.0.112 to build 7.0.0.128

Compression formats Supported on PVS1100 with software build 5.4.9.1328

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
DVCAM	Yes	Yes	Yes	Yes	16	Yes	No	No
DVCPRO25	Yes	Yes	Yes	Yes	16	Yes	No	No
DVCPRO50	Yes	Yes	Yes	Yes	16	Yes	No	No
D10 30 Mb.	Yes	Yes	Yes	Yes	16	Yes	No	No
D10 40 Mb.	Yes	Yes	Yes	Yes	16	Yes	No	No
D10 50 Mb.	Yes	Yes	Yes	Yes	16	Yes	No	No

NOTE: For PVS, ingest is only supported if Windows XP operating system are used on the Avid editor and transfer manager.

Compression formats Supported on K2 with software build 3.3.2.1412

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
DVCAM	Yes	Yes	Yes	Yes	16	Yes	Yes	No
DVCPRO25	Yes	Yes	Yes	Yes	16	Yes	Yes	No
DVCPRO50	Yes	Yes	Yes	Yes	16	Yes	Yes	No
D10 30 Mb.	Yes	Yes	Yes	Yes	16	Yes	Yes	No
D10 40 Mb.	Yes	Yes	Yes	Yes	16	Yes	Yes	No
D10 50 Mb.	Yes	Yes	Yes	Yes	16	Yes	Yes	No

Compression formats Supported on K2 Summit system with software build 7.3.8.1432

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
DVCAM	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
DVCPRO25	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
DVCPRO50	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
D10 30 Mb.	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
D10 40 Mb.	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
D10 50 Mb.	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
DV100 1080I	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
DV100 720P	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
AVCI 720P 50Mb	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
AVCI 720P 100Mb	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
AVCI 1080 50Mb	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
AVCI 1080 100Mb	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
XDCAM-HD 1080 18Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-HD 1080 25Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-HD 1080 35Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-HD422 1080 50Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-EX 1080 35Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-EX-HD422 720P 50Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-EX 720P 25Mb	No	No	No	No	No	No	No	No
XDCAM-EX 720P 35Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes

K2-AvidTM Build 7.0.0.129 and up supports Interplay Engine 2.5.0.1

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
DVCAM	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
DVCPRO25	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
DVCPRO50	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
D10 30 Mb.	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
D10 40 Mb.	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
D10 50 Mb.	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
DV100 1080I	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
DV100 720P	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
AVCI 720P 50Mb	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
AVCI 720P 100Mb	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
AVCI 1080 50Mb	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
AVCI 1080 100Mb	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
XDCAM-HD 1080 18Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-HD 1080 25Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-HD 1080 35Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-HD422 1080 50Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-EX 1080 35Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-EX-HD422 720P 50Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-EX 720P 25Mb	No	No	No	No	No	No	No	No
XDCAM-EX 720P 35Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
DNxHD 120 (HD1080i)	No	Yes	Yes	Yes	16	Yes	Yes	Yes
DNxHD 185 (HD1080i)	No	Yes	Yes	Yes	16	Yes	Yes	Yes
DNxHD 185x (HD1080i)	No	Yes	Yes	Yes	16	Yes	Yes	Yes
DNxHD 120 (HD720p)	No	Yes	Yes	Yes	16	Yes	Yes	Yes
DNxHD 185 (HD720p)	No	Yes	Yes	Yes	16	Yes	Yes	Yes
DNxHD 185x (HD720p)	No	Yes	Yes	Yes	16	Yes	Yes	Yes
DNxHD 145 (HD1080i)	Yes	No	Yes	Yes	16	Yes	Yes	Yes
DNxHD 220 (HD1080i)	Yes	No	Yes	Yes	16	Yes	Yes	Yes
DNxHD 220x (HD1080i)	Yes	No	Yes	Yes	16	Yes	Yes	Yes
DNxHD 145 (HD720p)	Yes	No	Yes	Yes	16	Yes	Yes	Yes
DNxHD 220 (HD720p)	Yes	No	Yes	Yes	16	Yes	Yes	Yes
DNxHD 220x (HD720p)	Yes	No	Yes	Yes	16	Yes	Yes	Yes

K2-AvidTM Build 7.0.0.143 and up supports Interplay Engine 2.7.0.2

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
DVCAM	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
DVCPRO25	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
DVCPRO50	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
D10 30 Mb.	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
D10 40 Mb.	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
D10 50 Mb.	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
DV100 1080I	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
DV100 720P	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes

Codec	FPS 29.97	FPS 25 Hz	PCM 16 bit	PCM 24 bit	Audio Track	Ingest	Playback	Metadata
AVCI 720P 50Mb	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
AVCI 720P 100Mb	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
AVCI 1080i 50Mb	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
AVCI 1080i 100Mb	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
AVCI 1080p 100Mb	Yes	Yes	Yes	Yes	16	Yes	Yes	Yes
XDCAM-HD 1080 18Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-HD 1080 25Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-HD 1080 35Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-HD422 1080 50Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-EX 1080 35Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-EX-HD422 720P 50Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
XDCAM-EX 720P 25Mb	No	No	No	No	No	No	No	No
XDCAM-EX 720P 35Mb	Yes	Yes	Yes	Yes	16	Yes	No	Yes
DNxHD 120 (HD1080i)	No	Yes	Yes	Yes	16	Yes	Yes	Yes
DNxHD 185 (HD1080i)	No	Yes	Yes	Yes	16	Yes	Yes	Yes
DNxHD 185x (HD1080i)	No	Yes	Yes	Yes	16	Yes	Yes	Yes
DNxHD 120 (HD720p)	No	Yes	Yes	Yes	16	Yes	Yes	Yes
DNxHD 185 (HD720p)	No	Yes	Yes	Yes	16	Yes	Yes	Yes
DNxHD 185x (HD720p)	No	Yes	Yes	Yes	16	Yes	Yes	Yes
DNxHD 145 (HD1080i)	Yes	No	Yes	Yes	16	Yes	Yes	Yes
DNxHD 220 (HD1080i)	Yes	No	Yes	Yes	16	Yes	Yes	Yes
DNxHD 220x (HD1080i)	Yes	No	Yes	Yes	16	Yes	Yes	Yes
DNxHD 145 (HD720p)	Yes	No	Yes	Yes	16	Yes	Yes	Yes
DNxHD 220 (HD720p)	Yes	No	Yes	Yes	16	Yes	Yes	Yes
DNxHD 220x (HD720p)	Yes	No	Yes	Yes	16	Yes	Yes	Yes

Installation and configuration

Installation instructions

Prior to installing build 7.0.0.104 or 7.0.0.105 you must install *Microsoft Visual C++ 2008 SP1 Redistributable Package (x86)*. This can be downloaded from Microsoft or from the same location build 7.0.0.104 or 7.0.0.104 downloaded from. The file is named *vcredist_x86.exe*.

Follow the installation instructions in K2 Avid Plug-in manual PN. 071-8551-02 for detail over how to install and configure build 7.0.0.104 or 7.0.0.105.

Installation of build 7.0.0.112 is much simpler as it only support Avid Interplay Transfer engine 2.2.1.1 but it's still highly recommended you refer to the K2 Avid Plug-in manual PN. 071-8551-02.

Installing Avid Media Access

Do the following steps to install Grass Valley AMA (Avid Media Access):

1. Install SNFS client software on the device hosting the Editing application.

   This provides guaranteed bandwidth, thereby ensuring smooth playback in the Editing application.

2. Use CIFS mounted `V:` volume on standalone K2 Summit system.

   It is recommended for you to use the latest generation K2 Summit system hardware since older hardware may not have the required hardware resources to sustain smooth playback in the Editing application.

3. Use media files on removable media if the original folder and file structure are kept intact.

   If the removable media cannot provide adequate edit playback, transcode or consolidate the media into one of Avids native codec formats.

Installing TServerSvc on the K2 Media Clients and K2 Summit Production Client

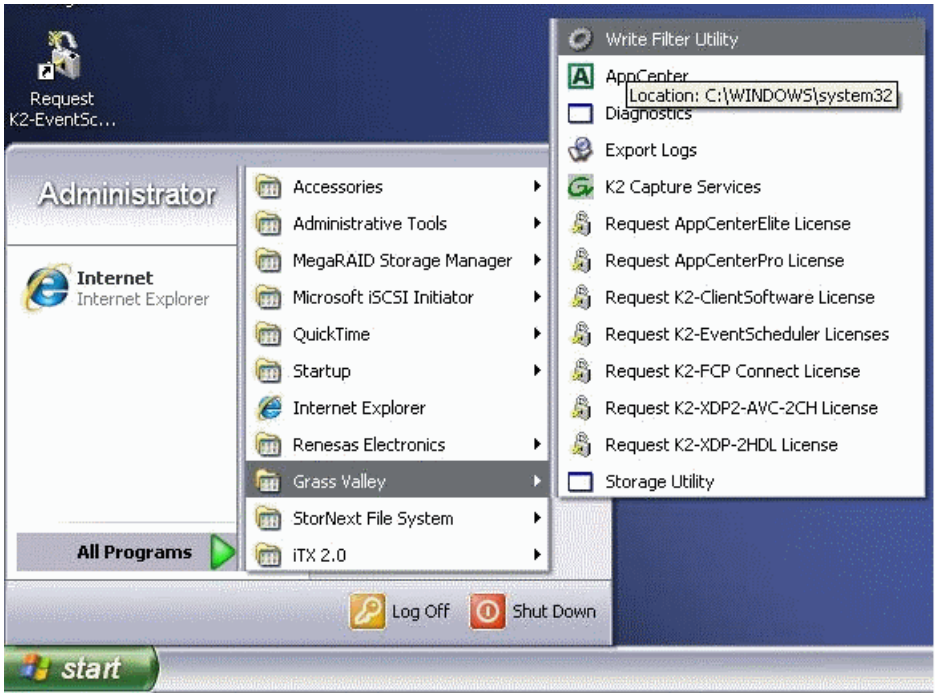
If you previously had the TserverSvc installed, then uninstall this prior to installing the new version.

- For Microsoft Windows XP Operating System, before you can install software on the K2 Summit Production Client, you need to disable the Write Filter utility.

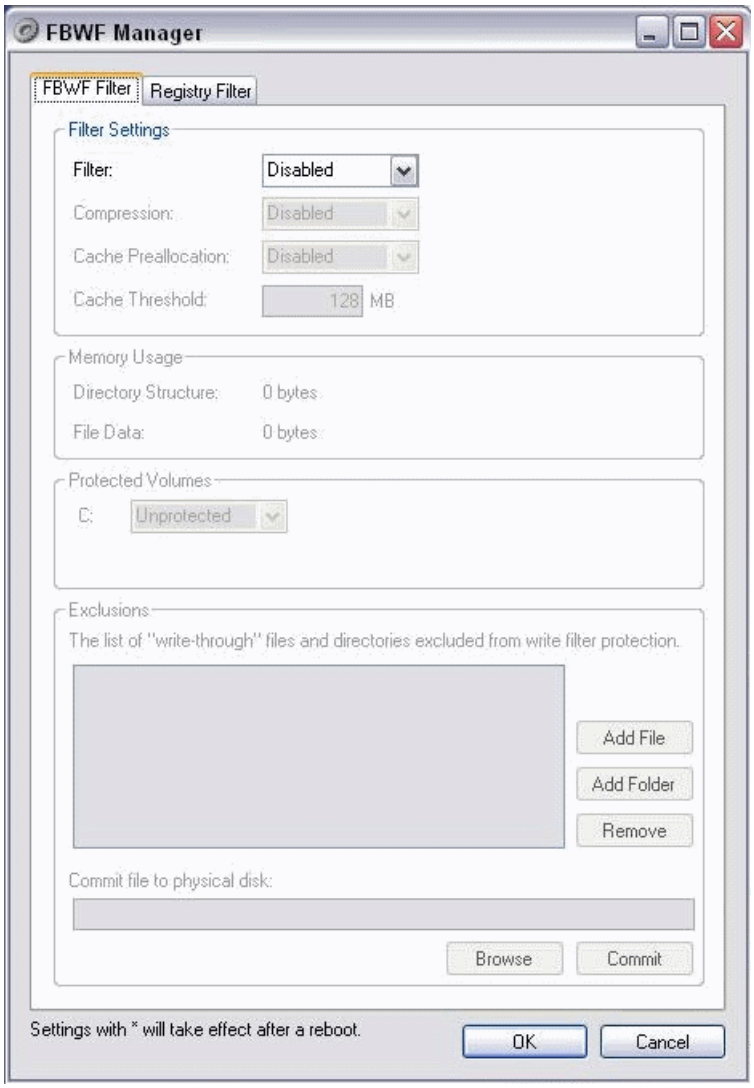
- For newer K2 Summit system with Microsoft Windows 7 (for 9.x) that use McAfee embedded security, you need to put the system in Update mode before installing the new software.

The TServerSvc can be installed on standalone K2 Media Clients, K2 Summit Production Clients, K2 Summit 3G Production Clients or K2 Media Servers (with the role of FTP servers) when configuring systems with external (shared) storage.

1. Navigate to the Write Filter Utility and launch the application.



2. Under Filter Settings, set the Filter to **Disabled** as shown.



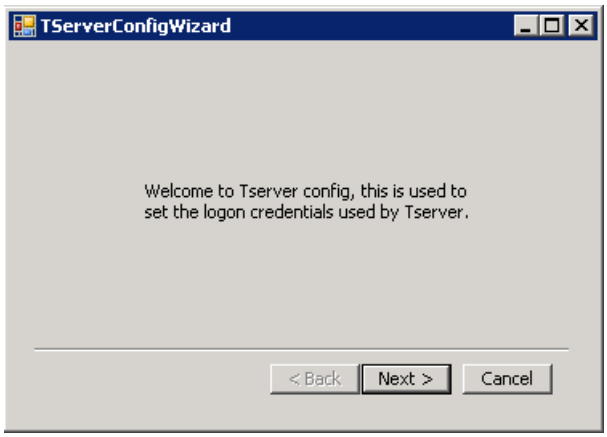
   If the filter setting is changed then you will be requested to reboot the K2 Summit Production Client before proceeding with the K2Tserver installation.

3. Browse the folder with the installers and access the folder \K2Tserver\.
4. Double-click Setup.exe.
5. Click **Next** in the "Welcome to the InstallShield Wizard for Grass Valley K2 AvidTM K2 Tserver" dialog box.

   Next the License Agreement is displayed.

6. Select "I accept the terms in the License agreement" and click **Next**.
7. Click **Install** to start the installation or **Cancel** in the "Ready to install" dialog box.
8. The status dialog then displays the progress of the installation.

9. The following Configuration Wizard is then displayed.



- This is used to override the default credentials.

10. Click **Next** to walk through the wizard.
11. To set the credential using the wizard, do one of the following:

Options	Description
Default credentials	• Username: Administrator • Password: adminGV!
If installing on a K2 Summit system version earlier than 8.x, use this default credentials	• Username: Administrator • Password: adminK2

12. Click **Next** and **Finish** to complete the wizard.

This wizard can be run at any time from `C:\profile\TserverConfigWizard.exe`.

13. Click **Finish** when installation completes in the "InstallShield Wizard Completed" dialog box.

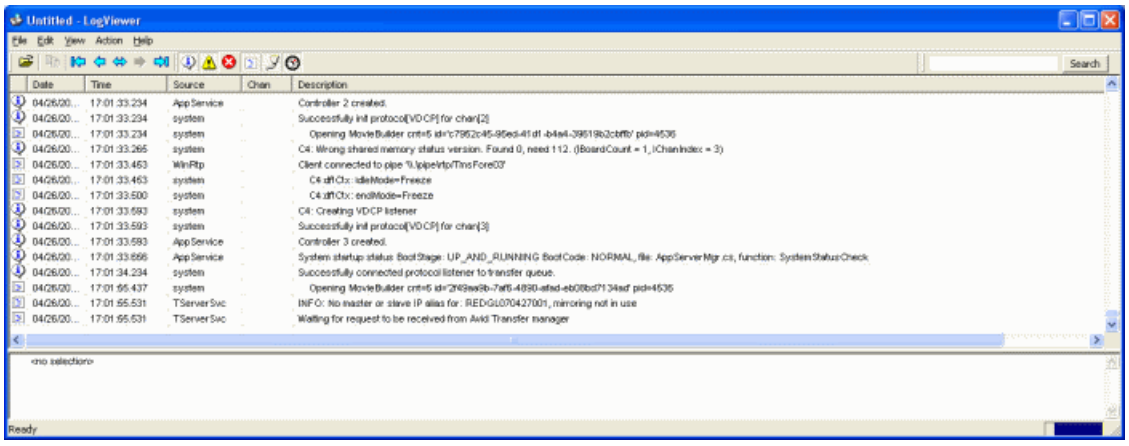
Verify TserverSvc is installed correctly

1. On the K2 Media Client or K2 Summit Production Client, open the Logviewer program in `c:\profile\log.exe`.

   NOTE: Make sure no filters are selected.

2. Then look for the following TServerSvc messages.

   - INFO: No master or slave IP alias for: DeviceHostName, mirroring not in use.
   - Waiting for request to be received from Avid Transfer manager.



This indicates the service is installed and running.

3. Repeat the above steps for each K2 Media Client or K2 Summit Production Client you wish to use.

   NOTE: Default username administrator and password adminK2 are used by the Tserver. You can overwrite the default credentials by running `C:\profile\TserverConfigWizard.exe`.

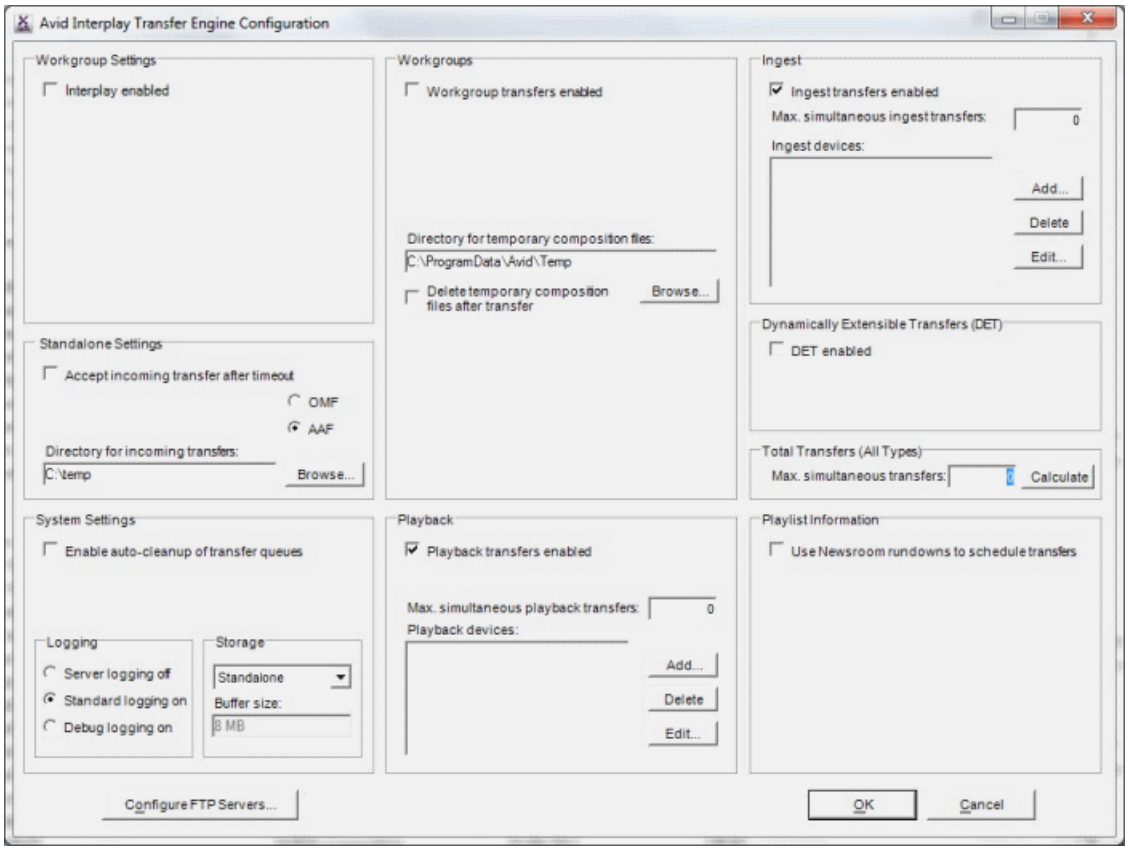
Prerequisites for installation of K2-AvidTM Software on Avid devices

1. NewsCutter® or MediaComposer® software is installed on editor clients.
2. Each Editor has Avid Interplay Transfer Client software installed.
3. Avid Interplay Transfer Engine software is installed.
4. Each Editor is configured for Transfers.
5. Transfer Engine has been configured with a valid Storage Type.
6. SNFS client software has been installed and configured if GV AMA is used to link to media files on GV SAN FS (K2 media file system).

Configuring Avid Interplay Transfer Engine

The following configuration is for a standalone Interplay Transfer Engine.

1. Open the Avid Interplay Transfer Engine Configuration by doing one of the following:
   - Click the icon on the desktop.
   - Find the configuration in `C:\Program Files\Avid\Avid Interplay Transfer Engine\TRANSFERMGRSERVERCONFIG\tmconfig.exe`.



2. Set the **Standalone Settings** by doing the following:
   a) Select the **Accept Incoming transfers after timeout** check box.
   b) Select **AAF**.
   c) Select the directory for incoming transfers.

3. Set the **System Settings** by doing the following:
   a) Select the **Enable auto-cleanup of transfer queues** check box.
   b) Set the Storage Type to **Standalone**.
4. Set the **Playback** by doing the following:
   a) Select the **Playback transfers enabled** check box.
   b) Set the **Max simultaneous playback transfers** to 4.
   c) Do not select the**Long GOP transfers enabled** check box.
5. Set the **Ingest** by doing the following:
   a) Select the **Ingest transfers enabled** check box.
   b) Set the **Max simultaneous ingest transfers** to 4.
6. Click **Calculate** to update the Max. Simultaneous Transfers in the **Total Transfers (All Types)** section.
7. Click **OK** to save the configuration or click **Cancel** to discard the changes.
8. If the Interplay engine is running, terminate and restart to use the new configuration.

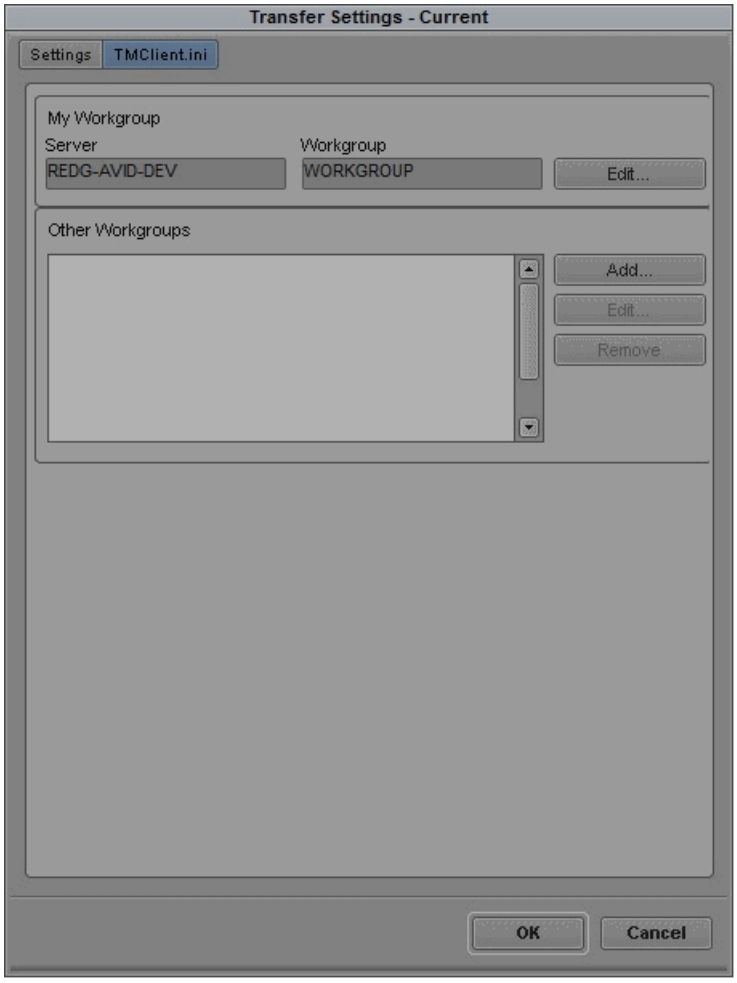
Configuring the Avid Editor for Transfers

The following configuration uses the Avid Media Composer.

1. Start the Avid Media Composer.
2. Click the **Edit** menu, and then select **Preferences**.
3. Select **Transfer** under the Settings tab.
4. In the Send To Playback, locate the Output Audio Mix and select **Direct channel output or Stereo output**.
5. Click on the TMClient.ini tab and click **Add**.

6. Add the host name of the device which is running the Avid Interplay Transfer Engine. In this example **REDG-AVID-DEV**, and set the Workgroup to **WORKGROUP**.

   NOTE: The names must match the names used to configure the Avid Interplay Transfer Engine.



7. Click **OK** to save and exit.
8. Restart the Editor.

   Configuration of the editor is complete.

Installing the K2AvidDHM software

Do the following steps to install the K2AvidDHM software on the PC that runs the Avid Interplay Transfer Engine.

1. Browse the folder of installers and navigate to `\K2AvidDhm\Disk1\`.
2. Double-click **Setup.exe**.
3. Click **Next** in the "Welcome to the InstallShield Wizard for K2AvidDHM" dialog box.

   The License Agreement dialog box is displayed.

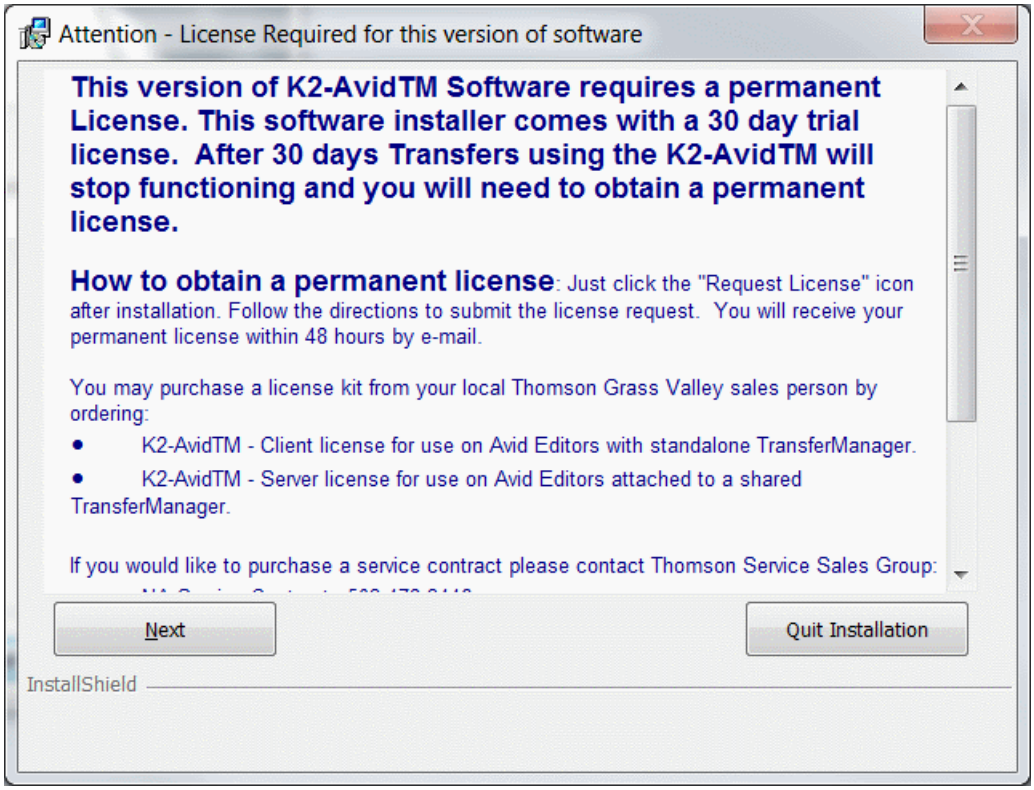
4. Select the **I accept the terms in the License agreement** check box.
5. Take the time to read the information provided on the license agreement and click **Next**.
6. Click **OK** if you get the following message when you are attempting to install on a device which do not have any Avid Interplay Transfer Engine installed.

NOTE: Ensure that you have installed Avid Interplay Transfer.

Likewise a message will be displayed if both Transfer Manager and Interplay Transfer engine are installed.

7. Click **Install** to start the installation in the "Ready to Install" dialog box.

8. Do take the time to read the information provided in the "License Required for this version of software" dialog box and click **Next**.



   The status dialog then displays the progress of the installation.

9. Click **Finish** when the install is completed.
10. Restart the Avid Interplay Transfer Engine to complete the DHM installation.

Verify K2 Avid DHM is installed correctly

1. Start the License Manager and verify licenses are installed.
2. On the Avid Transfer manager / Interplay engine device, locate the License manager icon on the desktop and double click to start this.
3. If you are upgrading from a previous version and a permanent license was previously installed, then verify that it is still present. Otherwise add the license which was backed up previously and verify that it is still valid.

4. If you do not have a permanent license, check if a temporary license was installed during the setup. Otherwise you can add a temporary license which can be found in:

Options	Description
32-bit Operating System	*C:\Program Files\Thomson Grass Valley\SabreTooth\TemporaryLicense.txt*
64-bit Operating System	*C:\Program Files (x86)\Grass Valley\SabreTooth*

NOTE: You will need a permanent license to operate beyond the 30 day trial period. Details on how to obtain permanent license can be found elsewhere in this manual.

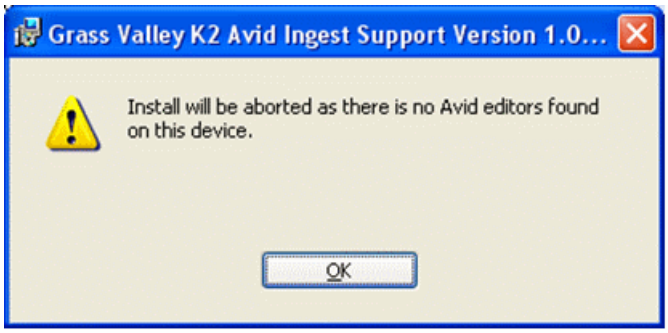
Installing the K2 Avid Ingest software

1. Browse the folder of installers and navigate to *\K2ingest\Disk1*.
2. Double-click **Setup.exe**.
3. Click **Next** in the "Welcome.." dialog box.

4. Click **OK** if you get one of the following below:

   Please refer to *Prerequisites for installation of K2-AvidTM Software on Avid devices* on page 996 if you encounter any of the following error warnings.

   a) You may get the following message if you are attempting to install on a device which does not have an Avid Editor installed.



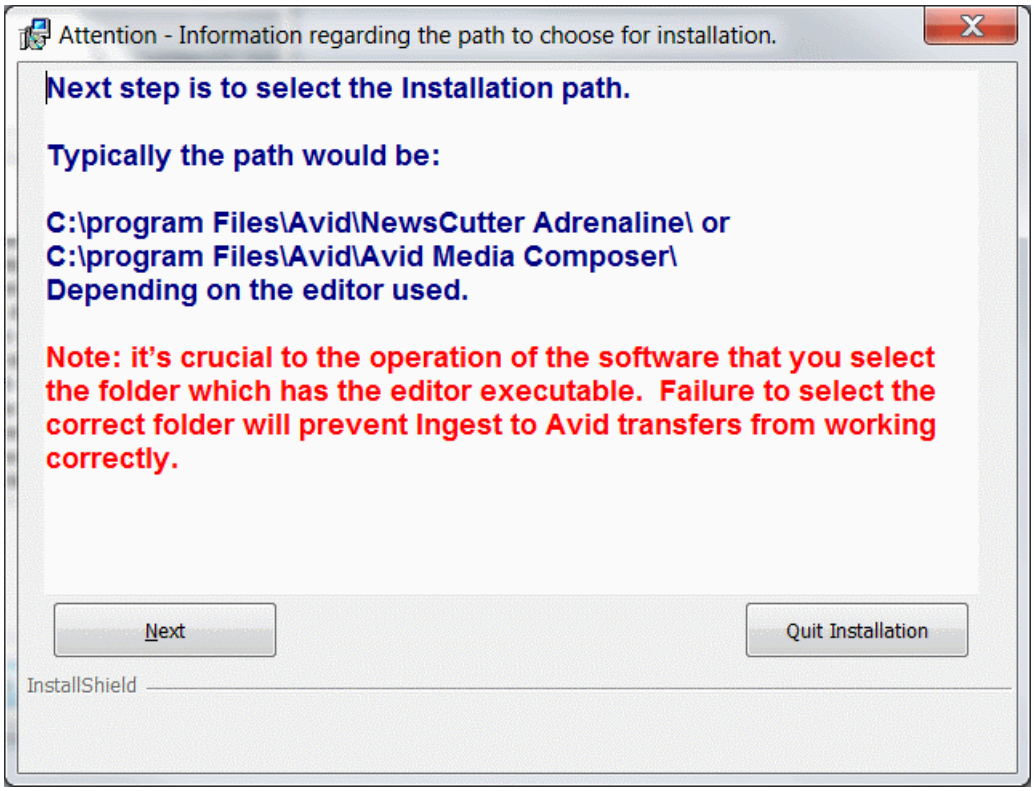
   b) You may get the following message if you are attempting to install on a device which has both AvidNewsCutter and Avid MediaComposer installed.

   c) Or if there is no TransferManager Clients or Avid Interplay Transfer Clients installed, you may see the following message.

   The "License Agreement" dialog box is displayed.

5. Select the **I accept the terms in the License agreement** check box.
6. Take the time to read the information provided on the license agreement and click **Next**.
7. Select the installation path. Take a moment to find out where the Avid Editor executable is located.

   NOTE: The Install program will attempt to locate the Avid editor executable and use the path found.

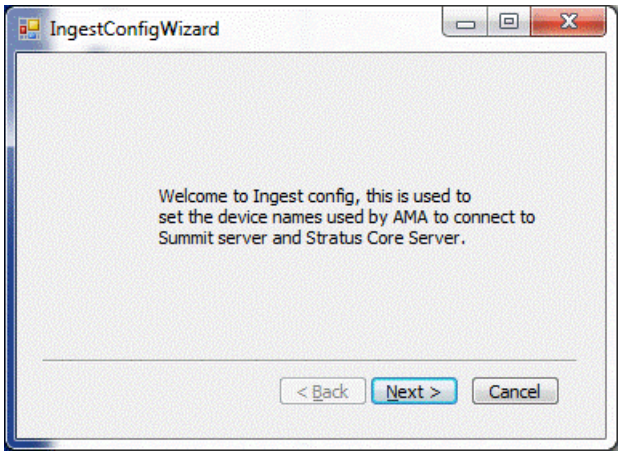


8. Click **Next**.

   The next dialog box displays the path found.
9. Verify that the path is correct, and click **Next**. Otherwise, click **Change** and browse to the correct destination folder.
10. Click **Install** to begin the installation.

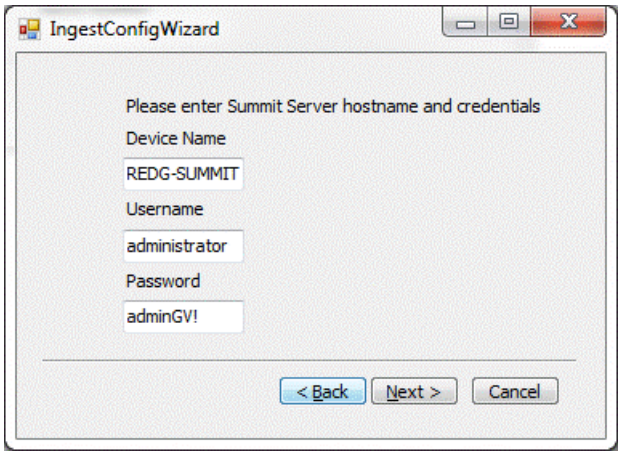
    The status dialog then displays the progress of the installation.

11. The following Configuration Wizard is then displayed.

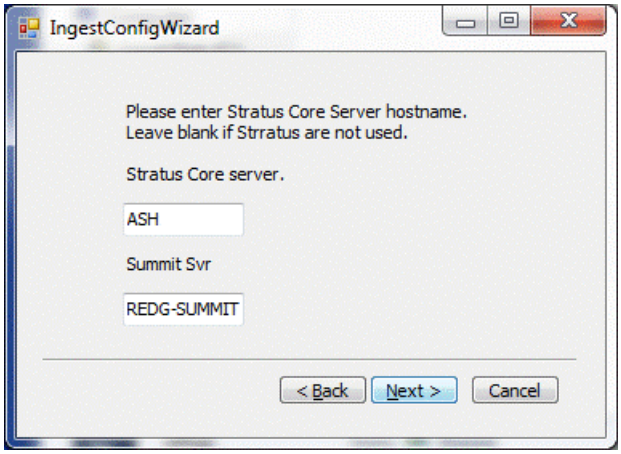


This is used to set the hostname of the K2 Media Server (FSM) used for AMA linking.

12. If GV STRATUS is used, you need to set the Core Server hostname and the hostname of the device the K2 Summit system MDI is connecting to.
13. Click **Next** to walk through the wizard.
14. Enter the hostname of the FSM and credentials if AMA is used, otherwise leave blank and click **Next**.

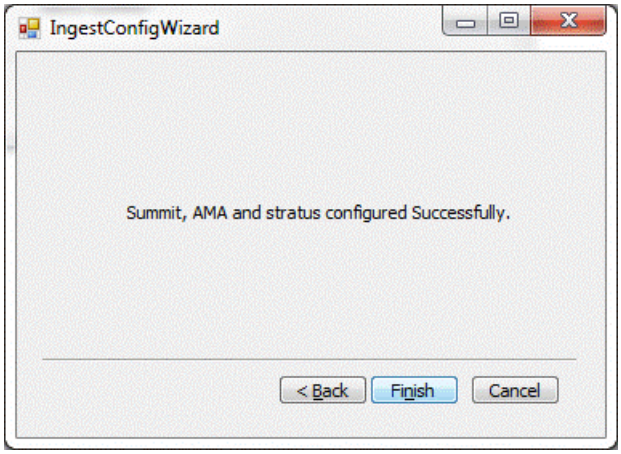


15. Enter the hostname of the Core Server and host name of the K2 Summit server used by the K2 Summit system MDI.



Leave the space blank if GV STRATUS integration is not used.

16. Click **Next** to complete this Wizard.



This can be run at any time from `C:\Program Files\Avid\Avid Media Composer\IngestConfig64.exe`.

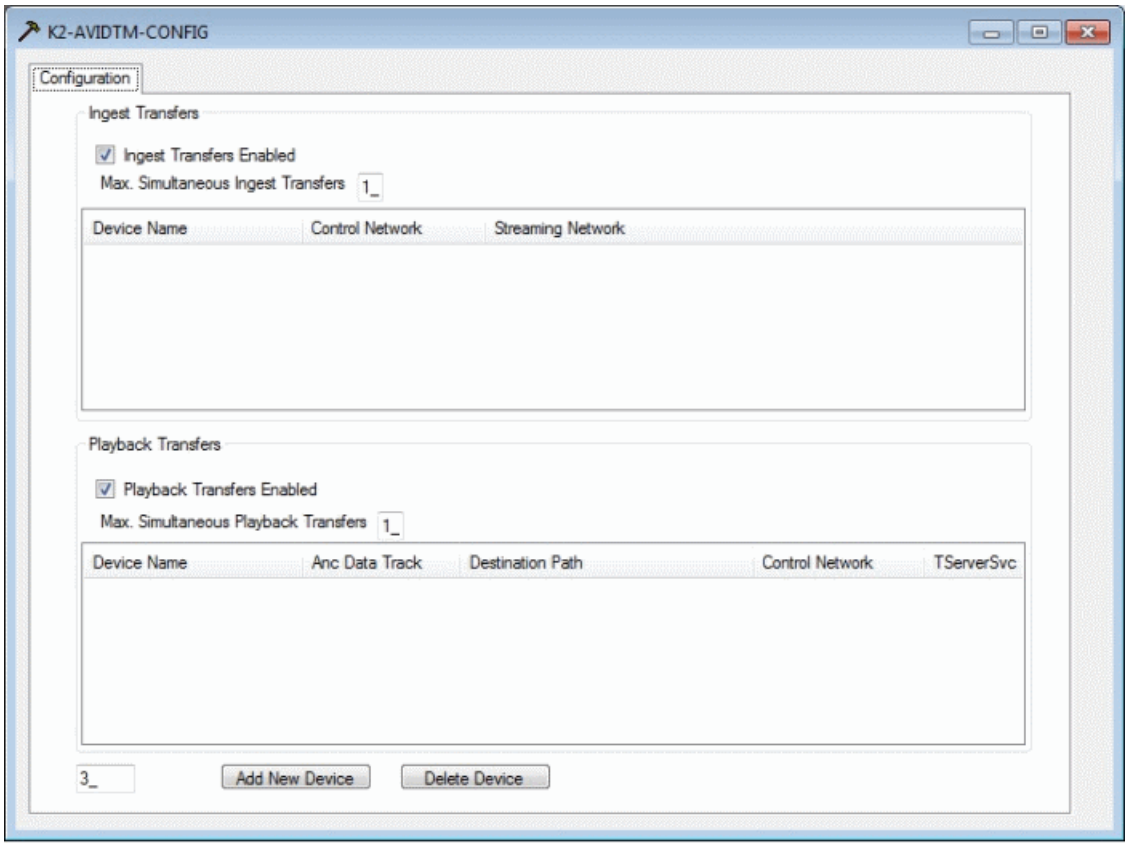
17. Click **Finish** when the install is completed.

NOTE: Default username "Administrator" and password "adminGV!" are used by the Ingest software.

Add and configure devices for Ingest and Playback

1. Start the K2-AVIDTM-CONFIG.

   If there are no configured devices, it will appear as shown below.

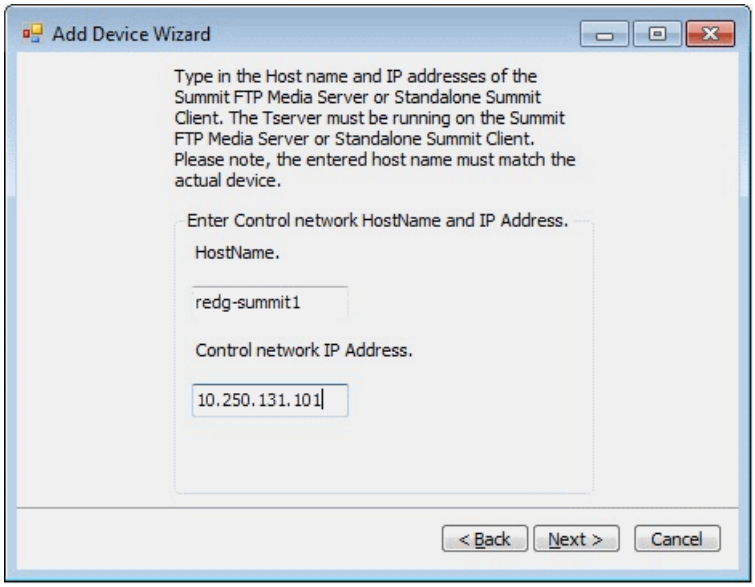


2. Click **Add New Device**.

   The Add Device Wizard displays.

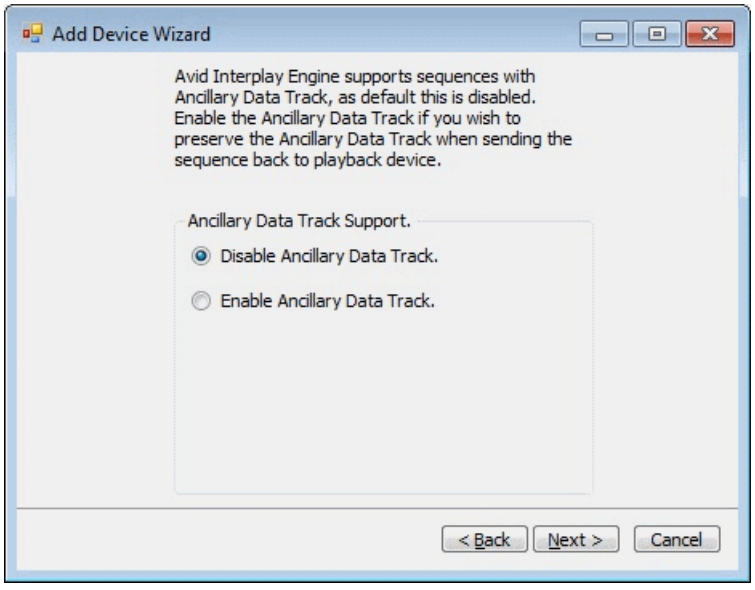
3. Select the type of network configuration.

4. Enter the host name of the standalone K2 Summit system or the host name of the K2 Media Server with the role of FTP server.



NOTE: The host name used must match the actual device name.

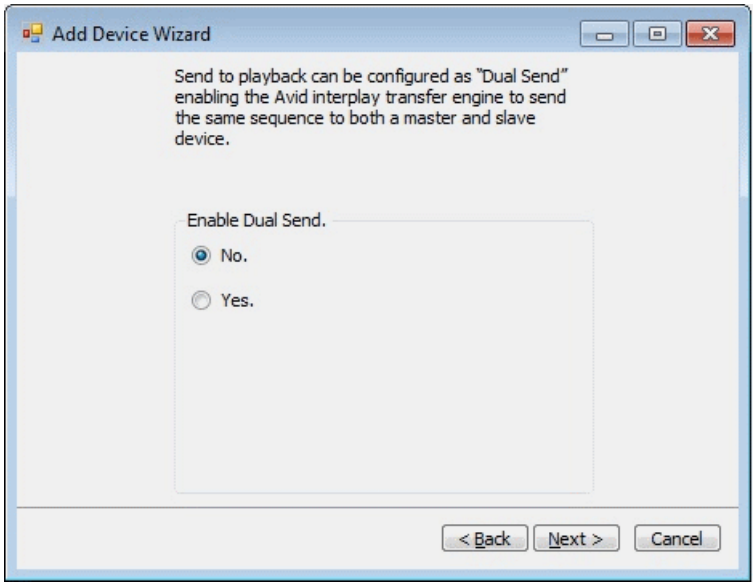
5. Select to enable Ancillary Data Track support if you want to preserve Ancillary data when sending sequences back to the playback device.



6. Select **Yes**, if you wish to send back to a different folder than default.

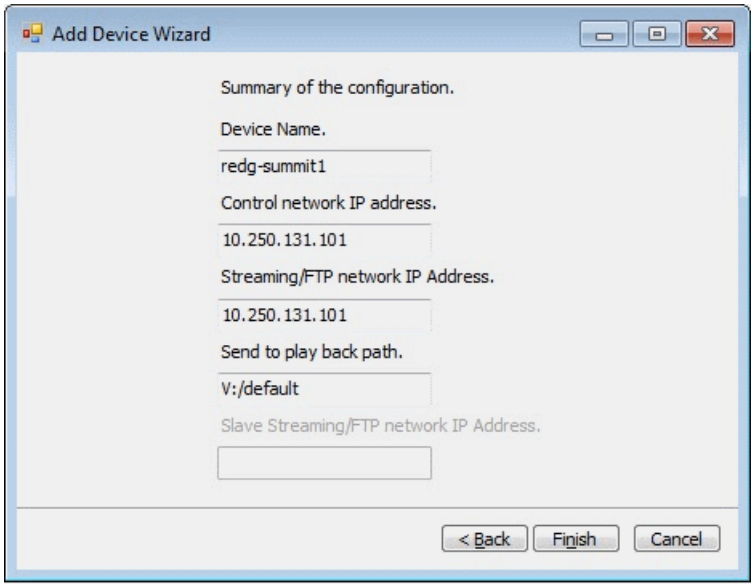
NOTE: You need to run the wizard twice when overwriting the folder. Once with no overwrite and then once more for the overwrite.

7. Select **Yes** if you want dual send support.



8. Click **Next**.

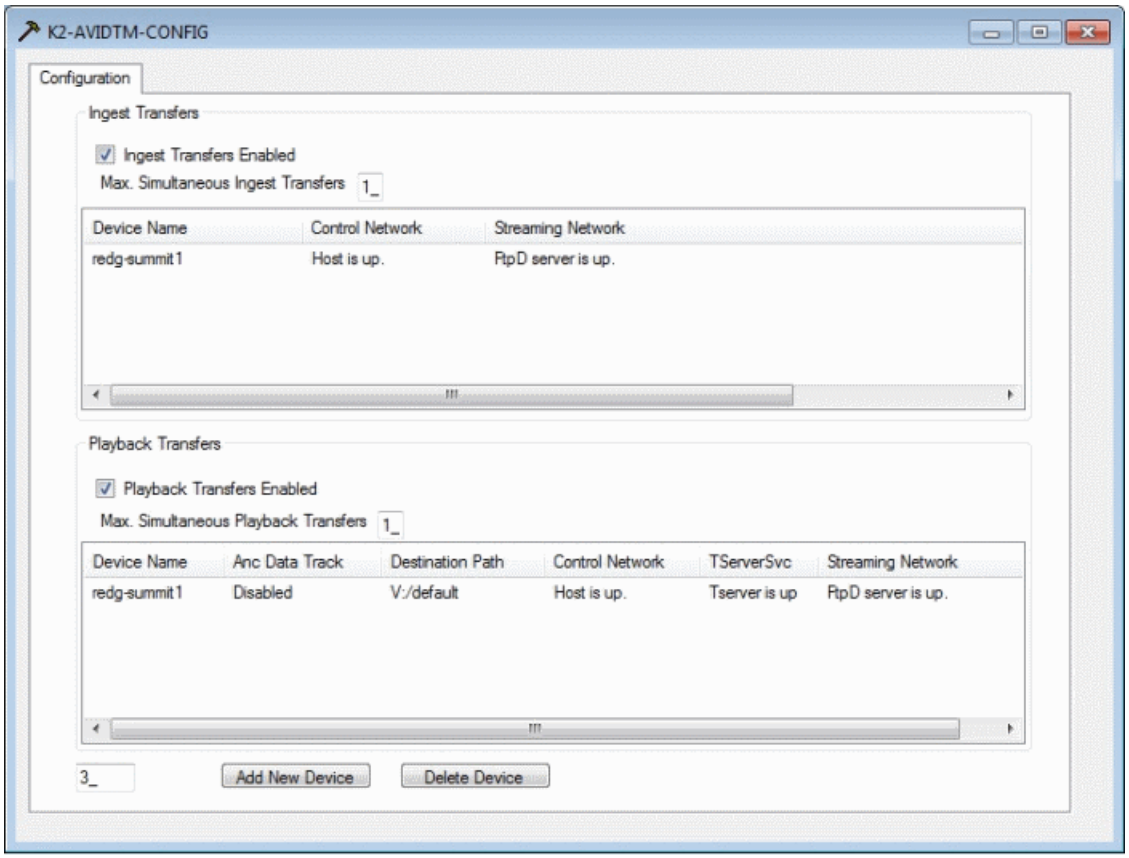
   The summary page displays.



9. Click **Finish** to exit from the Add Device Wizard.

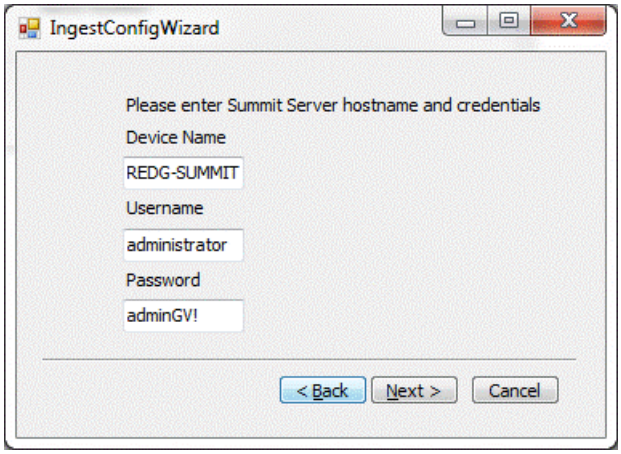
   The Configuration page displays.

   NOTE: This may take several seconds as the program verifies the network connection, if Tserver and FtpD is up.

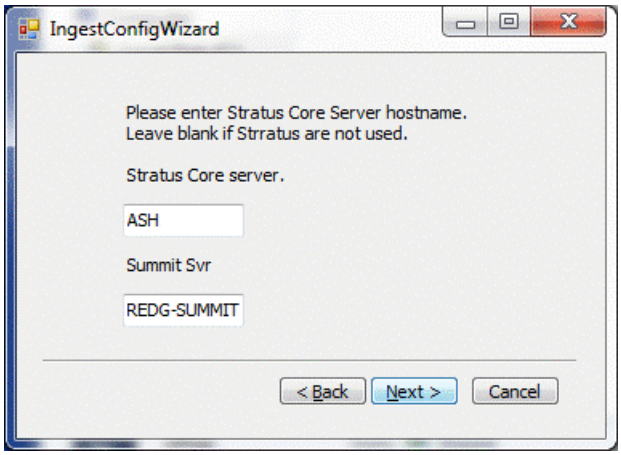


10. If GV STRATUS is used, set the GV STRATUS Core Server hostname and the hostname of the device to which the GV STRATUS K2 Summit system MDI connects.
11. Click **Next** to walk through the wizard.

12. Enter the hostname of the FSM and credentials if AMA is used, otherwise leave blank and click **Next**.

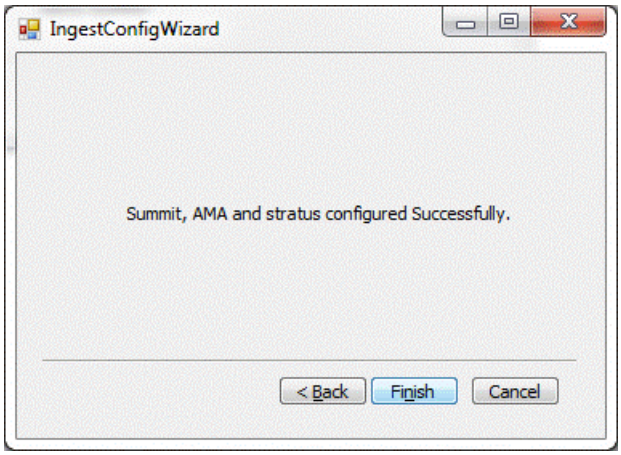


13. Enter the hostname of the Core Server and host name of the K2 Summit server used by the K2 Summit system MDI.



Leave the space blank if GV STRATUS integration is not used.

14. Click **Next** to complete this Wizard.



This can be run at any time from `C:\Program Files\Avid\Avid Media Composer\IngestConfig64.exe`.

15. Click **Finish** when the install is completed.

NOTE: Default username "Administrator" and password "adminGV!" are used by the Ingest software. You can overwrite the default credentials used by the Ingest software. This is done in the registry in the following location: `HKEY_LOCAL_MACHINE\SOFTWARE\Grass Valley Group\Applications\K2-AvidTM\Setup` and for the K2-AvidExplorer at `HKEY_LOCAL_MACHINE\SOFTWARE\Grass Valley Group\Applications\K2-AvidTM\K2-AvidExplorer`.

Using the GV AMA plug-in

Before you can link to any files, verify the following:

- Check the GV AMA plug-ins are installed. At the Editing software, select **TOOLS** and choose **Console** to call up the console window. At the bottom of the window, type AMA_ListPlugins. A report is displayed below:

  ```
  AMA PLUG-IN NAME COMPANY NAME VERSION
  ```

  - `Avid MXF MSP Plug-In Avid Technology, Inc. 1.1`
  - `Sphere (5850 1.1.5964899) Avid Technology, Inc. 1.1`
  - `AS-02 Plug-In Avid Technology, Inc. 1.2`
  - `AS-11 Plug-In Avid Technology, Inc. 1.0`
  - `MSP_GrassValley for 64Bit OS Grass Valley USA, LLC. 0.3`
  - `MSP_MXF Plug-In Avid Technology, Inc. 1.9`
  - `QuickTime Plug-In Avid Technology, Inc. 1.3`
  - `WaveAiff Plug-In Avid Technology, Inc. 1.0`

- Verify the MSP_GrassValley and MVP_GrassValley plug-ins are listed.
- Confirm the plug-ins are correctly installed and configured.

- To verify and configure the volumes, the volume must be mounted and mapped using driver letter `V:` before the GV AMA plug-ins can be used to link any files.

  If SNFS client are used: SNFS client mounting are used if K2 SAN's are used. Verify the SNFS client are installed and configured to use driver letter `V:`.

  If CIFS client are used: CIFS client mounts are used when working on standalone K2 Summit system. The K2 Summit system `V:` drive must be shared at root level with the Share Name **V** before this drive can be mounted using the command shown below: The volume is mounted, using the following command. net use `V: \\SummitHostname\V /USER:SummitHostname\administrator /PERSISTENT:YES`.

  If Removable drives are used: If the original media on the K2 Summit system existed in `V:\media\default\Myclip.cmf \`, then the removable drive should have the same path `media\default\Myclip.cmf \` and all the media files should reside in the `Myclip.cmf` folder.

  The GV AMA plug-in supports linking to files in two ways:

- Manually link to files using **FILE | AMA LINK**.
- Manually link to volumes (folders) **FILE | LINK TO AMA VOLUMES**.

1. To manually link to files, do the following:
   a) Open and select the bin in which you want the master clip or sequence to appear.
   b) Select **FILE | AMA LINK**, navigate to the filepath, and select the file or files for linking.
   c) Choose the type of linking:

      - XML files: Creates a master clip or sequence which references all the media files and metadata as described by the XML.
      - IDX files: Creates master clips with just one track. Timecode and data files are not supported.

      The linked files appear as master clips or sequences.

2. To manually link to volumes (folders), do the following:
   a) Select **FILE | LINK TO AMA VOLUMES** and file type as below:

      - Summit Media Volume Plug-in (MVP) (Folder) for volume linking.
      - Summit (*.XML *.IDX) for link to media files.

   b) Navigate to the required folder, such as `V:\media\default`.

      A new bin is created and populated with all the assets found in the folder. The linked asset appears as master clips or sequences.

   c) To limit the number of assets in each folder, use **Link to files** and select only the files needed.

      When you link to volumes, only the content within a folder can be linked. All the assets within the selected folder are enumerated and linked. Master clips or sequences are created using all the media files and metadata as described by each of the assets XML found in the folder.

When you use AMA linked files and you are done editing the sequence, you must consolidate or transcode the sequence before this can be sent to the playout device using Avid Interplay transfer engine. Consolidate or transcode of the sequence will also share the media / sequence amongst a pool of Avid Media Composer or News Cutters sharing the same Avid storage device as the process of consolidating / transcoding checks the media into Avid Interplay.

Operational considerations

- Transfers of Mixed formats video and audio are not supported by the DHM.
- Frame chase editing (Media under construction) are reported as *In-progress* clips by the AMA plug-in. They appear in the bin with a special AMA FrameChase icon. *In-progress* clips can be refreshed using the *Refresh in-progress AMA clips* command on the Bin menu.

Installing K2 FCP Connect

Overview of K2 connections

About connecting to K2 storage with Final Cut Pro

This topic describes the different ways you can access K2 media for editing with Final Cut Pro.

Connection types are as follows:

- iSCSI – This is a connection as a client to an iSCSI K2 SAN. The connection requires a K2 FCP Connect license and supporting software on the Macintosh system. The connection uses the K2 SAN's iSCSI Gigabit Ethernet network.

Access methods are as follows:

- Edit-in-place – With this method you edit the K2 media in Final Cut Pro across the network while the media is still in place in K2 storage. You can do this over any connection type.
- File transfer – With this method you transfer (copy) the K2 media to the Macintosh system and then edit it in Final Cut Pro across the network while the media is still in place in K2 storage. You can do this over any connection type. You can initiate the transfer as file copy over iSCSI, or via FTP.

With all access methods, after you are done editing the K2 media you export it back to K2 storage via a K2 HotBin.

Software components that support various workflows are as follows:

- K2 FCP Connect – This is a Grass Valley product that supports all connection types for optimal performance. It is a toolset that must be purchased, installed, licensed, and configured. It includes GV Connect, which is a Final Cut Pro plug-in. GV Connect supports edit-in-place and file transfer over iSCSI.

Refer to product release notes for information about connections, access, and software that apply to K2 storage and versions.

For detailed instructions refer to documentation as follows:

- iSCSI – Refer to topics in this manual, as well as in the following documents:
  - K2 FCP Connect Release Notes
  - GV Connect User Manual

About QuickTime reference files

The following formats are supported as QuickTime reference files:

- DV
- AVC-Intra
- XDCAM-EX
- XDCAM-HD

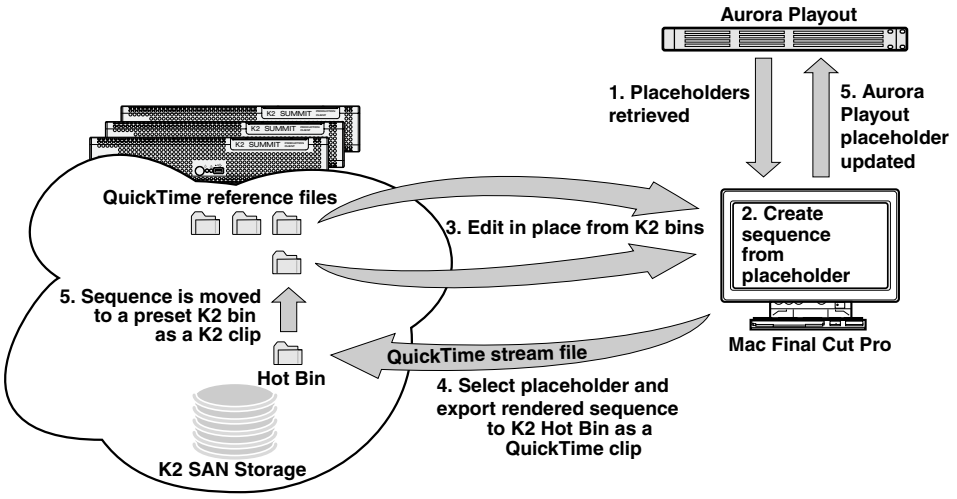
- XDCAM-HD 422
- IMX
- Avid DNxHD

The K2 clip must be a simple clip in order to create the reference file. With the QuickTime reference file you can open the K2 clip with QuickTime tools, such as Final Cut Pro, for playback and editing. For some formats the QuickTime tool does not provide default support, so you must configure the tool as necessary to support the format. The QuickTime tool must be run on another system. Running the QuickTime player or other QuickTime tools on the K2 system is not supported. You have options for connections, access, and software to support your workflow requirements.

About K2 FCP Connect

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

The workflow on a K2 SAN with GV STRATUS Rundown 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
- GV STRATUS Rundown workflow

An Aurora Edit workflow is no longer supported. Refer to previous versions of this manual for Aurora Edit information.

You have several options for connecting your Macintosh systems to K2 storage with K2 FCP Connect, all of which support the full range of K2 FCP Connect features, as follows:

- Fibre Channel SCSI to K2 SAN — Excellent performance

- Gigabit Ethernet iSCSI to K2 SAN — Excellent performance

Installing and configuring K2 FCP Connect

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 with Fibre Channel SCSI access or Gigabit iSCSI access. This checklist assumes that the K2 SAN has been installed/commissioned and is fully operational.

Prerequisites

	Task	Comment
☐	Verify K2 SAN, Macintosh, and Aurora system requirements as applicable.	—

On all Macintosh client computers

	Task	Comment
☐	Install Final Cut Pro, if not already installed.	—
☐	Install K2 FCP Connect software.	The software install file is `K2FCPConnect.pkg`. ***NOTE: Before installing the software, you must be logged in as a user with administrative privileges on the domain.*** Xsan software, which is a prerequisite for K2 FCP Connect, is included in the Macintosh operating system.
☐	Cable network connections, including Fibre Channel, if used.	—
☐	Configure for control network, if not already done.	—
☐	Configure the hosts file for networking.	Copy in host table information from the K2 SAN's hosts file.
☐	Optional: Configure Active Directory Domain	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
☐	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.
☐	When the license XML is received, install it on the K2 Media Server (FSM).	—
☐	Configure hosts files on SAN devices.	Enter Macintosh devices in hosts files.
☐	Optional: Enable Access Control Lists	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
☐	Configure hosts file.	Enter Macintosh devices in hosts file.
☐	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
☐	Test access to K2 SAN storage.	From the Macintosh system, create, modify, delete a text file.

Final tasks

	Task	Comment
☐	Optional: Verify Access Control Lists.	Do this if you are using Access Control Lists.
☐	Optional: Verify bandwidth.	Use Xbench.
☐	Test connection	Launch Final Cut Pro and open GV Connect. GV Connect automatically detects and displays K2 storage that is mounted as a volume on the Macintosh system.

	Task	Comment
☐	Verify SNFS configuration file and configure if necessary.	Check GlobalSuperUser setting.
☐	Configure K2 SAN HotBin to receive finished Final Cut Pro files.	Refer to the *K2 System Guide*.
☐	If using an Aurora Playout workflow, configure your Aurora Playout system.	The Aurora Playout system must be operational and available to the Macintosh system.

K2 SAN System Requirements

To support K2 FCP Connect your K2 SAN must meet requirements as follows. Some product/component versions have dependencies on others. Refer to compatibility matrix information in release notes for complete and updated requirements.

- K2 SAN devices with K2 software.
- On K2 SAN K2 Media Servers (FSMs), the SNFS configuration file must be configured to `GlobalSuperUser Yes`.
- The K2 SAN must have unused bandwidth sufficient to support the Mac clients.
- For GV STRATUS Rundown, requires Aurora Playout system with XMOS interface.

Macintosh System Requirements

To support K2 FCP Connect for connection to a K2 storage, your Final Cut Pro Macintosh systems have requirements as follows. Some product/component versions have dependencies on others. Refer to compatibility matrix information in release notes for complete and updated requirements.

- MacPro
- Intel processor
- Two GigE ports
- Mac OS X.
- Final Cut Pro

GV STRATUS Rundown System Requirements

If using the GV STRATUS Rundown workflow the GV STRATUS Rundown system must meet requirements as follows. Refer to compatibility matrix information in release notes for complete and updated requirements.

- GV STRATUS Rundown system with XMOS interface.

Compatible versions

At the time of this writing, versions are compatible as in the following table. However, versions of inter-related products can change at any time. Some product/component versions have dependencies

on others. Refer to compatibility matrix information in the latest release notes for complete and updated requirements.

Component	Product/Version	Comments
K2 (K2 Summit Production Client) software	9.2.0.1964	—
K2 Media File System (SNFS) software	4.2.2.b27249	—
Macintosh system	MacPro with Intel Processor, two GigE ports	—
Macintosh operating system	OS X 10.8.5	Mountain Lion Compatible version of Apple Xsan software included in Macintosh operating system.
Final Cut Pro software	7.0.3	—
Aurora Playout	8.1.0.19	
Aurora Edit	Not supported	—
K2 3.x	Not supported	—
K2 7.x	Not supported	—
K2 8.x	Not supported	—

Install K2 FCP Connect software on Macintosh systems

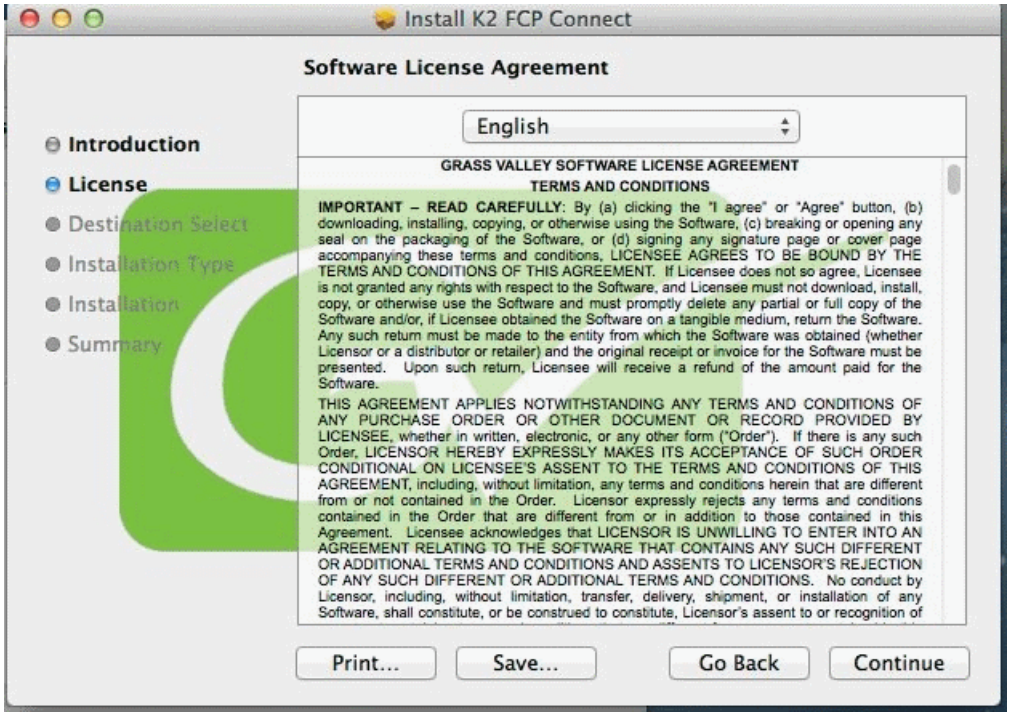
Before doing this task, procure the K2 FCP Connect installation files via download or as appropriate for your Grass Valley product.

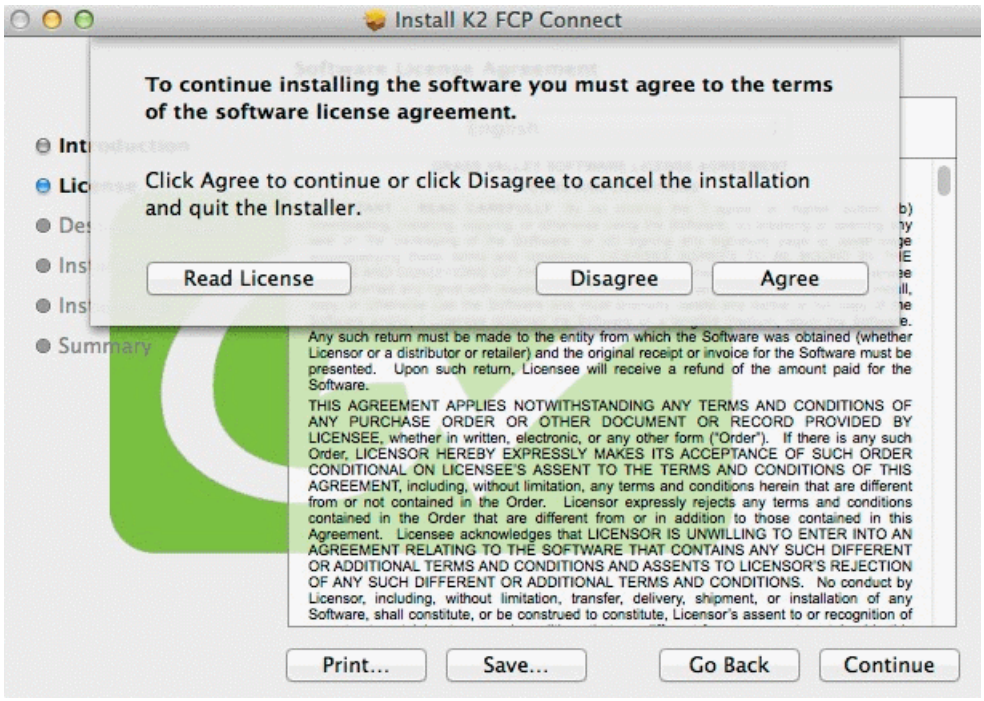
1. Prepare the Macintosh system for the restart that is required at the end of the installation process. Close any open applications as necessary.
2. Close the System Preferences window, if it is currently open.
3. From the Macintosh system, access the K2 FCP Connect installation files.

4. Double-click *K2FCPConnect.pkg*.

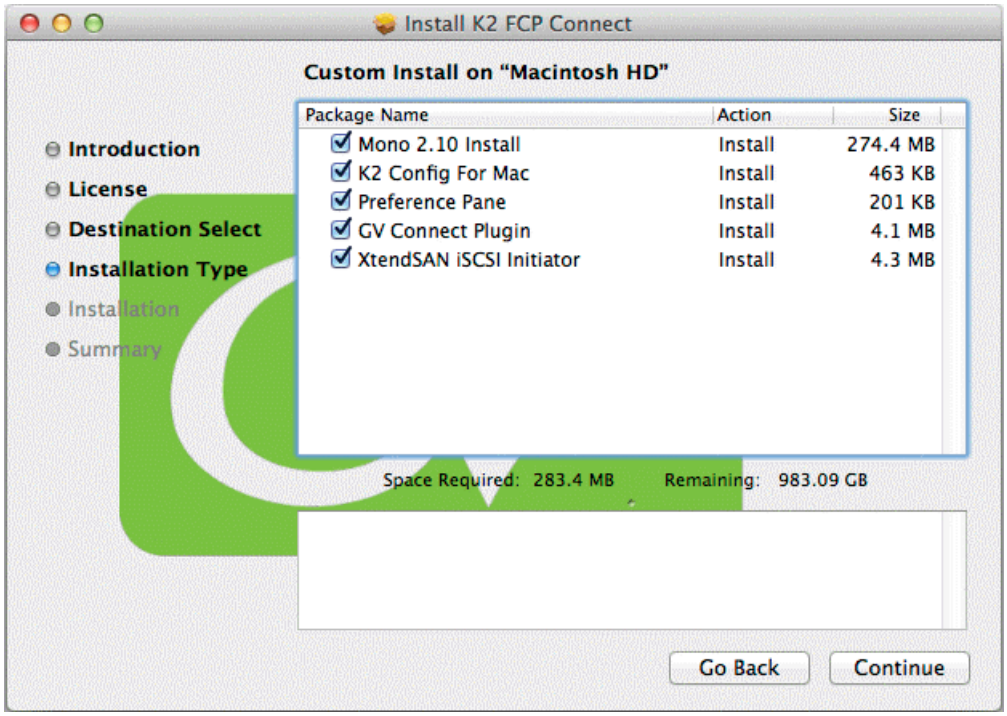
The Installer opens.

5. Click **Continue**, agree to software license terms as appropriate.

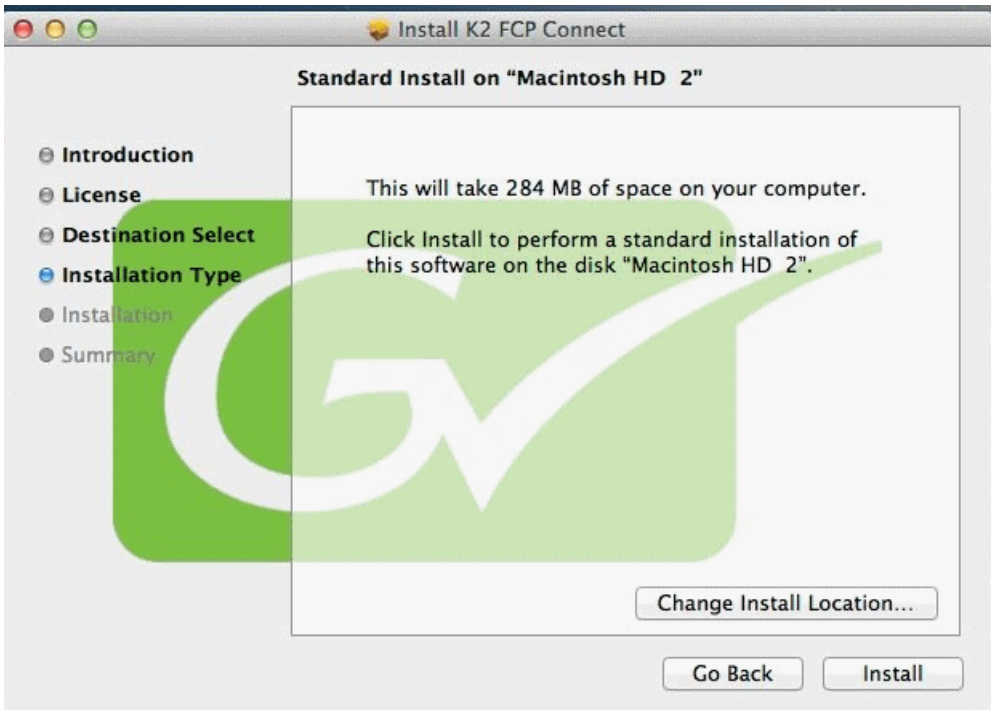




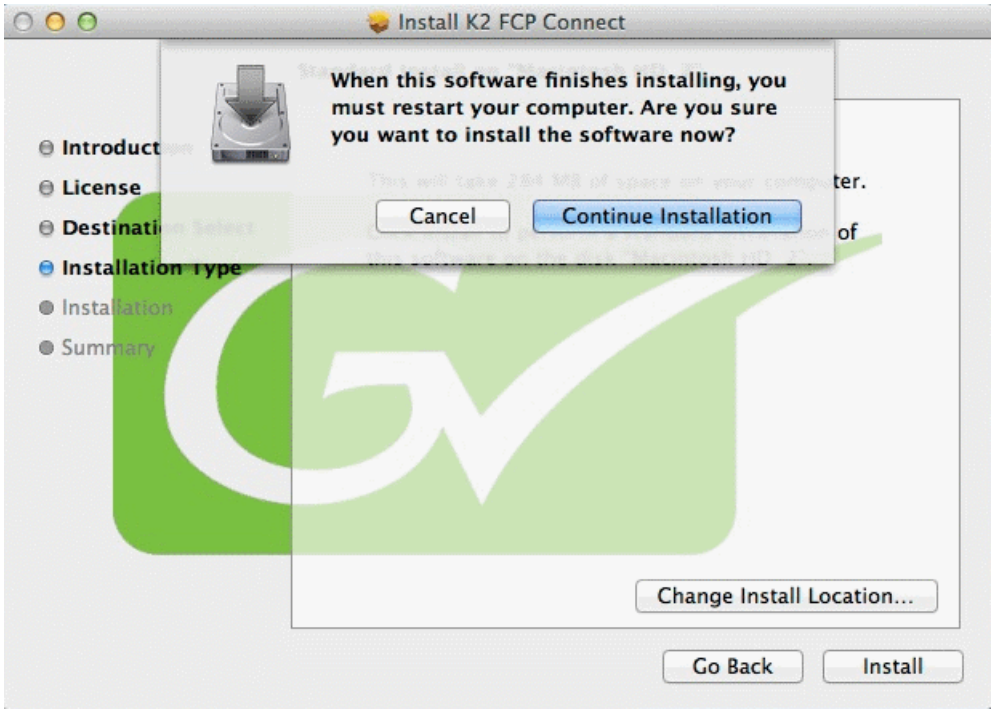
6. On the Custom Install screen, accept all default packages.



The Installation Type screen opens.

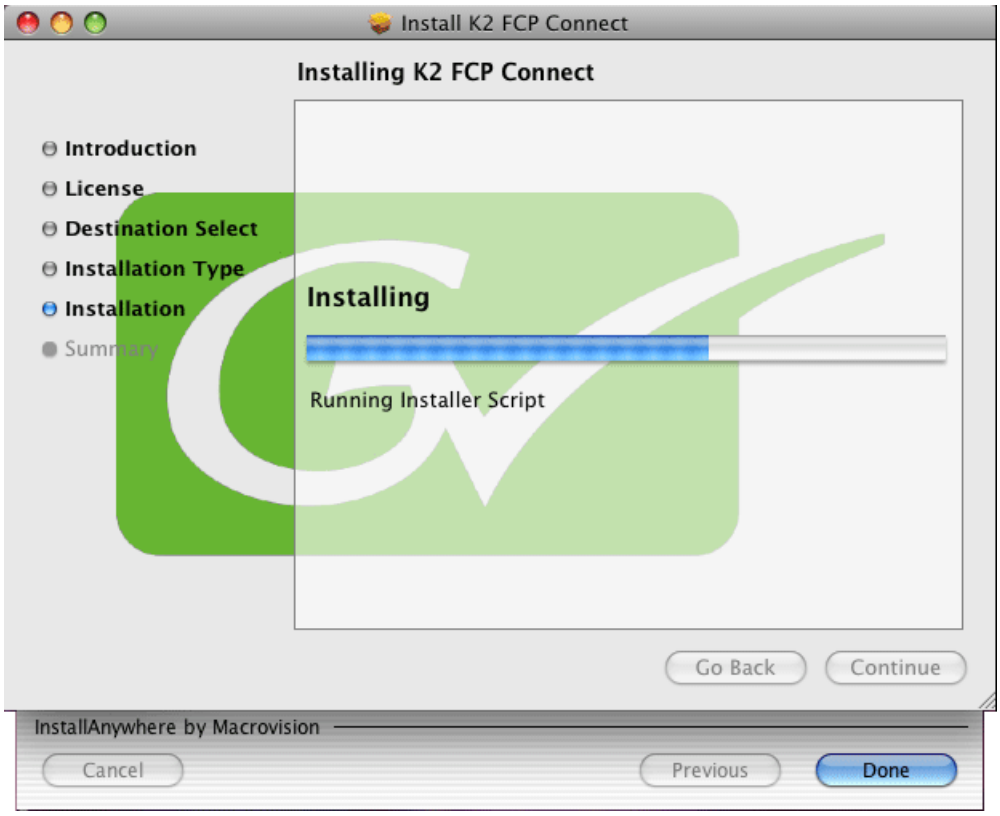


7. A screen displays a warning statement to restart the computer once installation is complete. Click **Continue Installation** to start the installation process.



8. Click **Install** and when prompted enter the Macintosh system's administrator username and password.

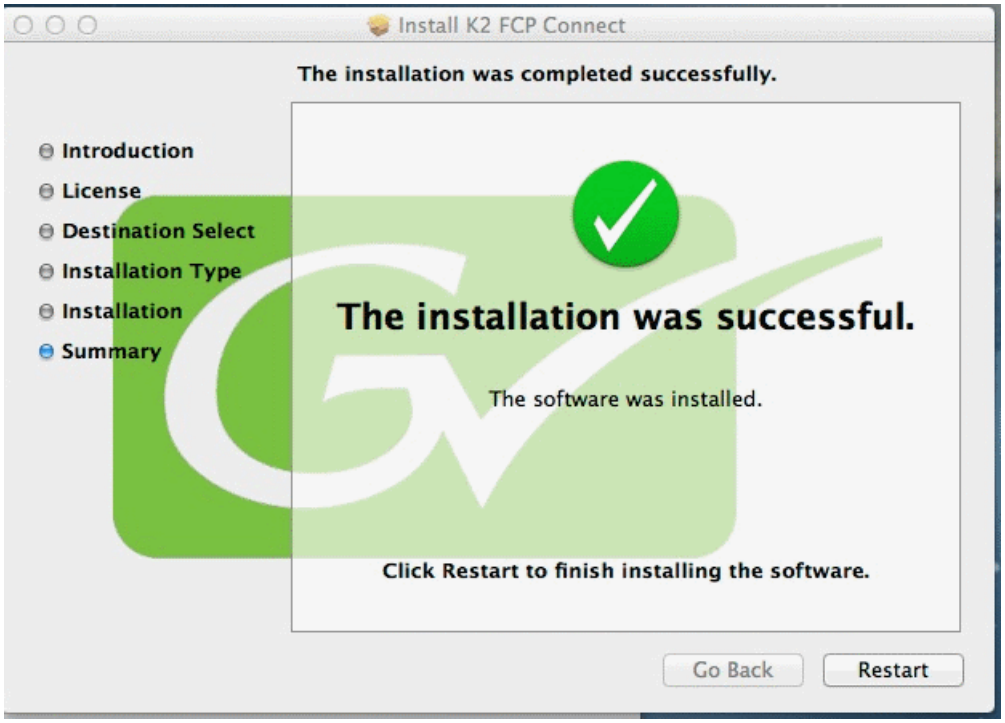
   Software installs.



9. 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.

10. Click **Restart** when the installation completes successfully.



The Macintosh system restarts.

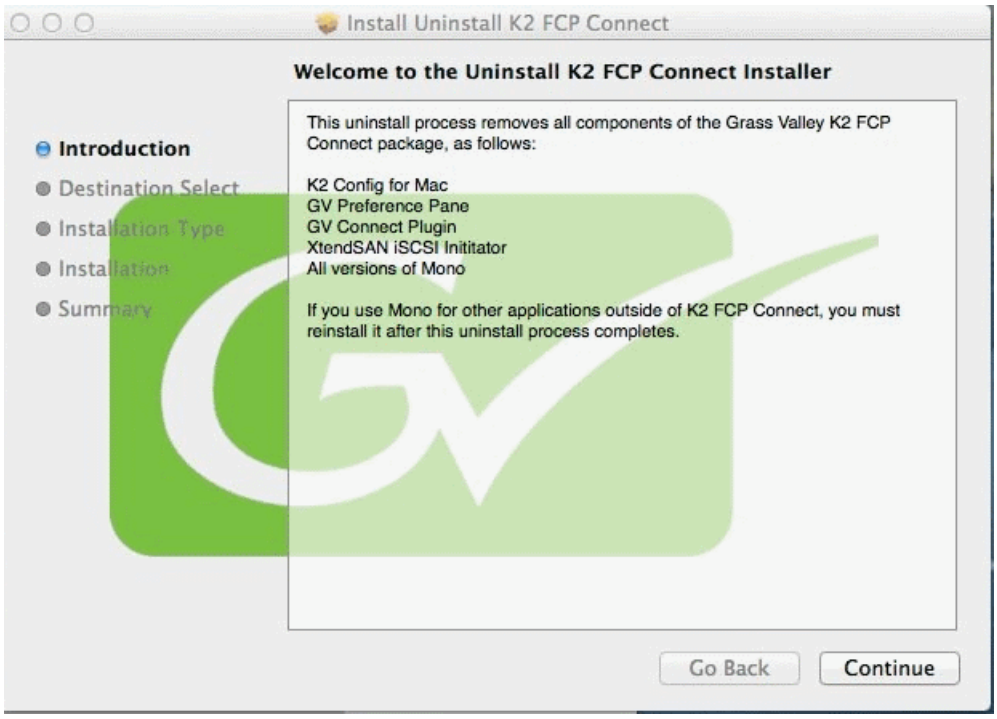
Uninstall K2 FCP Connect software on Macintosh systems

If you ever need to uninstall K2 FCP Connect from your Macintosh system, use the following procedure. This removes all files associated with K2 FCP Connect from the Macintosh system, including Mono software.

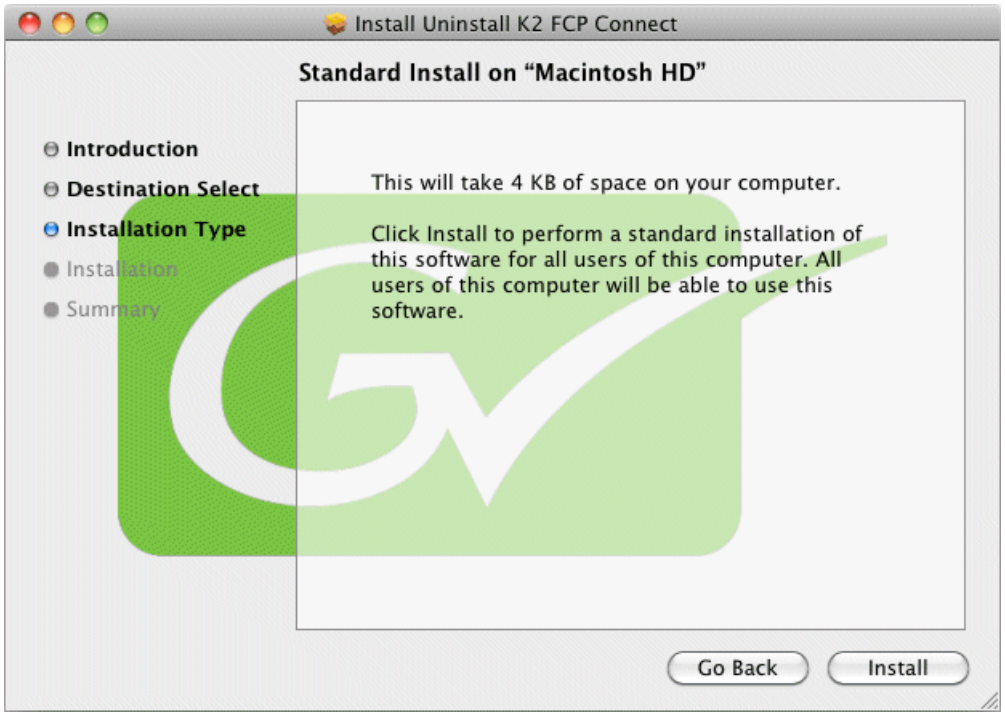
1. Procure the K2 FCP Connect uninstall program file.

   Refer to *K2 FCP Connect Release Notes* for information on obtaining the uninstall program file.

2. On the Macintosh system, double-click `UninstallK2FCPConnect.pkg`.
   The uninstall program opens.

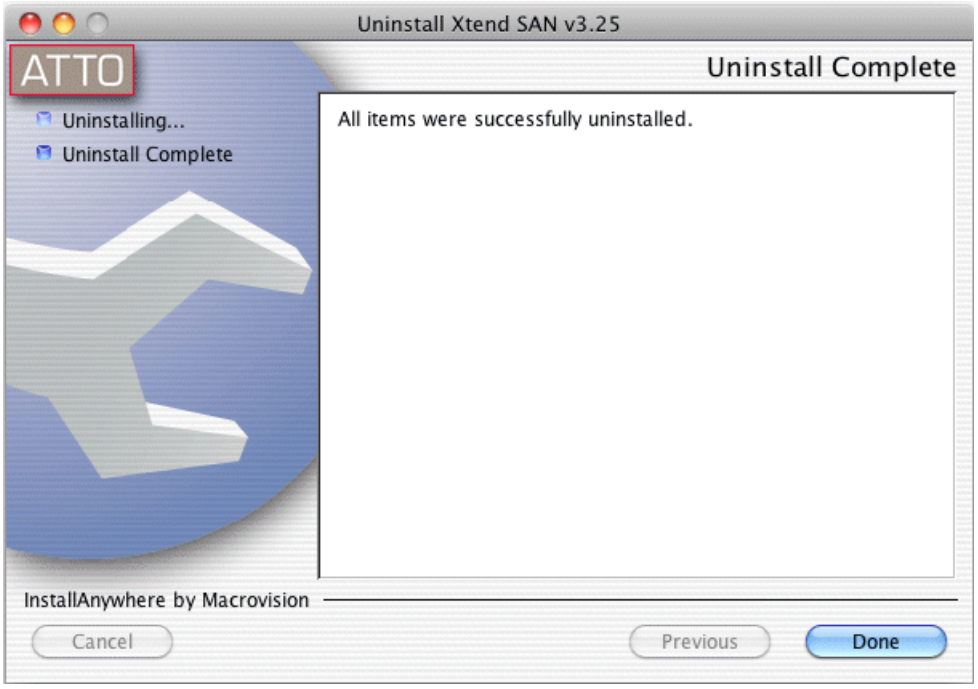


3. Click **Continue**.
   The Installation Type screen opens.



4. Click **Install** and when prompted enter the Macintosh system's administrator username and password.

   Software uninstalls.



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

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

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

All files associated with K2 FCP Connect are removed from the Macintosh system.

If an application that is currently installed on the Macintosh system requires Mono software, you must re-install the Mono software.

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. Refer to the *K2 SAN Installation and Service Manual* for more information about SAN connections.

1. Connect GigE port 1 to a control port on the Ethernet switch.
2. Do one of the following:

   - If iSCSI access, connect GigE port 2 to a media port on the K2 SAN Ethernet switch. This connection is for the media (iSCSI) network.
   - If Fibre Channel access, connect the Fibre Channel port to the K2 SAN Fibre Channel switch or to a Fibre Channel port on the K2 RAID controller.

Configure Macintosh systems for control network

Depending on the version of your Macintosh operating system, the steps in this task can vary. Refer to your Macintosh documentation as necessary.

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 control network.

Configure Macintosh systems for Domain

Depending on the version of your Macintosh operating system, the steps in this task can vary. Refer to your Macintosh documentation as necessary.

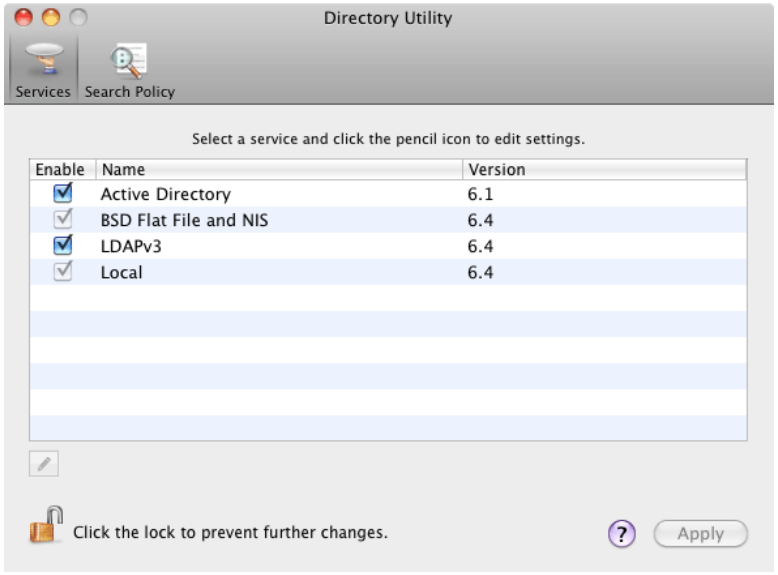
If desired, MAC OS X can be configured to use Active Directory (AD) resources such as users and groups. Once a computer is bound to an AD domain, users belonging to that domain may login to the Macintosh system at the main login prompt. If you do this task, you must also enable Access Control Lists on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

1. Open System Preferences and click **Accounts**.
2. If the **Lock** icon is locked, unlock it by clicking it and entering the administrator name and password.
3. Click **Login Options**, then click **Join** or **Edit**. If you see an **Edit** button, your computer has at least one connection to a directory server.

4. Click the **Add (+)** button.
5. From the "Add a new directory of type" pop-up menu, choose **Active Directory**.
6. 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.
7. Click **OK**.

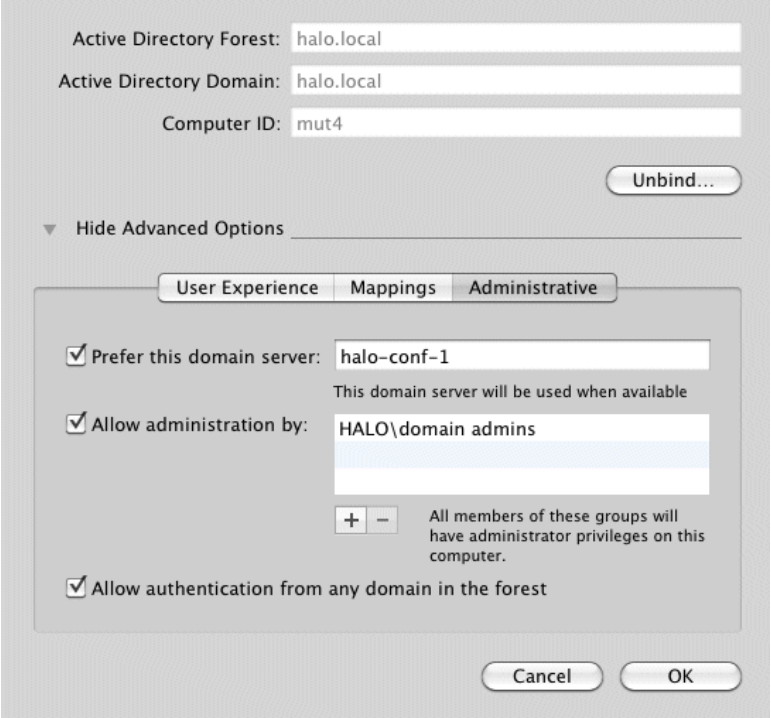
   The Macintosh computer goes through the binding process. If successful, the domain name is listed with the status message, "This server is responding normally".
8. Click **Open Directory Utility** or, if desired, click **Done** and open the **Directory Utility** from the `System/Library/Core Services` folder.
9. Click **Services**.



10. Verify that the Active Directory option is checked.

    If you need to change options, first double-click the Lock icon on the lower left hand corner and authenticate as administrator.

11. 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 the **Prefer this domain server** and **Allow administration by** check boxes are 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 K2 systems

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. The license allows a set number of connections for Macintosh systems to access K2 storage. The license is made available via a Grass Valley SabreTooth licensing web service. When a Macintosh system attempts to connect to a K2 system, the connection is verified with the service and either allowed or disallowed.

K2 FCP Connect licenses are installed as follows:

- For K2 SAN 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.
- No Grass Valley license is required to be installed on the Macintosh system or on the control point PC.

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

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

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

Apply licensing instructions according to your requirements for Macintosh access to K2 SAN or stand-alone K2 systems.

Requesting a license

This topic applies to Grass Valley SabreTooth licenses. For the system you are licensing, you must provide a generated unique ID to Grass Valley. Grass Valley uses the ID 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 shortcut on the Windows desktop or in the *`Grass Valley License Requests`* folder.

   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 from Grass Valley.

   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 Solo 3G system at a K2 software version lower than 9.0 and 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. Double click on the License Manager icon on the Windows Desktop.

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

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

You should archive the permanent license to a backup system.

Enable SabretoothWS service

Do this task on the K2 system that is your Sabretooth licensing server for access to stand-alone K2 systems.

1. Open the Windows **Services** control panel.
2. Right-click **Grass Valley SabretoothWS**, open **Properties** and click the **General** tab.
3. Set Startup Type to **Automatic**.
4. Click **OK** to save settings and close.

Add Macintosh systems to K2 system hosts file

1. On a K2 system, 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 K2 systems.
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 system

- The K2 system must have current compatible versions of the Windows operating system and SNFS software.
- The K2 system must have standard C:, D:, E: and V: disk volumes.
- SNFS must be configured with Grass Valley's Storage Utility.
- The SNFS configuration file must be located in the *D:\SNFS\config* directory.

If desired, you can enable Access Control Lists (ACLs). For SAN access enable ACLs on the K2 Media Server(s). For stand-alone K2 storage access enable ACLs on the stand-alone K2 system. 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 the SNFS configuration file in a text editor. The file is named either *default.cfg* or *gvfs_hostname.cfg* where hostname is the name of the K2 system—if a redundant SAN, the name of the primary FSM.
3. Confirm/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 system (WindowsSecurity set to Yes), they cannot be disabled.
4. Save the SNFS configuration file.
5. Restart the K2 system.
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

- 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.

- The K2 SAN's K2 Media Server(s) with role of file system server (FSMs) must have the K2 FCP Connect license installed.
- You must be logged in to the K2 System Configuration (K2Config) application with permissions equivalent to K2 administrator or higher.
- The client device must be added to the K2 SAN and must appear in the K2 System Configuration application tree view.
- The K2 SAN must have adequate bandwidth available to meet the bandwidth needs of the client device you are adding.
- The client device must be connected to appropriate networks and must be powered up.
- The client device's IP address and other network properties must be configured for the control network.
- Host table information for K2 SAN devices, the control point PC, and the client device must be in the hosts file on the client device.
- The devices of the K2 SAN are not required to be offline, and a restart of devices is not required.

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

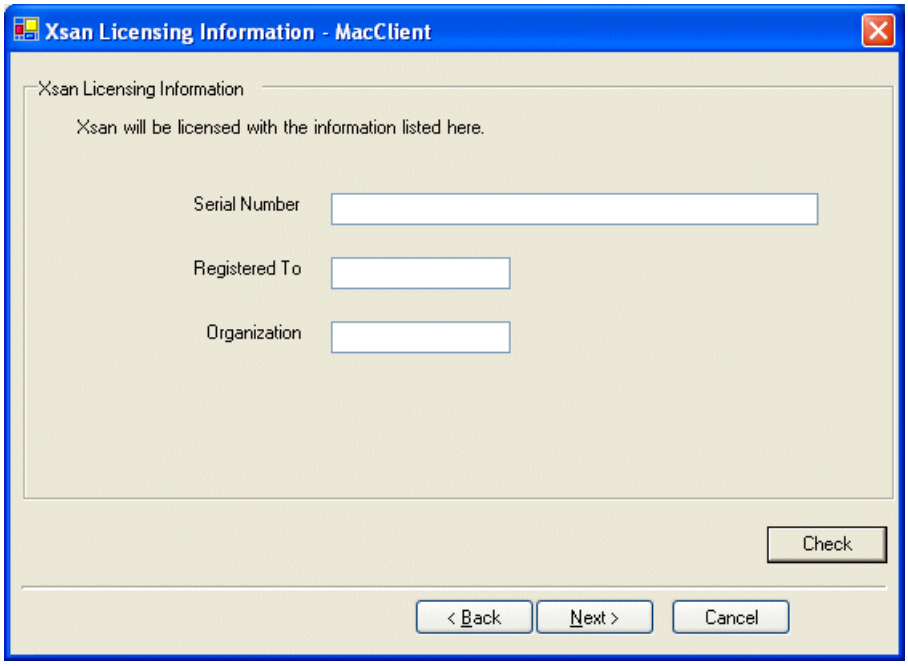
   The Client Configuration wizard opens.

   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.



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.

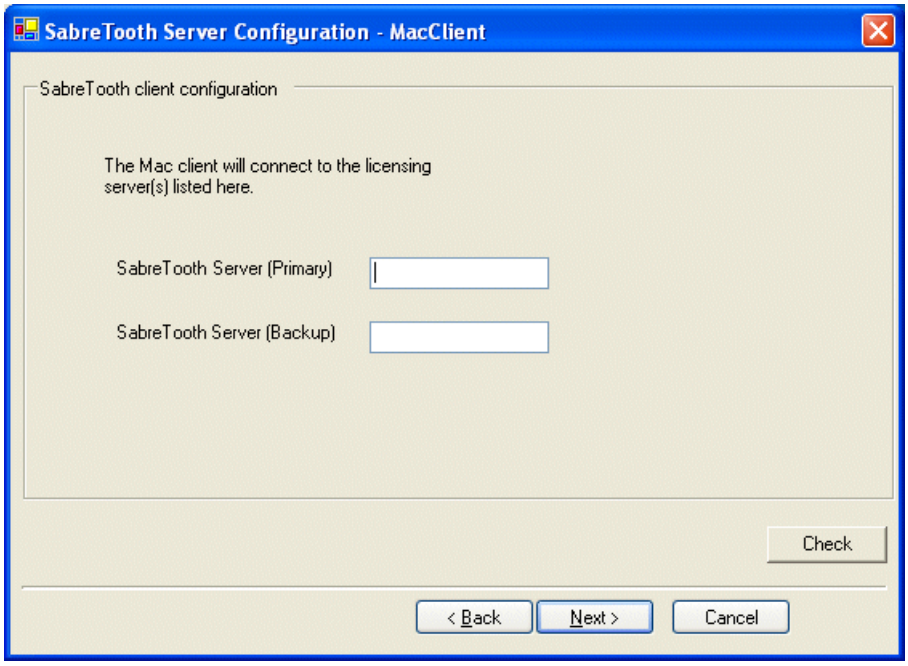
8. Identify software installed on the client device and proceed as follows:

   - 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. Proceed as follows:

    - If a Fibre Channel connected client, skip ahead to step 21 and configure the File System Client Configuration page.
    - If an iSCSI connected client, proceed with the next step.

13. Select the media (iSCSI) port and click **Modify**.

    A network configuration dialog box opens.

14. Enter the media network IP address and subnet mask and then click **OK**.

15. 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.

16. Click **Modify**.

    The Bandwidth Input dialog box opens.

17. Enter the bandwidth of the Mac Client. This is calculated according to your system design, and provided to you by your Grass Valley representative.

18. 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.

19. 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.

20. 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.

21. 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.

22. Click **Next**.

    The Completing the Configuration Wizard page opens.

23. Click **Finish**.

    When prompted, restart the client device.

Test K2 system file access

K2 storage is automatically mounted as a volume on the Macintosh system. From a Macintosh system, perform create, read, write, and delete operations on a file on the K2 storage volume. This verifies the media file system.

1. On the Macintosh desktop, verify that the K2 storage volume is present.
2. From the Macintosh system, open a text editor, create a text file, enter text, and save it on the K2 storage volume.
3. Close the text editor.
4. In Finder, browse to the K2 storage volume 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 Access Control Lists on a Macintosh system

Verify the following before you begin:

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

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

1. Test permissions on the K2 system as follows. For K2 SAN access, test permissions on the primary K2 Media Server FSM. For stand-alone K2 storage access, test permissions on the stand-alone K2 system.
   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 volume.

      If the SNFS file system is named "default" type the following and press **Enter**:

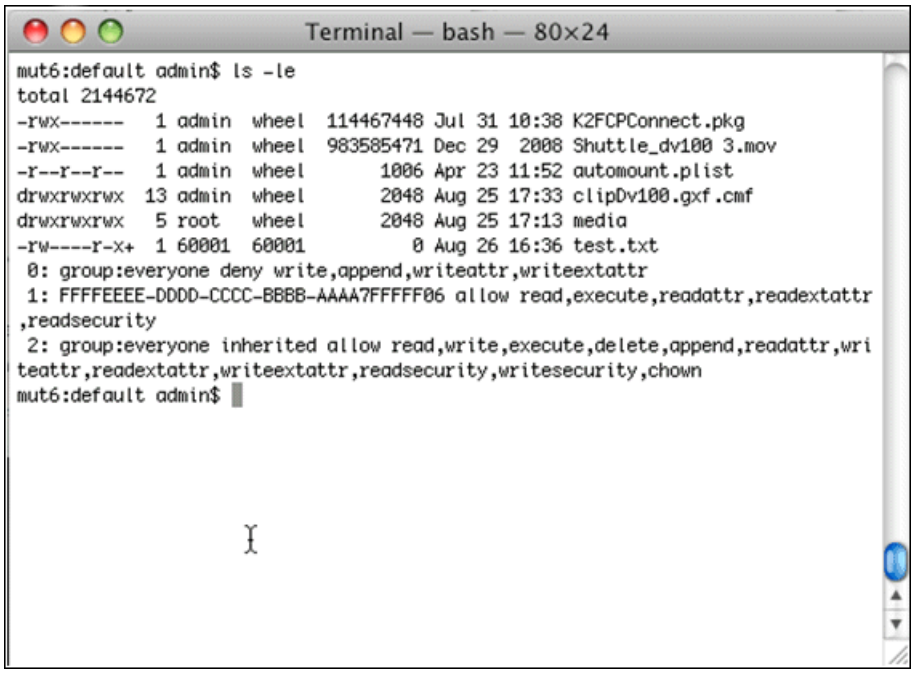
      ```
      cd /Volumes/default
      ```

      If the SNFS file system is named "gvfs_hostname" (where hostname is the name of the K2 system) type the following and press **Enter**:

      ```
      cd /Volumes/gvfs_hostname
      ```

   d) Type the following command:

      ```
      ls -le
      ```

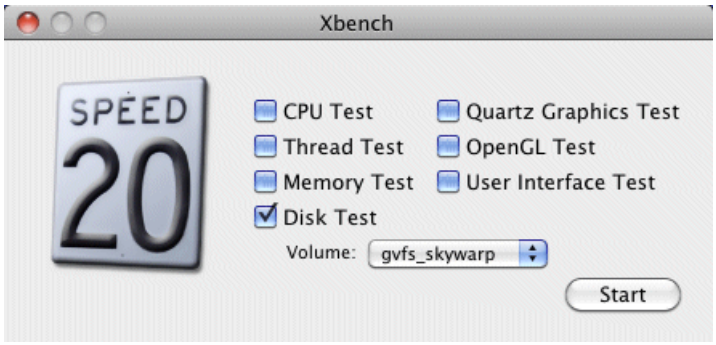


   e) Verify that there is a "+" next the text file, plus a list of permissions below. If this is true then cross-platform ACLs are enabled.
   f) Open the Finder, go to the default volume and try to edit the text file. This should fail as the file should not be writeable.
   g) In the Finder, go to the 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.

Verify bandwidth of connection to K2 storage

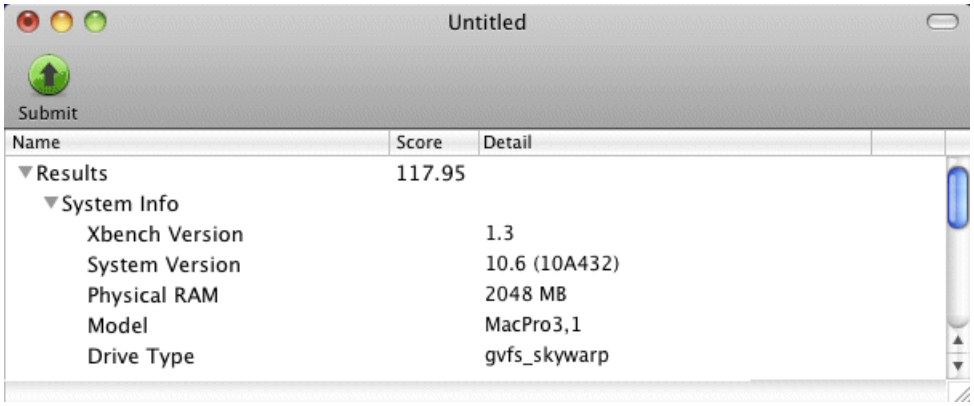
Before starting this task, procure the Xbench software. You can download it from http://www.xbench.com.

1. Install Xbench on the Macintosh system.
2. Open Xbench.



3. Select the K2 system volume.
4. Click **Start**.

   It might take several minutes to create the test results.



5. Verify bandwidth and other performance parameters.

Verify/configure SNFS configuration file on K2 Media Servers

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

Do this task if you access media on a K2 SAN and in the SNFS configuration file, WindowsSecurity is set to No. If you are not sure about the WindowsSecurity setting, proceed with this task to check the setting.

You can verify and, if necessary, modify the media file system (SNFS) configuration file and still keep your media file system intact if you carefully follow the steps in this procedure.

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. On a K2 Media Server, using Notepad, open the media file system (SNFS) configuration file:

   The configuration file can be either *D:\SNFS\config\default.cfg.* or *D:\SNFS\config\gvfs_hostname.cfg*, where *hostname* is the name of the primary file system server (FSM).

2. Locate the WindowsSecurity setting and proceed as follows:

   - If WindowsSecurity is set to Yes, skip the remainder of this procedure. Do not modify or save the SNFS configuration file.
   - If WindowsSecurity is set to No, continue with this procedure.

3. 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
# ********************************************************
.
WindowsSecurity No

GlobalSuperUser Yes

UnixDirectoryCreationModeOnWindows 0777
UnixFileCreationModeOnWindows 0666
.
```

4. Close, and if necessary save, the SNFS configuration file.

If you made changes, the K2 system must be restarted for the changes to take effect.

If you made changes to *UnixDirectoryCreationModeOnWindows* and *UnixFileCreationModeOnWindows* parameters, to apply changes to existing assets you must delete and then re-create files and/or bins, such as HotBins.

Configure HotBin

If a K2 SAN, the SNFS configuration file must have settings as follows:

- If Windows Security is No, GlobalSuperUser must be set to Yes.
- If Windows Security is Yes, no GlobalSuperUser setting is required.

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

1. In K2 AppCenter, create a bin with an appropriate name, such as "dstBin".
2. Configure *dstBin* as a HotBin.

   Refer to the *K2 System Guide* for instructions.

3. 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, when you configure a K2 HotBin you can configure the QuickTime import delay setting. This setting 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.

Configure GV STRATUS Rundown workflow

- A playout destination must be a location on configured and licensed K2 storage.
- A HotBin must be configured so that when it receives media, it imports that media into K2 storage, to the bin that Aurora Playout monitors.

In this procedure you specify the GV STRATUS Rundown server on which GV Connect accesses placeholders/rundowns and one or more K2 storage locations to which GV Connect exports sequences.

1. Close GV Connect, if it is currently open.
2. In **System Preferences** open **K2 FCP GV Connect**.
3. Click the **Playout** tab.
4. For **Display Name**, enter the name that you want displayed on the GV Connect drop-down list.

   This is name of the location on K2 storage to which GV Connect exports the GV STRATUS Rundown associated sequences.
5. For **Location**, click the browse arrow to navigate to and select the HotBin that is configured to import the sequence to the bin that Aurora Playout monitors.
6. For **Format**, select the format in which the sequences are exported to K2 storage.
7. Click **Add** to add the location as a playout destination.
8. Repeat these steps to add multiple locations.
9. Select an item in the list and use the **Modify** or **Delete** buttons to manage the list.
10. For **GV SimpleDB Server IP Address**, enter the IP address of the GV STRATUS Rundown server on which GV connect accesses placeholders/rundowns.
11. If you are using NRCS, do the following:
    a) Next to **GV XMOS Rundowns/Script Path:**, select **Active**.
    b) Browse to and select the directory where XMOS scripts are stored.
    c) For **GV Mos Id**, enter the MOS ID that is configured in XMOS.

Using and maintaining K2 FCP Connect

About GV Connect

GV Connect is a Grass Valley plug-in for Final Cut Pro. With the plug-in you can quickly and easily locate QuickTime files on a K2 SAN System. Then you can add the files to the current Final Cut Pro project to allow editing of the files directly over the network or after transfer locally. The capability to add files without file transfer is called Edit in Place. The plug-in also includes Final Cut Pro support for sequences, growing file support, and export/render/flattening of Final Cut Pro finished sequences on a K2 system for sharing or playout.

With GV Connect you can do the following:

Import

- Browse K2 SAN file structure to find, preview and add or transfer clips to bin
- Browse K2 file structure to find, preview and add or transfer clips to bin
- Browse K2 file structure to find and add Sequences to bin
- Browse local or network path for QuickTime files to preview and add or transfer to bin as well as adding sequences to bin.

Export

- Export one or multiple clips or sequence to a K2 SAN system
- Two presets available: Export and Quick Export

Send to Playout

- Interface with GV STRATUS Rundown placeholders.
- Create a sequence from a placeholder. GV Connect locks the placeholder on the GV STRATUS Rundown system.
- Export a finished sequence to K2 storage to be tied to a placeholder on the GV STRATUS Rundown rundown.

The GV Connect Final Cut Pro plug-in is installed in the Final Cut Pro plug-in folder and is available on the Final Cut Pro Tools menu.

Operation guidelines

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

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

About administrative and maintenance tools

When you install K2 FCP Connect on your Macintosh system, the K2 FCP GV Connect Preferences is also installed, which 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.

- Stop/start the K2Config for Mac service
- Access logs
- Edit hosts file
- Run diagnostics
- Configure export locations, formats, and server for GV STRATUS Rundown workflow
- Add non-K2 media storage

K2 FCP GV Connect Preferences incorporates the features of the former GV Helper Tool.

Stopping and starting the K2Config for Mac service

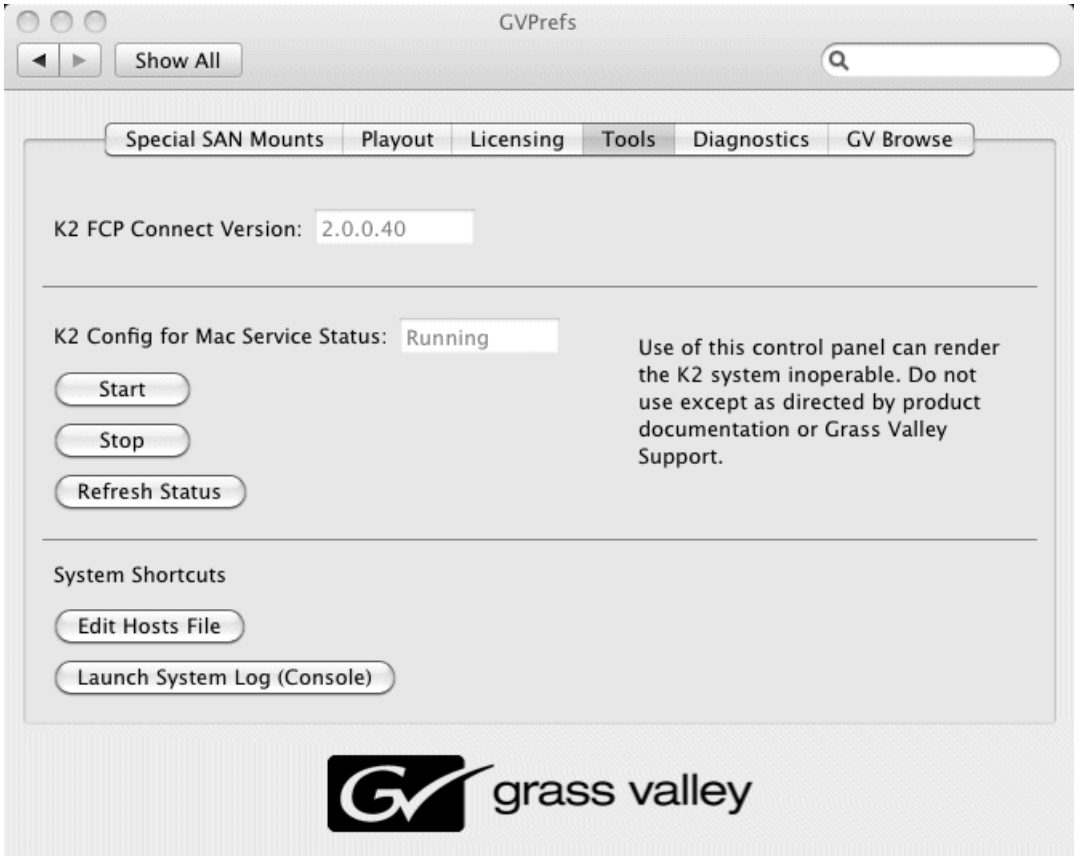
1. Close GV Connect, if it is currently open.
2. In **System Preferences** open **K2 FCP GV Connect**.
3. Click the **Tools** tab.
4. To start the K2Config for Mac service, click **Start** and then enter username and password with administrator privileges.
5. To stop the K2Config for Mac service, click **Stop**, when prompted "...Are you sure..." click **Yes**, and then enter username and password with administrator privileges.
6. To view any recent status change, click **Refresh Status**.

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

Accessing logs

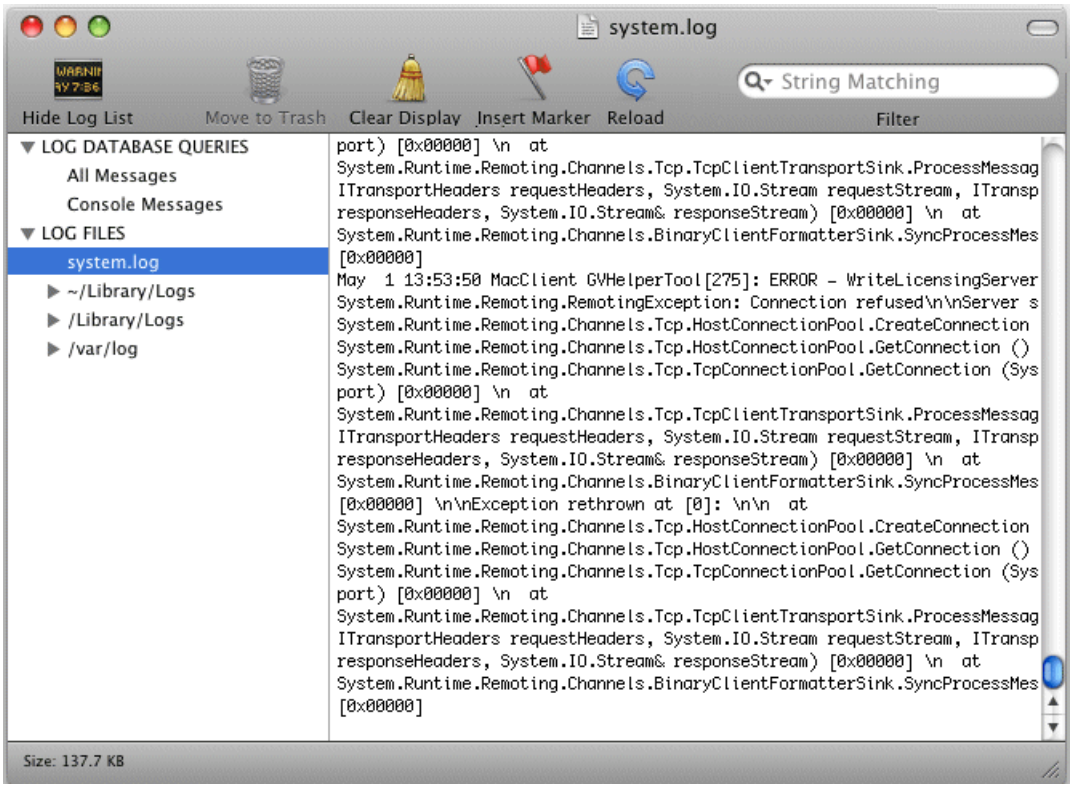
1. Close GV Connect, if it is currently open.
2. In **System Preferences** open **K2 FCP GV Connect**.

3. Click the **Tools** tab.



4. Click **Launch System Log (Console)**.

   A Console window opens and displays logs.



5. Select **system.log**.

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

6. 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.

Running diagnostics

1. Close GV Connect, if it is currently open.
2. In **System Preferences** open **K2 FCP GV Connect**.
3. Click the **Diagnostics** tab.
4. Click **Print System Diagnostics To Log**.
5. A message prompts you to authenticate. Do one of the following:

   - Click **Yes** and then enter administrator username and password. All diagnostics run.
   - Click **No**. A subset of the diagnostics run.

   .

6. When a message appears to confirm diagnostic results are written to the system log, click **OK**.

7. Access the system log to view diagnostic results.

Configuring non-K2 storage

If you must access media that is not stored on a K2 system, the non-K2 storage must be a mounted volume available to the Macintosh system.

You can add non-K2 storage so it is available from the GV Connect Import tab.

1. Close GV Connect, if it is currently open.
2. In **System Preferences** open **K2 FCP GV Connect**.
3. Click the **Special SAN Mounts** tab.
4. For **Display Name**, enter the name of the non-K2 storage that GV Connect displays.
5. For **Location**, click the browse arrow to locate and select the non-K2 storage.
6. Click **Add** to add the non-K2 storage.
7. Repeat these steps to add multiple non-K2 storage locations.

Modifying the export format list

You can remove items from the GV Connect export format list so that the only formats available are those that match your workflow policies.

1. On the Macintosh system, close GV Connect.
2. On the Macintosh system's main hard drive, navigate to `..\Applications\Grass Valley`.

3. Open *allowedpresets.xml* with TextEdit or some other text editor.

   The contents of the file are displayed as in the following example:

   NOTE: This is an example only. It is not intended to be the definitive list of formats supported in any particular version.

```
<?xml version="1.0" encoding="UTF-8"?>
<GVPresets>
 <FCPPreset>DV NTSC 48 kHz</FCPPreset>
 <FCPPreset>DV PAL 48 kHz</FCPPreset>
 <FCPPreset>DVCPRO - PAL 48 kHz</FCPPreset>
 <FCPPreset>DV50 NTSC 48 kHz</FCPPreset>
 <FCPPreset>DV50 PAL 48 kHz</FCPPreset>
 <FCPPreset>DVCPRO HD - 1080i50</FCPPreset>
 <FCPPreset>DVCPRO HD - 1080i60</FCPPreset>
    <FCPPreset>DVCPRO HD - 720p50</FCPPreset>
 <FCPPreset>DVCPRO HD - 720p60</FCPPreset>
 <FCPPreset>IMX NTSC (30 Mb/s)</FCPPreset>
 <FCPPreset>IMX NTSC (40 Mb/s)</FCPPreset>
 <FCPPreset>IMX NTSC (50 Mb/s)</FCPPreset>
 <FCPPreset>IMX PAL (30 Mb/s)</FCPPreset>
 <FCPPreset>IMX PAL (40 Mb/s)</FCPPreset>
 <FCPPreset>IMX PAL (50 Mb/s)</FCPPreset>
 <FCPPreset>HDV - 1080i50</FCPPreset>
 <FCPPreset>HDV - 1080i60</FCPPreset>
 <FCPPreset>HDV - 720p50</FCPPreset>
 <FCPPreset>HDV - 720p60</FCPPreset>
    <FCPPreset>XDCAM EX 1080i50 VBR</FCPPreset>
    <FCPPreset>XDCAM EX 1080i60 VBR</FCPPreset>
    <FCPPreset>XDCAM EX 720p50 VBR</FCPPreset>
    <FCPPreset>XDCAM EX 720p60 VBR</FCPPreset>
 <FCPPreset>XDCAM HD 1080i50 CBR</FCPPreset>
 <FCPPreset>XDCAM HD 1080i50 VBR</FCPPreset>
 <FCPPreset>XDCAM HD 1080i60 CBR</FCPPreset>
 <FCPPreset>XDCAM HD 1080i60 VBR</FCPPreset>
    <FCPPreset>XDCAM HD422 1080i50 CBR</FCPPreset>
    <FCPPreset>XDCAM HD422 1080i60 CBR</FCPPreset>
    <FCPPreset>XDCAM HD422 720p50 CBR</FCPPreset>
    <FCPPreset>XDCAM HD422 720p60 CBR</FCPPreset>
</GVPresets>
```

4. Identify the presets that you do not want to be displayed in the export format list.
5. For each format that you do not want to be displayed, delete the entire row.

   For example, if you want to remove IMX NTSC (30 Mb/s), delete the following row:

```
<FCPPreset>IMX NTSC (30 Mb/s)</FCPPreset>
```

   NOTE: Only delete one or more preset rows. Do not add rows, add text, modify XML tags, or otherwise modify the file.

6. Save and close *allowedpresets.xml*.
7. Open GV Connect.

The presets you deleted are no longer displayed in the export format list.

Using GV Connect

Getting started

About GV Connect

GV Connect is a Grass Valley plug-in for Final Cut Pro. With the plug-in you can quickly and easily locate QuickTime files on a K2 SAN System. Then you can add the files to the current Final Cut Pro project to allow editing of the files directly over the network or after transfer locally. The capability to add files without file transfer is called Edit in Place. The plug-in also includes Final Cut Pro support for sequences, growing file support, and export/render/flattening of Final Cut Pro finished sequences on a K2 system for sharing or playout.

With GV Connect you can do the following:

Import

- Browse K2 SAN file structure to find, preview and add or transfer clips to bin
- Browse K2 file structure to find, preview and add or transfer clips to bin
- Browse K2 file structure to find and add Sequences to bin
- Browse local or network path for QuickTime files to preview and add or transfer to bin as well as adding sequences to bin.

Export

- Export one or multiple clips or sequence to a K2 SAN system
- Two presets available: Export and Quick Export

Send to Playout

- Interface with GV STRATUS Rundown placeholders.
- Create a sequence from a placeholder. GV Connect locks the placeholder on the GV STRATUS Rundown system.
- Export a finished sequence to K2 storage to be tied to a placeholder on the GV STRATUS Rundown rundown.

The GV Connect Final Cut Pro plug-in is installed in the Final Cut Pro plug-in folder and is available on the Final Cut Pro Tools menu.

Launching GV Connect

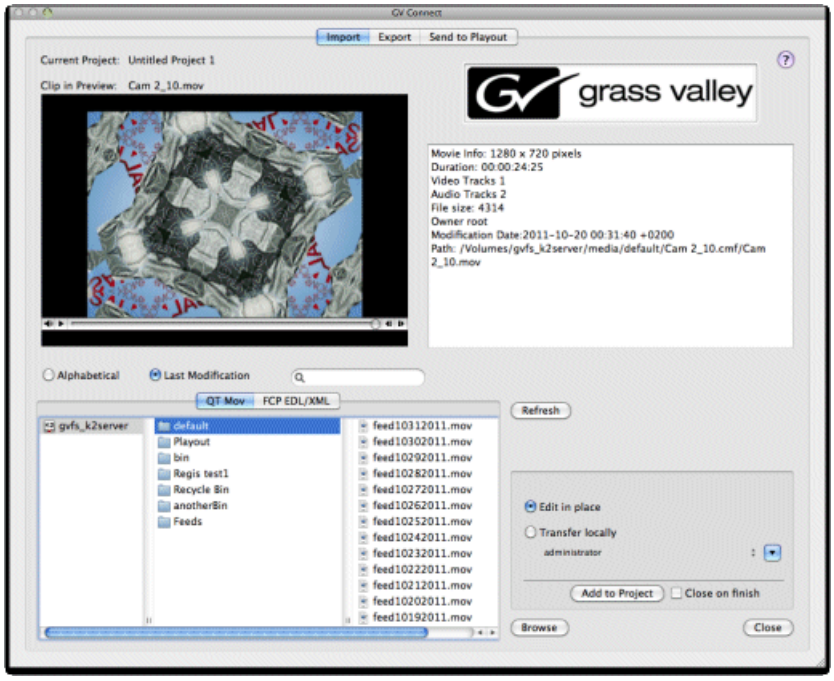
- K2 FCP Connect must be licensed
- A K2 storage volume must be mounted
- The project window (Browser) in Final Cut Pro must be active and contain a project or bin

1. In Final Cut Pro select the project or bin.

   The project must be selected to enable the GV Connect selection on the Tools menu.

2. Click **Tools | GV Connect**.

   The GV Connect window opens with the Import tab selected by default.



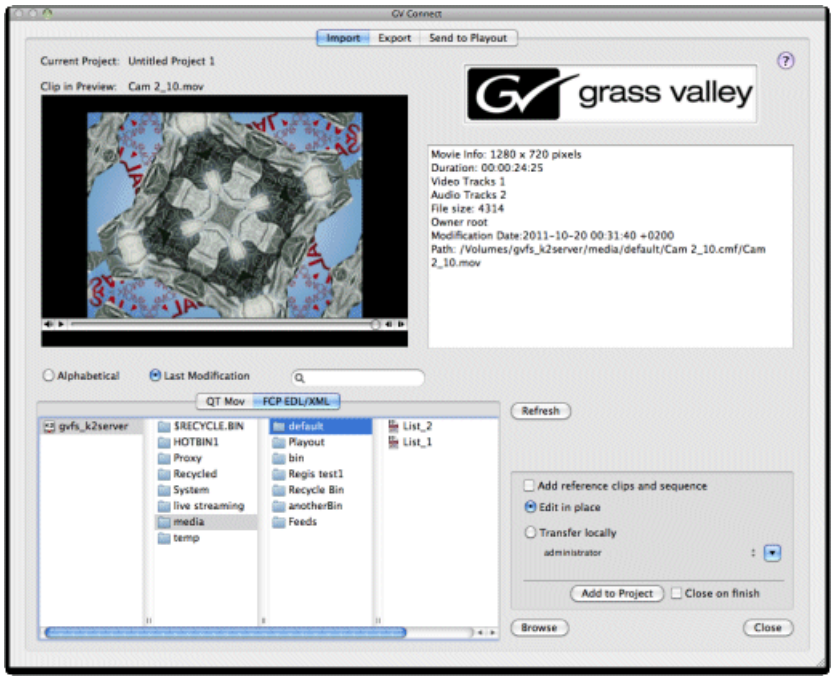
3. Switch between tabs to accomplish your tasks, as follows:

   - **Import tab**: Access media, K2 8.0 sequences, and/or Final Cut Pro XML projects and sequences.
   - **Export tab**: Export edited content to K2 storage.
   - **Send to Playout**: Access GV STRATUS Rundown placeholders/rundowns, create associated sequences, and export sequences to K2 storage.

Importing K2 media

Locating media

1. Select the **Import** tab.



   The Import tab provides a browser to locate media.

2. Select the browser tab for the type of media you are locating.

   - QT Mov – Select this tab to find QuickTime files.
   - FCP EDL/XML – Select this tab to find sequences, Final Cut Pro projects, or K2 exported XML.

3. If desired, sort or filter media as follows:

   - Alphabetical – Sort view alphabetically A to Z.
   - Last Modification – Sort by last modified date on top.
   - Search – Filter the view by typing a keyword. This is especially useful when your folder contains thousands of clips.

4. Click **Refresh** to view recently added media in the browser.

   If you add media while GV Connect is open, you must refresh in order to locate the media.

5. Double-click media to preview.

   The clip loads in the preview window and displays clip metadata.

After you have located the media to edit, add it to your Final Cut Pro project using the **Add to Project** button.

Adding media to your Final Cut Pro project

1. Locate and select the media to add to your project.
2. Select the method for adding the media to your project.
   - Add reference clips and sequence — Select to add the associated assets to the Final Cut Pro project.
   - Edit in place – Use this method to add a clip to the bin without moving the media. With this method you are playing and editing the clip over the network. This is the preferred method on a shared storage system such as a K2 SAN.
   - Transfer Locally – Use this method to transfer the media corresponding to the clip to your desired location. This is the preferred method if your editor is connected via CIFS to a stand-alone K2 client. Depending on clip size, the transfer can take a significant amount of time. Wait until the cursor no longer indicates that the operation is in progress before proceeding.

     NOTE: Do not add media to a project if the transfer is still underway.
3. Click **Add to Project**.

   The media is added to your Final Cut Pro project.
4. To return to Final Cut Pro, close the GV Connect plug-in.

Edit the media as desired in Final Cut Pro. When you are finished you can export the media back to K2 storage.

Updating growing files

1. In the Final Cut Pro menu bar (in the upper right in the Mac OSX toolbar), identify the GV icon. 

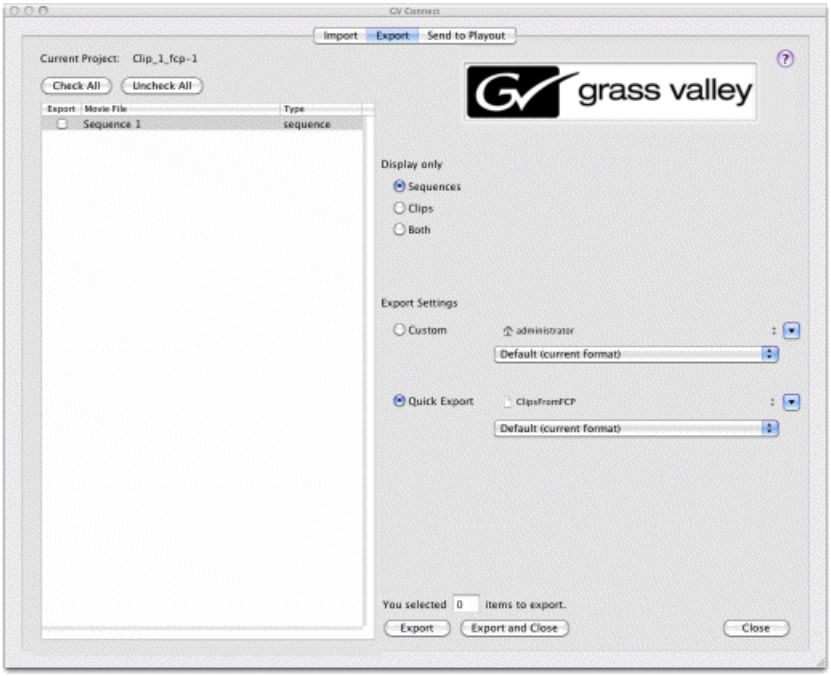
   When this icon displays a green color, it means that a clip that is in your Final Cut Pro project is currently growing in the K2 system and is ready for updating in your project.
2. When the GV icon displays a green color  , click the icon and select an individual file or **Refresh All**.

   The file or files are updated in your Final Cut Pro project.

Exporting K2 media

Exporting to K2 storage

1. Select the **Export** tab.



2. Under "Display only", select whether to display Sequences, Clips, or Both.
3. In the list of media, select the media to export to K2 storage.

   You can make one selection or multiple selections.
4. Under Export Settings, select **Custom**.
5. In the drop-down list select the format in which the media is exported.
6. Click the down-arrow.

   The "Choose a Directory for Export" dialog box opens.
7. Browse to the location in K2 Storage to which the media is exported.

   Export to K2 HotBin recommended. The HotBin does the processing required so that you can play the media on the K2 system.
8. Click **Export**.

   A message box displays progress for each clip or sequence exported.

Using Quick Export

You can save and reuse export settings with the Quick Export feature. Once you have configured your Quick Export settings you can use the GV Quick Export menu entry. This bypasses the GV

Connect plug-in main interface and automatically exports the selected items in the Final Cut Pro bin to your predetermined location on K2 storage. This feature can be very useful if you export all your finished material to a K2 HotBin.

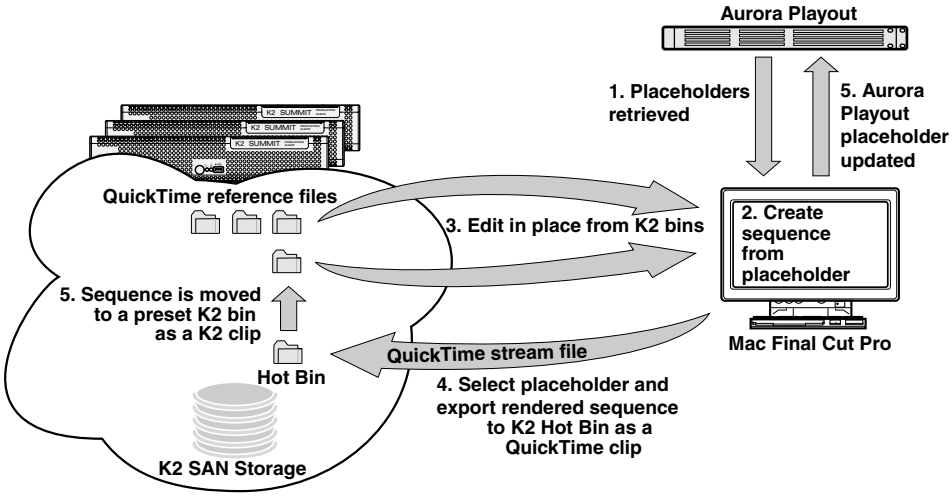
1. Configure your Quick Export settings as follows:
   a) Select the **Export** tab.
   b) Click **Quick Export**.
   c) Make export settings.
2. After your Quick Export settings are configured, you can repeatedly reuse the settings as follows:
   a) On the Final Cut Pro menu click **Tools | GV Quick Export**.

   GV Connect automatically exports the clip to K2 storage, as specified by the currently configured Quick Export settings.

Sending media to playout

About the GV STRATUS Rundown workflow

The workflow on a K2 SAN with GV STRATUS Rundown is illustrated as follows:



Before you can use GV Connect to access placeholders/rundowns and create/edit/export associated sequences, GV Connect must be configured for your site's specific systems and workflow, as follows:

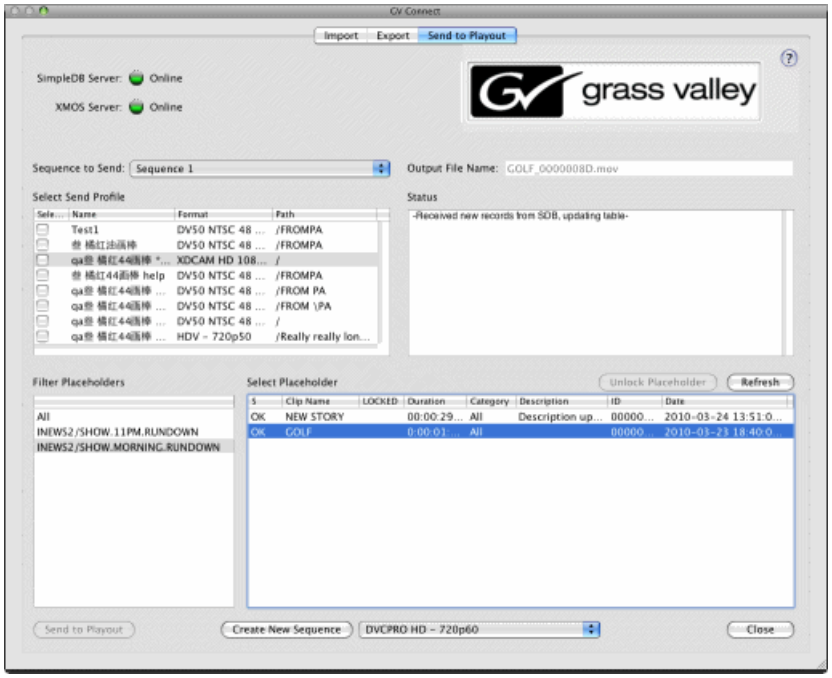
- The network address of the server and other system settings
- The formats in which sequences are exported
- The location(s) to which sequences are exported

This is configured in K2 FCP GV Connect Preferences by your system administrator. Refer to the *K2 FCP Connect Installation Manual* for more information.

Accessing placeholders/rundowns

If you are using the GV STRATUS Rundown workflow, start by choosing the placeholder or rundown on which you are working.

1. Select the **Send to Playout** tab.



In the **Select Placeholder** list, GV Connect automatically displays all placeholders present on the GV STRATUS Rundown system.

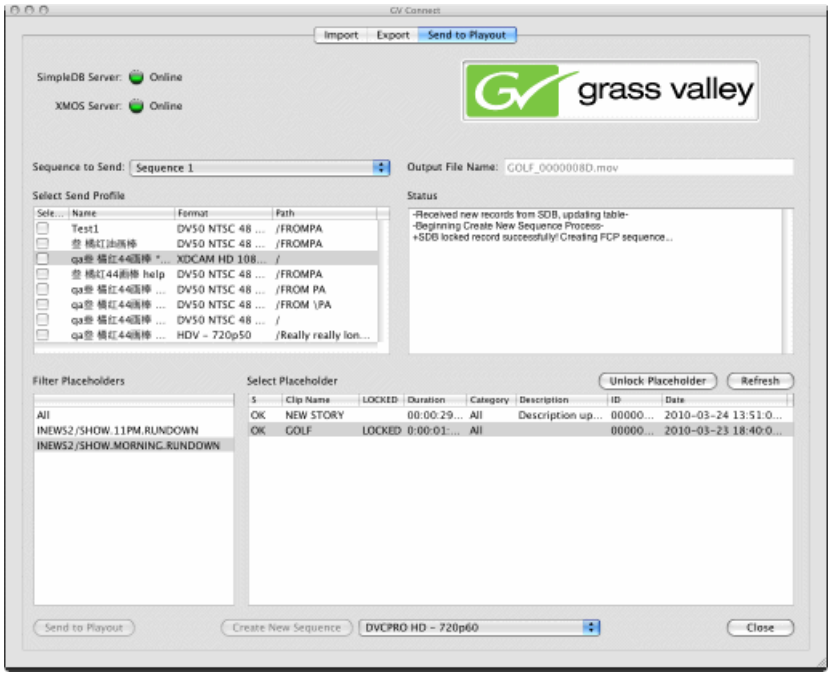
If configured for an NRCS system, under **Filter Placeholders** GV Connect also displays rundowns.

2. To access recently added placeholder or rundowns, click **Refresh**.
3. If configured for an NRCS system, under **Filter Placeholders** do one of the following:
   - Select a rundown to display the rundown's list of placeholders.
   - Select **All** to display all placeholders.
4. Select the desired placeholder from the **Select Placeholder** list.
5. If desired, click **Unlock Placeholder** to manage the lock status of the placeholder.

Creating a sequence

If you are using the GV STRATUS Rundown workflow, you can create a sequence from a placeholder.

1. Select the **Send to Playout** tab.



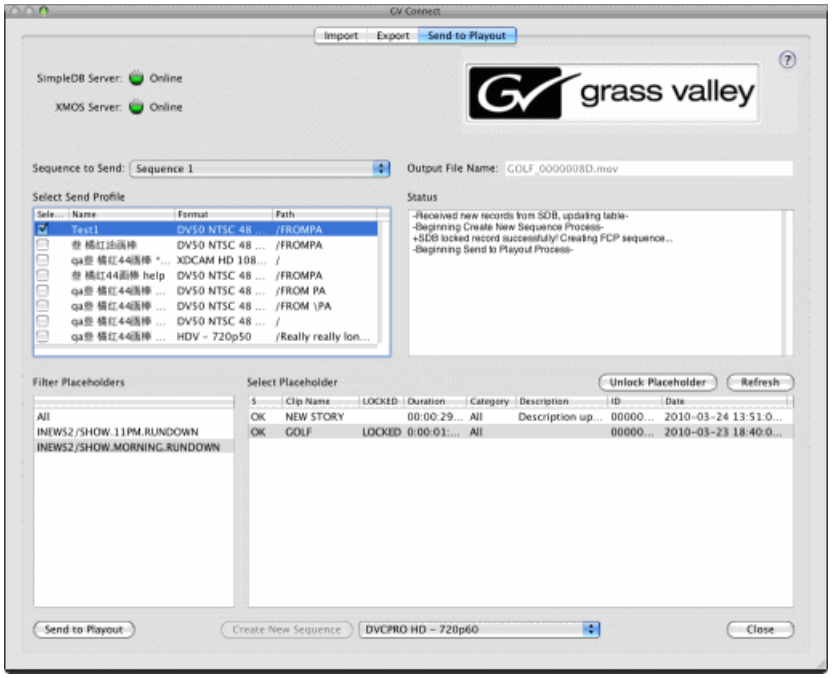
2. Access and select the placeholder from which you are creating a sequence.
3. Select the format in which the sequence is created in the Final Cut Pro project.
4. Click **Create New Sequence**.

   GV Connect attempts to the placeholder in the GV STRATUS Rundown system. If the lock is successful, GV Connect creates the sequence, names it according to the placeholder name, and adds it to the Final Cut Pro project.
5. Edit the sequence in Final Cut Pro.

Exporting a sequence and linking to Aurora Playout

Using the GV STRATUS Rundown workflow, when you export a sequence to K2 storage, GV Connect automatically links the sequence to an GV STRATUS Rundown placeholder.

1. Select the **Send to Playout** tab.



2. In the **Sequence to Send** drop-down list, select the sequence you are exporting to K2 storage.

   The sequence can be either a sequence GV Connect created from a placeholder or a sequence that you manually created in Final Cut Pro.

3. Access and select the placeholder associated with the sequence you are exporting.
4. In the **Select Send Profile** list, select the location that is configured to receive the GV STRATUS Rundown workflow sequences.

   NOTE: You must export to a HotBin that is configured to place the media in the bin that* GV STRATUS Rundown *is monitoring.

5. Click **Send to Playout**.

   GV Connect exports the sequence to K2 storage.

6. If desired, click **Unlock Placeholder** to manage the lock status of the placeholder.

About This Release

Version 9.3

- **4K** — The K2 Summit 3G system supports 4K Ultra High Definition workflow with the requirement of 3G licenses, 4K licenses, 3G codec module, codec option cards, and high endurance solid state drives.
- **6x Super-Slo-Mo** — The K2 Summit 3G system supports 6x Super-Slow-Mo (SSM) workflow with LDX XtremeSpeed and LDX Compact XtremeSpeed 6x ultra slow-motion cameras.
- **1080p 50/60** — The K2 Summit 3G system supports 3G Level B Dual Stream 1080p 50/60 input and output. This includes support for 1080p AVC-Intra Class 100 format for 3D/Video+Key and 3x Super-Slow-Mo. Requires a 3G codec module plus HD, 3G, and AVC licenses.
- **6-in/2-out support** — The support of 3-input Multi-Cam recorder which records video for each three 720p/1080i SDI inputs in a channel for a clip. Two 3-input Multi-Cam recorders, and 2 players enable the 6-in/2-out support.
- **Enhanced K2 Dyno integration with 4K/UHD Pan & Zoom** — The K2 Summit 3G system supports 4K/UHD Pan & Zoom feature in K2 Dyno S Replay Controller. Requires the DynoZoom Frame and GV DynoZoom software.
- **High endurance SSD Internal Storage** — Required for features with high storage bandwidths such as 6-in/2-out support, 6x Super-Slo-Mo (SSM), and 4K/UHD workflow. Available options are 8-drive and 12-drive in a RAID-0 or RAID-1 configuration.
- **Type IV CPU carrier module** — Updated components on CPU board. Functionally equivalent to Type III CPU carrier module.
- **USB 3.0 support** — A USB 3.0 card is available as an option or as a field kit upgrade.
- **Documentation** — PDF manuals are replaced by an online HTML format Topic Library. Refer to *Topic Library replaces PDF manuals* on page 1066.
- **Revised compatibility between K2 hardware components and software versions** — K2 Summit systems shipping from Grass Valley after 20140901 have hardware components that require compatible K2 software versions. Refer to *Compatible K2 systems hardware* on page 1087.
- Topic Library republished 20140829 to restore missing section "Installing and Servicing the K2 SAN system".

Not supported in this release

The following devices and functionality are not supported with this version of K2 software. Check with your Grass Valley representative regarding availability.

- Generation of MXF Reference Files is no longer supported.
- Export of AVI files is no longer supported.
- K2 Media Client — Compatible with 3.x versions of K2 software only.

NOTE: Not supported with 9.0 versions and later: First-generation K2 Summit and K2 Solo systems with Type I CPU carrier module and CompactFlash system drive size below 16GB. Field upgrade kits are available to upgrade a first-generation K2 Summit system as required to support this version of K2 software.

Changes and features in previous releases

The following sections describe changes and features in past releases.

Version 9.2

- **1080p 50/60** — The K2 Summit 3G system supports 3G Level A ,with 3 Gb/s input and output on an SDI connection. This includes support for 1920 x 1080p AVC-Intra Class 100 format. Requires a 3G codec module and a 3G license.
- **MXF AS-02, AS-03** — Import and generic export of MXF AS-02 supported. Import of MXF AS-03 supported. Requires a K2 Extended File Services license.
- **XML Import** — Expanded to support all K2 Summit system formats.
- **FTP Overwrite** — In K2 AppCenter Configuration Manager you can configure the K2 Summit system to overwrite files when it does an FTP transfer. Do not use this setting unless required by your specific workflow.
- **Force PCM Status Bit** — In K2 AppCenter Configuration Manager you can configure the K2 Summit system to set the status of all playout audio tracks to PCM. This setting applies to both PCM audio tracks and non-PCM audio tracks. Do not use this setting unless required by your specific workflow.
- **Documentation** — Use the K2/GV STRATUS Documentation Set 071-8910-03, in addition to these release notes, with this release of K2 software. The following manuals are new/revised:
  - K2 AppCenter User Manual 071-8723-05
  - K2 System Guide 071-8726-05
  - K2 Storage Area Network Installation and Service Manual 071-8779-04
  - K2 Storage Cabling Guide 071-8780-04
  - K2 Summit 3G Production Client Quick Start Guide 071-8873-01
  - K2 Solo 3G Media Server Quick Start Guide 071-8872-01
  - K2 Summit 3G Service Manual 071-8725-04
  - K2 Solo 3G Media Server Service Manual 071-8881-01
  - K2 Summit/Solo Field Kit Upgrade Instructions 071-8721-07
  - K2 Dyno Replay Controller Release Notes 071-8743-13
  - K2 Dyno Replay Controller User Manual 071-8909-01
  - K2 FCP Connect Release Notes 071-8740-07
  - GV Connect User Manual 071-8739-04
  - K2 FCP Connect Installation Manual 071-8738-05
  - K2 Avid Connect Installation Manual and Release Notes 071-8904-01

Version 9.1

- **ShareFlex** - Supports sharing a K2 Dyno S Replay Controller's record train from one K2 Summit system with another K2 Summit system over the network. For more information, refer to K2 Dyno S Replay Controller User Manual and Release Notes for software version 3.1.

- **Enhance network bandwidth** - As part of upgrading to this version of K2 system software, there are additional tasks to enhance network bandwidth. This is required for K2 Summit/Solo systems using ShareFlex and highly recommended for all systems.
- **Closed Captioning support** - CEA 608 to CEA 708 DTV CC transcoder.
- **Compatibility** - Option to export MXF files in either SMPTE 377M or SMPTE 377-1 style.
- **Compression** - AVC-LongG; supports new Panasonic AVC-LongG cameras.
- **Password and security on Grass Valley systems** - The GVAdmin user account is now a member of the Administrators group, with full Windows administrator rights. If you need a user account with K2 administrator rights only, use the pre-configured K2Admin account or configure your own site-specific account.
- **Documentation** – Use the K2/GV STRATUS Documentation Set 071-8910-00, in addition to these release notes, with this release of K2 software. The following manuals are new/revised:
  - K2 10Gv2 SAN Installation and Service Manual 071-8779-03
  - K2 Storage Cabling Guide 071-8780-03
  - K2 Summit/Solo Field Kit Upgrade Instructions 071-8721-06
  - K2 AVID Connect Installation Manual and Release Notes 071-8904-00
  - K2 Dyno S Replay Controller User Manual 071-8909-00

Version 9.0.2

- **Windows operating system** — K2 Summit/Solo systems now run Windows Embedded Standard 7 64-bit operating system.
- **SNFS file system** — Upgrade to version 4.2 is required.
- **Security** — An Embedded Security solution for protection against viruses and other unauthorized programs replaces the write filter.
- **Format** — Avid DNxHD is suppported as an option.
- **CPU carrier module** — K2 Summit/Solo systems shipping new from Grass Valley have a Type III CPU carrier module with 8 GB RAM.
- **AVID support** — K2 AVID Connect allows edit in place
- **Transitions** — Improvements for live production.
- **PitchBlue support** — Playout of PitchBlue H.264 clips
- **K2 FTP server** — Supports simultaneous movie and file transfers
- **Multi-cam audio** — 8 tracks of audio for Multi-cam inputs.
- **K2 Solo 3G Media Server** — Hosts a 3G codec module. Does not support codec option cards. Supports features similar to K2 Summit 3G Production Client.
- **Compatibility with Grass Valley products** — Supports K2 Dyno S and GV STRATUS version 2.5.
- **K2 10Gv2 SAN** — The K2 SAN with 8 Gig Fibre Channel and 10 Gig iSCSI connections. Includes support for 2.5 inch drives and large capacity drives. Introduced in late 2012.

- **Documentation** – Use K2/GV STRATUS Documentation Set 063-8289-11 November 2012, in addition to these release notes, with this release of K2 software. The following manuals are new/revised:
  - K2 AppCenter User Manual 071-8723-04
  - K2 System Guide 071-8726-04
  - K2 SAN Installation and Service Manual 071-8779-02
  - K2 Storage Cabling Guide 071-8780-02
  - K2 Summit 3G Client Quick Start Guide 071-8873-00
  - K2 Summit Client Quick Start Guide 071-8722-04
  - K2 Solo 3G Media Server Quick Start Guide 071-8872-00
  - K2 Solo Media Server Quick Start Guide 071-8710-03
  - K2 Summit 3G Service Manual 071-8725-03
  - K2 Solo 3G Media Server Service Manual 071-8881-00
  - K2 Summit/Solo Field Kit Upgrade Instructions 071-8721-05

Version 8.1.10

- **K2 Dyno** — Compatibility with K2 Dyno version 2.0.3. Refer to the "About This Release" section of the K2 Dyno Topic Library for more information on the following:
  - **Simplified SuperOut setup in AppCenter** – Channel properties can still be turned on or off, but their screen positions are now fixed. This reduces the number of decisions that need to be made at setup time and eliminates configurations that cause properties to overlap.
  - **SuperOut reflects the information on the Dyno screen** – Dyno status information is now available on the SuperOut monitor.
  - **Larger SuperOut font** – The font is larger and the outline is thicker.

Version 8.1.9

- **GV STRATUS** — Compatibility with GV STRATUS 2.0.
- **Solo** — Support K2 Solo systems with 300GB drives.
- **Documentation** – Use K2/GV STRATUS Documentation Set 063-8289-09 June 2012, in addition to these release notes, with this release of K2 software. The following manuals are new/revised:
  - K2 Summit/Solo Field Kit Upgrade Instructions 071-8721-03

Version 8.1

- **K2 Summit 3G Production Client** — The next generation K2 Summit Production Client. Supports the same feature set and expands upon it as follows:
  - AVCHD play output (decode) support as an option.
  - 3G codec module hosts codec option cards that are programmable for multiple formats and functions, including multi-cam configurations with XDCAM HD format, Super Slow-motion in both DVCPRO HD and AVC-Intra formats, and playback of H.264 clips.
  - Ready for 1080p 50/60 fps applications in the future with a software only upgrade.
  - 2.5 inch internal storage media storage drives. Capacity increased by 50% (12 x 600GB).
  - mSATA SSD system drive with larger capacity, protected by a file-based write filter.
  - USB 3.0 interface for file exchange

  NOTE: K2 Transmission Clients/Servers and K2 Solo models continue to be available and are not replaced by K2 Summit 3G Production Client.
- **SNFS file system** — Upgrade to version 3.5.3.b21398 is required.
- **Documentation** – Use K2/GV STRATUS Documentation Set 063-8289-08 February 2012, in addition to these release notes, with this release of K2 software. The following manuals are new/revised:
  - K2 AppCenter User Manual 071-8723-03
  - K2 System Guide 071-8726-03
  - K2 Summit 3G Service Manual 071-8725-02
  - K2 SAN Installation and Service Manual 071-8779-01
  - K2 Storage Cabling Guide 071-8780-01
  - K2 Summit 3G Client Quick Start Guide 071-8722-03
  - K2 Summit/Solo Field Kit Upgrade Instructions 071-8721-03
  - K2 Summit 3G Field Kit Upgrade Instructions 071-8826-00

Version 8.0.x

- **GV STRATUS** — Support for Grass Valley's GV STRATUS™ Media Workflow Application Framework.
- **Proxy/live streaming** — When licensed and configured to do so, the K2 Summit system creates low-resolution representations of high-resolution media. The system generates a live stream at inputs and outputs. The system also creates proxy files for recorded assets. Proxy/live streaming functionality is included in AppCenter Pro and AppCenter Elite licenses. This functionality requires the currently shipping Type II carrier module. To access proxy/live streaming for application workflows, you must use a supported GV STRATUS system configuration, which includes a separate proxy server. Direct access on a K2 Summit system alone is not supported.
- **Unified file system** — The media file system supports direct access and interchange with the GV STRATUS™ Media Workflow Application Framework.
- **Credentials** — Default user accounts and passwords change for better integration across all Grass Valley products.
- **USB Recovery Flash Drive** — The size increased to 16 GB.

- **Upgrade** — Upgrading existing K2 Summit systems to software version 8.0.x is a disk image process and requires upgraded hardware as well. Software-only upgrade is not supported. Therefore, you must procure an upgrade field kit from Grass Valley, as follows:
  - K2-XDP-CPU-FK — Includes a Type II carrier module with the new higher performance CPU/COM Express board. Order this field kit if you require proxy/live streaming support and your K2 Summit system does not already have a Type II carrier module.
  - K2-XDP-V8x-FK — Does not include a Type II carrier module. Order this field kit if your K2 Summit system already has a Type II carrier module or if you do not require proxy/live streaming support.

  Both field kits include the disk image, CompactFlash, USB Recovery Flash Drive, and documentation required for the upgrade to version 8.0.x software.
- **Documentation** – Use K2/GV STRATUS Documentation Set 063-8289-07 October 2011, in addition to these release notes, with this release of K2 software. The following manuals are revised:
  - K2 AppCenter User Manual 071-8723-02
  - K2 System Guide 071-8726-02
  - K2 Solo Media Server Quick Start Guide 071-8710-02
  - K2 Summit Client Quick Start Guide 071-8722-02
  - K2 Summit/Solo Field Kit Upgrade Instructions 071-8721-02
  - K2 TimeDelay User Manual 071-8727-01
  - SiteConfig User Manual 071-8693-03

Additional notes

The following sections contain additional information about this release.

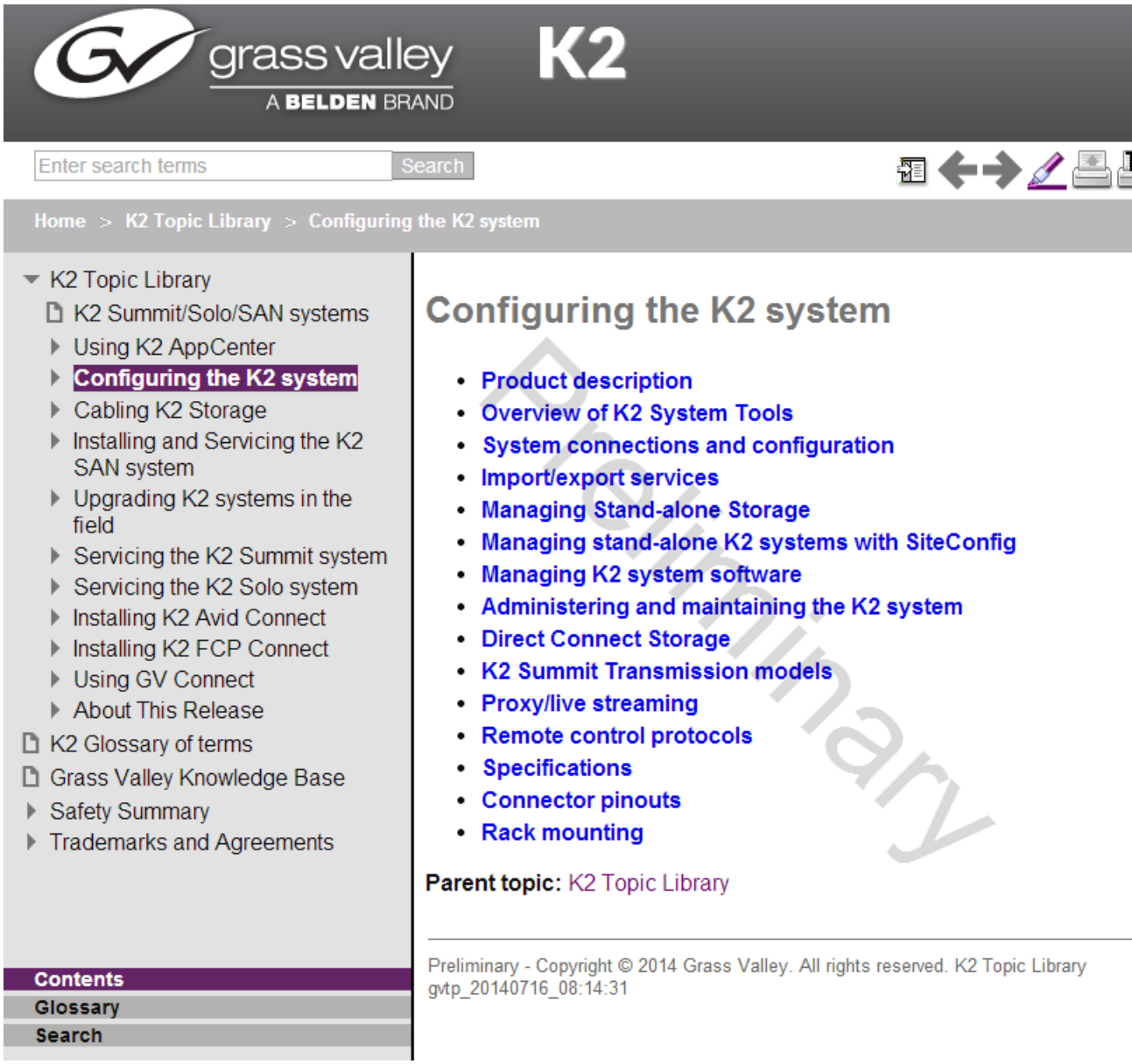
Topic Library replaces PDF manuals

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

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

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

For example, the content of the "K2 System Guide" PDF manual is in the Topic Library section highlighted in the following illustration.



For the K2 product, find information as follows:

Information from this PDF manual...	Is in this Topic Library section:
"K2 Summit/Solo 3G Quick Start Guide"	K2 Quick Start Guides
"K2 AppCenter User Manual"	Using K2 AppCenter
"K2 System Guide"	Configuring the K2 system
"K2 Storage Cabling Guide"	Cabling K2 Storage
"K2 SAN Installation and Service Manual"	Installing and Servicing the K2 SAN system
"K2 Summit/Solo/Media Server Field Kit Upgrade Instructions"	Upgrading K2 systems in the field

Information from this PDF manual...	Is in this Topic Library section:
"K2 Summit 3G Service Manual"	Servicing the K2 Summit system
"K2 Solo 3G Service Manual"	Servicing the K2 Solo system
"K2 Avid Connect Installation Manual and Release Notes"	Installing K2 Avid Connect
"K2 FCP Connect Installation Manual"	Installing K2 FCP Connect
"GV Connect User Manual"	Using GV Connect
"K2 Summit/Solo/SAN Release Notes and Upgrade Instructions"	About This Release

A Topic Library is hosted online on the Grass Valley website. Access to a Topic Library is available at the same location as PDF manuals. For example, if a reader is accustomed to downloading PDF manuals on the Grass Valley website from a Product Software Download page or from a Product Documentation Library page, a link to the Topic Library is provided on the same page.

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

- Print a single topic or a group of topics with **Print topic**  or **Print topic and sub-topics**  toolbar buttons. If your printer options support creating a PDF file, you can create a PDF file rather than printing.
- Download the entire Topic Library as PDF file or as HTML. Access these options on the top-most Topic Library page.

K2 Summit/Solo formats, models, licenses, and hardware support

Formats are supported as in the following tables.

Table 56: First-generation K2 Summit/Solo system

Formats	Compression	1x	Multi-Cam, 3D/Video + Key	3x Super Slo-Mo	4K
SD	DV	Encode/decode	Encode/decode	Not supported.	Not supported.
	MPEG-2	Decode is standard. Encode requires codec option card.	Decode is standard. Encode requires codec option card.	Not supported.	Not supported.
	AVCHD	Not supported.	Not supported.	Not supported.	Not supported.
1080i/720p	DV	Encode/decode. Requires HD license.	Encode/decode. Requires HD license.	Encode/decode. Requires HD license.	Not supported.

Formats	Compression	1x	Multi-Cam, 3D/Video + Key	3x Super Slo-Mo	4K
	MPEG-2	Decode is standard. Encode requires codec option card. Requires HD license.	Decode is standard. Encode requires codec option card. Requires HD license.	Not supported.	Not supported.
	AVC-Intra	Encode/decode. Requires codec option card. Requires HD license.	Encode/decode. Requires codec option card. Requires HD license.	Not supported.	Not supported.
	AVCHD	Not supported	Not supported	Not supported	Not supported.
	AVC - LongG	Not supported	Not supported	Not supported	Not supported.
	Avid DNxHD	Not supported	Not supported	Not supported	Not supported.
1080p	AVC-Intra Class 100	Not supported	Not supported	Not supported	Not supported.

To add support for additional formats, contact your Grass Valley representative for upgrade information.

Table 57: K2 Summit 3G system

Formats	Compression	1x	3x Super Slo-Mo, Multi-Cam, 3D/Video + Key	6x Super Slo-Mo	4K
SD	DV	Encode/decode	Encode/decode	Not supported.	Not supported.
	MPEG-2	Encode/decode	Encode/decode. Requires codec option card.	Not supported.	Not supported.
	AVCHD/H.264	Decode only. Requires AVC license.	Not supported	Not supported	Not supported.

Formats	Compression	1x	3x Super Slo-Mo, Multi-Cam, 3D/Video + Key	6x Super Slo-Mo	4K
1080i/720p	DV	Encode/decode. HD license is required.	Encode/decode. HD license is required.	Encode/decode. Requires codec option card, plus HD and 6xSSM licenses. Requires K2 Summit 3G chassis with 2.5” hard drives for one channel or high endurance solid state drives for full features with two channels.	Not supported.
	MPEG-2	Encode/decode. HD license is required.	Encode/decode. Requires codec option card. HD license is required.	Not supported.	Not supported.
	AVC-Intra	Encode/decode. Requires HD and AVC licenses.	Encode/decode. Requires HD and AVC licenses.	Encode/decode. Requires codec option card, plus HD, 6xSSM and AVC licenses. Requires K2 Summit 3G chassis with 2.5” hard drives for one channel or high endurance solid state drives for full features with two channels.	Not supported.
	AVCHD/H.264	Decode only. Requires HD and AVC licenses.	Not supported	Not supported	Not supported.

Formats	Compression	1x	3x Super Slo-Mo, Multi-Cam, 3D/Video + Key	6x Super Slo-Mo	4K
	AVC - LongG	Decode only. Requires HD and AVC licenses.	Not supported	Not supported	Not supported.
	Avid DNxHD	Encode/decode. Requires HD and DNxHD licenses.	Encode/decode. Requires HD and DNxHD licenses.	Not supported	Not supported.
1080p	AVC-Intra Class 100	Encode/decode. Requires HD, 3G and AVC licenses.	Encode/decode. Requires codec option card, plus HD, 3G and AVC licenses.	Not supported	Encode/decode. Requires codec option cards and high endurance solid state drives. Requires HD, 3G, 4K and AVC licenses.

Table 58: K2 Solo 3G system

Formats	Compression	1x	Multi-Cam, 3D/Video + Key	3x Super Slo-Mo	4K
SD	DV	Encode/decode	Encode/decode	Not supported.	Not supported.
	MPEG-2	Encode/decode	Not supported	Not supported	Not supported.
	AVCHD/H.264	Decode only. Requires AVC license.	Not supported	Not supported	Not supported.
1080i/720p	DV	Encode/decode. HD license is required.	Encode/decode. HD license is required.	Encode/decode. HD license is required.	Not supported.
	MPEG-2	Encode/decode. HD license is required.	Not supported	Not supported	Not supported.
	AVC-Intra	Encode/decode. Requires HD and AVC licenses.	Encode/decode. Requires HD and AVC licenses.	Encode/decode. Requires HD and AVC licenses.	Not supported.
	AVCHD/H.264	Decode only. Requires HD and AVC licenses.	Not supported	Not supported	Not supported.

Formats	Compression	1x	Multi-Cam, 3D/Video + Key	3x Super Slo-Mo	4K
	AVC - LongG	Decode only. Requires HD and AVC licenses.	Not supported	Not supported	Not supported.
	Avid DNxHD	Encode/decode. Requires HD and DNxHD licenses.	Encode/decode. Requires HD and DNxHD licenses.	Encode/decode. Requires HD and DNxHD licenses.	Not supported.
1080p	AVC-Intra Class 100	Encode/decode. Requires HD and 3G licenses.	Not supported	Not supported	Not supported.

Passwords and security on Grass Valley systems

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

The following table shows the different types of users and their privileges. Passwords are case sensitive.

	Windows administrator	Grass Valley product administrator	K2 product administrator	Grass Valley product user
User name	Administrator	GVAdmin	K2Admin	GVUser
Password	adminGV!	adminGV!	adminK2	userGV!
AppCenter Configuration Manager	Full access	Full access	Full access	Can view
AppCenter	Full access	Full access	Full access	Full access; requires an account on the K2 Summit/Solo system
Storage Utility	Full access	Full access	Full access	Can’t access
K2Config	Full access	Full access	Full access	Can’t access
Server Control Panel	Full access	Full access	Can view	Can view

	Windows administrator	Grass Valley product administrator	K2 product administrator	Grass Valley product user
Windows Operating System	Full access	Full access	Limited access (based on Windows user account privileges).	Limited access (based on Windows user account privileges)

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

About application security on the K2 SAN

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

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

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

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

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

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

About credentials in SiteConfig

SiteConfig requires administrative privileges on devices in order to perform most of the network configuration and deployment tasks. For known devices types, SiteConfig has a default administrator account and password. These default credentials depend on the SiteConfig version, so check your SiteConfig Release Notes for any changes. When you add a device based on a known device type,

SiteConfig references the default administrator account and password. Then, when you use remote desktop or perform software deployment to the device, SiteConfig automatically uses these credentials. These credentials are called "global" credentials for the device since the same credentials are used on all devices of that type in the system.

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

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

About proxy/live streaming

The K2 Summit system writes proxy files to a CIFS share, using credentials for the internal system account, which by default is GVAdmin. A proxy file contains the video track, up to eight audio tracks, and timecode. The file is a fragmented MPEG-4 file, which can record/play in chunks. This allows you to play a growing proxy file while it is still recording.

Each K2 Summit system channel multicasts a low-resolution live stream. The K2 Summit system has an HTTP server over which it makes the SDP file available to applications that play the live stream.

A Type II, Type III, or Type IV CPU module is required to support proxy/live streaming.

An AppCenter Pro or AppCenter Elite license on the K2 Summit system enables proxy/live streaming. If licensed for AppCenter Pro, a live stream is available from each of the four channels. If licensed for AppCenter Elite, ChannelFlex features allow you to configure up to eight inputs/outputs, so up to eight live streams are similarly available. When a K2 Summit system is licensed, in Configuration Manager (a part of the K2 AppCenter application) you can configure proxy/live streaming for each channel. You can turn proxy file recording on or off, and you can turn live network streaming on or off. When you turn proxy file recording on, you can then select up to eight audio tracks to include in the proxy file. You can also turn automatic scene detection on or off. When you turn scene detection on, you can configure the minimum scene length. When you turn proxy live network streaming on, you can then select two audio tracks (one pair) to include in the proxy stream.

If licensed for AppCenter Elite, a ChannelFlex channel generates proxy/live streaming as follows:

- Multi-cam Recorder — Both high-resolution assets have their own proxy file. Two live streams are also available. If shared audio, the proxy file and live stream are generated as follows: the first input includes video, audio, and timecode; the second input includes video but does not include audio and timecode.
- 3D / Video + Key — Two live streams are available as follows: the first input/output includes video, audio, and timecode; the second input/output includes video but does not include audio and timecode. Proxy files are not created.
- Super Slo-Mo Recorder — A video-only proxy file and a video-only live stream are generated that are normal speed, which means that they are one half or one third the Super Slo-Mo record rate.

Proxy recording is not supported for continuous record mode.

Network switches and firewalls must be configured to allow the multicast live streaming traffic. IGMP Snooping must be enabled on the network that carries the low-resolution live streaming traffic.

The GV STRATUS product accesses proxy files through a shared CIFS folder. There is a limit to the number of proxy access connections on the server that hosts the share. Therefore full proxy recording is only supported using one of the recommended GV STRATUS configurations with a proxy server. Recording and storing proxy on the local media storage on a K2 Summit/Solo system is not recommended.

Installing and configuring support for Windows 7 generic iSCSI clients

With the Windows 7 operating system, additional steps are required for generic iSCSI clients, to support configuration via SiteConfig and K2Config. The system requirement for .NET is version 4.0 update KB2468871. The complete procedure is as follows:

1. On the PC that hosts the SiteConfig application, navigate to the directory at which SiteConfig is installed.

   By default the location is `C:\Program Files (x86)\Grass Valley\SiteConfig`.

2. Copy the contents of the `ConnectivityKit` directory and the `DiscoveryAgent Setup` directory to a USB thumb drive, network drive, or some other shared location to make it easier to distribute to each PC.

3. To install and configure SiteConfig support locally at a control network PC, do the following:
   a) Copy the contents of the `ConnectivityKit` directory and the `DiscoveryAgent Setup` directory to the control network PC.
   b) On the control network PC, check the Microsoft .NET Framework version and compare to system requirements for the software you intend to deploy with SiteConfig.
   c) If necessary, install .NET software and the required Windows update.

      You can find the installation file for a .NET version in the `ConnectivityKit` directory.
   d) On the control network PC, run `\DiscoveryAgent Setup\setup.exe`.

      The install wizard opens.
   e) Work through the install wizard and when prompted to select the device type, select **GenericDevice**.
   f) Finish the install wizard.
   g) Open firewall port settings on the PC as follows.

      445 Protocol: TCP. Used by SDB and XMOS Server and NAS. Used by SiteConfig. File and printer sharing. Used by CIFS/SMB.

      3389 TCP: Used by Remote Desktop for use by SiteConfig.

      18262 TCP: Used by GV ProductFrame Configuration Service, ProductFrame Discovery Agent Service for use by SiteConfig. Used by GV NetConfig Service. gv-pf. UDP: Used by GV NetConfig Service. gv-pf.

      18263 UDP: Used by ProductFrame Discovery Agent Service for GV NetConfig Device Broadcast/Unicast Protocol. Used by SiteConfig. Sent by ControlPoint, received by Devices

      18264 UDP: Used by ProductFrame Discovery Agent Service for GV NetConfig Controller Protocol. Used by SiteConfig. Sent by Devices, received by ControlPoint

      49168 HTTP/TCP: Used by Grass Valley K2 Config for K2Config application connection between a control point PC and the K2 system device configured. Used for most functions.

      49169 TCP: Used by Grass Valley K2 Config for K2Config application connection between a control point PC and the K2 system device configured. Used for a few functions that require longer time periods.

   h) Restart the control network PC.

Extent Manager for K2 SANs

Extent Manager is a service that reclaims hard drive disc space that might be lost by the creation of proxy media files. It runs automatically on standalone K2 Solo 3G systems. You must run it manually on your online or production K2 SAN system if you store proxy media files in the same storage (on the V: drive) as your high-resolution media files.

You should run Extent Manager periodically as instructed below during times when system performance is not critical, such as while the system is off the air. To see how many proxy files are in queue to be operated on by the Extent Manager service, look in the default proxy location

V:\proxy\journal. Each journal file in that location represents a proxy file in the queue. A large number of files indicates that you should run Extent Manager.

1. Open the Windows **Services** Control Panel.
2. Start the **Grass Valley Extent Manager Service**.

   A message notifies you that the service started successfully.
3. Monitor progress by observing files in *V:\proxy\journal*. A decreasing number of files indicates the service is working. You can estimate 4 minutes per 1000 files.
4. If desired, you can safely stop and start Extent Manager at any time, using the Windows **Services** Control Panel.
5. When the journal folder is empty or contains only a few files, the Extent Manager process is complete.

Embedded Security modes and policies

The Embedded Security solution protects against viruses and other unauthorized programs on the following Grass Valley systems:

- K2 Summit/Solo system
- All types/roles of K2 Media Server
- All types/roles of GV STRATUS server

Embedded Security prevents any unauthorized programs from running on the system. It contains a whitelist of programs that are authorized to run. Whenever a program attempts to run, it is checked against the whitelist. If the program is not on the whitelist, Embedded Security blocks the program from running. SiteConfig, and any software deployed by SiteConfig, is on the whitelist, so you do not need to manage Embedded Security in any way when using SiteConfig to deploy software. All versions of SiteConfig are compatible with Embedded Security.

When installing software manually (without SiteConfig) it might be necessary to manage Embedded Security. When necessary, you can put Embedded Security in Update mode. This mode allows you to manually install software that is not on the whitelist. Do not confuse Update mode with the idea that Embedded Security is "disabled". When in Update mode, Embedded Security is still active. While in Update mode, Embedded Security keeps track of any software you run or install and adds it to the whitelist. When you are done installing software and any required restarts, you must take Embedded Security out of Update mode so that it can protect the system. For software that requires a restart after installation, such as K2 system software and SNFS media file system software, Embedded Security must remain in Update mode until after the restart is complete.

No system restarts are required for entering or leaving Update mode, and a restart does not change the Update mode status. If in Update mode before a restart, the system remains in Update mode after a restart. You use the Embedded Security Manager to enter and leave Update mode.

The following policies apply to the Embedded Security:

- Use Update mode only as instructed by Grass Valley product documentation or as directed by Grass Valley Support. Do not do any other operations with Embedded Security Manager, unless under the direct supervision of Grass Valley Support.
- Do not keep Embedded Security in Update mode long-term, as Embedded Security does extra processing while in Update mode and eventually problems arise when attempting to run software.

- Make sure that Embedded Security is not in Update mode when using SiteConfig to install software. Update mode interferes with SiteConfig's automatic management of Embedded Security and causes problems running the software installed.
- Leave Embedded Security enabled for normal operation of your Grass Valley system. Do not disable Embedded Security except as instructed by Grass Valley product documentation or as directed by Grass Valley Support. Enabling and disabling Embedded Security requires a restart.
- Do not install any programs or modify any operating system settings unless approved by Grass Valley. By design, Embedded Security prevents any programs from being installed or from running that are not present when you receive the system new from Grass Valley. These Grass Valley systems are not general purpose Windows workstations. The applications and configuration have been specifically optimized on each system for its intended use as part of the Grass Valley system.
- While Embedded Security is the key anti-virus component on these systems, you should still follow the Grass Valley anti-virus scan policy and scan all the devices in your Grass Valley system to ensure viruses are not propagated between machines.

Embedded Security is part of the K2 Solo 3G system generic disk image and the K2 Media Server generic disk image compatible with K2 software version 9.0 or higher. Both K2 Media Servers and GV STRATUS servers use the same generic disk image, so GV STRATUS servers inherit the Embedded Security solution. On K2 Solo 3G systems, the Embedded Security solution introduced with K2 software version 9.0 replaces the write filter from previous versions.

Deploy Embedded Security solution - One-time process

You must have a system system-specific recovery disk image of the computer on which you are doing the Embedded Security one-time process.

NOTE: A re-image of the computer might be necessary if the Embedded Security one-time process is done incorrectly. Follow instructions carefully.

This is a two-phase task:

1. Run a script on the local system to which you are deploying software.
2. Deploy software with SiteConfig.

NOTE: You must carefully read and verify that you have completed each step in the task. Do not assume the task is the same as other software install tasks with which you are familiar.

On the computers in your system that are running the Grass Valley Embedded Security solution, you must do a one-time initial deployment process, as instructed by this task. This task isolates the steps required for the one-time process. If you have sufficient knowledge of systems and upgrades, you can modify your software upgrade steps as necessary to do the one-time process at the same time as your other software upgrades, rather than as isolated steps. After you have done this one-time process, you can do future upgrades using the normal upgrade process.

This applies to the following:

- K2 Summit/Solo system
- All types/roles of K2 Media Server

- All types/roles of GV STRATUS server

1. Determine the status of the Embedded Security solution on the computer. You can use SiteConfig check/view software to make this determination or on the local computer you can use the Programs and Features Control Panel to make this determination. Proceed as follows:
   - If the computer does not have **McAfee Solidifier**, which is a component of the Embedded Security solution, do not continue with these steps. The computer must already have the Embedded Security solution before the one-time process is applied.
   - If the computer has **McAfee Solidifier** at version 6.1.1.369, do not continue with these steps. That version indicates that the computer already has the one-time process applied, through either a software installation or a disk image process.
   - If the computer has **McAfee Solidifier** at a version lower than 6.1.1.369, continue with these steps.
2. Procure the McAfee script from the software download page on the Grass Valley website.
   The filename to download is *McAfee-6.1.1.zip*.
3. Unzip and copy the directory containing the McAfee script files to any location on the local computer.
4. Use Embedded Security Manager and put the local computer in Update Mode.
5. On the local computer, in the directory of McAfee script files that you downloaded from the Grass Valley website, run *UpdateMcAfee.cmd*.
6. Delete the directory of McAfee script files from the local computer.
7. In SiteConfig, do the following:
   a) Add the **GV Embedded Security Manager** role to the device.
   b) Add cab file as necessary to the device's deployment group so that the *GVEmbeddedSecurityManager* cab file is available for deployment.
   c) Do a **Check Software** operation on the device.
   d) Deploy software to the device.
8. Use Embedded Security Manager and leave the Update Mode.
   Embedded Security Manager now reports **Enabled**.
9. Do Windows updates on the local computer.
   You can now install Windows updates KB2859537 and KB2872339, which were previously not allowed on Grass Valley systems.

- For future Windows updates, it is no longer necessary to exclude KB2859537 and KB2872339.
- For future deployment of K2 and GV STRATUS software using SiteConfig, it is no longer necessary to put Embedded Security in Update Mode.
  NOTE: If not using SiteConfig, it can still be necessary to put Embedded Security in Update Mode. Refer to your product's software install/upgrade instructions.

Grass Valley Recommended Deployment and Monitoring Solutions

To maximize up-time, a maintenance strategy must provide the ability to easily identify the root cause of an unanticipated hardware or software failure and to quickly compile failure data. The ability to proactively predict failures and to quickly notify those who can rectify them makes the

maintenance strategy even more powerful. Grass Valley has a long history of building the necessary functionality into critical broadcast products. Beginning with Grass Valley's longstanding monitoring application NetCentral and progressing to the next generation tool GV GUARDIAN, remote monitoring and proactive predictive failure analysis are important contributors to Grass Valley system solutions. Both NetCentral and GV GUARDIAN run on commercial off-the-shelf server PCs, such as the K2 system control point PC. Grass Valley and 3rd party devices report status via Window Messaging, Simple Network Management Protocol (SNMP), or syslog to the NetCentral or GV GUARDIAN application. Each application provides easy to use, fully autonomous remote monitoring to predict errors, provide proactive notifications, and centrally consolidate error logs and hardware failure information. Grass Valley recommends using a remote monitoring tool like NetCentral or GV GUARDIAN. With NetCentral, and even more so with GV GUARDIAN, you can maximize your up-time with less manpower, as compared to manual system monitoring. Watching for indicator lights, physically scanning logs, and other manual monitoring is far more time consuming, more error-prone, and much less accurate. If you have an existing NetCentral installation you install a NetCentral device provider on the NetCentral server PC for each type of device you are monitoring. Refer to NetCentral product documentation for installation and operating instructions. With GV GUARDIAN, only SNMP MIBs are required. Separate device providers are not necessary. Refer to the on-line GV GUARDIAN Topic Library for information.

Operation considerations

- If you have problems using SiteConfig to discover a Windows Server 2008 K2 Media Server, make sure the server has an IP address. SiteConfig cannot discover Windows Server 2008 systems that do not have an IP address, such as those configured for DHCP.
- Do not neglect to make a "first birthday" image of each K2 product shortly after installation and configuration is complete.
- Changing system timing requires a restart. This takes effect immediately as soon as the new video standard (NTSC/PAL) is selected. Save all your configuration changes prior to changing the system timing.
- Refer to the "Remote control protocols" appendix in the *K2 System Guide* for operation considerations related to AMP, VDCP, BVW, Harris, RS-422, etc.
- To import/export between systems using AppCenter, in Configuration Manager on the Remote tab, add each system that you want to have available as a source or a destination. Do this for K2 systems as well as non-K2 systems, such as Profile XP.
- When transferring between K2 systems and other types of systems, such as Profile XP, you must specify the IP address, path, and file name to initiate a transfer.
- Constrain media names and filepaths for support across systems. While AppCenter allows you to create bin names and clip names longer than 32 characters, names of this length are not supported on all products.
- Before configuring a channel, eject all clips from the channel. This is required to put changes into effect.
- K2 Summit/Solo systems and K2 Media Servers can operate continuously for a long period of time. A restart at least once every six months is the recommended operational practice. A restart once every year is required.
- Mix effects (an AppCenter Pro feature) are not supported between different compression formats.
- A 3D/Video+Key player channel does not support agile playback or transition (mix) effects.
- A 3D/Video+Key player channel does not support a two-head player model.

- A 3D/Video+Key player channel does not support offspeed play greater than 1 or less than -1. During these offspeed play operations the video is not synchronized between the two video tracks. However, both video outputs will resync when recued.
- On a K2 Solo Media Server, before making a new file system, first upgrade drive firmware to the latest version, as specified in *Compatible K2 Summit/Solo components* on page 1083. Failure to do so generates a Storage Utility error.
- Grass Valley recommends that you use a frame synchronizer on incoming video sources that are recorded in AVC-Intra format.
- If Dyno PA connects to an internal storage first generation K2 Summit system, there are special requirements for media disk labels. Refer to the *Dyno Production Assistant Configuration Manual*.
- When configuring editors on a K2 SAN with 1 Gig TOEs, do not assign editors and K2 clients (K2 Summit or K2 Media Client) to the same TOE. Instead, assign editors to their own TOE.
- A K2 10G (NEC D4) RAID controller connected to a Fibre Channel switch must have its "Link Attach" parameter set to "Point-to-Point". A K2 10G RAID controller connected directly to a K2 Summit system must have its "Link Attach" parameter set to "LOOP". When you purchase your K2 10G RAID system from Grass Valley, it comes configured correctly for your intended use. If you re-use a K2 10G RAID system and change the way it is connected, contact Grass Valley for instructions to change the Fiber Channel port configuration. The K2 10Gv2 (NEC M100) RAID controller detects this automatically and so no manual configuration is required.
- A best practice is to check the K2 Summit log weekly to monitor the database size. Every 15 minutes the K2 Summit system reports a "Completed database backup..." message that includes the database size. If the size exceeds 80 MB, reduce the number of markers and/or the amount of metadata in clips.
- If you have a first generation K2 Summit system with a Type II (ADLINK with 4GB RAM), Type III (ADLINK with 8GB RAM), or Type IV (ADLINK with 8GB RAM) CPU carrier module or a 3G codec, consult 3G service procedures in the "Servicing the K2 Summit system" section of the K2 Topic Library when doing any service work or replacing any Field Replaceable Units (FRUs). This is true even if replacing an original FRU that has not been upgraded. System dependencies involving FRUs require 3G service procedures.
- It is not recommended to use 720p tri-level sync for interlace output formats (such as SD and 1080i) Output timing can be off by a field.
- In the AppCenter Import dialog box there can be a long wait time while network devices are discovered. An improvement with the Windows 7 operating system is that a message opens asking if you want to continue waiting. If you continue waiting, eventually network devices are discovered and AppCenter continues operating.

Version compatibility

Versions qualified for compatibility with this version 9.3 release of K2 software are summarized in the following sections.

Compatible Grass Valley products

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

Product	Version	Comments
GV STRATUS	3.5	Check with your Grass Valley representative for version availability
GV STRATUS Rundown	8.2.0.29	—
K2 Dyno Replay Controller	3.3	Check the "About This Release" section of the K2 Dyno Topic Library for compatible disk image version.
K2 Dyno PA	2.0.2.1870	—
Aurora Browse	Not supported	The GV STRATUS product now provides this functionality.
Aurora Suite	Not supported	
Aurora Ingest	Not supported	
NetCentral	5.2.2.10 and higher	—
Profile XP Media Platform	5.4.9 or higher	Media assets can be transferred to/from a Profile XP system but cannot be browsed.
SiteConfig application	2.1.1.579 or higher	—
UIM	2.1.1	—
K2 TimeDelay	9.1.0.23	Check with your Grass Valley representative for version availability
K2 InSync	4.0.3.17	Check with your Grass Valley representative for version availability
K2 AVID Connect	7.0.0.164	Check with your Grass Valley representative for version availability. Refer to the "Installing K2 Avid Connect" section of the K2 Topic Library.
K2 FCP Connect	2.3.0.66	Contact Grass Valley Support for additional information and version availability.

Product	Version	Comments
Grass Valley LDK8300 Super SloMo Camera	—	3x and 2x frame rates supported. Requires AppCenter Elite license.
Grass Valley LDK8000 SportElite HD Super SloMo Camera	—	2x frame rate. Requires AppCenter Elite license.
Sony 3300 Super SloMo Camera	—	3x frame rate only; 2x is not supported. Requires AppCenter Elite license.
EDIUS Elite	7.3.1.1540	—
Kayenne/Karrera	—	Check with your Grass Valley representative for version availability.

Compatible K2 Summit/Solo components

The following components are part of K2 Summit Production Client, K2 Solo Media Server, or K2 Summit Transmission Client/Server products. Components are compatible with this release of K2 software as listed in the following table. Compatible versions are pre-installed on the K2 system when you receive it new from Grass Valley. For microcode and firmware filenames, refer to tables later in this section.

Table 59: Component versions

Component	Version	Comments
GrassValley K2 Client software	9.3	Includes AppCenter
Media File System (SNFS)	4.2.2.b27249	—
SiteConfig Discovery Agent, also known as SiteConfig Network Configuration Connect Kit	2.0.0.200 and higher	A minimum version of 1.0.8 is required to support device discovery. Then when you deploy software to the device, the SiteConfig application prompts you to upgrade to the correct version of the Discovery Agent on the device.
Windows Operating System	Windows Embedded Standard 7 64-bit	—
Windows update	—	—
Microsoft .NET Framework	2.0 SP2, 3.0 SP2, 3.5 SP1, 4.0	—
QuickTime	7.6 and higher	—
Intel Network Connections	13.3	—

Component	Version	Comments
Microsoft iSCSI Initiator	2.08	—
MS XML	4.0 SP2, 6.0	—
MegaRAID Storage Manager (internal storage only)	v2.91-05	—
RAID controller microcode (internal storage only)	1.40.342-1650	—
RAID disk drive firmware Hitachi ViperB drives	570	First generation Summit internal storage only
RAID disk drive firmware Hitachi ViperC drives	510	First generation Summit internal storage only
RAID disk drive firmware Hitachi CobraD drives	360	Summit 3G and Solo internal storage only. 10K
RAID disk drive firmware 7.2K SAS drives	N004	Summit Transmission storage only. This version is still compatible.
	N104	Summit Transmission storage only. This is the currently shipping version. Upgrade is not required and not recommended.
	N002	Summit Transmission storage only. Muskie Plus (+)
RAID disk drive firmware Intel DC S3500 drives	D2010355	Solid State drives. Summit 3G internal storage only
RAID disk drive firmware Intel DC S3700 drives	5DV10270	Solid State drives. Summit 3G internal storage only
RAID disk drive firmware	4101	Solo internal storage only
RAID disk drive firmware	2269	Solid State drives. Solo internal storage only
LSI RAID controller driver	5.2.127.64	Internal storage only. Windows 7 operating system and K2 9.x or higher software.
LSI Adaptor 4GbFC driver Models 7104,7204, 7404W, 949X	1.26.1.0	—
USB Controller	2.1.28.0	Compatible with Front interconnect board 771-0574-01 on systems with 2013 or lower serial number.
	2.1.39.0	Compatible with Front interconnect board 771-0574-01 on systems with 2013 or lower serial number. Required for Front interconnect board 771-0574-02 on systems with 2014 or higher serial number.

Component	Version	Comments
Disk image	7.0.8, 7.0.9, 7.0.13	—
BIOS	GV09	—

Table 60: K2 Summit Production Client internal storage RAID controller microcode file names

Version	Microcode file
1.40.342-1650	SAS1078_FW_1.40.342.1650.rom
Find files at *C:\profile\microcode\Internal Storage\LSI Controller*.	

Table 61: First generation K2 Summit Production Client internal storage drive firmware file names

Drive type	Drive size	Storage Utility Identifier	Version	Firmware file
ViperB	300GB	HUS154530VLS300	570	HITACHI_ViperB_15K_A570.bin
	450GB	HUS154545VLS300	570	HITACHI_ViperB_15K_A570.bin
ViperC	300GB	HUS156030VLS600	510	HITACHI_ViperC_15K_A510.bin
	450GB	HUS156045VLS600	510	HITACHI_ViperC_15K_A510.bin
	600GB	HUS156060VLS600	510	HITACHI_ViperC_15K_A510.bin
Find files at *C:\profile\microcode\Internal Storage\Hitachi*.				

Table 62: K2 Summit 3G Production Client internal storage drive firmware file names

Drive type	Drive size	Storage Utility Identifier	Version	Firmware file
CobraD	600GB	HUC106060CSS600	360	HITACHI_CobraD_10K_A360.bin
CobraE	600GB	HUC106060CSS600	360	HITACHI_CobraE_10K_A350.bin
	900GB	HUC106060CSS600	360	HITACHI_CobraE_10K_A350.bin
Find files at *C:\profile\microcode\Internal Storage\Hitachi*.				

Table 63: K2 Summit 3G Production Client solid state drive firmware file names

Drive type	Drive size	Storage Utility Identifier	Version	Firmware file
DC S3700	400GB	SSDSC2BA40	5DV10270	5DV10270_signed.bin
DC S3500	480GB	SSDSC2BB48	D2010355	D2010355_signed.bin
Find files at *C:\profile\microcode\Internal Storage\Intel*.				

Table 64: K2 Solo and K2 Solo 3G Media Server drive Hitachi firmware file names

Drive type	Drive size	Storage Utility Identifier	Version	Firmware file
CobraD	300GB	HUC106030CSS600	360	HITACHI_CobraD_10K_A360.bin
CobraE	300GB	HUC106030CSS600	360	HITACHI_CobraE_10K_A350.bin

Find files at *C:\profile\microcode\Internal Storage\Hitachi*.

Table 65: K2 Solo and K2 Solo 3G Media Server drive Fujitsu firmware file names

Drive size	Storage Utility Identifier	Version	Firmware file
136GB	MBE2147RC	4101	FUJITSU_15K_25_4101.frm

Find files at *C:\profile\microcode\Internal Storage\Fujitsu*.

Table 66: K2 Summit Transmission internal storage 7.2K SAS Muskie drives

Disk Drive	Storage Utility Identifier	Firmware Version	Firmware file
500G	ST3500414SS	N004	MU_7K_SAS_1T_500G_N004.bin
		N104	MU_7K_SAS_1T_500G_N104.bin
1TB	ST31000424SS	N004	MU_7K_SAS_1T_500G_N004.bin
		N104	MU_7K_SAS_1T_500G_N104.bin
2TB	ST32000444SS	N004	MU_7K_SAS_2T_N004.bin
		N104	MU_7K_SAS_2T_N104.bin

Find files at *C:\profile\microcode\External Storage\K2_L10-L40 Condor\Drive\7.2K\Muskie*.

Table 67: K2 Summit Transmission internal storage 7.2K SAS Muskie+ drives

Disk Drive	Storage Utility Identifier	Firmware Version	Firmware file
500G	ST500NM0001	N002	MUP_7K_SAS_500G_N002.bin
500G and 1TB	ST1000NM0001	N002	MUP_7K_SAS_1T_N002.bin. Available via FTP download.
2TB	ST2000NM0001	N002	MUP_7K_SAS_2T_N002.bin

Find files at *C:\profile\microcode\External Storage\K2_L10-L40 Condor\Drive\7.2K\Muskie+*.

Table 68: K2 Summit Transmission internal storage 7.2K SATA Ultrastar

Disk Drive	Storage Utility Identifier	Firmware Version	Firmware file
2TB	HUS723020ALS640	A350	Hitachi_Ultrastar_7K_A350.bin
2TB	HUS724020ALS640	A1C4	Hitachi_Ultrastar_7K_A1C4.bin
Find files at `C:\profile\microcode\Internal Storage\Hitachi`.			

Compatible K2 systems hardware

The following hardware and supporting components are specified for compatibility with this version of K2 software. Systems that meet compatibility requirements are qualified for a software-only upgrade to this version of K2 software. If your system does not meet compatibility requirements, contact your Grass Valley representative for upgrade information.

Product/Features	CPU carrier module	System drive	USB recovery flash drive	Current disk image version	Current K2 software version
K2 Summit 3G	Type II, Type III, or Type IV	30M mSATA	32GB		9.x
K2 Summit 3G with ShareFlex, HTTP server, and advanced features	Type III or Type IV with 8 GB RAM	30M mSATA	32GB		9.x
First generation K2 Summit	Type II, Type III, or Type IV	16GB	32GB		9.x
First generation K2 Summit with ShareFlex, HTTP server, and advanced features	Type III or Type IV with 8 GB RAM	16GB	32GB		9.x
K2 Solo 3G with ShareFlex, HTTP server, and advanced features	Type III or Type IV with 8 GB RAM	16GB	32GB		9.x
K2 Summit 3G Transmission Client		16GB	32GB		9.x
K2 Media Server and GV STRATUS Server (Dell platform)	NA	NA	NA	8.1.x or higher	9.x
K2 Media Server and GV STRATUS Server (Dell platform) with Embedded Security	NA	NA	NA	9.x	9.x
First generation K2 Solo	Not supported				
First generation K2 Summit Transmission Client/Server	Type II, Type III, or Type IV	16GB	32GB		9.x

Product/Features	CPU carrier module	System drive	USB recovery flash drive	Current disk image version	Current K2 software version
K2 Media Client	Not supported				

K2 Summit systems shipping from Grass Valley after 20140901 have hardware components that require compatible K2 software versions, as follows:

Hardware component	Part Number	Software Version for 9.2	Software Version for 9.3
3G Codec option (mezzanine) card	771051302	9.2.1.2076	9.3.4.2081
3G Codec module	751040802 (FRU - 761050102)	9.2.1.2076	9.3.4.2081

⚠ ***CAUTION: Do not downgrade K2 software. Hardware and software incompatibility can occur when downgrading software.***

Related Topics

Codec module removal on page 891

Codec option card removal on page 892

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	9.3	—
Media File System (SNFS)	4.2.2.b27249	—
SiteConfig Discovery Agent, also known as SiteConfig Network Configuration Connect Kit	2.0.0.200 and higher with Windows 2008 Server	This version required for device discovery on systems with the Microsoft® Windows® Server 2008 operating system
Windows Operating System	Windows 2008 Server R2 SP1 64-bit	With the latest update
Windows update	2.0.50727.4022	—
Microsoft .NET Framework	2.0 SP2, 3.0 SP2, 3.5 SP1, 4.0	—
QuickTime	7.6 and higher	—
Adobe Acrobat Reader	7.0 and higher	—
ATI Display Driver	8.24.3.0	—
Dell OpenManage	6.5.0	R610

Component	Version	Comments
	7.2.0	R620
J2SE Runtime Environment	6, Update 3	—
MSXML	4.0 and higher	—
Dell Server Models	R610, 2950, R620	As provided by Grass Valley for specific K2 storage levels and applications.
LSI Adaptor 4GbFC driver Models 7104,7204, 7404W, 949X	1.25.7.0	—
Broadcom driver	7.0.11.0	—
Disk image	9.0.3	R610
	12.0.9	R620 with 300GB Drives
	12.0.10	R620 with 146GB Drives

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	9.3	—
K2 System Configuration	9.3	
Windows operating system	Server 2008 64-bit	—
Windows update	2.0.50727.4022	—
Disk image	C9.0.3 for R610/2950, 12.0.9 for R620	—
SQL Server Express	2005	—
.NET Framework	1.1, 1.1 Hotfix, 2.0 SP2, 3.0 SP2, 3.5 SP1, Version 4.0 update KB2468871, 4.5	—
QuickTime	7.6 and higher	—
MS XML	4.0	—
Windows Installer	3.1	—
SiteConfig application	2.1.1.579	Upgrade to this version before deploying software to any devices.

Software	Version	Comments
SiteConfig Discovery Agent, also known as SiteConfig Network Configuration Connect Kit	2.0.0.200	A minimum version of 1.0.8 is required to support device discovery. Then when you deploy software to the device, the SiteConfig application prompts you to upgrade to the correct version of the Discovery Agent on the device.
Adobe Reader	11.0	—

Compatible HP ProCurve GigE switch components

Components that reside on 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 2920 series firmware	Use firmware received with the HP switch.	Check with the manufacturer for firmware updates.
HP ProCurve 2910al series firmware	W.15.08.0012	-
HP ProCurve 2900 series firmware	T.11.12	This older version is no longer recommended.
	T.13.23	Upgrade to this version is required. After upgrade, configure QOS settings.
HP ProCurve 3400cl series firmware	M.08.66	This older version is still compatible
	M.08.86	Upgrade to this version is recommended

Compatible K2 RAID components

This compatibility specification applies to K2 10Gv2 RAID (M100), K2 10G RAID (D4), and K2 Lx0 RAID (D3) on a K2 SAN, both basic and redundant. RAID firmware is compatible with this release of K2 software as follows:

Find firmware on the K2 client (for direct-connect storage) or the K2 Media Server (for shared storage) at `C:\profile\microcode\External Storage\K2_L10-L40 Condor\Controller` and at `C:\profile\microcode\External Storage\K2_L10-L40-M100\Controller`.

Component	Version	File Name	Comments
Level 10/20 controller firmware for primary chassis with 15K SAS drives or SATA drives	07VS	D1_07VS.BIN	This version is still compatible for 300 and 450 GB drives
	07VV	D1_07VV.BIN	This version is still compatible for 300 and 450 GB drives

Component	Version	File Name	Comments
	07VW	D1_07VW.BIN	This version required for 600 GB drives, recommended for 300 and 450 GB drives. Requires version 050B for expansion chassis.
Level 10/20 controller firmware for expansion chassis with 15K SAS drives or SATA drives	030F	ENCL_030F.BIN	This version is still compatible for 300 and 450 GB drives with 07VS or 07VV controller firmware.
	050B	ENCL_050B.BIN	This version is compatible for 300 and 450 GB with 07VS, 07VV, or 07VW controller firmware. Required for 600 GB drives with 07VW controller firmware.
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 for 300 and 450 GB drives
	07VV	D3_07VV.BIN	This version is still compatible for 300 and 450 GB drives
	07VW	D3_07VW.BIN	This version required for 600 GB drives, recommended for 300 and 450 GB drives. Requires 050B for expansion chassis.
Level 30/35 controller firmware for expansion chassis with 15K SAS drives or SATA drives	030F	ENCL_030F.BIN	This version is still compatible for 300 and 450 GB drives with 07VS or 07VV controller firmware.
	050B	ENCL_050B.BIN	This version is compatible for 300 and 450 GB with 07VS, 07VV, or 07VW controller firmware. Required for 600 GB drives with 07VW controller firmware.
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 with 7.2K SAS drives	050B	ENCL_050B.BIN	
10G controller firmware for primary chassis with either 7.2K or 15K drives	01VP	D4_ 01VP.BIN	—
10G controller firmware for primary chassis with either 7.2K or 15K drives	01VR	D4_ 01VR.BIN	Upgrade to this version is recommended but not required.

Component	Version	File Name	Comments
10G controller firmware for expansion chassis with either 7.2K or 15K drives	020F	ENCL_020F.BIN	—
10Gv2 controller firmware for expansion chassis with either 7.2K or 10K drives	U22R	91SC022R_101.bin	M91_SC082R_101_U22R_101.inf

Compatible K2 RAID disk drive firmware

This compatibility specification applies to K2 10Gv2 RAID (M100), K2 10G RAID (D4), and K2 Lx0 RAID (D3) on a K2 SAN, both basic and redundant.

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

Disk drive firmware is compatible with this release of K2 software as summarized in the following tables:

K2 10Gv2 RAID (M100)

Table 69: 7.2K Nearline/Production 10Gv2 controllers compatible versions

Disk Drive	Storage Utility Identifier	Firmware Version	Comments
1TB 3.5in	ST1000NM0001	N002	—
	ST31000424SS	N008	—
	ST1000NM0023	NM04	—
3TB 3.5in	ST33000650SS	NM05	—
	HUS723030ALS640	A1D4	—
	ST3000NM0023	NM04	—
Find files for these versions at *C:\profile\microcode\External Storage\K2_L10-L40-M100\Drive\7.2K*.			

Table 70: 10K Online 10Gv2 controllers compatible versions

Disk Drive	Storage Utility Identifier	Firmware Version	Comments
600G 2.5in	ST9600205SS	N003	—
	ST9600204SS	NS06	—
	HUC106060CSS600	A202	—
	HUC109060CSS600	A2D0	—
900G 2.5in	ST9900805SS	N003	—

Disk Drive	Storage Utility Identifier	Firmware Version	Comments
Find files for these versions at *C:\profile\microcode\External Storage\K2_L10-L40-M100\Drive\10K*.			

Table 71: Metadata Online/Production 10Gv2 controllers compatible versions

Disk Drive	Storage Utility Identifier	Firmware Version	Comments
300G HDD 15K 3.5in	ST3300657SS	N007	—
	HUS156030VLS600	A630	—
300G HDD 15K 2.5in	ST9300653SS	N002	—
100G SSD 2.5in	MK1001GRZB	3408	—
Find files for these versions at *C:\profile\microcode\External Storage\K2_L10-L40-M100\Drive\15K*.			

K2 10G RAID (D4), and K2 Lx0 RAID (D3)

Table 72: 15K SAS Cheetah 5 drives with 4G controllers compatible versions

Disk Drive	Storage Utility Identifier	Firmware Version	Comments
73G	ST373685SS	0002	—
146G	ST3146685SS	0002	—
300G	ST3300655SS	0002	—
Find files for these versions at *C:\profile\microcode\External Storage\K2_L10-L40 Condor\Drive\15K\Cheetah 5*. Refer to "Firmware file names" below to identify files.			

Table 73: 15K SAS Cheetah 6 drives with 4G controllers compatible versions

Disk Drive	Storage Utility Identifier	Firmware Version	Comments
146G	ST3146356SS	0004	This version is still compatible
		N005	This is the currently shipping version. Upgrade is recommended but not required.
300G	ST3300656SS	0004	This version is still compatible
		N005	This is the currently shipping version. Upgrade is recommended but not required.

Disk Drive	Storage Utility Identifier	Firmware Version	Comments
450G	ST3450856SS	0004	This version is still compatible
		N005	This is the currently shipping version. Upgrade is recommended but not required.
Find files for these versions at *C:\profile\microcode\External Storage\K2_L10-L40 Condor\Drive\15K\Cheetah 6*. Refer to "Firmware file names" below to identify files.			

Table 74: 15K SAS Cheetah 7 drives with 4G controllers compatible versions

Disk Drive	Storage Utility Identifier	Firmware Version	Comments
300G	ST3300657SS	N005	N005 is compatible with 4G controllers only. Not compatible with 8G controllers.
		N006	This is the currently shipping version and is compatible with 4G controllers. Upgrade is recommended. If you must load disk firmware, load version N006.
450G	ST3450857SS	N005	N005 is compatible with 4G controllers only. Not compatible with 8G controllers.
		N006	This is the currently shipping version and is compatible with both 4G and 8G controllers. Upgrade is recommended. If you must load disk firmware, load version N006.
600G	ST3600057SS	N005	N005 is compatible with 4G controllers only. Not compatible with 8G controllers.
		N006	This is the currently shipping version and is compatible with both 4G and 8G controllers. Upgrade is recommended. If you must load disk firmware, load version N006.
Find files for these versions at *C:\profile\microcode\External Storage\K2_L10-L40 Condor\Drive\15K\Cheetah 7*, except for N005[29] versions. The files for these N005 versions are removed from *C:\profile\microcode\...* directories when you upgrade your K2 software. Refer to "Firmware file names" below to identify files.			

[29] Do not use file CH_15K7_SAS.N005 for any drive

Table 75: 15K SAS Cheetah 7 drives with 8G controllers compatible versions

Disk Drive	Storage Utility Identifier	Firmware Version	Comments
450G	ST3450857SS	N006	This is the currently shipping version and is compatible with both 4G and 8G controllers.
600G	ST3600057SS	N006	This is the currently shipping version and is compatible with both 4G and 8G controllers.
Find files for these versions at *C:\profile\microcode\External Storage\K2_L10-L40 Condor\Drive\15K\Cheetah 7*. Refer to "Firmware file names" below to identify files.			

Table 76: 7.2K SAS drives with 4G controllers compatible versions

Disk Drive	Storage Utility Identifier	Firmware Version	Comments
500G	ST3500620SS	N001	—
1TB	ST31000640SS	N001	—
Find files for these versions at *C:\profile\microcode\External Storage\K2_L10-L40 Condor\Drive\7.2K*. Refer to "Firmware file names" below to identify files.			

Table 77: 7.2K SAS Muskie drives with 8G controllers compatible versions

Disk Drive	Storage Utility Identifier	Firmware Version	Comments
500G	ST3500414SS	N004	This version is still compatible. Upgrade is not required and not recommended, because upgrading bound disks takes a very long time, degrades performance, and puts the file system at risk if a disk fails.
		N104	
2TB	ST32000444SS	N004	
		N104	
Find files for these versions at *C:\profile\microcode\External Storage\K2_L10-L40 Condor\Drive\7.2K\Muskie*. Refer to "Firmware file names" below to identify files.			

Table 78: 7.2K SAS Muskie+ drives with 8G controllers compatible versions

Disk Drive	Storage Utility Identifier	Firmware Version	Comments
500G	ST500NM0001	N002	This is the currently shipping version.
500G and 1TB	ST1000NM0001	N002	
2TB	ST2000NM0001	N002	

Disk Drive	Storage Utility Identifier	Firmware Version	Comments

Find files for these versions at `C:\profile\microcode\External Storage\K2_L10-L40 Condor\Drive\7.2K\Muskie+`. Refer to "Firmware file names" below to identify files.

Firmware file names

Disk Drive	Firmware Version	Firmware Type	Firmware File Name
Cheetah 5 15K SAS 73G	0002	Interface	CT15K5SAS.01_
		Servo	CT15K5SAS_73.__1
Cheetah 5 15K SAS 146G	0002	Interface	CT15K5SAS.01_
		Servo	CT15K5SAS_146.__1
Cheetah 5 15K SAS 300G	0002	Interface	CT15K5SAS.01_
		Servo	CT15K5SAS_300.__1
Cheetah 6 15K SAS 146G	0004	Interface/Servo	CH_15K6_SAS.N004
	N005	Interface/Servo	CH_15K6_SAS.N005
Cheetah 6 15K SAS 300G	0004	Interface/Servo	CH_15K6_SAS.N004
	N005	Interface/Servo	CH_15K6_SAS.N005
Cheetah 6 15K SAS 450G	0004	Interface/Servo	CH_15K6_SAS.N004
	N005	Interface/Servo	CH_15K6_SAS.N005
Cheetah 7 15K SAS 300G	N006	Interface/Servo	CH_15K7_SAS_300G_N006.bin
Cheetah 7 15K SAS 450G	N006	Interface/Servo	CH_15K7_SAS_450G_N006.bin
Cheetah 7 15K SAS 600G	N006	Interface/Servo	CH_15K7_SAS_600G_N006.bin
Cobra 10K SAS 600G	A202	Interface/Servo	COB_10K_SAS_600GB_A202.bin
Cobra 10K SAS 1.2TB	A3E0	Interface/Servo	COB_10K_SAS_1_2TB_A3E0.bin
Firestorm 10K SAS 600G	NS06	Interface/Servo	FIRE_10K_SAS_600GB_NS06.bin
Compass 10K SAS 600G	N003	Interface/Servo	COM_10K_SAS_600GB_N003.bin
Compass 10K SAS 900G	N003	Interface/Servo	COM_10K_SAS_900GB_N003.bin
7.2K SAS 500G	N001	Interface	BA_7K_ Interface.N001
		Servo	BA_7K_ ST3500620SS_ Servo.C30D
7.2K SAS 1TB	N001	Interface	BA_7K_ Interface.N001
		Servo	BA_7K_ ST31000640SS_ Servo.B30D
7.2K SAS 1TB MantaRay	NM05	Interface/Servo	MRAY_7K_SAS_1TB_NM05.bin
7.2K SAS 3TB MantaRay	NM05	Interface/Servo	MRAY_7K_SAS_3TB_NM05.bin
7.2K SAS 1TB Mars	A1D4	Interface/Servo	MARS_7K_SAS_1TB_A1D4.bin

Disk Drive	Firmware Version	Firmware Type	Firmware File Name
7.2K SAS 3TB Mars	A1D4	Interface/Servo	MARS_7K_SAS_3TB_A1D4.bin
7.2K SAS 500G Muskie	N004	Interface/Servo	MU_7K_SAS_1T_500G_N004.bin
	N104	Interface/Servo	MU_7K_SAS_1T_500G_N104.bin
7.2K SAS 2TB Muskie	N004	Interface/Servo	MU_7K_SAS_2T_N004.bin
	N104	Interface/Servo	MU_7K_SAS_2T_N104.bin
7.2K SAS 1TB Muskie	N008	Interface/Servo	MU_7K_SAS_1T_N008.bin
7.2K SAS 500G Muskie+	N002	Interface/Servo	MUP_7K_SAS_500G_N002.bin
7.2K SAS 500G/1TB Muskie+	N002	Interface/Servo	MUP_7K_SAS_1T_N002.bin. Available via FTP download.
7.2K SAS 2TB Muskie+	N002	Interface/Servo	MUP_7K_SAS_2T_N002.bin
15K SSD 100G	3408	Interface/Servo	PHE_SSD_SAS_100GB_3408.bin

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	Applicable to R610, 2950. Acronis TrueImage 8162.
	Recovery CD part number 063-8246-07	Applicable to R620. Acronis 11.5.
Grass Valley Control Point PC	Recovery CD part number 063-8246-04	Applicable to R610, 2950. Acronis TrueImage 8162.
	Recovery CD part number 063-8246-07	Applicable to R620. Acronis 11.5.

Upgrading K2 systems

This section contains the tasks necessary for a software-only upgrade on standalone and SAN K2 systems. A software-only upgrade is an upgrade that does not require re-imaging or the installation of any hardware.

Do not do the tasks in this section if the system you want to upgrade is not supported for software-only upgrade, as follows:

- A K2 Summit 3G system currently at a 8.x version
- A first generation K2 Summit system currently at a 7.x version or a 8.x version
- A first generation K2 Solo system
- A K2 Media Server or GV STRATUS server with a disk image version lower than 8.1.x.
- A K2 Media Server or GV STRATUS server with a version 8.1.x or higher disk image and you require the Embedded Security solution on the server.

If the system you want to upgrade is not supported for software-only upgrade, you must procure one or more of the following K2 Field Kits and follow the included instructions:

- K2-XDP2-CPU-FK: Processor upgrade Field Kit. Includes updated Type IV CPU carrier module required for advanced features such as ShareFlex. NOT AVAILABLE for K2-SOLO models.
- K2-XDP2-V9-FK: K2 Summit / K2 Solo 9.x Upgrade Field Kit. Includes 9.x system software license, 16GB CompactFlash system drive with image, and 16GB USB recovery flash drive with Acronis backup software and new Windows Embedded System 7 license with Embedded Security Solution. Requires either Type II, Type III, or Type IV CPU carrier module.

Do the tasks in this section if the system you want to upgrade is supported for software-only upgrade, as follows:

- A first generation K2 Summit system or a K2 Summit/Solo 3G systems currently at a 9.x version of K2 software.
- A K2 Media Server or GV STRATUS server with a version 8.1.x or higher disk image, if you do not require the Embedded Security solution on the server.

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

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 on your SAN-attached K2 Summit systems, the current K2 software is at version 9.x or higher. If the current K2 software is at a version lower than 9.x, you must upgrade K2 Summit systems using the appropriate Grass Valley Field Kit, which includes a disk image and hardware. Once upgraded via the field kit to an 9.x version, you can then use these upgrade instructions.

About upgrading the K2 SAN with SiteConfig

This section provides instructions to upgrade the following K2 SAN devices:

- K2 Media Servers

- K2 Summit Production Clients

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.

If this is the first time using SiteConfig for software upgrade, follow instructions in *K2 SAN Installation and Service Manual* rather than instruction in these release notes. You must first have SiteConfig set up for system management and software deployment of the K2 SAN. Also refer to the *SiteConfig User Manual* or *SiteConfig Help Topics*. Then, after you have completed this initial SiteConfig set up, you can follow the instructions in this section to upgrade software.

NOTE: If this is the first time using SiteConfig for software upgrade do not follow instructions in these release notes alone.

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 9.3 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 Grass Valley 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 Summit Client SAN software installation (**.cab*) file.
   - K2 Media Server software installation (**.cab*) file. Use file with *x86* in filename for 32-bit systems and file with *x64* in filename for 64-bit systems.
   - SNFS software installation (**.cab*) file. Use file with *x86* in filename for 32-bit systems and file with *x64* in filename for 64-bit systems.
   - Summit SNFS software installation (**.cab*) file.
   - Control Point software installation (**.cab*) file.
2. On the K2 Media Server, check for the *C:\SNFS* directory and then proceed as follows:
   - If *C:\SNFS* exists on the K2 Media Server, then SNFS 3.5.1 is on the C: drive. In this case you must move SNFS to the D: drive. To do this you must procure the *35c235d.reg* file and use it as instructed with special tasks in the upgrade process below. The *35c235d.reg* file is on the version 9.3.x.xxxx K2 software CD in the SNFS directory. It can also be obtained at *http://www.grassvalley.com/downloads*.
   - If *C:\SNFS* does not exist on the K2 Media Server, continue with this procedure. No special tasks are required.
3. If a newer version of SiteConfig is available for upgrade and you have not yet upgraded SiteConfig, do the following:
   a) From Windows **Programs and Features**, uninstall the current version of SiteConfig from the control point PC.
   b) Install the new version of SiteConfig on the control point PC.
4. 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 9.3.x.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.

   NOTE: If an "Unable to copy ... to target" error appears for a device that has Grass Valley Embedded Security, put Embedded Security in Update mode.

3. Configure and run deployment tasks to upgrade software.

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. 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 to make this determination.
2. Shut down the backup server.
3. Upgrade the primary server.
4. Continue with upgrade 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

- The SiteConfig control point PC must have access to the software installation files for this release.

Install High Priority Windows updates (recommended)

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

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

  NOTE: If a computer does not have the Grass Valley* Embedded Security *solution one-time initial deployment process applied, do not install updates KB2859537 or KB2872339. If these updates have been installed on the computer, remove the update and restart the computer.

Upgrade .NET

Do not do this task if:

- The computer has .NET 4.5 installed

Do this task if:

- The computer does not have .NET 4.5 installed

This task applies to the following:

- K2 Summit/Solo systems
- All types/roles of K2 Media Servers
- All types/roles of GV STRATUS servers.

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

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

Upgrade QuickTime

Do not do this task if:

- QuickTime is currently at version 7.6 or higher.

Do this task if:

- QuickTime is at a version lower than 7.6.

1. Access the QuickTime installation files.
2. Locate and open the following QuickTime install file:

   `QuickTimeInstaller-7.6.exe`
3. Work through the install wizard.

   Configure settings so that the software does not automatically update Quicktime and other Apple software.

   NOTE: Unless instructed to do so by Grass Valley, do not update or install Apple software.

   Accept the default destination folder and other default settings.

Configure GlobalSuperUser in 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:

- You have already modified the configuration file with the required settings.

Do this task if:

- The configuration file does not have the required settings.

Prerequisites for this task are as follows:

- K2 systems must be offline

You can verify and, if necessary, modify the media file system (SNFS) configuration file and still keep your media file system intact if you carefully follow the steps in this procedure.

As an alternative to manually modifying the configuration file, if you need to make a new file system after upgrading K2 software, the required 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. On a K2 Media Server, using Notepad, open the media file system (SNFS) configuration file:

   The configuration file can be either *D:\SNFS\config\default.cfg.* or *D:\SNFS\config\gvfs_hostname.cfg*, where *hostname* is the name of the primary file system server (FSM).

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
.
ReservedSpace No
```

3. Close, and if necessary save, the SNFS configuration file.

If you made changes, the K2 system must be restarted for the changes to take effect.

The restart later in this upgrade procedure is sufficient to put the changes into effect.

Configure Macintosh access in SNFS configuration 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 SAN has no iSCSI or Fibre Channel connected Macintosh clients
- The K2 SAN has iSCSI connected or Fibre Channel connected Macintosh clients and Windows Security is configured to Yes on the SNFS file system.

Do this task if:

- The K2 SAN has iSCSI connected or Fibre Channel connected Macintosh clients and Windows Security is configured to No on the SNFS file system.

Prerequisites for this task are as follows:

- The Macintosh client connection requires K2 FCP Connect.
- The K2 SAN must be offline

You can verify and, if necessary, modify the media file system (SNFS) configuration file and still keep your media file system intact if you carefully follow the steps in this procedure.

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. On a K2 Media Server, using Notepad, open the media file system (SNFS) configuration file:

   The configuration file can be either *D:\SNFS\config\default.cfg.* or *D:\SNFS\config\gvfs_hostname.cfg*, where *hostname* is the name of the primary file system server (FSM).

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
# ********************************************************
.
.
WindowsSecurity No

UnixDirectoryCreationModeOnWindows 0777
UnixFileCreationModeOnWindows 0666
```

3. Close, and if necessary save, the SNFS configuration file.

If you made changes, the K2 system must be restarted for the changes to take effect.

The restart later in this upgrade procedure is sufficient to put the changes into effect.

If you made changes to *UnixDirectoryCreationModeOnWindows* and *UnixFileCreationModeOnWindows* parameters, to apply changes to existing assets you must delete and then re-create files and/or bins, such as HotBins.

If SNFS is on C: uninstall SNFS manually

Do not do this task if:

- SNFS is on the D: drive of the K2 Media Server.

Do this task if:

- SNFS 3.5.1 is on the C: drive of the K2 Media Server. If *C:\SNFS* exists on the K2 Media Server, then SNFS 3.5.1 is on the C: drive.

If SNFS 3.5.1 is on the C: drive of the K2 Media Server, you must move it to the D: drive. This is best accomplished as part of the upgrade process. After you uninstall SNFS, you must reset registry

settings, install SNFS, then copy files from C: to D:. To do this, use the following procedure and other steps as instructed later in the upgrade process.

1. If you have not already done so, procure the `35c235d.reg` file.

   The `35c235d.reg` file is on the version 9.3.x.xxxx K2 software CD in the SNFS directory. It can also be obtained at `http://www.grassvalley.com/downloads`.

2. Copy `35c235d.reg` to the local K2 Media Server.
3. On the local K2 Media Server open Windows **Programs and Features** and uninstall SNFS.
4. Double-click `35c235d.reg` to run the file.

   The file resets registry entries in preparation for moving SNFS from C: to D:.

5. When prompted "Are you sure...", answer **Yes**.
6. When a message confirms the registry change, dismiss the message.
7. Restart the K2 Media Server.

Check all currently installed software on K2 Media Servers

- The device must be assigned in the SiteConfig system description and network connectivity must be present.
- SiteConfig must be able to log in to the device using the username/password credentials assigned to the device.
- The SiteConfig PC must not have a network drive mapped to an administrative share (such as C$) on a device on which you are checking software.

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.

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

   The Check Software dialog box appears. SiteConfig searches for software on the selected device or devices and gathers information. Progress is reported.

2. When the check is complete, close the Check Software dialog box.

An updated list of all currently installed software is displayed in the **Software Deployment | Devices | Installed Software** list view. If software is a SiteConfig managed software package, information is displayed in the Managed Package and Deployment Group columns.

Add software package to deployment group for K2 Media Servers

- The SiteConfig control point PC must have access to the software package file.
- The K2 Media Servers to which you are deploying software must be 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 for 64-bit systems	*GrassValleyK2Server_x64_9.3.x.xxxx.cab*
SNFS software for 64-bit systems	*SNFS_x64_4.2.2.b27249.cab*

You can add files for both 32 bit and 64 bit systems because when SiteConfig deploys software it automatically deploys the 32 bit or 64 bit software appropriate for the target device.

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 from SNFS 3.5.3 or lower on K2 Media Servers

Do not do this task if:

- SNFS is at version 4.2.x or higher. If this is the case, upgrade K2 and SNFS software at the same time, as instructed in the next task.

Do this task if:

- SNFS is at version 3.5.3 or lower. If this is the case, you must use these special instructions and upgrade first to SNFS 4.1, then upgrade to SNFS 4.2.

  NOTE: Upgrade to SNFS 4.1 only as a temporary step in the upgrade to SNFS 4.2.x. Do not operate the K2 system with SNFS 4.1 installed.

Verify the following before doing this task:

- The K2 Media Servers you are upgrading are in a deployment group.
- You have added managed software packages for SNFS 4.1.x and SNFS 4.2.x to the deployment group.
- If SNFS was on C:, you have uninstalled SNFS manually as instructed earlier in this upgrade procedure.
- A SiteConfig "Check Software" operation must be performed on the devices you are upgrading.
- ***NOTE: On a K2 system, if a SNFS version lower than 3.0 is installed, do not uninstall using SiteConfig. You must manually uninstall using a special batch file. Follow instructions in the release notes for your current version of K2 software.***

If you are upgrading multiple software components for which there is a required sequence, you must check and uncheck tasks and run multiple deployment sessions to control the sequence. For some

software components, SiteConfig aids you by enforcing dependencies. For each individual software component, SiteConfig enforces an uninstall of the current version of software before installing the upgrade version. SiteConfig provides uninstall deployment tasks and install deployment tasks to indicate the taskflow. SiteConfig can do the uninstall/install in a single deployment session.

1. In the **Software Deployment | Deployment Groups** tree view, select the K2 Media Server on which you are upgrading SNFS.

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

2. Uninstall SNFS 3.x and install SNFS 4.1.x as follows:
   a) For the SNFS 3.x software you are uninstalling, select the **Deploy** check box in the row for the uninstall task.
   b) For the SNFS 4.1.x software you are installing, select the **Deploy** check box in the row for the install task.
   c) Clear check boxes for all other deployment tasks.

Deploy	Managed Package	Action
✓	SNFS xxxxxx or SNFS x64 xxxxxx	Uninstall
✓	SNFS x64 4.1.3.b21767	Install

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

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

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

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

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

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

Next, you must install SNFS at a 4.2.x version or higher. Do not operate the K2 system with SNFS 4.1.x installed.

Upgrade software on K2 Media Servers

Do not do this task if:

- SNFS is at version 3.5.3 or lower. If this is the case, you must do the previous task and upgrade first to SNFS 4.1, then upgrade to SNFS 4.2.

Do this task if:

- SNFS is at a 4.1.x version. This is the case only if 4.1.x is installed as a temporary step in the upgrade to SNFS version 4.2.x or higher. Do not operate the K2 system with SNFS 4.1 installed.

  -OR-

- SNFS is at a 4.2.x version.

Verify the following before doing this task:

- The devices that you are upgrading must be in a deployment group.
- For the software you are upgrading, a newer version of that managed software package must be added to the deployment group.
- If SNFS was on C:, you have uninstalled SNFS manually as instructed earlier in this upgrade procedure.
- A SiteConfig "Check Software" operation must be performed on the devices you are upgrading.
- ***NOTE: On a K2 system, if a SNFS version lower than 3.0 is installed, do not uninstall using SiteConfig. You must manually uninstall using a special batch file. Follow instructions in the release notes for your current version of K2 software.***

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

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

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

2. For the software you are deploying, select the **Deploy** check box in the row for the uninstall task.

3. For the software you are installing, select the **Deploy** check box in the row for the install task.

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

Deploy	Managed Package	Action
✓	GrassValleyK2Server xxxxx.xxxx or GrassValleyK2Server_x64 xxxxx.xxxx	Uninstall
✓	GrassValleyK2Server_x64 9.3.x.xxxx	Install

   Also, when upgrading SNFS, configure deployment tasks to upgrade (uninstall/install) SNFS. Deploy the following tasks to K2 Media Servers with role of file system server:

Deploy	Managed Package	Action
✓	SNFS xxxxxx or SNFS x64 xxxxxx	Uninstall
✓	SNFS x64 4.2.2.b27249	Install

   If you previously uninstalled SNFS manually and then did a Check Software operation, only the install task is present.

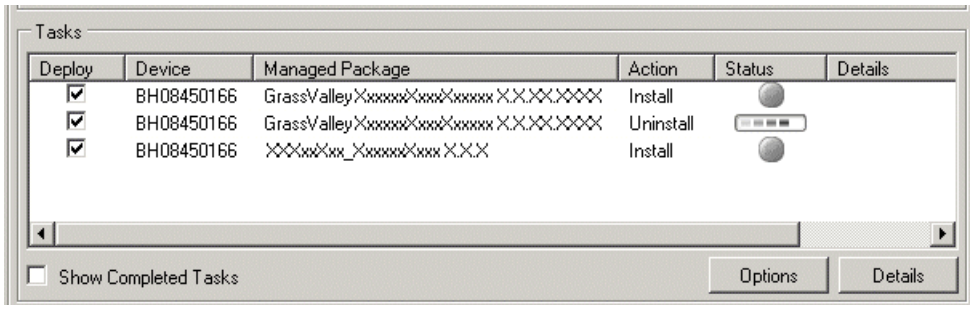
   You can deploy packages for both 32 bit and 64 bit systems because when SiteConfig deploys software it automatically deploys the 32 bit or 64 bit software appropriate for the target device. You must install SNFS as a separate cab file.

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

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

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

5. Click the **Start Deployment** button.



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

When upgrading both K2 and SNFS software, SiteConfig uninstalls both in the proper sequence.

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

   - For K2 software, when Details displays a **Restart required** link (but not "Visible dialog pending..."), click the link and when prompted "...are you sure...", click **Yes**.

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

   When upgrading SNFS software, this is also the restart required by the SNFS uninstall.

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

   If upgrading both K2 and SNFS software, SiteConfig uninstalls both in the proper sequence.

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

   - For K2 software, when Details displays a **Restart required** link (but not "Visible dialog pending..."), click the link and when prompted "...are you sure...", click **Yes**.

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

   If upgrading both K2 and SNFS software, SiteConfig uninstalls both in the proper sequence.

8. Monitor progress as indicated by both the Status and Details column. When finished, the Status column indicates complete.
9. If you previously uninstalled SNFS manually because SNFS was on C:, copy directories/files from C: to D:, overwriting files on D:, as follows.
   a) Copy the `C:\SNFS\config` directory to `D:\SNFS\config`.
   b) Copy the `C:\SNFS\data` directory to `D:\SNFS\data`. This directory can be large, so allow adequate time to complete the copy operation.
   c) A restart is required to put the change into effect. If you do a subsequent upgrade task that also requires a restart, that restart is sufficient. Otherwise restart now.
   d) After the entire K2 SAN upgrade process is complete, test media access. If successful, delete the `C:\SNFS` directory and its files on the K2 Media Server.

Upgrading the Discovery Agent

Do this task if SiteConfig does not prompt you to upgrade to the compatible version of the Discovery Agent when you deploy software.

Prerequisites for this task are as follows:

- Your devices are in one or more deployment groups
- A check software operation has been performed either on the device or the deployment group that you are upgrading

1. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.
2. Click **Add Package**
3. Click **Browse** in the add package dialog and browse to the Discovery Agent Setup folder under your SiteConfig install location on the SiteConfig PC.
4. Select the required *DiscoveryAgent_<version>.cab* file and click **Open**.

   SiteConfig generates deployment tasks to uninstall the existing version and installs the selected version and enables the **Start Deployment** button.
5. Check the uninstall and install deploy tasks for the Discovery Agent and click the **Start Deployment** button when you are ready to deploy.

   SiteConfig runs the deployment tasks.

Verify/upgrade switch firmware

Do not do this task if:

- Your HP ProCurve 29xx series switch already has the current required firmware version.

Do this task if:

- Your HP ProCurve 29xx series switch does not have the current required firmware version.

Refer to compatibility information earlier in these release notes for firmware version requirements.

1. Telnet to the switch and login with the administrator username and password.
2. At the switch console command (CLI) prompt, type the following, then press **Enter**:

   `menu`

   If prompted to save the current configuration, answer no (press the n key) to proceed.

   The main menu opens.
3. From the main menu, tab to **Command Line (CLI)** and press **Enter**. The command prompt appears.
4. Check the version of firmware on the switch. To do this, type the following, then press **Enter**:

   `show flash`

   Information is displayed similar to the following example:

```
HP_iSCSI_switch1# show flash
Image           Size(Bytes)   Date    Version
-----           ----------  --------  -------
Primary Image   : 6737518   07/25/08  T.13.23
Secondary Image : 5886358   10/26/06  T.11.12
Boot Rom Version: K.12.12
Current Boot    : Primary
```

5. Check the Primary Image Version and refer to compatibility information earlier in these release notes. If instructed to change the firmware on the switch, do so before continuing.

Upgrade RAID controller microcode

Do not do this task if:

- The K2 RAID controller and expansion chassis microcode is already at compatible versions, as listed in *Compatible K2 RAID components* on page 1090.
- The K2 RAID is a Level 2 or Level 3.

Do this task if:

- The K2 RAID controller and/or expansion chassis microcode is at a version that is not compatible.

The microcode files are copied on to the K2 Media Server when the K2 system software is installed.

1. Refer to the K2 RAID compatibility specifications earlier in these release notes for the version to which you must upgrade and for the file names for the microcode files.
2. Use Storage Utility to upgrade microcode.

   Refer to the *K2 SAN Installation and Service Manual* for procedures.

   The procedure for K2 10Gv2 RAID is different than the procedure for other types of K2 RAID. For the K2 10Gv2 RAID procedure, you can refer to a related topic in this document, as well as in the *K2 SAN Installation and Service Manual*.
3. On 100% completion, proceed as follows:
   - If the RAID controller chassis has redundant controllers, power cycle the RAID controller chassis, then restart the K2 Media Server.
   - If the RAID controller chassis does not have redundant controllers, no power cycle is required. The firmware download is complete.

Upgrade RAID disk drive firmware

Do not do this task if:

- The K2 RAID disk drive firmware is already at compatible versions, as listed in *Compatible K2 RAID disk drive firmware* on page 1092.
- The K2 RAID is Level 2 or Level 3 SAN.

Do this task if:

- The K2 RAID disk drive firmware is at a version that is not compatible.

Prerequisites:

- The RAID system is offline.
- Only the primary K2 Media Server is powered up.

- K2 software has been upgraded on the K2 Media Server. This is required because the firmware files are copied onto the K2 Media Server when the K2 software is installed.

1. Determine if disk drive firmware upgrades are required as follows:
   a) Select a disk drive icon in the Storage Utility tree view, then note the drive properties reported in the right-hand pane.
   b) Refer to the K2 RAID compatibility specifications earlier in these release notes for drive-type identifiers and firmware versions.
2. If an upgrade is required, continue with this procedure to upgrade disk drive firmware.

   Refer to the *K2 SAN Installation and Service Manual* for complete procedures.
3. In Storage Utility, right-click a controller in the tree view, then select **Advanced | Download Disk Firmware** in the context menu.

   NOTE: You can download firmware to a single disk by right-clicking a disk icon in the tree view.

   The Open File dialog box opens.
4. In the Open File dialog box, browse to the desired firmware file for your disks, select the file, and click **OK**.

   As instructed by a message that appears, watch the lights on the drives. For each drive, one at a time, the lights flash as firmware loads. Wait until the lights on all the drives on which you are downloading firmware have completed their flashing pattern. This can take several minutes.

   The Progress Report window appears showing the disk firmware download task and the percentage complete.
5. When finished, restart the K2 Media Server.

Reset Capture Services

Do not do this task if:

- You do not use any of the K2 Capture Services.

Do this task if:

- You are using one or more K2 Capture Services, such HotBin, XML Import, Export, P2, etc.

Do this task on the K2 system running your K2 Capture Service, which is the K2 system that receives the media to be imported into K2 storage. This can be a K2 Solo Media Server, a stand-alone K2 Summit Production Client, or the K2 Media Server with the role of primary FTP server on a K2 SAN.

When you configure a K2 Capture Service for the first time, the service is set to startup type Automatic. However, if you upgrade or otherwise re-install your K2 System Software, the service is re-set to startup type Manual. Therefore, you must re-configure the service after K2 System Software upgrade/ reinstall in order to set the startup type back to Automatic.

1. From the **Start** menu, access the **Programs** menu and select **Grass Valley | K2 Capture Services**.

   The K2 Capture Services utility dialog box is displayed.

2. Click **Apply**.

   For import capture services, the service checks the source directory for files. If files are present, the service moves them to the Archive sub-directory. It does not import the files into the destination bin on the K2 system.

Update Broadcom driver

This task applies to the following:

- Dell 610 platform Grass Valley servers with 9.x base image.

Do not do this task if:

- In Device manager under Network Adapters, the Broadcom driver version is 7.0.11.0.

Do this task if:

- In Device manager under Network Adapters, the Broadcom driver version is earlier than 7.0.11.0.

Before doing this task, procure the following file:

- *Network_Driver_2T17H_WN32_17.0.1_A00.EXE*

The file is available on the Grass Valley website software download page. It is in *StratusMiscellaneousSoftware2.0.zip*.

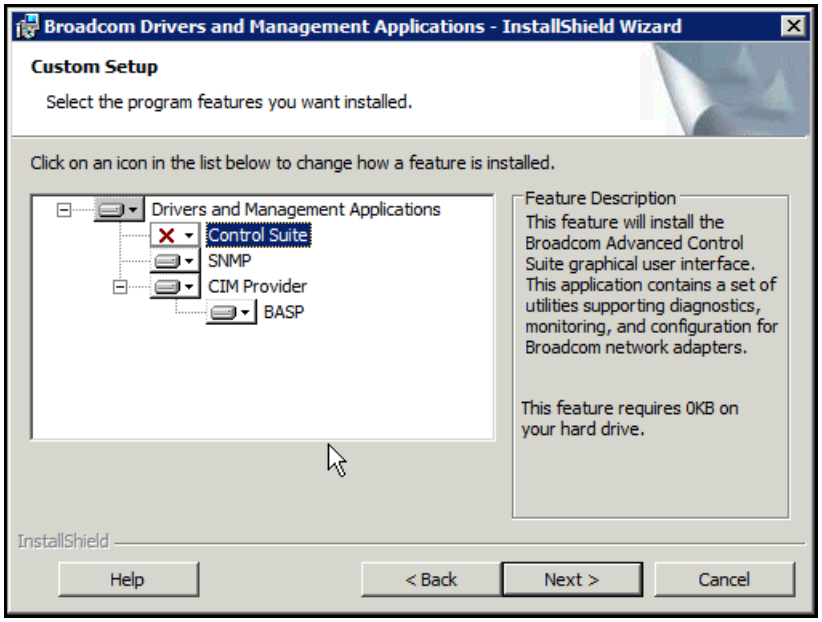
This task fixes potential network and performance problems.

1. Login to the server as Administrator.
2. Double-click *Network_Driver_2T17H_WN32_17.0.1_A00.EXE*.

   A Dell Update Package dialog box opens.
3. Click **Install**.

   The Broadcom Drivers and Application Management Applications wizard opens.

4. Work through the wizard, clicking **Next**, **I accept**, and **Next**.
   The Custom Setup page opens.



5. For each of the following nodes, click the drop-down list and select **This Feature, and all sub-features, will be installed on the local hard drive**:
   - **SNMP**
   - **CIM Provider**

   NOTE: Do not install Control Suite.
6. Click **Next** and **Install**.
7. If prompted to enable System TCP Chimney Offload, click **Yes**.
8. Click **Finish** to complete the wizard.
   The Dell Update Package dialog box appears.
9. Click **OK**.
10. Restart the server to put changes into effect.

Next, configure fsnameservers.cfg files. This is required when updating the Broadcom driver.

Configure fsnameservers on servers-class devices

This task applies to SAN systems with one or more SNFS servers that have had their Broadcom driver updated to version 7.0.11.0. On those SAN systems, all devices with a `v:` drive to the SAN's

storage (all SNFS servers and SNFS clients) must have their `fsnameservers` file configured. This includes the following type of SAN systems:

- An online or production K2 SAN — If the SAN's SNFS server, which is the K2 Media Server with role of media file system server (FSM), has had its Broadcom driver updated to version 7.0.11.0, then this task applies to the following server-class devices on that SAN:
  - The one K2 Media Server (if non-redundant) or two K2 Media Servers (if redundant). This device is the SAN's SNFS server.
  - If a GV STRATUS system, the GV STRATUS Proxy Encoder. This device is an SNFS client on the SAN.
  - If an A1 GV STRATUS system, the GV STRATUS Proxy Server. This device is an SNFS client on the SAN.
  - Any other SAN-attached server-class devices, such as NH FTP servers. This device is an SNFS client on the SAN.
- A nearline K2 SAN — If the SAN's SNFS server, which is the K2 Media Server with role of media file system server, has had its Broadcom driver updated to version 7.0.11.0, then this task applies to the following server-class devices on that SAN:
  - The one K2 Media Server (if non-redundant) or two K2 Media Servers (if redundant). This device is the SAN's SNFS server.
  - Any other SAN-attached server-class devices, such as NH FTP servers. This device is an SNFS client on the SAN.
- A GV STRATUS Proxy Storage system — If the SAN's SNFS server, which is the Proxy Storage file system server, has had its Broadcom driver updated to version 7.0.11.0, this task applies to the following server-class device:
  - The Proxy Storage file system server. This device is the SAN's SNFS server.

The SAN must be in an offline mode before doing this task.

You must know your server's names and IP addresses.

1. On the SAN's SNFS server that has had its Broadcom driver updated, login to the server as Administrator.
2. In Notepad, open the following file:

   `D:\SNFS\config\fsnameservers`
3. In the file, identify the server name of the local server.

   If a redundant SAN, identify the server names of both of the redundant servers.
4. Edit the line of text and replace the server name with the server's IP address.

   If a redundant SAN, replace both server names with their IP addresses.

   Make sure you leave text lines intact. Do not alter the line returns, spaces, other elements of the text line.
5. Save the file.
6. Copy the `fsnameservers` file to an external location, such as a network share or a USB drive, that allows access by the other devices of the SAN.
7. Restart the server.

8. If redundant SNFS servers, do the following on the other redundant server:
   a) Copy (overwrite) the `fsnameservers` file onto the device.
      On SNFS servers, the file's location is `D:\SNFS\config\fsnameservers`.
   b) Restart the device.
9. On other server-class devices that are SNFS clients, do the following:
   a) Copy (overwrite) the `fsnameservers` file onto the device.
      On SNFS clients, the file's location is `C:\SNFS\config\fsnameservers`.
   b) Restart the device.

You must also configure fsnameservers on all remaining SNFS clients on the SAN. Refer to the related topic later in the upgrade process.

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.

Upgrade K2 client

Work through the following topics sequentially to upgrade K2 clients.

NOTE: These upgrade instructions assume that on your SAN-attached K2 Summit systems, the current K2 software is at version 9.x or higher. If the current K2 software is at a version lower than 9.x, you must upgrade K2 Summit systems using the appropriate Grass Valley Field Kit, which includes a disk image and hardware. Once upgraded via the field kit to an 9.x version, you can then use these upgrade instructions.

Prepare for K2 system upgrade

Before upgrading K2 systems, do the following:

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

Upgrade .NET

Do not do this task if:

- The computer has .NET 4.5 installed

Do this task if:

- The computer does not have .NET 4.5 installed

This task applies to the following:

- K2 Summit/Solo systems
- All types/roles of K2 Media Servers
- All types/roles of GV STRATUS servers.
- Client PCs hosting one or more of the following:
  - GV STRATUS
  - GV STRATUS Control Panel
  - EDIUS XS
  - EDIUS Elite

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

Check all currently installed software on SAN K2 clients

- The device must be assigned in the SiteConfig system description and network connectivity must be present.
- SiteConfig must be able to log in to the device using the username/password credentials assigned to the device.
- The SiteConfig PC must not have a network drive mapped to an administrative share (such as C$) on a device on which you are checking software.

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.

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

   The Check Software dialog box appears. SiteConfig searches for software on the selected device or devices and gathers information. Progress is reported.
2. When the check is complete, close the Check Software dialog box.

An updated list of all currently installed software is displayed in the **Software Deployment | Devices | Installed Software** list view. If software is a SiteConfig managed software package, information is displayed in the Managed Package and Deployment Group columns.

Add software package to deployment group for SAN K2 clients

- The SiteConfig control point PC must have access to the software package file.
- The SAN K2 clients to which you are deploying software must be 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	*GrassValleyK2SummitSANClient_9.3.x.xxxx.cab*
SNFS software	*SNFS_Summit_4.2.2.b27249.cab*

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

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

   SiteConfig adds the package to the deployment group.

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

Upgrade software on SAN K2 clients

- The devices that you are upgrading must be in a deployment group.
- For the software you are upgrading, a newer version of that managed software package must be added to the deployment group.
- A SiteConfig "Check Software" operation must be performed on the devices you are upgrading.

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

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

   The corresponding software deployment tasks are displayed in the Tasks list view.
2. For the software you are deploying, select the **Deploy** check box in the row for the uninstall task.

3. For the software you are installing, select the **Deploy** check box in the row for the install task.

   For upgrading SAN K2 clients to this release, configure **Deploy** check boxes as follows:

Deploy	Managed Package	Action
✓	GrassValleyK2SummitSANClient xxxx.xxxx	Uninstall
✓	GrassValleyK2SummitSANClient 9.3.x.xxxx	Install

   Also, when upgrading SNFS, configure deployment tasks to upgrade (uninstall/install) SNFS. Deploy the following tasks at the same time:

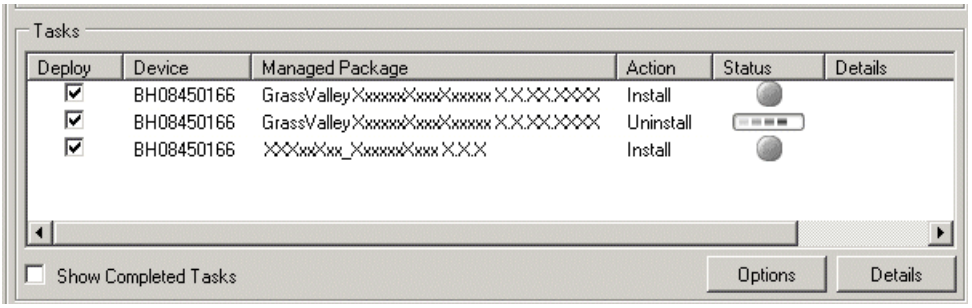
Deploy	Managed Package	Action
✓	SNFS Summit xxxxxx	Uninstall
✓	SNFS Summit 4.2.2.b27249	Install

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

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

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

5. Click the **Start Deployment** button.



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

   When upgrading both K2 and SNFS software, SiteConfig uninstalls both in the proper sequence.

6. When the Status or Details columns indicate next steps, identify the software in the row, then do one of the following:
   - For SNFS software, when Details displays a **Restart required** link, click the link and when prompted "...are you sure...", click **Yes**. After this restart, continue with other restarts as indicated.
   - For K2 software, if the version from which you are upgrading is 8.0 or higher, when Details displays a **Restart required** link, click the link and when prompted "...are you sure...", click **Yes**.
7. Monitor progress as indicated by both the Status and Details column. When finished, the Status column indicates complete.

Upgrading the Discovery Agent

Do this task if SiteConfig does not prompt you to upgrade to the compatible version of the Discovery Agent when you deploy software.

Prerequisites for this task are as follows:

- Your devices are in one or more deployment groups
- A check software operation has been performed either on the device or the deployment group that you are upgrading

1. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.
2. Click **Add Package**
3. Click **Browse** in the add package dialog and browse to the Discovery Agent Setup folder under your SiteConfig install location on the SiteConfig PC.
4. Select the required *DiscoveryAgent_<version>.cab* file and click **Open**.

   SiteConfig generates deployment tasks to uninstall the existing version and installs the selected version and enables the **Start Deployment** button.
5. Check the uninstall and install deploy tasks for the Discovery Agent and click the **Start Deployment** button when you are ready to deploy.

   SiteConfig runs the deployment tasks.

Enhance network bandwidth

On K2 Summit/Solo systems with K2 system software 9.x, the on-board network adapters have a performance limitation that causes them to function at half the expected bandwidth. On most systems, there are no symptoms related to this limitation, as network traffic is below the limitation. Systems using ShareFlex or having other requirements for high network bandwidth might be impacted to some degree. Symptoms include general network bandwidth restrictions, slow iSCSI I/O performance, slower than expected FTP traffic, and other slowness not caused by other factors.

Grass Valley requires that you remove the limitation and enhance the network performance. Once the limitation is removed, the change persists throughout normal software upgrades. However, if you reimage the K2 Summit/Solo system you must check and reapply the change if necessary.

To remove the limitation, disable "Large Send Offloads" on the network adapters and disable "CPU Power Technology" in the BIOS.

Refer to Grass Valley Knowledge Base Article *#000011688* for more information.

Disable Large Send Offloads

1. From the Windows operating **Start** menu, open **Control Panel**.
2. In **Control Panel**, open **Network and Sharing Center**.
3. In **Network and Sharing Center**, select **Change adapter settings**.
   Network Connections opens and displays network adapters, including the following:
   - Control Connection #1
   - Control Connection #2
   - Media Connection #1
   - Media Connection #2
4. For each Control Connection and each Media Connection, do the following:
   a) Right-click the connection and select **Properties**.
      The **Connection Properties** dialog box opens.
   b) In the **Connection Properties** dialog box, click **Configure**.
      The **Adapter Properties** dialog box opens.
   c) In the **Adapter Properties** dialog box, click the **Advanced** tab.
   d) On the Advanced tab, in the Settings list select **Large Send Offload v2 (IPv4)** and then in the Value drop-down list select **Disabled**.
   e) Click **OK** to save settings and close.
   f) Repeat these steps for each Control Connection and each Media Connection.

Next, disable CPU power technology.

Disable CPU Power Technology

1. Restart the K2 Summit/Solo system.
2. During the BIOS startup screen, press **F2** repeatedly until `Entering Setup...` appears.
   The BIOS screen opens.
3. On the BIOS screen, use arrow keys and select the **Advanced** tab.
4. On the Advanced tab select **CPU Core Configuration** and then press **Enter**.
   The CPU Core Configuration screen opens.
5. On the CPU Core Configuration screen, select **Power Technology** and then press **Enter**.
   A **Power Technology** dialog box opens.
6. In the **Power Technology** dialog box select **Disable** and then press **Enter**.
7. Press **F4** to save and exit.
   A **Save & Exit Setup** dialog box opens.
8. In the **Save & Exit Setup** dialog box, select **Yes** and then press **Enter**.
9. The K2 Summit/Solo system restarts.

Next, install the SiteConfig Discovery Agent.

Configure fsnameservers on SNFS clients

This task applies to SAN systems with one or more SNFS servers that have had their Broadcom driver updated to version 7.0.11.0. On those SAN systems, all devices with a `V:` drive to the SAN's storage (all SNFS servers and SNFS clients) must have their `fsnameservers` file configured. This includes the following type of SAN systems:

- An online or production K2 SAN — If the SAN's SNFS server, which is the K2 Media Server with role of media file system server (FSM), has had its Broadcom driver updated to version 7.0.11.0, then this task applies to the following SNFS clients of that SAN:
  - All K2 Summit systems attached to the K2 SAN
  - Any GV STRATUS high resolutions client PCs attached to the K2 SAN
  - Any Macintosh (K2 FCP Connect) clients attached to the K2 SAN
  - Any other SNFS client devices attached to the K2 SAN

The SNFS clients must be in an offline mode before doing this task.

You must know your SNFS client's names and IP addresses.

You must have access to the `fsnameservers` file that you copied from the SAN's SNFS server.

1. On the SNFS client, login to as Administrator.
2. Copy (overwrite) the `fsnameservers` file onto the device.
   On SNFS clients, the file's location is `C:\SNFS\config\fsnameservers`.
3. Restart the SNFS client.
4. Repeat these steps on all the SAN's SNFS client devices.

Upgrade MPIO

Do not do this task if:

- In Device Manager under System Devices, the **GV Multi-Path Device Specific Module** properties list the driver version as 2.3.0.0 or higher.
- The K2 client has internal storage.
- The K2 client has shared storage on a non-redundant K2 SAN.
- The K2 client has a 2 Gb/s GVG SCSI Fibre Channel card with shared (SAN) storage or direct-connect storage.
- The K2 client has a dual port 4 Gb/s LSI Fibre Channel card with direct-connect storage, but only one port is connected to a RAID controller.

Do this task if:

- The K2 client has iSCSI-connected shared storage on a redundant K2 SAN.
- The K2 client has a dual port 4 Gb/s LSI Fibre Channel card with shared storage on a redundant K2 SAN.

- The K2 client has a dual port 4 Gb/s LSI Fibre Channel card with direct-connect storage with each port connected to a different RAID controller.

The installation files for the Multi-Path I/O software are copied on to the K2 client when the K2 software is installed.

1. On the K2 client, click **Start | Run**, type cmd and press **Enter**.

   The MS-DOS command prompt window opens.

2. From the command prompt, navigate to the *C:\profile\mpio* directory.
3. Type the following at the command prompt:

   ```
   gdsminstall64.exe -i c:\profile\mpio gdsm.inf Root\GDSM
   ```

4. Press **Enter**. The software is installed. The command prompt window reports the following:

   ```
   Pre-Installing the Multi-Path Adapter Filter...
   Success

   Installing the Multi-Path Bus Driver...
   Success

   Installing the Device Specific Module...
   Success

   Installing the Multi-Path Device Driver...
   Success

   Restarting all SCSI adapters...
   Success (but need a reboot)
   ```

5. Restart the K2 Media Client.
6. After restart, to verify that the software is installed, on the Windows desktop click **Start | Control Panel | System**.
7. In the left pane select **Device Manager**.
8. Expand the **System devices** node, right-click on **GVG Multi-Path Device Specific Module** and select **Properties**.
9. Click on the **Driver** tab, and verify that the latest driver version is installed.

Upgrade GV STRATUS and GV STRATUS Rundown systems

- K2 systems must be upgraded to the compatible version of K2 system software.
- All GV STRATUS and GV STRATUS Rundown devices must be offline (all media access stopped) or shut down.

  Upgrade your GV STRATUS and GV STRATUS Rundown systems to the compatible versions of software. This includes the GV STRATUS Proxy Storage system, if present in your system. Refer to each product's documentation 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 distibution 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 tasks similar to those you followed for upgrading software so that as you take systems offline you manage redundancy, servers, and clients, as appropriate for your system.

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

Upgrading stand-alone K2 systems with SiteConfig

This section contains the tasks for using SiteConfig to upgrade stand-alone K2 systems to this release of K2 software.

Work through the tasks sequentially to complete the upgrade.

NOTE: These upgrade instructions assume that on your K2 Summit/Solo system, the current K2 software is at version 9.x or higher. If on a K2 Summit system the current software is at a version lower than 9.x, you must upgrade it using a Grass Valley Field Kit, which includes a disk image and hardware. K2 Solo systems are available with 9.x software only as shipped from Grass Valley.

About upgrading stand-alone K2 systems with SiteConfig

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

- K2 Summit Production Client internal storage
- K2 Summit Production Client direct-connect storage
- K2 Solo Media Server

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

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 system and use keyboard, monitor, and mouse to upgrade software.

You can find instructions for a manual upgrade without SiteConfig at *Upgrading stand-alone K2 systems with SiteConfig* on page 1127 in these release notes.

If this is the first time using SiteConfig for software upgrade, follow instructions in *K2 System Guide* rather than instruction in these release notes. You must first have SiteConfig set up for system management and software deployment of the stand-alone K2. Also refer to the *SiteConfig User Manual* or *SiteConfig Help Topics*. Then, after you have completed this initial SiteConfig set up, you can follow the instructions in this section to upgrade software.

NOTE: If this is the first time using SiteConfig for software upgrade do not follow instructions in these release notes alone.

The following installation tasks provide information specifically for the upgrade to this version of 9.3 software. Read the information in these sections carefully before attempting any upgrade to software on a stand-alone K2 system.

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 Grass Valley 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 system upgrade

Before upgrading K2 systems, do the following:

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

Upgrade .NET

Do not do this task if:

- The computer has .NET 4.5 installed

Do this task if:

- The computer does not have .NET 4.5 installed

This task applies to the following:

- K2 Summit/Solo systems
- All types/roles of K2 Media Servers
- All types/roles of GV STRATUS servers.
- Client PCs hosting one or more of the following:
  - GV STRATUS
  - GV STRATUS Control Panel
  - EDIUS XS
  - EDIUS Elite

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

Prepare SiteConfig for software deployment to stand-alone K2 systems

Do the following to prepare SiteConfig for the software upgrade.

1. Make the following files accessible to the SiteConfig control point PC:
   - K2 Summit Client Standalone software installation (`*.cab`) file.
   - Summit SNFS software installation (`*.cab`) file.
2. If a newer version of SiteConfig is available for upgrade and you have not yet upgraded SiteConfig, do the following:
   a) From Windows **Programs and Features**, uninstall the current version of SiteConfig from the control point PC.
   b) Install the new version of SiteConfig on the control point PC.
3. If not already present in the SiteConfig system description, configure deployment groups as follows:
   - A deployment group that contains your stand-alone K2 systems
   - A deployment group that contains your control point PC

Check all currently installed software on stand-alone K2 systems

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

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

Do the following steps on the stand-alone K2 systems that you are upgrading.

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

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

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

   The Check Software dialog box appears. SiteConfig searches for software on the selected device or devices and gathers information. Progress is reported.

2. When the check is complete, close the Check Software dialog box.

An updated list of all currently installed software is displayed in the **Software Deployment | Devices | Installed Software** list view. If software is a SiteConfig managed software package, information is displayed in the Managed Package and Deployment Group columns.

Add software package to deployment group for stand-alone K2 systems

- The SiteConfig control point PC must have access to the software package file.
- The stand-alone K2 systems to which you are deploying software must be 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 systems. For this release of K2 software, identify and add software installation files as follows:

Software	File name
K2 Client software	*GrassValleyK2SummitStandalone_9.3.x.xxxx .cab*
SNFS software	*SNFS_Summit_4.2.2.b27249.cab*

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

   The Add Package(s) dialog box opens.

3. Do one of the following to select the software package:

   - Select from the list of packages then click **OK**.
   - Click **Browse**, browse to and select the package, then click **Open**.

4. If one or more EULAs are displayed, accept them to proceed. If you do not accept a EULA, the associated software is not assigned to the deployment group.

   SiteConfig adds the package to the deployment group.

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

Upgrade software on stand-alone K2 systems

- The devices that you are upgrading must be in a deployment group.
- For the software you are upgrading, a newer version of that managed software package must be added to the deployment group.
- A SiteConfig "Check Software" operation must be performed on the devices you are upgrading.

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

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

   The corresponding software deployment tasks are displayed in the Tasks list view.
2. For the software you are deploying, select the **Deploy** check box in the row for the uninstall task.
3. For the software you are installing, select the **Deploy** check box in the row for the install task.

   For upgrading stand-alone K2 systems to this release, configure **Deploy** check boxes as follows:

Deploy	Managed Package	Action
✓	GrassValleyK2SummitStandalone xxxx.xxxx	Uninstall
✓	GrassValleyK2SummitStandalone 9.3.x.xxxx	Install

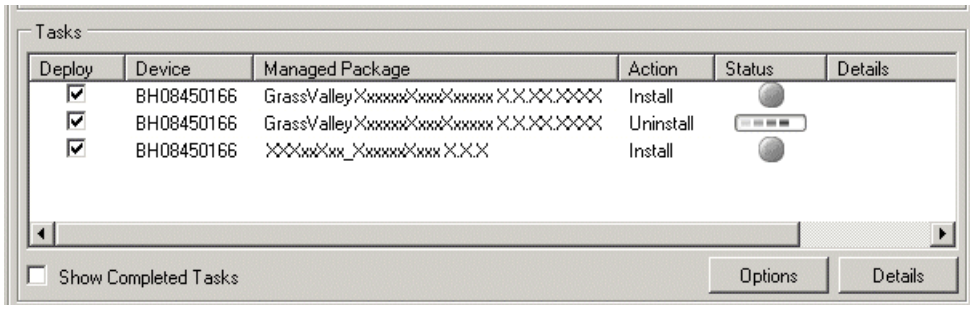
   Also, when upgrading SNFS, configure deployment tasks to upgrade (uninstall/install) SNFS. Deploy the following tasks at the same time:

Deploy	Managed Package	Action
✓	SNFS Summit xxxxxx	Uninstall
✓	SNFS Summit 4.2.2.b27249	Install

   NOTE: If there are dependencies, SiteConfig can enforce that some tasks be deployed together.
4. Check the area next to the Start Deployment button for a message.

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

5. Click the **Start Deployment** button.



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

When upgrading both K2 and SNFS software, SiteConfig uninstalls both in the proper sequence.

6. When the Status or Details columns indicate next steps, identify the software in the row, then do one of the following:
   - For SNFS software, when Details displays a **Restart required** link, click the link and when prompted "...are you sure...", click **Yes**. After this restart, continue with other restarts as indicated.
   - For K2 software, if the version from which you are upgrading is 8.0 or higher, when Details displays a **Restart required** link, click the link and when prompted "...are you sure...", click **Yes**.
7. Monitor progress as indicated by both the Status and Details column. When finished, the Status column indicates complete.

Upgrading the Discovery Agent

Do this task if SiteConfig does not prompt you to upgrade to the compatible version of the Discovery Agent when you deploy software.

Prerequisites for this task are as follows:

- Your devices are in one or more deployment groups
- A check software operation has been performed either on the device or the deployment group that you are upgrading

1. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.
2. Click **Add Package**
3. Click **Browse** in the add package dialog and browse to the Discovery Agent Setup folder under your SiteConfig install location on the SiteConfig PC.
4. Select the required *DiscoveryAgent_<version>.cab* file and click **Open**.

   SiteConfig generates deployment tasks to uninstall the existing version and installs the selected version and enables the **Start Deployment** button.

5. Check the uninstall and install deploy tasks for the Discovery Agent and click the **Start Deployment** button when you are ready to deploy.

   SiteConfig runs the deployment tasks.

Enhance network bandwidth

On K2 Summit/Solo systems with K2 system software 9.x, the on-board network adapters have a performance limitation that causes them to function at half the expected bandwidth. On most systems, there are no symptoms related to this limitation, as network traffic is below the limitation. Systems using ShareFlex or having other requirements for high network bandwidth might be impacted to some degree. Symptoms include general network bandwidth restrictions, slow iSCSI I/O performance, slower than expected FTP traffic, and other slowness not caused by other factors.

Grass Valley requires that you remove the limitation and enhance the network performance. Once the limitation is removed, the change persists throughout normal software upgrades. However, if you reimage the K2 Summit/Solo system you must check and reapply the change if necessary.

To remove the limitation, disable "Large Send Offloads" on the network adapters and disable "CPU Power Technology" in the BIOS.

Refer to Grass Valley Knowledge Base Article *#000011688* for more information.

Disable Large Send Offloads

1. From the Windows operating **Start** menu, open **Control Panel**.
2. In **Control Panel**, open **Network and Sharing Center**.
3. In **Network and Sharing Center**, select **Change adapter settings**.

   Network Connections opens and displays network adapters, including the following:

   - Control Connection #1
   - Control Connection #2
   - Media Connection #1
   - Media Connection #2

4. For each Control Connection and each Media Connection, do the following:
   a) Right-click the connection and select **Properties**.

      The **Connection Properties** dialog box opens.

   b) In the **Connection Properties** dialog box, click **Configure**.

      The **Adapter Properties** dialog box opens.

   c) In the **Adapter Properties** dialog box, click the **Advanced** tab.
   d) On the Advanced tab, in the Settings list select **Large Send Offload v2 (IPv4)** and then in the Value drop-down list select **Disabled**.
   e) Click **OK** to save settings and close.
   f) Repeat these steps for each Control Connection and each Media Connection.

Next, disable CPU power technology.

Disable CPU Power Technology

1. Restart the K2 Summit/Solo system.
2. During the BIOS startup screen, press **F2** repeatedly until `Entering Setup...` appears.
   The BIOS screen opens.
3. On the BIOS screen, use arrow keys and select the **Advanced** tab.
4. On the Advanced tab select **CPU Core Configuration** and then press **Enter**.
   The CPU Core Configuration screen opens.
5. On the CPU Core Configuration screen, select **Power Technology** and then press **Enter**.
   A **Power Technology** dialog box opens.
6. In the **Power Technology** dialog box select **Disable** and then press **Enter**.
7. Press **F4** to save and exit.
   A **Save & Exit Setup** dialog box opens.
8. In the **Save & Exit Setup** dialog box, select **Yes** and then press **Enter**.
9. The K2 Summit/Solo system restarts.

Upgrade RAID Controller microcode on stand-alone K2 system

Do not do this task if one of the following is true:

- A K2 Solo Media Server
- A K2 Summit Production Client with internal storage and with RAID controller microcode already upgraded to a compatible version, as listed in compatibility specifications.
- A K2 Summit Production Client with direct-connect storage and with RAID controller and/or expansion chassis microcode already at compatible versions, as listed in compatibility specifications.

Do this task if:

- A K2 Summit Production Client with internal storage and with RAID controller microcode that you need to upgrade, as listed in compatibility specifications.
- A K2 Summit Production Client with direct-connect storage and with RAID controller and/or expansion chassis microcode that you need to upgrade, as listed in compatibility specifications.

For internal storage K2 Summit/Solo systems, find compatibility specifications at *Compatible K2 Summit/Solo components* on page 1083. For a K2 Summit Production Client with direct-connect storage, find compatibility specifications at *Compatible K2 RAID components* on page 1090.

1. Open AppCenter Workstation, either on the local K2 system or on the control point PC and logon.

   Make sure you logon to AppCenter with appropriate privileges, as this logon is passed to Storage Utility. Administrator-level permission is necessary for most Storage Utility operations. If you log in with user-level permissions, the Storage Utility menu item is disabled.

2. If you are running AppCenter from a control point PC and you have channels from multiple K2 systems in your channel suite, select a channel from the stand-alone K2 system whose storage you intend to configure with Storage Utility. This is important as Storage Utility automatically connects to the K2 system that hosts the currently selected channel.

   NOTE: Make sure you are connecting to a stand-alone K2 system. You should never connect Storage Utility directly to a K2 system that uses shared (SAN) storage.

3. From the AppCenter **System** menu, select **Storage Utility**.

   Storage Utility opens.

4. If you are connecting from a control point PC, you should verify that you are connected to the correct K2 system. To verify this, use the Identify feature to flash the disks on the K2 system.
5. Select the controller in the Storage Utility tree view, then in the properties reported in the right-hand pane, note the controller microcode version. Proceed if you need to upgrade the controller microcode.
6. Right-click the controller in the tree view and do one of the following:

   - For internal storage, select **Load Controller Microcode** in the context menu.
   - For direct-connect storage, select **Advanced | Load Controller Microcode** in the context menu.

7. If online, messages appear "…offline mode now?" and "…continue?". Click **Yes** to put the K2 system in offline mode.

   AppCenter channels go offline. The Open File dialog box opens.

8. In the Open File dialog box, browse to and select the microcode file for the required version. Refer to the following for locations and filenames:

   - For internal-storage, refer to *Compatible K2 Summit/Solo components* on page 1083.
   - For direct-connect storage, refer to *Compatible K2 RAID components* on page 1090.

9. Click **OK.**

   The Progress Report window appears showing the microcode download task and the percentage completion.

10. If direct-connect storage and upgrading expansion chassis microcode, do the following:
    a) Right-click the controller in the tree view, then select **Advanced | Load Disk Enclosure Microcode** in the context menu.
    b) In the Open File dialog box, browse to the directory and file as listed in K2 RAID compatibility specifications earlier in these release notes.
    c) Click **OK.**

       The Progress Report window appears showing the microcode download task and the percentage completion.

11. When finished, exit Storage Utility.
12. If direct-connect storage, on 100% completion, proceed as follows:

    - If the RAID controller chassis has redundant controllers, no power cycle is required. The microcode download is complete.
    - If the RAID controller chassis does not have redundant controllers, power cycle the RAID controller chassis.

13. Put AppCenter channels back online.
14. Restart.

Upgrade disk drive firmware on stand-alone K2 system

Do not do this task if:

- A K2 system with disk drive firmware already at a compatible version, as listed in compatibility specifications.

Do this task if:

- A K2 system with disk drive firmware that you need to upgrade, as listed in compatibility specifications.

For internal storage K2 Summit/Solo systems, find compatibility specifications at *Compatible K2 Summit/Solo components* on page 1083. For a K2 Summit Production Client with direct-connect storage, find compatibility specifications at *Compatible K2 RAID components* on page 1090.

NOTE: The disk drives are upgraded one at a time which can take as long as 2 minutes per drive. Take this into consideration when scheduling the upgrade.

1. Open AppCenter Workstation, either on the local K2 system or on the control point PC and logon.

   Make sure you logon to AppCenter with appropriate privileges, as this logon is passed to Storage Utility. Administrator-level permission is necessary for most Storage Utility operations. If you log in with user-level permissions, the Storage Utility menu item is disabled.

2. If you are running AppCenter from a control point PC and you have channels from multiple K2 systems in your channel suite, select a channel from the stand-alone K2 system whose storage you intend to configure with Storage Utility. This is important as Storage Utility automatically connects to the K2 system that hosts the currently selected channel.

   NOTE: Make sure you are connecting to a stand-alone K2 system. You should never connect Storage Utility directly to a K2 system that uses shared (SAN) storage.

3. From the AppCenter **System** menu, select **Storage Utility**.

   Storage Utility opens.

4. If you are connecting from a control point PC, you should verify that you are connected to the correct K2 system. To verify this, use the Identify feature to flash the disks on the K2 system.
5. Select a disk drive icon in the Storage Utility tree view, then note the firmware version in drive properties reported in the right-hand pane. Proceed if you need to download disk drive firmware.
6. Right-click a disk in the tree view, then select **Advanced | Download Disk Firmware** in the context menu.
7. If online, messages appear "…offline mode now?" and "…continue?". Click **Yes** to put the K2 system in offline mode.

   AppCenter channels go offline. The Open File dialog box opens.

8. In the Open File dialog box browse to the directory and file as listed in compatibility tables earlier in these release notes. You must select the correct file for the device, storage type, and drive size/type.

9. Click **OK**.

   For internal drives, watch the lights on the drive to which you are downloading firmware. The lights flash as firmware loads. Wait until the lights have completed their flashing pattern. This can take several minutes.

   The Progress Report window appears showing the disk firmware download task and the percentage completion.

10. Repeat this procedure on each drive.
11. When finished, exit Storage Utility.
12. Put AppCenter channels back online.
13. Restart.

Reset Capture Services

Do not do this task if:

- You do not use any of the K2 Capture Services.

Do this task if:

- You are using one or more K2 Capture Services, such HotBin, XML Import, Export, P2, etc.

Do this task on the K2 system running your K2 Capture Service, which is the K2 system that receives the media to be imported into K2 storage. This can be a K2 Solo Media Server, a stand-alone K2 Summit Production Client, or the K2 Media Server with the role of primary FTP server on a K2 SAN.

When you configure a K2 Capture Service for the first time, the service is set to startup type Automatic. However, if you upgrade or otherwise re-install your K2 System Software, the service is re-set to startup type Manual. Therefore, you must re-configure the service after K2 System Software upgrade/ reinstall in order to set the startup type back to Automatic.

1. From the **Start** menu, access the **Programs** menu and select **Grass Valley | K2 Capture Services**.

   The K2 Capture Services utility dialog box is displayed.

2. Click **Apply**.

   For import capture services, the service checks the source directory for files. If files are present, the service moves them to the Archive sub-directory. It does not import the files into the destination bin on the K2 system.

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 tasks similar to those you followed for upgrading software so that as you take systems offline you manage redundancy, servers, and clients, as appropriate for your system.

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

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 9.3.x.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.

   NOTE: If an "Unable to copy ... to target" error appears for a device that has Grass Valley Embedded Security, put Embedded Security in Update mode.

3. Configure and run deployment tasks to upgrade software.

Upgrading stand-alone K2 systems without SiteConfig

This section contains the tasks for upgrading stand-alone K2 systems to this release of K2 software.

With these instructions you go to each local K2 system 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 on your K2 Summit/Solo system, the current K2 software is at version 9.x or higher. If on a K2 Summit system the current software is at a version lower than 9.x, you must upgrade it using a Grass Valley Field Kit, which includes a disk image and hardware. K2 Solo systems are available with 9.x software only as shipped from Grass Valley.

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 Grass Valley 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 system upgrade

Before upgrading K2 systems, do the following:

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

Upgrade .NET

Do not do this task if:

- The computer has .NET 4.5 installed

Do this task if:

- The computer does not have .NET 4.5 installed

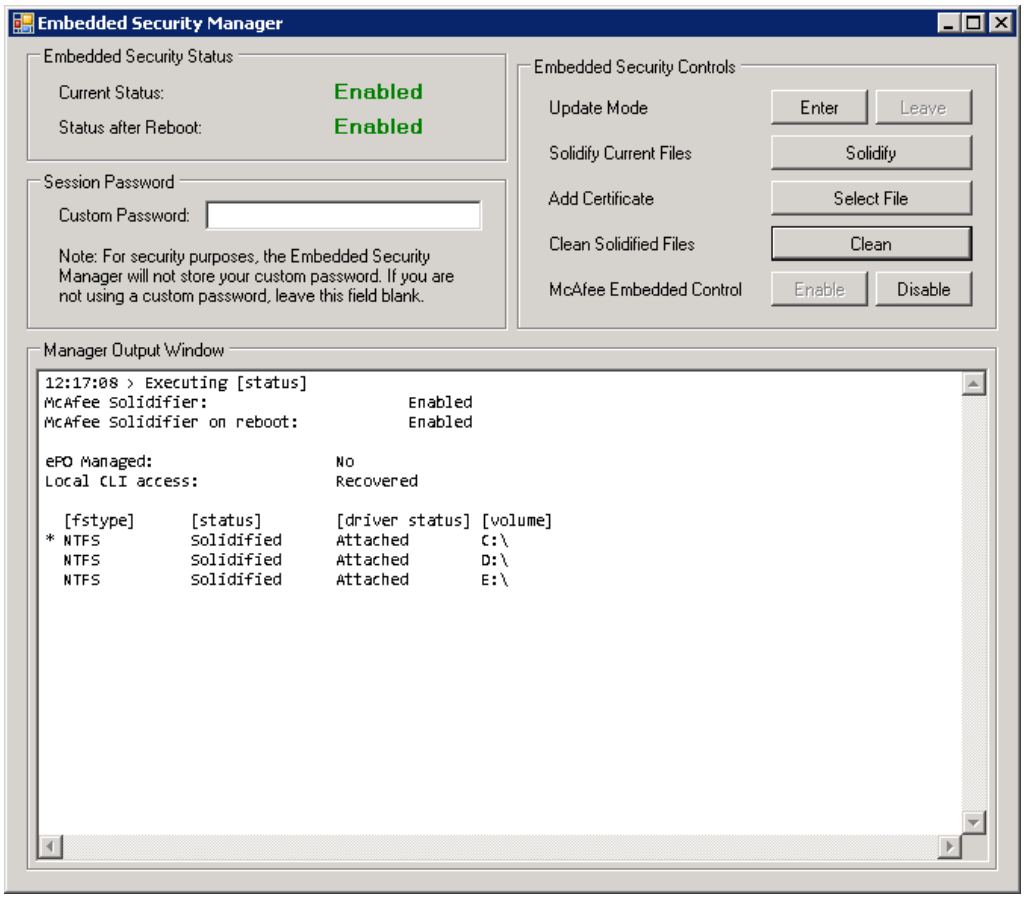
This task applies to the following:

- K2 Summit/Solo systems
- All types/roles of K2 Media Servers
- All types/roles of GV STRATUS servers.
- Client PCs hosting one or more of the following:
  - GV STRATUS
  - GV STRATUS Control Panel
  - EDIUS XS
  - EDIUS Elite

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

Enter Update mode

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



   Interpret Current Status as follows:

   - **Enabled**: Embedded Security is enabled but is not in Update mode.
   - **Update**: Embedded Security is enabled and is in Update mode, ready for software installation.

2. Under **Update**, manage the Update mode as follows:

   - Click **Enter** to put Embedded Security in Update mode.

   A restart is not required after you enter the Update mode.

Uninstall K2 software from stand-alone K2 system

Before doing this task, make sure Embedded Security is in Update mode.

1. Open the Windows **Programs and Features** control panel.
2. Select **GrassValleyK2Client**. and click **Uninstall**.
3. When prompted "Are you sure...?", click **Yes**.

4. Manage the required restart as follows:
   - Restart later, to combine this restart with those required by other tasks. This is appropriate when you have other tasks next that also require a restart, such as uninstalling SNFS software.

Uninstall SNFS from K2 client

Do not do this task if:

- The desired version of SNFS is already installed and the installation (including required restarts) is complete.

Do this task if:

- A SNFS version lower than 4.2.2.b27249 is currently installed

Before doing this task, make sure Embedded Security is in Update mode.

1. Make sure you are logged in with an administrator account.
2. Use the Windows **Programs and Features** control panel and uninstall SNFS.
3. Manage the required restart as follows:
   - Restart now.

Install SNFS on stand-alone K2 system

The computer must be restarted at least once since the previous version of SNFS software was uninstalled.

1. Access the installation files.
2. Locate and open the file for your system:

   Use the following installation file for a K2 Summit system.

File	Description
`gvSnfs422SetupSummit.bat`	For K2 Solo 3G system

   The command window appears. After a pause, messages confirm setup complete.
3. Press any key to proceed.
4. Restart the computer using the Windows operating system restart procedure.

Install K2 software

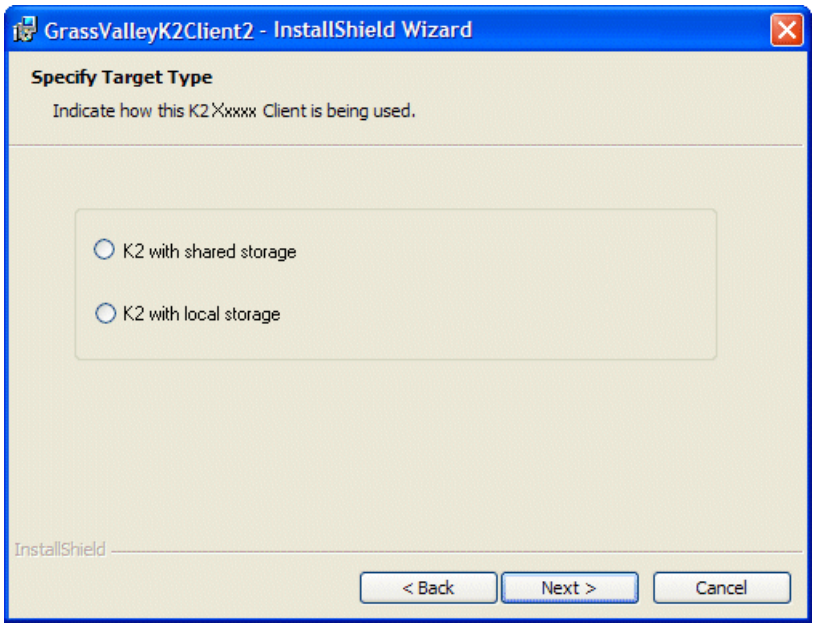
If you uninstalled the previous version of K2 software, you must restart the K2 client at least once before installing the new version of K2 software.

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. If installation files are on a connected external USB drive, copy the installation files to the local drive before proceeding.
3. Access the installation files.
4. Locate and open the following file:

   For K2 Summit Production Client or K2 Solo Media Server — `K2SummitClient.exe`
5. Follow the install wizard onscreen instructions, and work through each page.



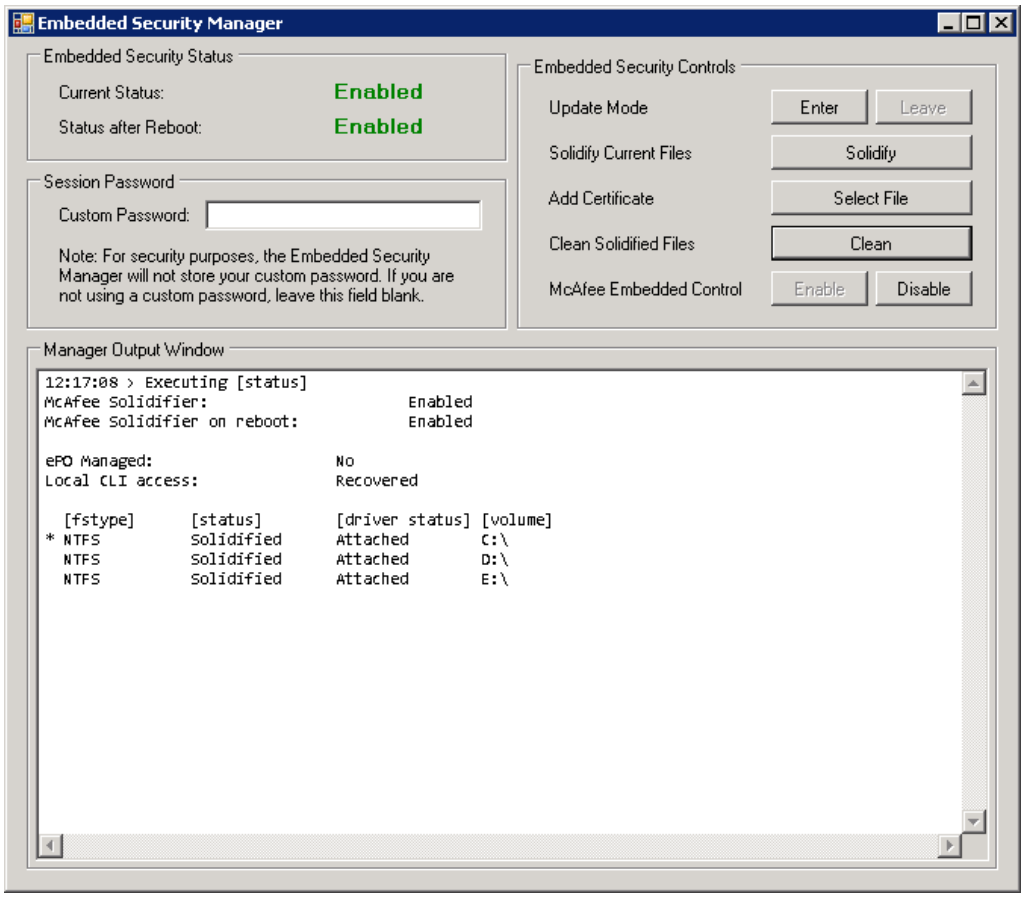
6. When you arrive at the Specify Target Type page, select the option as follows:

Option	Description
K2 with local storage	For installing on an internal storage K2 system or on a direct-connect storage K2 system.

7. Click **Next** and **Finish** to complete the installation.
8. Manage the required restart as follows:
   - Restart now.

Leave Update mode

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



   Interpret Current Status as follows:

   - **Enabled**: Embedded Security is enabled but is not in Update mode.
   - **Update**: Embedded Security is enabled and is in Update mode, ready for software installation.

2. Under **Update**, manage the Update mode as follows:

   - Click **Leave** to take Embedded Security out of Update mode.

   A restart is not required after you leave the Update mode.

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	9.3.xxx	These should both report the same version number. This is the K2 System Software version number.
RTS Version	9.3.xxx	
Media File System	4.2.2.b27249	This is the SNFS version.

Enhance network bandwidth

On K2 Summit/Solo systems with K2 system software 9.x, the on-board network adapters have a performance limitation that causes them to function at half the expected bandwidth. On most systems, there are no symptoms related to this limitation, as network traffic is below the limitation. Systems using ShareFlex or having other requirements for high network bandwidth might be impacted to some degree. Symptoms include general network bandwidth restrictions, slow iSCSI I/O performance, slower than expected FTP traffic, and other slowness not caused by other factors.

Grass Valley requires that you remove the limitation and enhance the network performance. Once the limitation is removed, the change persists throughout normal software upgrades. However, if you reimage the K2 Summit/Solo system you must check and reapply the change if necessary.

To remove the limitation, disable "Large Send Offloads" on the network adapters and disable "CPU Power Technology" in the BIOS.

Refer to Grass Valley Knowledge Base Article *#000011688* for more information.

Disable Large Send Offloads

1. From the Windows operating **Start** menu, open **Control Panel**.
2. In **Control Panel**, open **Network and Sharing Center**.
3. In **Network and Sharing Center**, select **Change adapter settings**.

   Network Connections opens and displays network adapters, including the following:

   - Control Connection #1
   - Control Connection #2
   - Media Connection #1
   - Media Connection #2

4. For each Control Connection and each Media Connection, do the following:
   a) Right-click the connection and select **Properties**.
      The **Connection Properties** dialog box opens.
   b) In the **Connection Properties** dialog box, click **Configure**.
      The **Adapter Properties** dialog box opens.
   c) In the **Adapter Properties** dialog box, click the **Advanced** tab.
   d) On the Advanced tab, in the Settings list select **Large Send Offload v2 (IPv4)** and then in the Value drop-down list select **Disabled**.
   e) Click **OK** to save settings and close.
   f) Repeat these steps for each Control Connection and each Media Connection.

Next, disable CPU power technology.

Disable CPU Power Technology

1. Restart the K2 Summit/Solo system.
2. During the BIOS startup screen, press **F2** repeatedly until `Entering Setup...` appears.
   The BIOS screen opens.
3. On the BIOS screen, use arrow keys and select the **Advanced** tab.
4. On the Advanced tab select **CPU Core Configuration** and then press **Enter**.
   The CPU Core Configuration screen opens.
5. On the CPU Core Configuration screen, select **Power Technology** and then press **Enter**.
   A **Power Technology** dialog box opens.
6. In the **Power Technology** dialog box select **Disable** and then press **Enter**.
7. Press **F4** to save and exit.
   A **Save & Exit Setup** dialog box opens.
8. In the **Save & Exit Setup** dialog box, select **Yes** and then press **Enter**.
9. The K2 Summit/Solo system restarts.

Next, install the SiteConfig Discovery Agent.

Upgrade RAID Controller microcode on stand-alone K2 system

Do not do this task if one of the following is true:

- A K2 Solo Media Server
- A K2 Summit Production Client with internal storage and with RAID controller microcode already upgraded to a compatible version, as listed in compatibility specifications.
- A K2 Summit Production Client with direct-connect storage and with RAID controller and/or expansion chassis microcode already at compatible versions, as listed in compatibility specifications.

Do this task if:

- A K2 Summit Production Client with internal storage and with RAID controller microcode that you need to upgrade, as listed in compatibility specifications.
- A K2 Summit Production Client with direct-connect storage and with RAID controller and/or expansion chassis microcode that you need to upgrade, as listed in compatibility specifications.

For internal storage K2 Summit/Solo systems, find compatibility specifications at *Compatible K2 Summit/Solo components* on page 1083. For a K2 Summit Production Client with direct-connect storage, find compatibility specifications at *Compatible K2 RAID components* on page 1090.

1. Open AppCenter Workstation, either on the local K2 system or on the control point PC and logon.

   Make sure you logon to AppCenter with appropriate privileges, as this logon is passed to Storage Utility. Administrator-level permission is necessary for most Storage Utility operations. If you log in with user-level permissions, the Storage Utility menu item is disabled.

2. If you are running AppCenter from a control point PC and you have channels from multiple K2 systems in your channel suite, select a channel from the stand-alone K2 system whose storage you intend to configure with Storage Utility. This is important as Storage Utility automatically connects to the K2 system that hosts the currently selected channel.

   NOTE: Make sure you are connecting to a stand-alone K2 system. You should never connect Storage Utility directly to a K2 system that uses shared (SAN) storage.

3. From the AppCenter **System** menu, select **Storage Utility**.

   Storage Utility opens.

4. If you are connecting from a control point PC, you should verify that you are connected to the correct K2 system. To verify this, use the Identify feature to flash the disks on the K2 system.
5. Select the controller in the Storage Utility tree view, then in the properties reported in the right-hand pane, note the controller microcode version. Proceed if you need to upgrade the controller microcode.
6. Right-click the controller in the tree view and do one of the following:

   - For internal storage, select **Load Controller Microcode** in the context menu.
   - For direct-connect storage, select **Advanced | Load Controller Microcode** in the context menu.

7. If online, messages appear "…offline mode now?" and "…continue?". Click **Yes** to put the K2 system in offline mode.

   AppCenter channels go offline. The Open File dialog box opens.

8. In the Open File dialog box, browse to and select the microcode file for the required version. Refer to the following for locations and filenames:

   - For internal-storage, refer to *Compatible K2 Summit/Solo components* on page 1083.
   - For direct-connect storage, refer to *Compatible K2 RAID components* on page 1090.

9. Click **OK.**

   The Progress Report window appears showing the microcode download task and the percentage completion.

10. If direct-connect storage and upgrading expansion chassis microcode, do the following:
    a) Right-click the controller in the tree view, then select **Advanced | Load Disk Enclosure Microcode** in the context menu.
    b) In the Open File dialog box, browse to the directory and file as listed in K2 RAID compatibility specifications earlier in these release notes.
    c) Click **OK.**

    The Progress Report window appears showing the microcode download task and the percentage completion.
11. When finished, exit Storage Utility.
12. If direct-connect storage, on 100% completion, proceed as follows:
    - If the RAID controller chassis has redundant controllers, no power cycle is required. The microcode download is complete.
    - If the RAID controller chassis does not have redundant controllers, power cycle the RAID controller chassis.
13. Put AppCenter channels back online.
14. Restart.

Upgrade disk drive firmware on stand-alone K2 system

Do not do this task if:

- A K2 system with disk drive firmware already at a compatible version, as listed in compatibility specifications.

Do this task if:

- A K2 system with disk drive firmware that you need to upgrade, as listed in compatibility specifications.

For internal storage K2 Summit/Solo systems, find compatibility specifications at *Compatible K2 Summit/Solo components* on page 1083. For a K2 Summit Production Client with direct-connect storage, find compatibility specifications at *Compatible K2 RAID components* on page 1090.

NOTE: The disk drives are upgraded one at a time which can take as long as 2 minutes per drive. Take this into consideration when scheduling the upgrade.

1. Open AppCenter Workstation, either on the local K2 system or on the control point PC and logon.

   Make sure you logon to AppCenter with appropriate privileges, as this logon is passed to Storage Utility. Administrator-level permission is necessary for most Storage Utility operations. If you log in with user-level permissions, the Storage Utility menu item is disabled.
2. If you are running AppCenter from a control point PC and you have channels from multiple K2 systems in your channel suite, select a channel from the stand-alone K2 system whose storage you intend to configure with Storage Utility. This is important as Storage Utility automatically connects to the K2 system that hosts the currently selected channel.

   NOTE: Make sure you are connecting to a stand-alone K2 system. You should never connect Storage Utility directly to a K2 system that uses shared (SAN) storage.

3. From the AppCenter **System** menu, select **Storage Utility**.

   Storage Utility opens.

4. If you are connecting from a control point PC, you should verify that you are connected to the correct K2 system. To verify this, use the Identify feature to flash the disks on the K2 system.
5. Select a disk drive icon in the Storage Utility tree view, then note the firmware version in drive properties reported in the right-hand pane. Proceed if you need to download disk drive firmware.
6. Right-click a disk in the tree view, then select **Advanced | Download Disk Firmware** in the context menu.
7. If online, messages appear "…offline mode now?" and "…continue?". Click **Yes** to put the K2 system in offline mode.

   AppCenter channels go offline. The Open File dialog box opens.

8. In the Open File dialog box browse to the directory and file as listed in compatibility tables earlier in these release notes. You must select the correct file for the device, storage type, and drive size/type.
9. Click **OK**.

   For internal drives, watch the lights on the drive to which you are downloading firmware. The lights flash as firmware loads. Wait until the lights have completed their flashing pattern. This can take several minutes.

   The Progress Report window appears showing the disk firmware download task and the percentage completion.

10. Repeat this procedure on each drive.
11. When finished, exit Storage Utility.
12. Put AppCenter channels back online.
13. Restart.

Reset Capture Services

Do not do this task if:

- You do not use any of the K2 Capture Services.

Do this task if:

- You are using one or more K2 Capture Services, such HotBin, XML Import, Export, P2, etc.

Do this task on the K2 system running your K2 Capture Service, which is the K2 system that receives the media to be imported into K2 storage. This can be a K2 Solo Media Server, a stand-alone K2 Summit Production Client, or the K2 Media Server with the role of primary FTP server on a K2 SAN.

When you configure a K2 Capture Service for the first time, the service is set to startup type Automatic. However, if you upgrade or otherwise re-install your K2 System Software, the service is re-set to startup type Manual. Therefore, you must re-configure the service after K2 System Software upgrade/ reinstall in order to set the startup type back to Automatic.

1. From the **Start** menu, access the **Programs** menu and select **Grass Valley | K2 Capture Services**.

   The K2 Capture Services utility dialog box is displayed.

2. Click **Apply**.

   For import capture services, the service checks the source directory for files. If files are present, the service moves them to the Archive sub-directory. It does not import the files into the destination bin on the K2 system.

Upgrade remaining stand-alone K2 systems

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

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 tasks similar to those you followed for upgrading software so that as you take systems offline you manage redundancy, servers, and clients, as appropriate for your system.

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

Licensing K2 products

The following sections contain instructions for managing K2 product licenses.

Licensable options

Optional applications, bundles of advanced features, and enhanced functionality are available as licensable options for K2 products.

AppCenter licenses are as follows:

	AppCenter Standard	AppCenter Pro	AppCenter Elite
Record	X	X	X
Continuous Record	X	X	X
Play	X	X	X
Sub-Clipping	X	X	X
Playlists	X	X	X
"Live" Mode (Chase Play)	X	X	X
Video Monitor in Control View	X	X	X
VM Multi-view	X	X	X
Playlist Import		X	X
Channel Ganging		X	X

	AppCenter Standard	AppCenter Pro	AppCenter Elite
Audio Track insert		X	X
CC Track insert		X	X
Audio Track assignments		X	X
Scheduled Record per channel (not playlist)		X	X
Scheduled Playback per channel (not playlist)		X	X
Super out on SDI 2 output		X	X
Playlist with M/E Transitions		X	X
Flying M/E Transitions		X	X
Proxy encoding - 4 Channels		X	X
Key+ Fill import (QT32)		X	X
Channel Flex Suite			X
- Multi-CAM			X
- 4K			X
- Video + Key			X
- 3D - Left + Right Eye			X
- Super Slo-Mo x2			X
- Super Slo-Mo x3			X
- Super Slo-Mo x6			X
Proxy encoding - 8 Channels			X

Other options and applications include the following:

- HD option
- AVC option (Summit/Solo 3G)
- Avid DNxHD option (Summit/Solo 3G)
- 3G option (Summit/Solo 3G)
- 3G 1080p option (Summit 3G)
- 4K option (Summit 3G)
- 3-input Multi-Cam channel (Summit/Solo 3G)
- K2 TimeDelay
- K2 XML Import capture service
- HotBin Export capture service
- P2 Import capture service
- K2 Extended File Services

- K2 InSync
- K2 FCP Connect

As development continues, new options become available. Contact your Grass Valley representative to learn more about current options.

About K2 system software licensing

K2 system software version 9.3 requires a license from Grass Valley. Licensing is enforced at the K2 Summit Production Client or K2 Solo Media Server, so every K2 client running version 9.3 must have a valid license in place. No software version license is required on the control point PC. The K2 Media Server can be licensed for K2 SAN bandwidth, but no K2 system software version license is required on the K2 Media Server.

K2 clients shipping new from the factory have version 9.3 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/Elite.

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

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

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

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

This topic applies to Grass Valley SabreTooth licenses. For the system you are licensing, you must provide a generated unique ID to Grass Valley. Grass Valley uses the ID 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 shortcut on the Windows desktop or in the *Grass Valley License Requests* folder.

   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 from Grass Valley.

   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. 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.

8. 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.

9. 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, or the License wizard is not available, try this alternate method:

1. Generate a unique ID of the device where you will install software, as follows:
   a) Double click on the License Manager icon on the Windows Desktop.
      The SabreTooth License Manager opens.
   b) Choose **File | Generate Unique Id** the License Manager.
   c) Click **Copy to clipboard** to copy the generated ID, and **OK** to exit.
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.
   - The license types you are requesting.
3. Send the email to GrassValleyLicensing@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. Double click on the License Manager icon on the Windows Desktop.
   The SabreTooth License Manager opens.
2. Do one of the following:
   - Choose **File | Import License** and navigate to the file location to open the text file.
   - Drag and drop the text file onto the License Manager.

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

You should archive the permanent license to a backup system.

Deleting licenses

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

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

Archiving licenses

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

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

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

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

ncb00003440	Description:	Bins nested more than nine levels deep are not supported. Database errors can occur.
	Workaround:	Constrain bins to nine levels deep or less. This includes the top-most bin.
ncb00003457	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.
ncb00039062	Description:	The system clock may not update when the TimeOfDay source is changed.
	Workaround:	If this happens reboot after the TimeOfDay source change.
ncb00003919	Description:	When reconfiguring channel security settings on Configuration Manager Security tab, AppCenter does not allow username/password fields to be blank.
	Workaround:	Enter username/password for a valid user account. Once configured, the fields require valid information.
ncb00004073	Description:	Recorded video is one frame late relative to timecode. This occurs if you record using Time-of-day timecode and the source is from channel four's LTC input.
	Workaround:	Connect the house LTC input to channel 1 and use it as the Time-of-day source.
ncb00002648	Description:	AppCenter does not allow a clip to be deleted if the clip is associated with a playlist, program, or subclip.

	Workaround:	First use the "Consolidate Media" feature on the clip, then delete the clip.
ncb00002781	Description:	Video faults continue to occur if Super Slo-Mo inputs lose and then regain phase alignment while recording is underway.
	Workaround:	If inputs lose phase alignment, first restore phase alignment and then stop and restart the recording.
ncb00035282	Description:	On K2 Summit Transmission models, only two audio tracks can be created for new Playlist.
	Workaround:	Switch the channel to a Player/Recorder, set the number of audio channels, then create the Playlist.
ncb00038746	Description:	Audio errors occur when playing a clip while importing from a USB device.
	Workaround:	Copy first, then play. Playback while importing from USB not supported.
ncb00075492	Description:	After a failover event occurs on the K2 SAN, there are multiple decoder errors when playing an Avid DNxHD, AVC-Intra, or DVCPROHD clip that was recorded at the time of the failover.
	Workaround:	Delete clips that exhibit these errors and re-record them.
DE8566	Description:	If a channel is running as a Playlist when it is configured to be a 4K Player, 4K Recorder, 3D/Video+Key Player or 3D/Video+Key Recorder then it will not play or record correctly.
	Workaround:	Be sure all channels are running as a Player/Recorder before changing the configuration to a 4K Player, 4K Recorder, 3D/Video+Key Player or 3D/Video+Key Recorder.
DE9040	Description:	E-to-E video is dim after switching a channel from 3xSSM to a Recorder/Player.
	Workaround:	Cue a clip after changing the channel from a SSM channel to a Recorder/Player channel. Once cued, either for play or for record, the channel configuration is complete and E-to-E operation will be correct for the new channel type.

Storage Utility

ncb00004104	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 **File System Server** node to open its property page. On the property page click **Launch Storage Utility**.

System

ncb00017096	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.
ncb00003449	Description:	Slow operations after restarting with a USB device connected.
	Workaround:	Disconnect then reconnect USB device. Normal operation speed is restored.
ncb00002672	Description:	Macintosh systems cannot write to a HotBin directory on the V: drive of an iSCSI or Fibre Channel connected K2 SAN. GV Connect export to the HotBin fails.
	Workaround:	Delete the HotBin, configure Macintosh access in the SNFS configuration file, then recreate the HotBin from the K2 Media Server. Configure the SNFS configuration file as part of the upgrade to this version of K2 software, as instructed in the upgrade procedure earlier in these release notes. If not upgrading, take systems offline, make the change as instructed in the upgrade procedure, then restart the K2 Media Server to put the change into effect.
ncb00004203	Description:	On a K2 Media Server with SNFS on the C: drive, media is lost if you re-image the C: drive
	Workaround:	Before re-imaging, use the `ssave.bat` and `srestore.bat` tools included on the USB drive included with the K2 Summit system or upgrade field kit.
ncb00060531	Description:	When configuring a HotBin Export destination folder and entering credentials, a "...cannot start service..." error message appears.
	Workaround:	In Windows Services Control Panel, for Grass Valley Import Service, enter the credentials and start the service.
ncb00038588	Description:	The K2Config application does not open.
	Workaround:	On the PC that hosts the K2Config application, disable the control network interface card, then open the K2Config application, then enable the control network interface card.
ncb00064016	Description:	AFD property is not passed with AVC clips.
	Workaround:	Add an ancillary data track to the AVC clip to carry the AFD property.
ncb00063992	Description:	Some USB 3.0 devices are not recognized as USB 3.0 on the front connectors.
	Workaround:	If the USB 3.0 device is recognized as a USB 2.0 device when plugged in, remove it and plug it in again to be recognized as a USB 3.0 device. If the USB 3.0 device is not recognized at all, plug in a USB 2.0 device, then plug in the USB 3.0 device again to use it. This only needs to be done once after booting. Thereafter the device will be recognized as a USB 3.0 device.
DE6716	Description:	3x Super Slow Motion in 720p record jitters for a few frames after changing the camera format.

	Workaround:	After a camera video format change, discard the first bad frames of the first recording. Recordings thereafter will be good until the camera video format is changed again.
DE6779	Description:	Ancillary data lost on import of P2 clip.
	Workaround:	Contact Grass Valley Support.
DE6940	Description:	An iSCSI-attached K2 Summit SAN client system fails to play or record two channels of 1080p when the other two channels are doing a continuous record of 1080p.
	Workaround:	Only two 1080p channels are supported for iSCSI connected SAN clients. Use FibreChannel connections to use 1080p on more than two channels on SAN clients. While two channels are doing a continuous record of 1080p, do not use the other two channels.
DE6954	Description:	In the K2 TimeDelay application, thumbnails are not updated.
	Workaround:	None. Thumbnails are no longer updated as records continue in K2 TimeDelay.
DE7330	Description:	A long continuous recorded clip might not delete successfully. The clip is deleted from the media file system, yet the clip is still displayed in AppCenter.
	Workaround:	Use the Storage Utility Clean Unreferenced Movies feature. This removes the display of the clip from AppCenter.
DE8525 ncb00075905	Description:	FTP transfers fail to/from a K2 Media Server with role of FTP server. This occurs on first start-up after re-image.
	Workaround:	Reboot the K2 Media Server, and restart the Grass Valley FTP Dameon service.
DE9019	Description:	4K and 6xSSM features do not work when the licenses are installed to a K2 Summit 3G system that is not properly configured to support them.
	Workaround:	Do not install 4K or 6xSSM licenses onto K2 Summit systems that are not properly configured to support these features. Proper configuration includes the correct hardware, media drives and K2 Summit 3G codec modules.
DE9664	Description:	6-in/2-out performance is slow when using ShareFlex on K2 Summit 3G systems with hard drives.
	Workaround:	Ensure your hardware is able to support this feature. You may also try the following to bring the system back into its operational rating: • Use split audio on the triple Multi-Cam channels instead of no split audio • Drop the video bit rate to 50Mbps • Do not use ShareFlex • Use SSDs instead of hard drives

Proxy/live streaming

ncb00041093	Description:	Live streaming can fail when the K2 Summit system's IP address is changed.
	Workaround:	On the K2 Summit system navigate to `V:\live streaming` and use Notepad or a similar text editor to open a `*.sdp` file. Check the first IP address listed in the file, on the `o=` line. If it is not the K2 Summit system's Control Connection IP address, delete the `*.sdp` files in the directory and restart the K2 Summit system.
ncb00061128	Description:	Remote desktop connections cause live streaming errors and audio/video sync problems.
	Workaround:	Do not use Remote Desktop on K2 Summit systems that are generating live streams. To restore live streaming audio/video sync, disable the proxy recording and live streaming for that channel, then re-enable live streaming.

Installation

ncb00003885	Description:	If uninstalling or installing K2 client software while applications or connections to AppService are open, the installation program becomes unresponsive.
	Workaround:	To prevent the problem from occurring, shutdown all applications and connections before uninstalling or installing. Then after all applications are shutdown, use Task Manager to stop AppService.
ncb00040814	Description:	Error messages appear during Generic iSCSI software install. This occurs when doing a manual (not SiteConfig) install on a Windows 7 PC. The error messages are similar to "The installation of VS2005.762 appears to have failed..." and "Setup could not find the update.inf file...".
	Workaround:	Ignore the error messages and continue with installation. The software installs successfully. The error messages are caused because the installation program tries to install components that are already present in Windows 7.

Compatibility

ncb00008524	Description:	Transfers to/from M-Series iVDR are not supported.
	Workaround:	Do not attempt to transfer to/from M-Series iVDR.
ncb00025753	Description:	MXF streaming transfer to XDCAM recorder fails.
	Workaround:	None. Some Sony deck models do not comply with the MXF standard.

Dyno PA/Dyno

ncb00002810	Description:	On a stand-alone K2 Summit/Solo configured for K2 Dyno PA, the V: drive is not available. This occurs if the K2 system is started without a network connection or otherwise used outside of the Dyno PA system.
	Workaround:	Remove the DLC configuration from the K2 Summit/Solo as instructed in Dyno PA documentation. Verify that the loopback adapter is at the top of the adapter order list. This is required for a stand-alone K2 system that is not part of a Dyno PA system.
ncb00076307	Description:	K2 Dyno playlists with more than four audio tracks do not have the associated audio file, causing problems when exported. This occurs with K2 Dyno software version 2.0.4.143 and K2 Summit software version 8.1.11.1810, in which only four audio tracks are configured.
	Workaround:	Before exporting the playlist, configure the K2 Summit system to record eight audio channels.
DE8555	Description:	Media storage fills rapidly each time a loop record is stopped and restarted with an append record. The amount of lost disk space may become significant after many stops and starts of append record.
	Workaround:	Start a record session and let it continue to run without stopping, and then restart with an append record.

Grass Valley Knowledge Base

Visit the Grass Valley Knowledge Base site for technical articles and FAQs (Frequently Asked Questions) about Grass Valley systems and products.

Grass Valley Knowledge Base

Safety Summary

Read and follow the important safety information below, noting especially those instructions related to risk of fire, electric shock or injury to persons. Additional specific warnings not listed here may be found throughout the manual.

⚠	***WARNING: Any instructions in this manual that require opening the equipment cover or enclosure are for use by qualified service personnel only. To reduce the risk of electric shock, do not perform any servicing other than that contained in the operating instructions unless you are qualified to do so.***

Safety terms and symbols

Terms in this manual

Safety-related statements may appear in this manual in the following form:

⚠	***WARNING: Warning statements identify conditions or practices that may result in personal injury or loss of life.***
⚠	***CAUTION: Caution statements identify conditions or practices that may result in damage to equipment or other property, or which may cause equipment crucial to your business environment to become temporarily non-operational.***

Terms on the product

These terms may appear on the product:

DANGER — A personal injury hazard is immediately accessible as you read the marking.

WARNING — A personal injury hazard exists but is not immediately accessible as you read the marking.

CAUTION — A hazard to property, product, and other equipment is present.

Symbols on the product

The following symbols may appear on the product:

⚠	Indicates that dangerous high voltage is present within the equipment enclosure that may be of sufficient magnitude to constitute a risk of electric shock.
⚠	Indicates that user, operator or service technician should refer to product manual(s) for important operating, maintenance, or service instructions.
⚠	This is a prompt to note fuse rating when replacing fuse(s). The fuse referenced in the text must be replaced with one having the ratings indicated.
⏚	Identifies a protective grounding terminal which must be connected to earth ground prior to making any other equipment connections.
⏚	Identifies an external protective grounding terminal which may be connected to earth ground as a supplement to an internal grounding terminal.
⚠	Indicates that static sensitive components are present which may be damaged by electrostatic discharge. Use anti-static procedures, equipment and surfaces during servicing.

Warnings

The following warning statements identify conditions or practices that can result in personal injury or loss of life.

Dangerous voltage or current may be present — Disconnect power and remove battery (if applicable) before removing protective panels, soldering, or replacing components.

Do not service alone — Do not internally service this product unless another person capable of rendering first aid and resuscitation is present.

Remove jewelry — Prior to servicing, remove jewelry such as rings, watches, and other metallic objects.

Avoid exposed circuitry — Do not touch exposed connections, components or circuitry when power is present.

Use proper power cord — Use only the power cord supplied or specified for this product.

Ground product — Connect the grounding conductor of the power cord to earth ground.

Operate only with covers and enclosure panels in place — Do not operate this product when covers or enclosure panels are removed.

Use correct fuse — Use only the fuse type and rating specified for this product.

Use only in dry environment — Do not operate in wet or damp conditions.

Use only in non-explosive environment — Do not operate this product in an explosive atmosphere.

High leakage current may be present — Earth connection of product is essential before connecting power.

Dual power supplies may be present — Be certain to plug each power supply cord into a separate branch circuit employing a separate service ground. Disconnect both power supply cords prior to servicing.

Double pole neutral fusing — Disconnect mains power prior to servicing.

Use proper lift points — Do not use door latches to lift or move equipment.

Avoid mechanical hazards — Allow all rotating devices to come to a stop before servicing.

Cautions

The following caution statements identify conditions or practices that can result in damage to equipment or other property

Use correct power source — Do not operate this product from a power source that applies more than the voltage specified for the product.

Use correct voltage setting — If this product lacks auto-ranging power supplies, before applying power ensure that the each power supply is set to match the power source.

Provide proper ventilation — To prevent product overheating, provide equipment ventilation in accordance with installation instructions.

Use anti-static procedures — Static sensitive components are present which may be damaged by electrostatic discharge. Use anti-static procedures, equipment and surfaces during servicing.

Do not operate with suspected equipment failure — If you suspect product damage or equipment failure, have the equipment inspected by qualified service personnel.

Ensure mains disconnect — If mains switch is not provided, the power cord(s) of this equipment provide the means of disconnection. The socket outlet must be installed near the equipment and must be easily accessible. Verify that all mains power is disconnected before installing or removing power supplies and/or options.

Route cable properly — Route power cords and other cables so that they ar not likely to be damaged. Properly support heavy cable bundles to avoid connector damage.

Use correct power supply cords — Power cords for this equipment, if provided, meet all North American electrical codes. Operation of this equipment at voltages exceeding 130 VAC requires power supply cords which comply with NEMA configurations. International power cords, if provided, have the approval of the country of use.

Use correct replacement battery — This product may contain batteries. To reduce the risk of explosion, check polarity and replace only with the same or equivalent type recommended by manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Troubleshoot only to board level — Circuit boards in this product are densely populated with surface mount technology (SMT) components and application specific integrated circuits (ASICS). As a result, circuit board repair at the component level is very difficult in the field, if not impossible. For warranty compliance, do not troubleshoot systems beyond the board level.

Sicherheit – Überblick

Lesen und befolgen Sie die wichtigen Sicherheitsinformationen dieses Abschnitts. Beachten Sie insbesondere die Anweisungen bezüglich

Brand-, Stromschlag- und Verletzungsgefahren. Weitere spezifische, hier nicht aufgeführte Warnungen finden Sie im gesamten Handbuch.

⚠	***WARNUNG: Alle Anweisungen in diesem Handbuch, die das Abnehmen der Geräteabdeckung oder des Gerätegehäuses erfordern, dürfen nur von qualifiziertem Servicepersonal ausgeführt werden. Um die Stromschlaggefahr zu verringern, führen Sie keine Wartungsarbeiten außer den in den Bedienungsanleitungen genannten Arbeiten aus, es sei denn, Sie besitzen die entsprechende Qualifikationen für diese Arbeiten.***

Sicherheit – Begriffe und Symbole

In diesem Handbuch verwendete Begriffe

Sicherheitsrelevante Hinweise können in diesem Handbuch in der folgenden Form auftauchen:

⚠	***WARNUNG: Warnungen weisen auf Situationen oder Vorgehensweisen hin, die Verletzungs- oder Lebensgefahr bergen.***
⚠	***VORSICHT: Vorsichtshinweise weisen auf Situationen oder Vorgehensweisen hin, die zu Schäden an Ausrüstungskomponenten oder anderen Gegenständen oder zum zeitweisen Ausfall wichtiger Komponenten in der Arbeitsumgebung führen können.***

Hinweise am Produkt

Die folgenden Hinweise können sich am Produkt befinden:

GEFAHR – Wenn Sie diesen Begriff lesen, besteht ein unmittelbares Verletzungsrisiko.

WARNUNG – Wenn Sie diesen Begriff lesen, besteht ein mittelbares Verletzungsrisiko.

VORSICHT – Es besteht ein Risiko für Objekte in der Umgebung, den Mixer selbst oder andere Ausrüstungskomponenten.

Symbole am Produkt

Die folgenden Symbole können sich am Produkt befinden:

	Weist auf eine gefährliche Hochspannung im Gerätegehäuse hin, die stark genug sein kann, um eine Stromschlaggefahr darzustellen.
	Weist darauf hin, dass der Benutzer, Bediener oder Servicetechniker wichtige Bedienungs-, Wartungs- oder Serviceanweisungen in den Produkthandbüchern lesen sollte.
	Dies ist eine Aufforderung, beim Wechsel von Sicherungen auf deren Nennwert zu achten. Die im Text angegebene Sicherung muss durch eine Sicherung ersetzt werden, die die angegebenen Nennwerte besitzt.
	Weist auf eine Schutzerdungsklemme hin, die mit dem Erdungskontakt verbunden werden muss, bevor weitere Ausrüstungskomponenten angeschlossen werden.

⏚	Weist auf eine externe Schutzerdungsklemme hin, die als Ergänzung zu einem internen Erdungskontakt an die Erde angeschlossen werden kann.
	Weist darauf hin, dass es statisch empfindliche Komponenten gibt, die durch eine elektrostatische Entladung beschädigt werden können. Verwenden Sie antistatische Prozeduren, Ausrüstung und Oberflächen während der Wartung.

Warnungen

Die folgenden Warnungen weisen auf Bedingungen oder Vorgehensweisen hin, die Verletzungs- oder Lebensgefahr bergen:

Gefährliche Spannungen oder Ströme – Schalten Sie den Strom ab, und entfernen Sie ggf. die Batterie, bevor sie Schutzabdeckungen abnehmen, löten oder Komponenten austauschen.

Servicearbeiten nicht alleine ausführen – Führen Sie interne Servicearbeiten nur aus, wenn eine weitere Person anwesend ist, die erste Hilfe leisten und Wiederbelebungsmaßnahmen einleiten kann.

Schmuck abnehmen – Legen Sie vor Servicearbeiten Schmuck wie Ringe, Uhren und andere metallische Objekte ab.

Keine offen liegenden Leiter berühren – Berühren Sie bei eingeschalteter Stromzufuhr keine offen liegenden Leitungen, Komponenten oder Schaltungen.

Richtiges Netzkabel verwenden – Verwenden Sie nur das mitgelieferte Netzkabel oder ein Netzkabel, das den Spezifikationen für dieses Produkt entspricht.

Gerät erden – Schließen Sie den Erdleiter des Netzkabels an den Erdungskontakt an.

Gerät nur mit angebrachten Abdeckungen und Gehäuseseiten betreiben – Schalten Sie dieses Gerät nicht ein, wenn die Abdeckungen oder Gehäuseseiten entfernt wurden.

Richtige Sicherung verwenden – Verwenden Sie nur Sicherungen, deren Typ und Nennwert den Spezifikationen für dieses Produkt entsprechen.

Gerät nur in trockener Umgebung verwenden – Betreiben Sie das Gerät nicht in nassen oder feuchten Umgebungen.

Gerät nur verwenden, wenn keine Explosionsgefahr besteht – Verwenden Sie dieses Produkt nur in Umgebungen, in denen keinerlei Explosionsgefahr besteht.

Hohe Kriechströme – Das Gerät muss vor dem Einschalten unbedingt geerdet werden.

Doppelte Spannungsversorgung kann vorhanden sein – Schließen Sie die beiden Anschlußkabel an getrennte Stromkreise an. Vor Servicearbeiten sind beide Anschlußkabel vom Netz zu trennen.

Zweipolige, neutrale Sicherung – Schalten Sie den Netzstrom ab, bevor Sie mit den Servicearbeiten beginnen.

Fassen Sie das Gerät beim Transport richtig an – Halten Sie das Gerät beim Transport nicht an Türen oder anderen beweglichen Teilen fest.

Gefahr durch mechanische Teile – Warten Sie, bis der Lüfter vollständig zum Halt gekommen ist, bevor Sie mit den Servicearbeiten beginnen.

Vorsicht

Die folgenden Vorsichtshinweise weisen auf Bedingungen oder Vorgehensweisen hin, die zu Schäden an Ausrüstungskomponenten oder anderen Gegenständen führen können:

Gerät nicht öffnen – Durch das unbefugte Öffnen wird die Garantie ungültig.

Richtige Spannungsquelle verwenden – Betreiben Sie das Gerät nicht an einer Spannungsquelle, die eine höhere Spannung liefert als in den Spezifikationen für dieses Produkt angegeben.

Gerät ausreichend belüften – Um eine Überhitzung des Geräts zu vermeiden, müssen die Ausrüstungskomponenten entsprechend den Installationsanweisungen belüftet werden. Legen Sie kein Papier unter das Gerät. Es könnte die Belüftung behindern. Platzieren Sie das Gerät auf einer ebenen Oberfläche.

Antistatische Vorkehrungen treffen – Es gibt statisch empfindliche Komponenten, die durch eine elektrostatische Entladung beschädigt werden können. Verwenden Sie antistatische Prozeduren, Ausrüstung und Oberflächen während der Wartung.

CF-Karte nicht mit einem PC verwenden – Die CF-Karte ist speziell formatiert. Die auf der CF-Karte gespeicherte Software könnte gelöscht werden.

Gerät nicht bei eventuellem Ausrüstungsfehler betreiben – Wenn Sie einen Produktschaden oder Ausrüstungsfehler vermuten, lassen Sie die Komponente von einem qualifizierten Servicetechniker untersuchen.

Kabel richtig verlegen – Verlegen Sie Netzkabel und andere Kabel so, dass Sie nicht beschädigt werden. Stützen Sie schwere Kabelbündel ordnungsgemäß ab, damit die Anschlüsse nicht beschädigt werden.

Richtige Netzkabel verwenden – Wenn Netzkabel mitgeliefert wurden, erfüllen diese alle nationalen elektrischen Normen. Der Betrieb dieses Geräts mit Spannungen über 130 V AC erfordert Netzkabel, die NEMA-Konfigurationen entsprechen. Wenn internationale Netzkabel mitgeliefert wurden, sind diese für das Verwendungsland zugelassen.

Richtige Ersatzbatterie verwenden – Dieses Gerät enthält eine Batterie. Um die Explosionsgefahr zu verringern, prüfen Sie die Polarität und tauschen die Batterie nur gegen eine Batterie desselben Typs oder eines gleichwertigen, vom Hersteller empfohlenen Typs aus. Entsorgen Sie gebrauchte Batterien entsprechend den Anweisungen des Batterieherstellers.

Das Gerät enthält keine Teile, die vom Benutzer gewartet werden können. Wenden Sie sich bei Problemen bitte an den nächsten Händler.

Consignes de sécurité

Il est recommandé de lire, de bien comprendre et surtout de respecter les informations relatives à la sécurité qui sont exposées ci-après, notamment les consignes destinées à prévenir les risques d'incendie, les décharges électriques et les blessures aux personnes. Les avertissements complémentaires, qui ne sont pas nécessairement repris ci-dessous, mais présents dans toutes les sections du manuel, sont également à prendre en considération.

⚠ ***AVERTISSEMENT: Toutes les instructions présentes dans ce manuel qui concernent l'ouverture des capots ou des logements de cet équipement sont destinées exclusivement à des membres qualifiés du personnel de maintenance. Afin de diminuer les risques de décharges électriques, ne procédez à aucune intervention d'entretien autre que celles contenues dans le manuel de l'utilisateur, à moins que vous ne soyez habilité pour le faire.***

Consignes et symboles de sécurité

Termes utilisés dans ce manuel

Les consignes de sécurité présentées dans ce manuel peuvent apparaître sous les formes suivantes :

⚠ ***AVERTISSEMENT: Les avertissements signalent des conditions ou des pratiques susceptibles d'occasionner des blessures graves, voire même fatales.***

⚠ ***MISE EN GARDE: Les mises en garde signalent des conditions ou des pratiques susceptibles d'occasionner un endommagement à l'équipement ou aux installations, ou de rendre l'équipement temporairement non opérationnel, ce qui peut porter préjudice à vos activités.***

Signalétique apposée sur le produit

La signalétique suivante peut être apposée sur le produit :

DANGER — risque de danger imminent pour l'utilisateur.

AVERTISSEMENT — Risque de danger non imminent pour l'utilisateur.

MISE EN GARDE — Risque d'endommagement du produit, des installations ou des autres équipements.

Symboles apposés sur le produit

Les symboles suivants peut être apposés sur le produit :

⚠ Signale la présence d'une tension élevée et dangereuse dans le boîtier de l'équipement ; cette tension peut être suffisante pour constituer un risque de décharge électrique.

⚠ Signale que l'utilisateur, l'opérateur ou le technicien de maintenance doit faire référence au(x) manuel(s) pour prendre connaissance des instructions d'utilisation, de maintenance ou d'entretien.

⚠ Il s'agit d'une invite à prendre note du calibre du fusible lors du remplacement de ce dernier. Le fusible auquel il est fait référence dans le texte doit être remplacé par un fusible du même calibre.

⏚	Identifie une borne de protection de mise à la masse qui doit être raccordée correctement avant de procéder au raccordement des autres équipements.
⏚	I dentifie une borne de protection de mise à la masse qui peut être connectée en tant que borne de mise à la masse supplémentaire.
	Signale la présence de composants sensibles à l'électricité statique et qui sont susceptibles d'être endommagés par une décharge électrostatique. Utilisez des procédures, des équipements et des surfaces antistatiques durant les interventions d'entretien.

Avertissements

Les avertissements suivants signalent des conditions ou des pratiques susceptibles d'occasionner des blessures graves, voire même fatales :

Présence possible de tensions ou de courants dangereux — Mettez hors tension, débranchez et retirez la pile (le cas échéant) avant de déposer les couvercles de protection, de défaire une soudure ou de remplacer des composants.

Ne procédez pas seul à une intervention d'entretien — Ne réalisez pas une intervention d'entretien interne sur ce produit si une personne n'est pas présente pour fournir les premiers soins en cas d'accident.

Retirez tous vos bijoux — Avant de procéder à une intervention d'entretien, retirez tous vos bijoux, notamment les bagues, la montre ou tout autre objet métallique.

Évitez tout contact avec les circuits exposés — Évitez tout contact avec les connexions, les composants ou les circuits exposés s'ils sont sous tension.

Utilisez le cordon d'alimentation approprié — Utilisez exclusivement le cordon d'alimentation fourni avec ce produit ou spécifié pour ce produit.

Raccordez le produit à la masse — Raccordez le conducteur de masse du cordon d'alimentation à la borne de masse de la prise secteur.

Utilisez le produit lorsque les couvercles et les capots sont en place — N'utilisez pas ce produit si les couvercles et les capots sont déposés.

Utilisez le bon fusible — Utilisez exclusivement un fusible du type et du calibre spécifiés pour ce produit.

Utilisez ce produit exclusivement dans un environnement sec — N'utilisez pas ce produit dans un environnement humide.

Utilisez ce produit exclusivement dans un environnement non explosible — N'utilisez pas ce produit dans un environnement dont l'atmosphère est explosible.

Présence possible de courants de fuite — Un raccordement à la masse est indispensable avant la mise sous tension.

Deux alimentations peuvent être présentes dans l'équipement — Assurez vous que chaque cordon d'alimentation est raccordé à des circuits de terre séparés. Débranchez les deux cordons d'alimentation avant toute intervention.

Fusion neutre bipolaire — Débranchez l'alimentation principale avant de procéder à une intervention d'entretien.

Utilisez les points de levage appropriés — Ne pas utiliser les verrous de la porte pour lever ou déplacer l'équipement.

Évitez les dangers mécaniques — Laissez le ventilateur s'arrêter avant de procéder à une intervention d'entretien.

Mises en garde

Les mises en garde suivantes signalent les conditions et les pratiques susceptibles d'occasionner des endommagements à l'équipement et aux installations :

N'ouvrez pas l'appareil — Toute ouverture prohibée de l'appareil aura pour effet d'annuler la garantie.

Utilisez la source d'alimentation adéquate — Ne branchez pas ce produit à une source d'alimentation qui utilise une tension supérieure à la tension nominale spécifiée pour ce produit.

Assurez une ventilation adéquate — Pour éviter toute surchauffe du produit, assurez une ventilation de l'équipement conformément aux instructions d'installation. Ne déposez aucun document sous l'appareil – ils peuvent gêner la ventilation. Placez l'appareil sur une surface plane.

Utilisez des procédures antistatiques - Les composants sensibles à l'électricité statique présents dans l'équipement sont susceptibles d'être endommagés par une décharge électrostatique. Utilisez des procédures, des équipements et des surfaces antistatiques durant les interventions d'entretien.

N'utilisez pas la carte CF avec un PC — La carte CF a été spécialement formatée. Le logiciel enregistré sur la carte CF risque d'être effacé.

N'utilisez pas l'équipement si un dysfonctionnement est suspecté — Si vous suspectez un dysfonctionnement du produit, faites inspecter celui-ci par un membre qualifié du personnel d'entretien.

Acheminez les câbles correctement — Acheminez les câbles d'alimentation et les autres câbles de manière à ce qu'ils ne risquent pas d'être endommagés. Supportez correctement les enroulements de câbles afin de ne pas endommager les connecteurs.

Utilisez les cordons d'alimentation adéquats — Les cordons d'alimentation de cet équipement, s'ils sont fournis, satisfont aux exigences de toutes les réglementations régionales. L'utilisation de cet équipement à des tensions dépassant les 130 V en c.a. requiert des cordons d'alimentation qui satisfont aux exigences des configurations NEMA. Les cordons internationaux, s'ils sont fournis, ont reçu l'approbation du pays dans lequel l'équipement est utilisé.

Utilisez une pile de remplacement adéquate — Ce produit renferme une pile. Pour réduire le risque d'explosion, vérifiez la polarité et ne remplacez la pile que par une pile du même type, recommandée par le fabricant. Mettez les piles usagées au rebut conformément aux instructions du fabricant des piles.

Cette unité ne contient aucune partie qui peut faire l'objet d'un entretien par l'utilisateur. Si un problème survient, veuillez contacter votre distributeur local.

Canadian certified power cords

Canadian approval includes the products and power cords appropriate for use in the North America power network. All other power cords supplied are approved for the country of use.

FCC emission control

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense. Changes or modifications not expressly approved by Grass Valley can affect emission compliance and could void the user's authority to operate this equipment.

Canadian EMC Notice of Compliance

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A préscrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

EN55103 1/2 Class A warning

This product has been evaluated for Electromagnetic Compatibility under the EN 55103-1/2 standards for Emissions and Immunity and meets the requirements for E4 environment.

This product complies with Class A (E4 environment). In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

FCC emission limits

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesirable operation.

Laser compliance

Laser safety requirements

This product may contain a Class 1 certified laser device. Operating this product outside specifications or altering its original design may result in hazardous radiation exposure, and may be considered an act of modifying or new manufacturing of a laser product under U.S. regulations contained in 21CFR Chapter 1, subchapter J or CENELEC regulations in HD 482 S1. People performing such an act are required by law to recertify and reidentify this product in accordance with provisions of 21CFR subchapter J for distribution within the U.S.A., and in accordance with CENELEC HD 482 S1 for distribution within countries using the IEC 825 standard.

Laser safety

Laser safety in the United States is regulated by the Center for Devices and Radiological Health (CDRH). The laser safety regulations are published in the "Laser Product Performance Standard," Code of Federal Regulation (CFR), Title 21, Subchapter J.

The International Electrotechnical Commission (IEC) Standard 825, "Radiation of Laser Products, Equipment Classification, Requirements and User's Guide," governs laser products outside the United States. Europe and member nations of the European Free Trade Association fall under the jurisdiction of the Comité Européen de Normalization Electrotechnique (CENELEC).

Safety certification

This product has been evaluated and meets the following Safety Certification Standards:

Standard	Designed/tested for compliance with:
ANSI/UL 60950-1	Safety of Information Technology Equipment, including Electrical Business Equipment (Second edition 2007).
IEC 60950-1 with CB cert.	Safety of Information Technology Equipment, including Electrical Business Equipment (Second edition, 2005).
CAN/CSA C22.2 No. 60950-1	Safety of Information Technology Equipment, including Electrical Business Equipment (Second edition 2007).
BS EN 60950-1	Safety of Information Technology Equipment, including Electrical Business Equipment 2006.

ESD Protection

Electronics today are more susceptible to electrostatic discharge (ESD) damage than older equipment. Damage to equipment can occur by ESD fields that are smaller than you can feel. Implementing the information in this section will help you protect the investment that you have made in purchasing Grass Valley equipment. This section contains Grass Valley's recommended ESD guidelines that should be followed when handling electrostatic discharge sensitive (ESDS) items. These minimal recommendations are based on the information in the *Sources of ESD and Risks* on page 1172 area. The information in *Grounding Requirements for Personnel* on page 1173 is provided to assist you in selecting an appropriate grounding method.

Recommended ESD Guidelines

Follow these guidelines when handling Grass Valley equipment:

- Only trained personnel that are connected to a grounding system should handle ESDS items.
- Do not open any protective bag, box, or special shipping packaging until you have been grounded.

  NOTE: When a Personal Grounding strap is unavailable, as an absolute minimum, touch a metal object that is touching the floor (for example, a table, frame, or rack) to discharge any static energy before touching an ESDS item.
- Open the anti-static packaging by slitting any existing adhesive tapes. Do not tear the tapes off.
- Remove the ESDS item by holding it by its edges or by a metal panel.
- Do not touch the components of an ESDS item unless it is absolutely necessary to configure or repair the item.
- Keep the ESDS work area clear of all nonessential items such as coffee cups, pens, wrappers and personal items as these items can discharge static. If you need to set an ESDS item down, place it on an anti-static mat or on the anti-static packaging.

Sources of ESD and Risks

The following information identifies possible sources of electrostatic discharge and can be used to help establish an ESD policy.

Personnel

One of the largest sources of static is personnel. The static can be released from a person's clothing and shoes.

Environment

The environment includes the humidity and floors in a work area. The humidity level must be controlled and should not be allowed to fluctuate over a broad range. Relative humidity (RH) is a major part in determining the level of static that is being generated. For example, at 10% - 20% RH a person walking across a carpeted floor can develop 35kV; yet when the relative humidity is increased to 70% - 80%, the person can only generate 1.5kV.

Static is generated as personnel move (or as equipment is moved) across a floor's surface. Carpeted and waxed vinyl floors contribute to static build up.

Work Surfaces

Painted or vinyl-covered tables, chairs, conveyor belts, racks, carts, anodized surfaces, plexiglass covers, and shelving are all static generators.

Equipment

Any equipment commonly found in an ESD work area, such as solder guns, heat guns, blowers, etc., should be grounded.

Materials

Plastic work holders, foam, plastic tote boxes, pens, packaging containers and other items commonly found at workstations can generate static electricity.

Grounding Requirements for Personnel

The information in this section is provided to assist you in selecting a grounding method. This information is taken from ANSI/ESD S20.20-2007 (Revision of ANSI/ESD S20.20-1999).

Product Qualification

Personnel Grounding Technical Requirement	Test Method	Required Limits
Wrist Strap System*	ANSI/ESD S1.1 (Section 5.11)	$< 3.5 \times 10^7$ ohm
Flooring / Footwear System – Method 1	ANSI/ESD STM97.1	$< 3.5 \times 10^7$ ohm
Flooring / Footwear System – Method 2 (both required)	ANSI/ESD STM97. 1ANSI/ESD STM97.2	$< 10^9$ ohm
	ANSI/ESD STM97.2	< 100 V

Product qualification is normally conducted during the initial selection of ESD control products and materials. Any of the following methods can be used: product specification review, independent laboratory evaluation, or internal laboratory evaluation.

Compliance Verification

Personnel Grounding Technical Requirement	Test Method	Required Limits
Wrist Strap System*	ESD TR53 Wrist Strap Section	$< 3.5 \times 10^7$ ohm
Flooring / Footwear System – Method 1	ESD TR53 Flooring Section and ESD TR53 Footwear Section	$< 3.5 \times 10^7$ ohm
Flooring / Footwear System – Method 2 (both required)	ESD TR53 Flooring Section and ESD TR53 Footwear Section	$< 1.0 \times 10^9$ ohm

***** For situations where an ESD garment is used as part of the wrist strap grounding path, the total system resistance, including the person, garment, and grounding cord, must be less than 3.5×10^7 ohm.

Trademarks and Agreements

Related Topics

Trademarks on page 1174

JPEG acknowledgment on page 1174

Trademarks

Belden, Belden Sending All The Right Signals, and the Belden logo are trademarks or registered trademarks of Belden Inc. or its affiliated companies in the United States and other jurisdictions. Grass Valley, GV STRATUS, GV Director, K2, Summit, ChannelFlex, Dyno, Solo, ClipStore, Infinity, Turbo, Profile, Profile XP and NetCentral, are trademarks or registered trademarks of Grass Valley. Belden Inc., Grass Valley, and other parties may also have trademark rights in other terms used herein, such as Microsoft® Windows® operating system, Windows Media® player, Internet Explorer® internet browser, and SQL Server™. QuickTime and the QuickTime logo are trademarks or registered trademarks of Apple Computer, Inc., used under license therefrom. AVCHD and the AVCHD logo are trademarks of Panasonic Corporation and Sony Corporation. Avid DNxHD is a registered trademark of Avid Technology, Inc., a Delaware corporation.

Related Topics

Trademarks and Agreements on page 1174

JPEG acknowledgment

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

Related Topics

Trademarks and Agreements on page 1174