grass valley

K2
Media Platform

System Guide
Software Version 7.2

www.grassvalley.com

KEMA

Affiliate with the N.V. KEMA in The Netherlands

CERTIFICATE

Certificate Number: 510040.001
The Quality System of:

Thomson Inc, and it's wordwide Grass Valley division affiliates DBA GRASS VALLEY

Headquarters
**400 Providence Mine Rd
Nevada City, CA 95959
United States**

**15655 SW Greystone Ct.
Beaverton, OR 97006
United States**

**10 Presidential Way
Suite 300
Woburn, MA 01801
United States**

**Kapittelweg 10
4827 HG Breda
The Nederlands**

**7140 Baymeadows Way
Ste 101
Jacksonville, FL 32256
United States**

**2300 So. Decker Lake Blvd.
Salt Lake City, UT 84119
United States**

**Rue du Clos Courtel
CS 31719
35517 Cesson-Sevigné Cedex
France**

**1 rue de l'Hautil
Z.I. des Boutries BP 150
78702 Conflans-Sainte
Honorine Cedex
France**

**Technopole Brest-Iroise
Site de la Pointe du Diable
CS 73808
29238 Brest Cedex 3
France**

**40 Rue de Bray
2 Rue des Landelles
35510 Cesson Sevigné
France**

**Spinnereistrasse 5
CH-5300 Turgi
Switzerland**

**Brunnenweg 9
D-64331 Weiterstadt
Germany**

**Carl-Benz-Strasse 6-8
67105 Schifferstadt
Germany**

Including its implementation, meets the requirements of the standard:

ISO 9001:2008

Scope:
The design, manufacture and support of video and audio hardware and software products and related systems.

This Certificate is valid until: June 14, 2012
This Certificate is valid as of: June 14, 2009
Certified for the first time: June 14, 2000

H. Pierre Sallé

H. Pierre Sallé
President
KEMA-Registered Quality

The method of operation for quality certification is defined in the KEMA General Terms And Conditions For Quality And Environmental Management Systems Certifications. Integral publication of this certificate is allowed.

Experience you can trust.

K2
Media Platform

System Guide

Software Version 7.2

QuickTime

Revision Status

Rev Date	Description
November 2005 – July 2007	Initial release and revisions for 3.1 and 3.2 releases — 071-8460-00, 071-8460-02, 071-8460-03
September 7, 2007	Revised information for direct-connect storage, teaming, HotBins, software version 3.2.5 — 071-8460-03
January 11, 2008	Added information for capture services and Type II motherboard — 071-8460-04
July 28, 2008	Added information for software version 3.2.7, XML Import capture service, ancillary/data track specs ,MIBs — 071-8460-05
March 20, 2009	Version for K2 Summit Client, removed K2 Media Client-specific information — 86231160
October 27, 2009	Added K2 Solo Media Server, MPEG-2, AVC-Intra and other information for software version 7.1 — 071-8726-00
April 7, 2010	Added ChannelFlex Suite features, K2 Transmission, and other information for software version 7.2 — 071-8726-01

Contents

Contents

Contents

Contents

Finding Information

This manual describes K2™ systems and provides the information you need to go beyond factory default settings and customize your system's configuration to meet your site-specific needs. The manual covers K2 Summit™ Production Client, K2 Solo™ Media Server, including ChannelFlex™ Suite features, and K2 SAN devices.

How this manual is organized

This manual is organized around the tasks required to install and configure K2 systems. The following chapters are included in this manual:

Chapter 1, *Product Description*

Chapter 2, *Using K2 system tools*

Chapter 3, *System connections and configuration*

Chapter 4, *Managing Stand-alone Storage*

Chapter 6, *Managing K2 system software*

Chapter 7, *Administering and maintaining the K2 system*

Chapter 8, *Direct Connect Storage*

Chapter 9, *K2 Summit Transmission Server Package*

Appendix A, *Remote control protocols*

Appendix B, *Specifications*

Appendix C, *Connector Pinouts*

Appendix D, *Rack mounting*

Getting more information

The following sections help you find the information you need in product manuals and elsewhere.

For the installer of a K2 product with internal storage

If you are installing a K2 client with stand-alone internal storage or a K2 Solo Media Server, refer to documentation in the following sequence:

	Find this document…	In these locations…	In these formats:
1	K2 Release Notes	K2 product shipping box	Printed
		Grass Valley Website	PDF file
2	Quick Start Guide for the K2 product	K2 product shipping box	Printed
		K2 Documentation CD	PDF file
		Grass Valley Website	PDF file
3	K2 System Guide	K2 Documentation CD	PDF file
		Grass Valley Website	PDF file

For the installer of a K2 client with direct connect storage

If you are installing a K2 client with stand-alone direct connect storage, refer to documentation in the following sequence:

	Find this document…	In these locations…	In these formats:
1	K2 Release Notes	K2 product shipping box	Printed
		Grass Valley Website	PDF file
2	K2 Storage Cabling Guide	K2 RAID shipping box	Printed
		K2 Documentation CD	PDF file
		Grass Valley Website	PDF file
2	Quick Start Guide for the K2 product	K2 product shipping box	Printed
		K2 Documentation CD	PDF file
		Grass Valley Website	PDF file
3	K2 System Guide	K2 Documentation CD	PDF file
		Grass Valley Website	PDF file

For the installer of K2 clients and K2 SAN shared storage

If you are installing a K2 SAN with connected K2 clients, refer to documentation in the following sequence:

	Find this document…	In these locations…	In these formats:
1	K2 Release Notes	K2 product shipping box	Printed
		Grass Valley Website	PDF file
2	K2 Storage Cabling Guide	K2 RAID shipping box	Printed
		K2 Documentation CD	PDF file
		Grass Valley Website	PDF file
2	Quick Start Guide for the K2 product	K2 product shipping box	Printed
		K2 Documentation CD	PDF file
		Grass Valley Website	PDF file
3	K2 SAN Installation and Service Manual	K2 Documentation CD	PDF file
		Grass Valley Website	PDF file
3	K2 System Guide	K2 Documentation CD	PDF file
		Grass Valley Website	PDF file

Quick Start Guide

You receive this guide in the product packaging with your K2 product. The Quick Start Guide provides step-by-step installation instructions for basic installation and operation of your K2 product, including recording and playing clips.

Release Notes

The K2 Release Notes contain the latest information about the software shipped on your system. The release notes include software upgrade instructions, software specifications and requirements, feature changes from the previous releases, and any known problems. Because release notes contain the latest information, they are printed out and included in the K2 product shipping box, rather than included in the Documentation CD-ROM. You should always check the Grass Valley Website to determine if there is an updated version of release notes available.

K2 Storage Cabling Guide

The cabling guide provides instructions for K2 Storage Area Network cabling and external configuration. The cabling guide provides instructions for each pre-defined level of K2 SAN and covers both redundant and basic (non-redundant) systems. You can find the cabling guide packaged with the primary RAID storage chassis.

Documentation CD

Except for the release notes, the full set of support documentation, including this manual, is available on the K2 Documentation CD-ROM that you received with your K2 product.

The K2 Documentation CD includes the following 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 K2 product.

- **K2 System Guide** — Contains the product specifications and instructions for modifying system settings.

- **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** — Contains diagrams for cabling the devices of the K2 Summit Production Client.

- **RAID Instruction Manuals** — There is an Instruction Manual for each type of RAID storage device that can be a part of a K2 Summit Production Client. These manuals contain procedures for configuring and servicing the device.

- **Fibre Channel Switch Installation Manual** — Contains information on configuring and servicing the Fibre Channel switch.

On-line Help Systems

K2 AppCenter Help — In the AppCenter user interface menu bar select **Help,** then choose **AppCenter Help Topics** from the drop-down menu.

SiteConfig Help — In the SiteConfig user interface menu bar select **Help,** then choose **SiteConfig Help Topics** from the drop-down menu.

NetCentral Help — From the NetCentral interface select **Help | NetCentral Help Topics**.

NetCentral documentation

The NetCentral product has its own documentation set, described as follows:

- **NetCentral Quick Start Guide** — Provides an overview of the installation process to quickly set up and run NetCentral.

- **NetCentral Installation Guide** — Identifies requirements and procedures to correctly set up servers and devices, as well as provides detailed instructions to install and configure NetCentral software.

- **NetCentral User Guide** — Describes how to use the NetCentral Manager to monitor devices.

- **NetCentral Help** — From the NetCentral interface access on-line help. Select **Help | NetCentral Help Topics**.

Grass Valley Web Site

This public Web site contains all the latest manuals and documentation, and additional support information. Use the following URL.

http://www.grassvalley.com.

Grass Valley Product Support

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

Web Technical Support

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

World Wide Web:http://www.grassvalley.com/support/

Technical Support E-mail Address:gvgtechsupport@grassvalley.com

Telephone Support

Use the following information to contact Product Support by phone.

International Support Centers

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

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

Authorized Local Support Representative

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

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

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

Region	County	Telephone
Asia	China	+86 10 5883 7575
	Hong Kong, Taiwan, Korea, Macau	+852 2531 3058
	Japan	+81 3 6848 5561
	Southeast Asia - Malaysia	+603 7492 3303
	Southeast Asia - Singapore	+65 6379 1313
	India	+91 22 676 10300
Pacific	Australia	1 300 721 495
	New Zealand	0800 846 676
	For callers outside Australia or New Zealand	+61 3 8540 3650
Central America, South America	All	+55 11 5509 3440
North America	North America, Mexico, Caribbean	+1 800 547 8949; +1 530 478 4148
Europe	UK, Ireland, Israel	+44 118 923 0499
	Benelux – Netherlands	+31 (0) 35 62 38 421
	Benelux – Belgium	+32 (0) 2 334 90 30
	France	+800 80 80 20 20; +33 1 48 25 20 20
	Germany, Austria, Eastern Europe	+49 6150 104 444
	Belarus, Russia, Tadzhikistan, Ukraine, Uzbekistan	+7 095 258 09 20; +33 (0) 2 334 90 30
	Nordics (Norway, Sweden, Finland, Denmark, Iceland)	+45 40 47 22 37; +32 2 333 00 02
	Southern Europe – Italy	Rome: +39 06 87 20 35 28 ; +39 06 8720 35 42. Milan: +39 02 48 41 46 58
	Southern Europe – Spain	+34 91 512 03 50
	Switzerland	+41 56 299 36 32
Middle East, Near East, Africa	Middle East	+971 4 299 64 40
	Near East and Africa	+800 80 80 20 20; +33 1 48 25 20 20

Waste Electrical and Electronic Equipment Directive

Chapter **1**

Product Description

The K2™ Summit™ Production Client and K2 Solo™ Media Server are cost-effective Broadcast Enterprise Servers that incorporate IT server platform and storage technologies to deliver a networked solution to facilities for ingest, playout, news integration, sports, and media asset management. They provides a suite of user applications and system tools. The manual contains information for all models and options, including ChanneFlex™ Suite. Refer to the sections that apply to your particular model and options.

Control Point PC

K2 Summit Production Clients, K2 Media Clients, and K2 Solo Media Servers

Communication over Ethernet network

Operation, configuration, and monitoring from a remote location
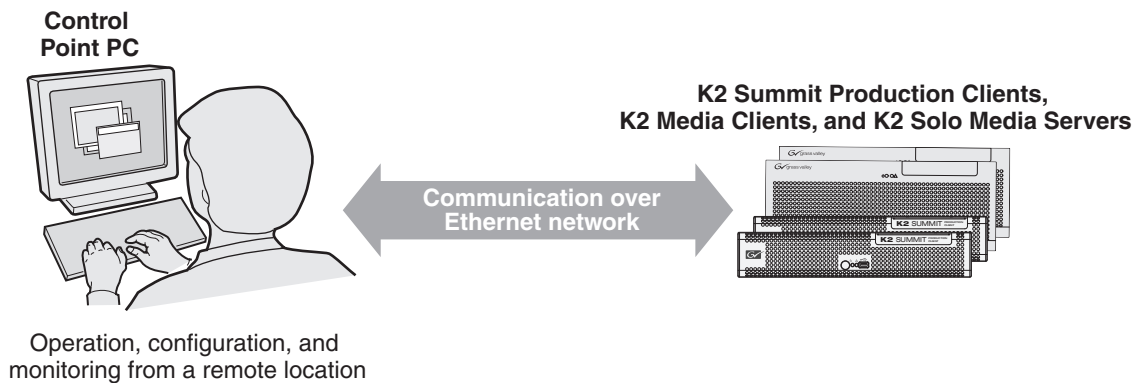
The K2 Summit Production Client and K2 Solo Media Server are designed for "headless" operation from a remote control point using Grass Valley Control Point software. You can also use the Microsoft Windows Remote Desktop Connection application on your PC to connect to the K2 system for configuration or administration.

The K2 Summit Production Client and K2 Solo Media Server products are further described in the following sections:

- "K2 Summit Production Client and K2 Solo Media Server features" on page 20
- "Product identification" on page 22
- "Front panel indicators" on page 23
- "Rear panel view" on page 24
- "K2 Summit Production Client and K2 Solo Media Server system overview" on page 27

Also refer to Chapter 9, *K2 Summit Transmission Server Package* for information unique to that product.

K2 Summit Production Client and K2 Solo Media Server features

The following features apply to the K2 Summit Production Client:

- Two or four channels per chassis

- SDI video inputs and outputs

- AES/EBU or embedded audio inputs and outputs.

- Redundant power supply, cooling fans for reliability

- System drive — compact flash protected by a file-based write filter

- RAID media storage

- Remote operation and configuration via AppCenter

- NetCentral™ provides remote error reporting and monitoring via SNMP (Optional for models using local storage only)

- 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

The following features apply to the K2 Solo Media Server:

- Two channels per chassis

- SDI video inputs and outputs

- AES/EBU or embedded audio inputs and outputs.

- System drive — compact flash protected by a file-based write filter

- RAID 0 media storage

- Remote operation and configuration via AppCenter

- NetCentral™ provides remote error reporting and monitoring via SNMP (Optional for models using local storage only)

- 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

The K2 Summit Production Client and K2 Solo Media Server have bi-directional video codecs, which means each channel supports both record and play operations. You can encode and decode video using the DVCPRO HD, DVCPRO 25/50, or DVcompression standards. You can also decode MPEG-2. Options include MPEG-2 encode and AVC-Intra encode/decode. All channels support Standard Definition (SD) video and, if licensed, each pair of channels can also support High Definition (HD) video. For more information on available codecs, see "Operational specifications" on page 198.

You can play a sequence of clips of different compression standards and, if licensed, HD and SD formats back-to-back on the same timeline with no channel configuration changes. Both HD and SD clips are played out in the format specified for the output assigned to the channel. All clips are either up- or down-converted appropriately to play on that output, and their aspect ratios are adjusted.

For the K2 Summit Production Client, stand-alone internal storage, stand-alone external direct-connect storage, and external shared (SAN) storage models are available.

Features of internal storage models

An internal storage K2 Summit Production Client can have eight media drives. A K2 Solo Media Server has two media drives. Compact Flash serves as the system drive. 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 the ExpressCard.

Features of external storage models

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

• Shared storage — Multiple external storage K2 Summit Production Clients 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 Production Client 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 Production Client a self-contained, stand-alone unit, with no external (non-shared) devices for storage, audio, or video connections required. You can transfer media in and out of the direct-connect K2 Summit Production Client via Gigabit Ethernet.

Product identification

The K2 Summit Production Client has labels affixed to the chassis that provide product identification as in the following diagram:

Serial Number
(e.g. K2—01AA00010)
This is also the factory
default hostname

USB compartment
(Compartment swivels up.)
Note: removing the bezel takes
the fans offline. Replace the bezel assembly
within one minute to maintain system cooling.
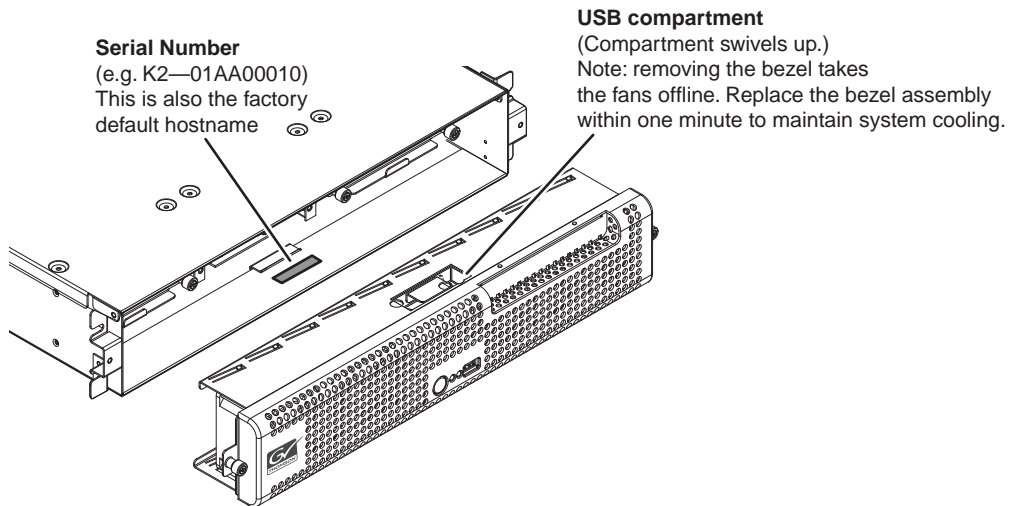
The K2 Solo Media Server has labels affixed to the chassis that provide product identification as in the following diagram:

Serial Number
(e.g. K2—01AA00010)
This is also the factory
default hostname
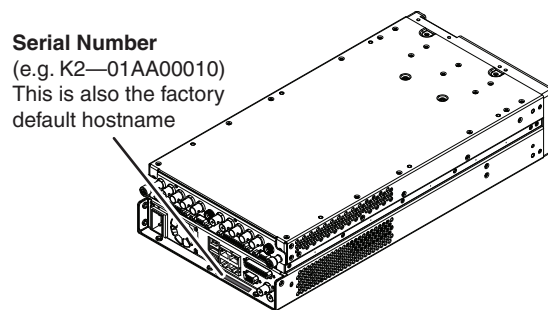
Front panel indicators

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.
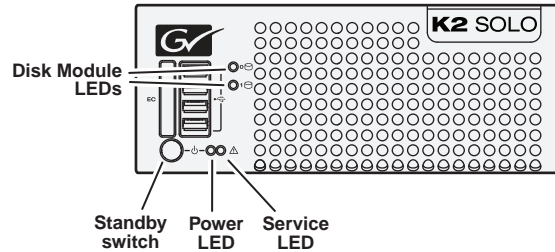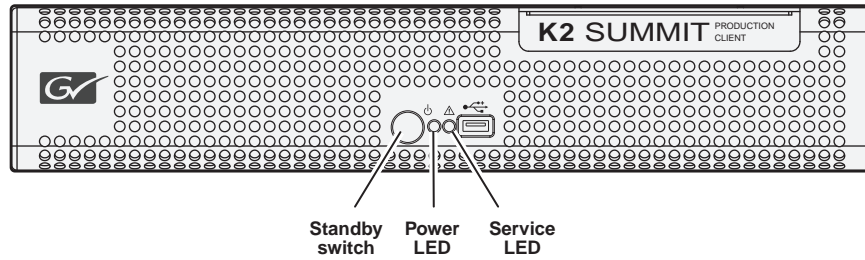
Rear panel view

The following drawings identify the rear panel connectors and components.

K2 Summit Production Client rear panel

SDI video in and out supports embedded audio.

SDI in [a]   Channel Flex [a]   SDI out [a]   SDI monitor out. [a, b]

LTC in/out

AES audio
(connect via optional
multi-connector cable)

RS-422

Channel 1   Channel 2   Channel 3   Channel 4

Power   Optional Fibre Channel
card for connection to
direct-connect storage
or shared (SAN) storage

IEEE
1394
(Do not
use)

USB
(keyboard,
mouse)

VGA
monitor

Reference
Loop Thru [c]

GPI   Power

Port 2: Media (iSCSI) A
Media Connection #1

Port 2: FTP/Streaming
Media Connection #1

Port 3: Media (iSCSI) B
for redundant SAN
Media Connection #2

Stand-alone direct-connect
or internal storage

Shared (SAN)
storage

Port 1: Control
Control Connection #1 [d]

Port 4: Control
(Optional)
Control Connection #2 [d]

Port 1: Control A
Control Connection #1 [d]

Port 4: Control B
for redundant SAN
Control Connection #2 [d]

[a] Supports
Channel Flex Suite,
which requires
AppCenter
Elite license

[b] Supports Super Out,
which requires
AppCenter Pro or
Elite license

[c] Tri-level sync
not supported

[d] Control Connections are teamed
and share the same IP address

K2 Solo Media Server rear panel

SDI video in and out supports embedded audio.

SDI in [a]   Channel Flex [a]   SDI out [a]   SDI monitor out. [a, b]

LTC in/out

AES audio
(connect via optional
multi-connector cable)

RS-422

Channel 1   Channel 2

Power   IEEE 1394 (Do not use)   USB (keyboard, mouse)   VGA monitor   Reference Loop Thru [c]   GPI

Port 2: FTP/Streaming
Media Connection #1

Port 1: Control
Control Connection #1 [d]

Port 4: Control (Optional)
Control Connection #2 [d]

[a] Supports Channel Flex Suite, which requires AppCenter Elite license

[b] Supports Super Out, which requires AppCenter Pro or Elite license

[c] Tri-level sync not supported

[d] Control Connections are teamed and share the same IP address

ChannelFlex Suite 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:

Multi-Cam Recorder

Video 1   Video 2

Super Slo-Mo Recorder

Phase 1   Phase 2   Phase 3

3D/Video + Key Recorder

Video or   Key or
Left eye   Right eye

3D/Video + Key Player

Video or   Key or
Left eye   Right eye
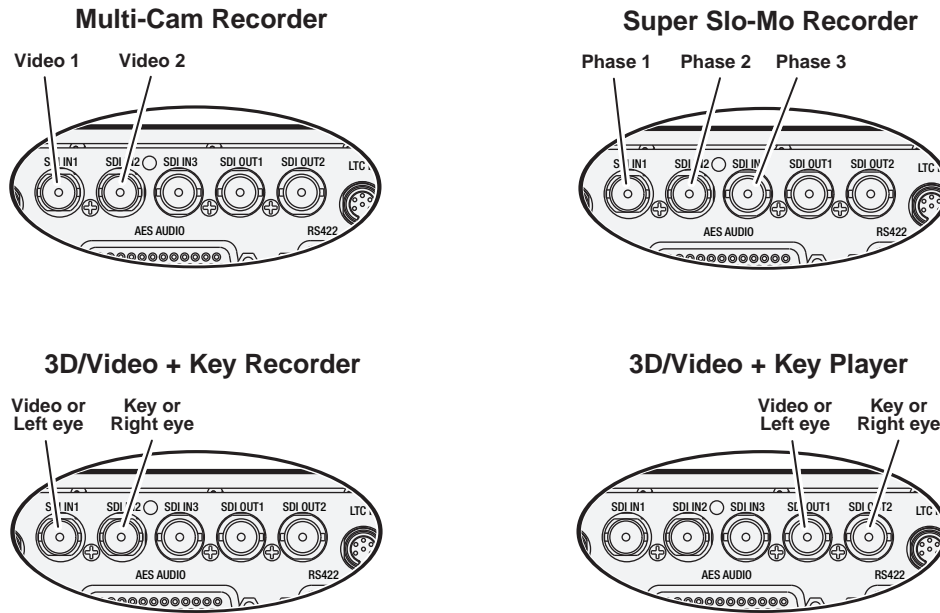
Refer to the *K2 AppCenter User Manual* for more information on ChannelFlex Suite features.

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.

The following are examples of the EULAs that you might see.

On a K2 Media Server, at first startup the following behavior occurs:

• A Windows Server 2003 End User License Agreement (EULA) opens on the screen.

K2 Summit Production Client and K2 Solo Media Server system overview

The K2 Summit Production Client and K2 Solo Media Server 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 XP 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:

The **Application system** is 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.

The **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.

The **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 sections. Also refer to Appendix A, *Remote control protocols* for information regarding E to E commands.

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 SD-00 K2 Media Client, the HD-00 K2 Media Client, 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 (K2 Summit Production Client, K2 Solo Media Server, or SD-00 K2 Media Client)

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, or SD-00 K2 Media Client, 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, such as that on the SDA-00 K2 Media Client. True E to E is not supported on theK2 Summit/Solo or SD-00 K2 Media Client.

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:

Port #	Type of connection	Service name	Description
20	TCP	Can be mpgsession.exe, mxfsession.exe, gxfsession.exe, or ftpd.exe	FTP
21	TCP	ftpd.exe	FTP data
161	UDP	snmp.exe	SNMP
162	UDP	snmptrap.exe	SNMP trap
3389	TCP	Remote Desktop	Used by SiteConfig.
3811	TCP	Grass Valley AppService	Used by 3rd party applications to communicate using AMP protocol
18262	TCP	GV ProductFrame Configuration Service, ProductFrame Discovery Agent Service	Used by SiteConfig.
18263	UDP	ProductFrame Discovery Agent Service	GV NetConfig Device Broadcast/Unicast Protocol. Used by SiteConfig. Sent by ControlPoint, received by Devices
18264	UDP	ProductFrame Discovery Agent Service	GV NetConfig Controller Protocol. Used by SiteConfig. Sent by Devices, received by ControlPoint
49168	HTTP	Grass Valley K2 Config	K2 System Configuration application connection between a control point PC and the K2 system device configured. Both HTTP and TCP connections are required. Most functions use the HTTP connection, but a few functions that require longer time periods use TCP.
49169	TCP		
49170	HTTP	Grass Valley Transfer Queue Service	Transfer Manager connection between source system and destination system.
49171	TCP	Grass Valley AppService	AppCenter connection for connection between control point PC and K2 client/Solo.
49172	HTTP	Grass Valley Storage Utility Host	Connection for Storage Utility between the control point PC and the K2 system being configured.

RAID drive numbering

In the K2 Summit Production Client, 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.

Disk2	Disk4	Disk7
Disk1	Disk3	Disk6
Disk0		Disk5

Drive numbering	Explanation
Disk0	When configured as RAID 1, these two RAID drives make up LUN 0.
Disk1	
Disk2	When configured as RAID 1, these two RAID drives make up LUN 1.
Disk3	
Disk4	When configured as RAID 1, these two RAID drives make up LUN 2.
Disk5	
Disk6	When configured as RAID 1, these two RAID drives make up LUN 3.
Disk7	

In the K2 Solo Media Server, internal RAID drives are numbered as follows:

Disk0
Disk1

NOTE: K2 Solo Media Server 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.

Chapter **2**

Using K2 system tools

Topics in this chapter include the following:

- "Configuration Manager"
- "K2 System Configuration"
- "Storage Utility"
- "NetCentral"
- "Windows Remote Desktop Connection"
- "SiteConfig — a ProductFrame application"

Configuration Manager

The Configuration Manager is the primary configuration tool for a K2 Summit Production Client or K2 Solo Media Server. It makes settings that apply to the overall internal storage K2 system as well as settings that apply to individual channels.

Configuration Manager settings are stored in a database. When the K2 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 Summit Production Client or K2 Solo Media Server.

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.

For Configuration Manager procedures, refer to the *K2 AppCenter User Manual*.

Accessing Configuration Manager

You access Configuration Manager through AppCenter from the local K2 Summit Production Client, K2 Solo Media Server, or 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 *DefaultConfig.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.

To restore all settings at once to their default values:

1. If you want to save current settings you should work through the previous procedure "Saving and restoring Configuration Manager settings" 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.

K2 System Configuration

The K2 System Configuration application (K2Config) is the primary tool for configuring the K2 SAN software. 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 K2 System Configuration application. When you use SiteConfig for network configuration, you can import the SiteConfig system description file into K2Config to get you started with your SAN configuration.

After your K2 SAN is initially installed and configured, as instructed in the installation and configuration chapters in the *K2 SAN Installation and Service Manual*, if you need to reconfigure the system you should do so using SiteConfig and the K2 System Configuration 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 K2 System Configuration 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:

- K2 client and K2 Media Server — These devices are configured directly by the K2 System Configuration application.

- K2 RAID storage devices — The K2 System Configuration 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 K2 System Configuration application can launch a switch's web-based configuration application.

To open the K2 System Configuration application do the following:

1. On the control point PC open the K2 System Configuration application shortcut on the desktop. The K2 System Configuration application log in dialog box opens.

2. Log in using the designated administrator account for configuring K2 SAN devices. By default this account is as follows:

    Username: Administrator

    Password: adminK2

3. The K2 System Configuration application opens.

When you select a K2 storage system, device, or subsystem in the tree view...

Toolbar buttons are displayed according to operations available...

And related information and configuration controls appear.
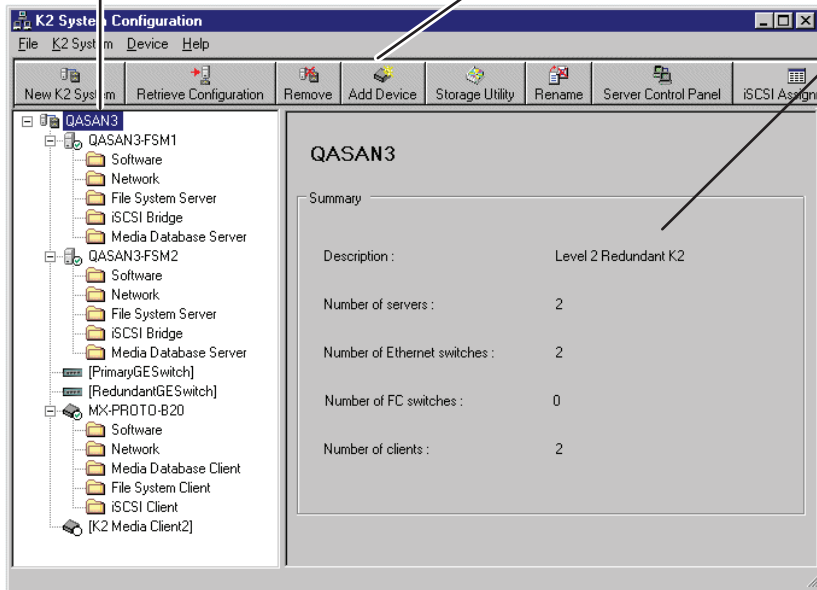
If you have one or more K2 SANs currently configured, the K2 System Configuration application displays the systems in the tree view.

If you have not yet configured a K2 SAN, the K2 System Configuration application opens with the tree view blank. Refer to the installation and configuration chapters in the *K2 SAN Installation and Service Manual* to add and configure a new K2 SAN.

You can expand and select nodes in the tree view to view K2 SANs, individual devices, and configuration settings. When you do so, the K2 System Configuration 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. The configuration file is updated and saved whenever you change a configuration using the K2 System Configuration application. That is why you must always use the K2 System Configuration application to change settings on the storage system, so the most recently changed configurations will always be stored in the configuration file and displayed.

Storage Utility

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 clients. 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 K2 System Configuration application.

The Storage Utility is your primary access to the media file system, the media database, and the media disks of the K2 Summit Production Client or K2 Solo Media Server for configuration, maintenance, and repair. It is launched from AppCenter workstation.

⚠️ **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 Summit Production Client 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.

NetCentral

NetCentral is Grass Valley's monitoring application. The NetCentral server component runs on a NetCentral server PC, which could also be a K2 system control point PC. Devices report status, primarily via Simple Network Management Protocol (SNMP), to NetCentral on the NetCentral server PC.

Refer to NetCentral manuals get the NetCentral system installed and operating. You must install a NetCentral device provider on the NetCentral server PC for each type of device you are monitoring.

NOTE: NetCentral is optional if you are using a stand-alone K2 system only. NetCentral is required if you are using a K2 SAN.

Windows Remote Desktop Connection

You can connect to a K2 client, K2 Solo Media Server, or a K2 Media Server remotely using the Microsoft Windows Remote Desktop Connection application. 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. Also, 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. You can use either the name or the IP address to access the K2 system.

NOTE: Before you can use the Remote Desktop Connection, you need network access and permissions to connect to the K2 system.

To access the Remote Desktop Connection, follow these steps:

1. Click the **Start** button on the Windows task bar

—or—

Press the Windows key   on the keyboard.

2. Select **Programs | Accessories | Communications | Remote Desktop Connection**. The

Remote Desktop dialog box displays.
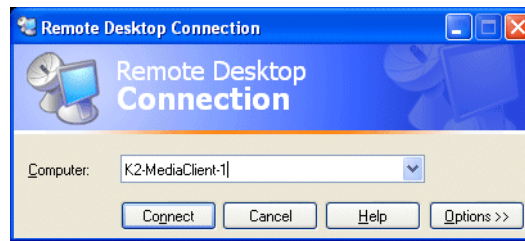
3. Enter the name or IP address of the K2 system and click the **Connect** button. Alternately, you can click the down arrow of the text box and browse for the K2 system or select a previously entered computer.

SiteConfig — a ProductFrame application

ProductFrame is an integrated platform of tools and product distribution processes for system installation and configuration. SiteConfig is a ProductFrame application and it is the recommended tool for network configuration and software deployment.

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 the control point 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 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 factility. This enforces consistent policy and allows SiteConfig to capture changes, which makes the system easier to maintain and aids in troubleshooting should a problem arise.

To open SiteConfig, do the following:

1. On the control point PC open the SiteConfig shortcut on the desktop.

   The SiteConfig application opens.

**Select a
module...**   **And a tree
view tab...**   **Then select an item
in the tree view...**   **To display list
view details...**
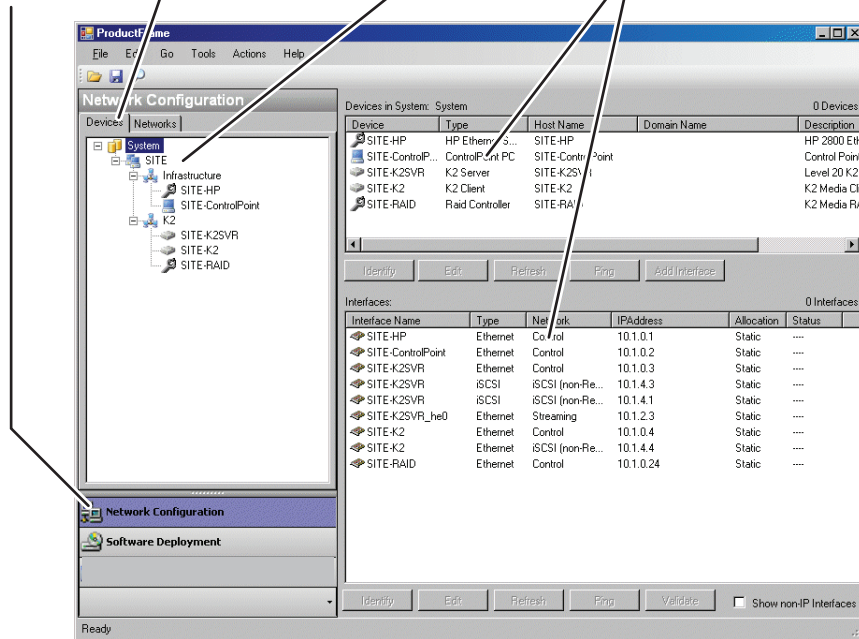
SiteConfig displays information from a system description file, which is an XML file.

SiteConfig has different modules that correspond to a system's life-cycle phases, such as network configuration and software deployment. You can expand nodes and select elements in the tree view and the list view to view and modify networks, systems, individual devices, software deployment, and configuration settings.

Chapter **3**

System connections and configuration

This chapter contains the following topics:

- "About networks"
- "Network connections"
- "Network configuration"
- "Using FTP for file transfer"
- "Using the HotBin service"
- "Using the Pathfire capture service"
- "Using the DG capture service"
- "Using the XML Import capture service"
- "Licensing K2 capture service software"
- "Pinnacle support"
- "Compressed VBI import"
- "Quicktime and Final Cut Pro support"
- "Connecting RS-422"
- "Connecting GPI"

Also refer to Chapter 9, *K2 Summit Transmission Server Package* for information unique to that product.

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 must be on a different subnet than the streaming/FTP network and the Media (iSCSI) network. 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. It must be on a different subnet than the control network and the Media (iSCSI) network. 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 host file with the *_heo* 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 connections

Use the information in this section as appropriate to connect the Gigabit (1GBaseT) Ethernet network for your application:

- "Cable requirements"

- "About network ports"

- "Making network connections"

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.
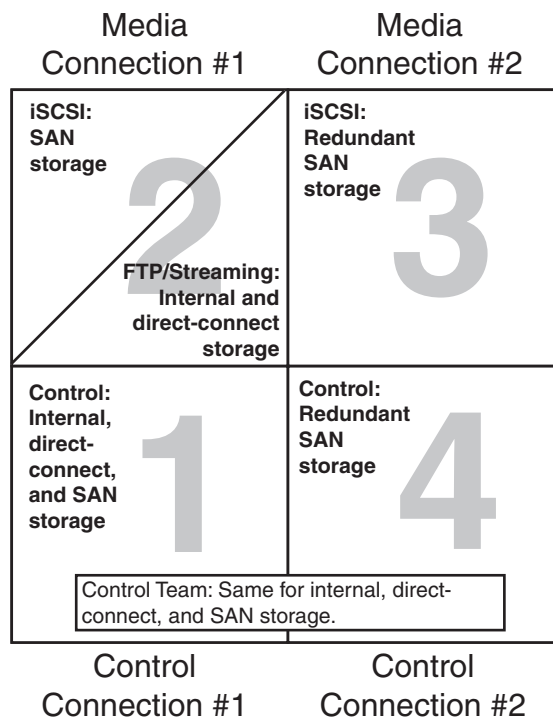
The K2 Solo Media Server is not supported for SAN (shared storage) connection.

Making network connections

Connect network ports as appropriate for the K2 Summit Production Client or K2 Solo Media Server storage option, as follows:

Stand-alone storage K2 Summit/Solo network connections
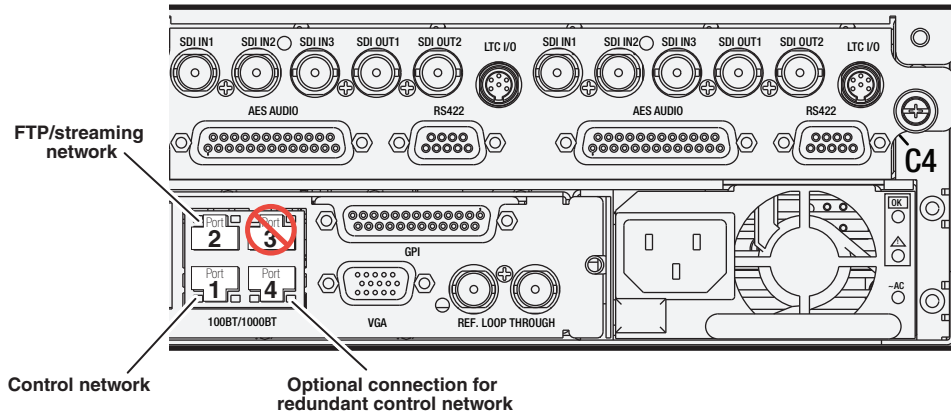
On a K2 Solo Media Server, an internal storage K2 Summit Production Client, or a direct-connect storage K2 Summit Production Client, connect the control network to port 1, which is the first port of the control team. If you have a FTP/streaming network, it is connected to port 2. Port 3 is not used. 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 Production Client network connections
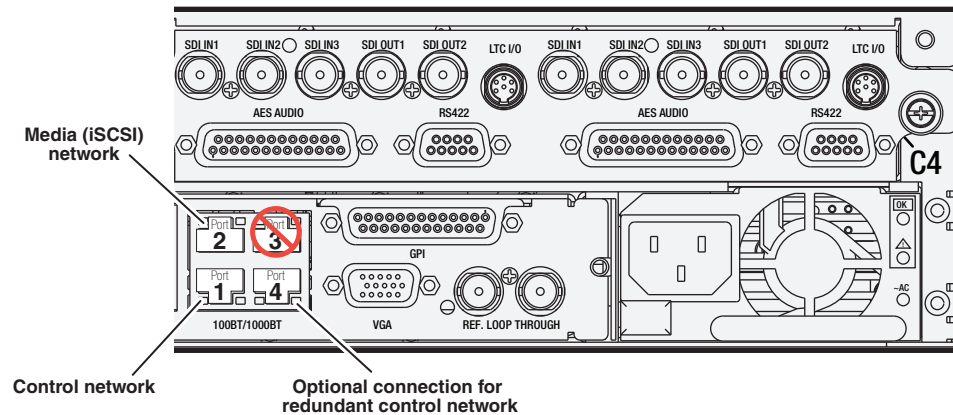
On a non-redundant shared storage (SAN) K2 Summit Production Client, connect the control network to port 1, which is the first port of the control team. Port 2 must be connected to the media (iSCSI) network. Port 3 is not used. Port 4, which is the second port of the control team, is not used except 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 the *K2 SAN Installation and Service Manual* for more information.

Redundant shared storage (SAN) K2 Summit Production Client network connections
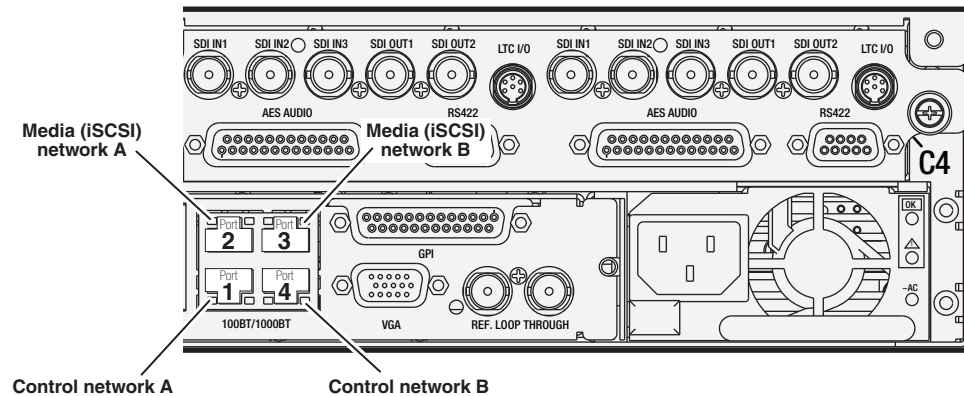
On a redundant shared storage (SAN) K2 Summit Production Client, you must connect both ports of the control team. Connect control network connection A to port 1 and control network connection B to port 4. You must also connect both media ports. Connect port 2 to the A media network and port 3 to the B media network. The media ports must not be teamed, as doing so interferes with failover functionality.

Refer to the *K2 SAN Installation and Service Manual* for more information.

Network configuration

This section contains instructions for configuring network connections as follows:

- "About network functionality"
- "About modifying or restoring network settings"
- "Configure network settings for a stand-alone K2 systems"
- "Streaming video between K2 systems"

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:

- Write filter — The K2 system has a write filter that must be disabled before making a network configuration change. Refer to "About the write filter" on page 155.

- 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 you model of K2 client.

  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.)

- 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 *K2 Summit Product Client Service Manual* for recovery image and network configuration procedures.

Configure network settings for a stand-alone K2 systems

⚠ **CAUTION: The K2 system is not a general purpose Windows workstation. The Windows configuration on the K2 system has been specifically set for use as a real-time device. To avoid partial or total system failure, do not modify any operating system settings unless approved by Grass Valley, including but not limited to the following:**
— Do not use the User Manager
— Do not use the Disk Administrator
— Do not load any third party software
— Do not install Windows updates

The internal storage internal storage K2 system and the direct-connect K2 Summit Production Client 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 for the stand-alone internal storage K2 system need to be configured, you must have Windows administrator security privileges on the K2 system.

To configure network settings on a stand-alone internal storage K2 system, do the following:

1. If you have not already done so, disable the write filter. Refer to "Disabling the write filter" on page 156.

2. 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.

3. Open the Network Connections dialog box:

   • In the Windows Classic view, select **Start | Settings | Network Connections**

   • In the Windows XP view, select **Start | Control Panel | Network Connections**

4. 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.

5. Configure the control connection on the stand-alone internal storage K2 system as follows:

   • 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.*

6. Configure the FTP/streaming connection (if needed) on the stand-alone internal storage 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:

   • Configure the network connection with the following name:

Media Connection #1

This is GigE port 2 on the rear panel.

7. If prompted, shutdown and restart Windows.

8. If you are going to FTP/stream video between K2 systems, proceed to "Streaming video between K2 systems"; otherwise, the K2 system is ready for standard data networking tasks.

9. Enable the write filter. Refer to "Enabling the write filter" on page 156.

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 must either reference host names through hosts files located on each networked device or edit the DNS entries. To edit the DNS entries, see your network administrator. To set up host files, see "Set up hosts files" on page 48.

• 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.

To see an example, refer to the "Sample K2 client configuration and hosts file" on page 50. Otherwise, proceed with the following steps to set up your hosts file.

On each K2 system, set up the hosts file as follows:

1. If you have not already done so, disable the write filter. Refer to "Disabling the write filter" on page 156.

2. Open the following file using Notepad or some other text editor.

   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. Remember to disable the write filter on all K2 Summit Production Clients.

8. Enable the write filter. Refer to "Enabling the write filter" on page 156.

9. Proceed to "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.
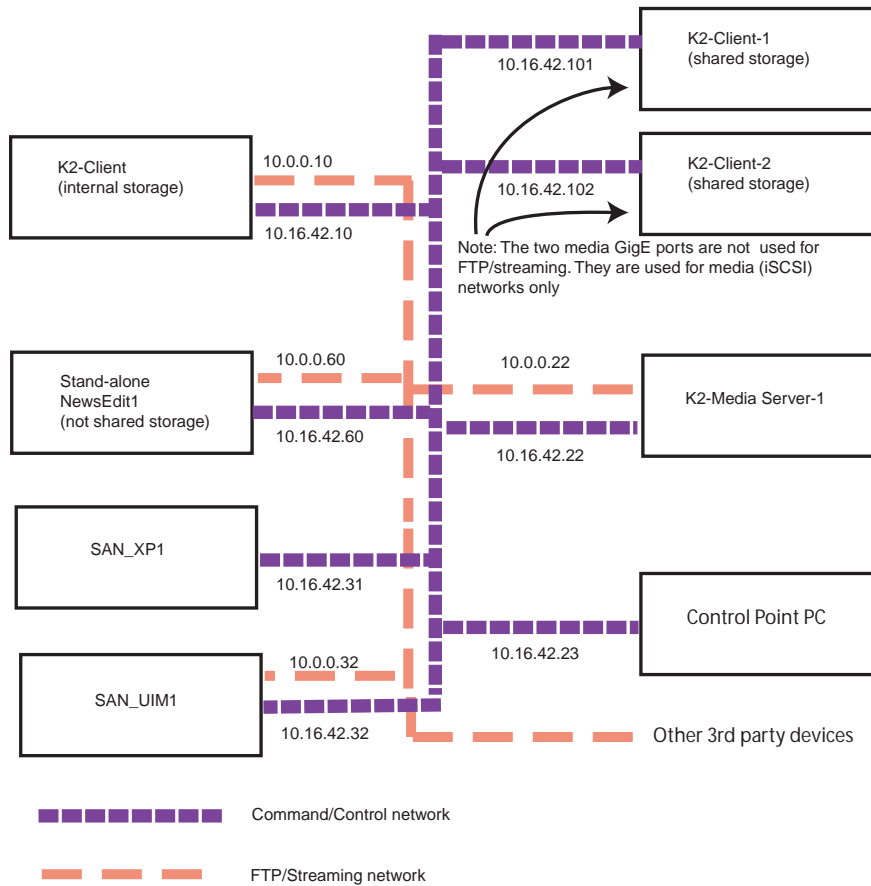
The following example shows the contents of a default Windows hosts file with new lines added that match the IP addresses and host names in the previous sample diagram.

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

127.0.0.1localhost

10.16.42.10K2-Client

10.0.0.10K2-Client_he0

10.16.42.101K2-Client-1
10.16.42.102K2-Client-2

10.16.42.22K2-MediaServer-1
10.0.0.22K2-MediaServer-1_he0

10.16.42.23ControlPointPC

10.16.42.60NewsEdit1
10.0.0.60NewsEdit1_he0

10.16.42.31SAN_XP1
10.0.0.32SAN_XP1_he0 SAN_UIM1_he0
10.16.42.32SAN_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 computer name. To determine the K2 system computer name, right-click K2 Client or K2 Media Server (My Computer) on the Windows desktop, then properties. Select the Network Identification tab and look for the "Full computer name".

To add network host names:

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.
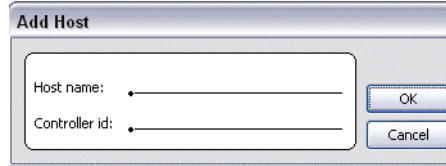
b. If you are using VDCP remote protocol to perform video network transfers, use the following steps to add a unique Controller ID for each host. Otherwise, you can ignore this step and proceed to the next step.

- 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 Appendix B, *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.*

Using FTP for file transfer

This section includes the following topics:

"About the K2 FTP interface"

"Limitations with complex media types"

"Transferring between different types of systems"

"Transfer mechanisms"

"FTP access and configuration"

"FTP access by automation"

"FTP security"

"FTP internationalization"

"FTP access by Internet Explorer"

"Using FTP on a K2 Nearline SAN"

About the K2 FTP interface

An application writer may choose to initiate media file transfers via FTP. The K2 FTP interface has a GXF folder and an MXF folder. Use the appropriate folder, depending on if you are transferring GXF or MXF. Refer to "FTP access by Internet Explorer" on page 56 for examples.

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. Refer to "Configuring K2 security" on page 158.

NOTE: 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 made from lists that contain movies with mixed video compression types or mixed audio types cannot stream to other devices, nor can they be exported to a file. Refer to release notes for the specific software versions for details.

- MXF OP1A supports transfer of simple media types only, which are a subset of the K2 encode/decode/metadata capabilities. For example, MXF OP1A does not support the transfer of complex clips, such as a subclip that spans two media files. Do not attempt MXF OP1A transfers of complex clips.

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.

If using remote control protocols to initiate transfers, refer to Appendix A, *Remote control protocols*.

Also refer to "Specifications" on page 189.

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. For example, 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. For more information, refer to "FTP access by automation" on page 54.

    - 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. For more information, refer to Appendix A, *Remote control protocols*.

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 security

Refer to "FTP and media access security" on page 163.

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" on page 214.

The Microsoft FTP client does not convert from a Unicode string to a UTF-8 string. Instead, it passes the Unicode string to the FTP server directly, 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.

To make this language setting, do the following:

1. If you have not already done so, disable the write filter. Refer to "Disabling the write filter" on page 156.

2. Open the **Regional and Language Options** control panel.
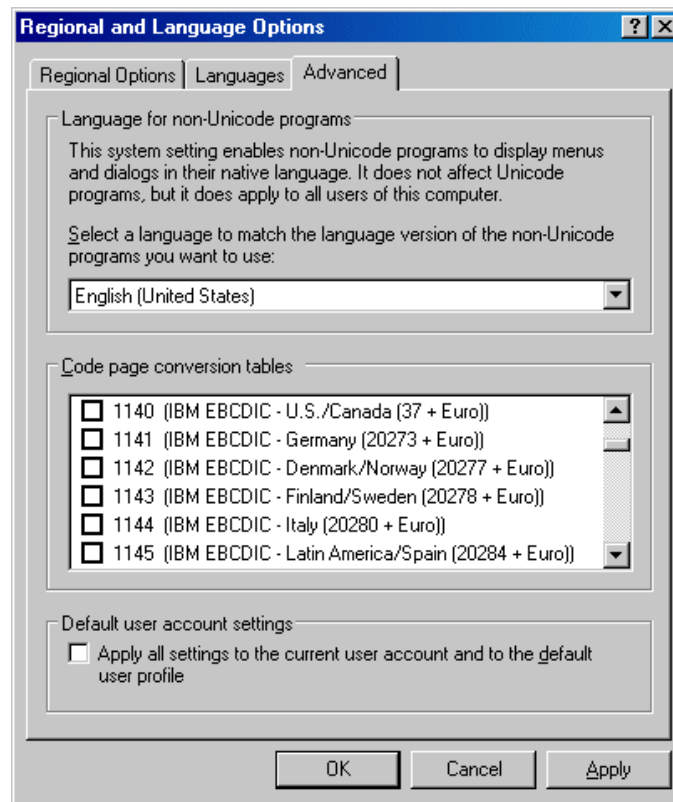
3. On the **Advanced** tab for the "Language for non-Unicode programs" setting, select **English (United States)**.

4. Click **Apply** and **OK**, and when prompted restart the computer to put the change into effect.

5. Enable the write filter. Refer to "Enabling the write filter" on page 156.

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. Also refer to "FTP and media access security" on page 163 for information about accounts and FTP access. 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.
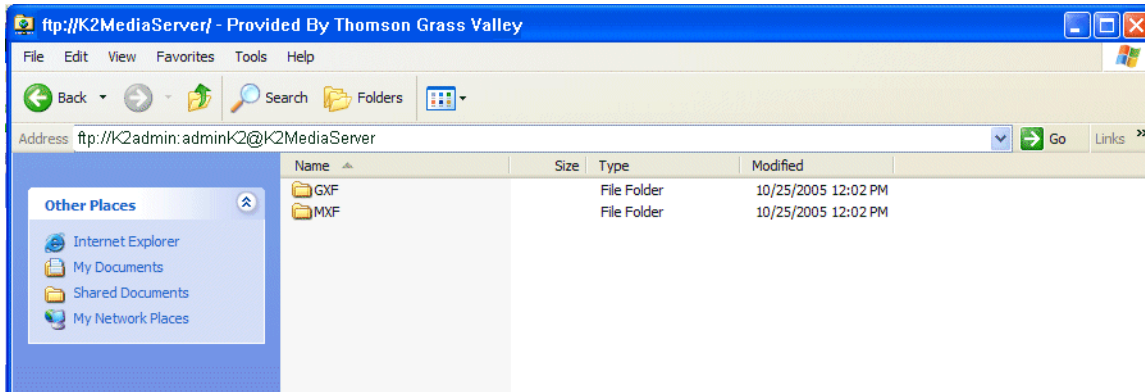
GXF — General Exchange Format (SMPTE 360M). This is the standard Grass Valley file interchange format. Refer to specifications later in this manual for media types supported.

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.
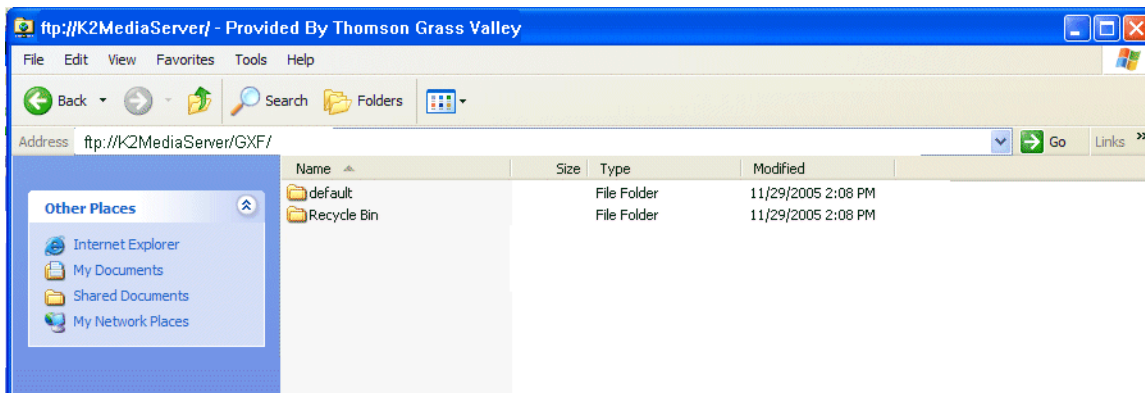
The subfolders are organized in typical Windows fashion, with columns denoting the file's name, size, etc. The Size column refers to the clip duration (in video fields).
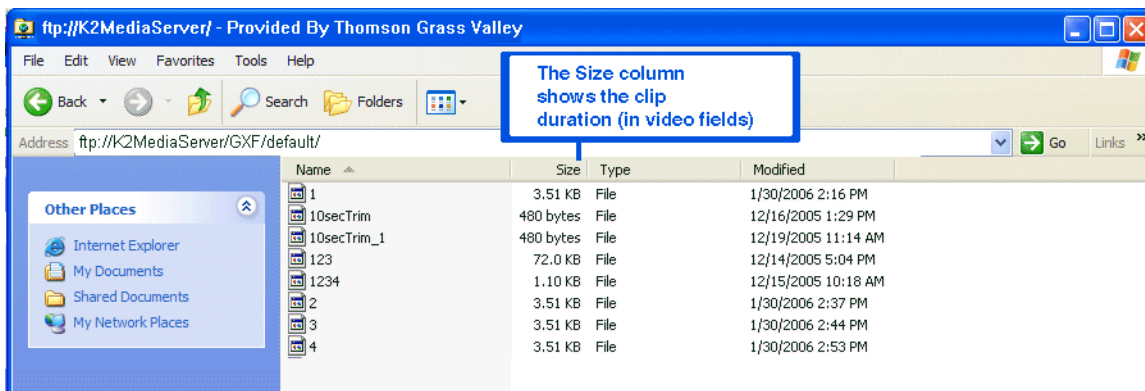
You can use Internet Explorer to drag a file from your stand-alone K2 system or K2 Media Server and drop it in a folder on your PC. You can also drag a file from your PC and drop it in the appropriate folder on your stand-alone K2 system or K2 Media Server.

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
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 size in number of video fields.
NLST	Name List	Supported
SITE	Site Parameters	Supported
SYST	System	Supported
SIZE	Size of file (clip)	Supported. Reports size in Bytes.

FTP command name	FTP command description	K2 FTP support
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. 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.

- K2 media must be transferred to/from the Nearline system as a GXF or MXF file.

- 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 does not have GXF and MXF folders to support format-specific functionality, as does the K2 FTP interface 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 the HotBin service

The following sections provide information for the K2 HotBin service.

- "About the HotBin service"
- "Prerequisite for using the HotBin service"
- "Configuring the HotBin service"
- "HotBin service components"

About the HotBin 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, as specified in "Specifications" on page 189.

By default, the HotBin service does not start automatically. If you have never configured or used the HotBin service, the service (Grass Valley Import Service) is set to startup type Manual. When you configure the HotBin 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.

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.

Prerequisite for using the HotBin service

- K2 system software must be at version 3.2.56 or higher.

Configuring the HotBin service

When configuring the HotBin service, bear in mind the following considerations:

- You must be logged with administrator privileges on the local K2 system as well as having the appropriate security permissions to access the source directory.

- If using the HotBin service on a K2 SAN, the K2 Capture Services utility must be on a K2 server that is also an FTP server. If your K2 SAN has multiple FTP servers, the utility must be on the primary FTP server.

- 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.

- 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 the root of C:\ as the source directory or 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.

- HotBin imports are serialized. For example, if fourteen items are already queued up from ordinary transfers, and you drop a clip into the HotBin, the HotBin clip will get transferred as the fifteenth clip in the transfer queue. Unlike the normal transfer process, the HotBin service does not queue the second clip until the first clip is imported.

Grass Valley recommends that you use the HotBin service as demonstrated in the following diagram.

Using the HotBin service with an internal storage (Stand-alone) or D

❶

On the K2 system,
make the
source directory
a shared folder.

Source directory
Destination bin

K2 system (stand-alone)

❷

On your system,
map a drive
to the shared folder.

Mapped drive

❸

Transfer media files
from your system to the shared folder
on the mapped drive.

❹

The HotBin service
automatically
imports files to the
destination bin
on the K2 system.

Using the HotBin service with a K2 SAN

❶

On the K2 Media Server,
make the
source directory
a shared folder.
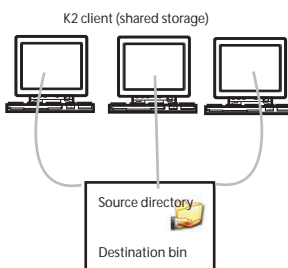
K2 client (shared storage)

Source directory
Destination bin

K2 Media Server

❷

On your system,
map a drive
to the shared folder.

Mapped drive

❸

Transfer media files
from your system to the shared folder
on the mapped drive.

❹

The HotBin service
automatically
imports files to the
destination bin
on the K2 System.

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**.)

To configure the HotBin service (Grass Valley Import Service), follow these steps:

1. From the **Start** menu, access the **Programs** menu and select **Grass Valley | K2 Capture Services**.

   If the write filter is enabled, a message appears that informs you about the write filter and prompts you to restart.

2. If the write filter is enabled, restart as prompted, then repeat previous steps.

3. The K2 Capture Services utility dialog box is displayed. Click on the HotBin tab.
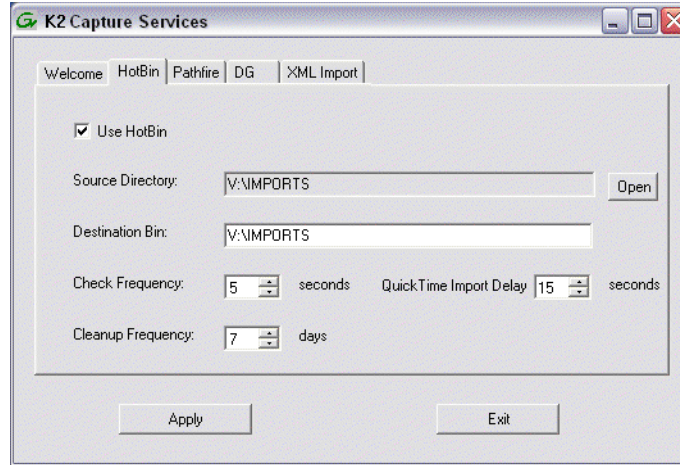
4. Select **Use HotBin**.

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. Specify how often you want the folder checked for new files and the file deletion age for files in the Success and Fail sub-directories.

7. 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.

8. 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.

9. Click **Apply**.

   A message appears that informs you about the write filter and prompts you to restart.

10.Click **OK**.

   The K2 system restarts.

   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.

11. Place files in the source directory to trigger the Hot Bin import processes.

HotBin service components

The following table describes the components of the HotBin service.

Name	Description
HotBin service (Grass Valley Import Service)	The service monitors a watched folder, also known as a source directory, that you specify. Files placed in this watched folder are automatically imported into the K2 system by the HotBin service.
K2 Capture Services utility	Configures the HotBin service
Source directory (HotBin)	The watched folder that you can specify. Files placed in this watched folder are automatically imported to the K2 system. By default, the location of the source directory is V:/IMPORTS.
Check frequency	Determines how often the source directory is checked for new files.
Cleanup frequency	Determines how long a file remains in the Success sub-directory or in the Fail sub-directory. A file with a file-creation date older than the specified number of days is deleted.
Destination bin	The clip bin on the K2 to which files from the source directory are imported. By default, V:/IMPORTS.

Using the Pathfire capture service

The following sections provide information for the K2 Pathfire capture service.

- "Prerequisites for using the Pathfire capture service"
- "Considerations for the Pathfire capture service"
- "Testing the Pathfire capture service"
- "Pathfire capture service components"
- "Installing Pathfire Transfer Service software"
- "Licensing Pathfire Transfer Service software"

About the Pathfire capture service

The K2 Pathfire capture service provides a way to have Pathfire-delivered content automatically imported into a K2 system. The Pathfire capture service has a watched folder. The watched folder is a standard file system directory that can be recognized by the Windows operating system. The K2 system that hosts this directory (the watched folder) appears as a destination in the Pathfire application on the Pathfire system, so you can push the Pathfire-delivered content to the directory using the Pathfire application.

When media files arrive in the watched folder, they are detected by the K2 Pathfire capture service. The capture service then goes into action and does the necessary processing to import the media into the K2 media storage. This is similar to what happens when you manually import media using K2 AppCenter import features. The media is then available as a K2 clip, ready for playout.

The K2 Pathfire capture service and its watched folder must be on a K2 system that hosts the K2 FTP interface, as follows:

- A stand-alone K2 system — When media files are pushed to the watched folder, the capture service imports the media into the internal media storage or direct-connect media storage of the K2 system. The watched folder must be on the K2 system's V: drive.

- A K2 Media Server with role of FTP server — When media files are pushed to the watched folder, the capture service imports the media into 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 Pathfire capture service

Before you can configure and use the Pathfire capture service, the following requirements must be satisfied:

- K2 system software must be at a version that supports the Pathfire capture service. Refer to *K2 Release Notes* for information on Pathfire capture service version compatibility.

- The K2 Pathfire capture service must be licensed on the stand-alone K2 system or on the K2 Media Server. This is a Grass Valley software license.

- Pathfire Transfer Service software must be installed on the stand-alone K2 system or on the K2 Media Server.

- The Pathfire Transfer Service software must be licensed on the stand-alone K2 system or on the K2 Media Server. This is a Pathfire software license. If you are importing both HD content and SD content, two licenses are required.

- The K2 Pathfire capture service's watched folder must be configured as a destination for Pathfire-delivered content. You do this configuration as a part of the installation of the Pathfire Transfer Service software on the stand-alone K2 system or on the K2 Media Server.

- The Pathfire system in your facility must be installed and operating correctly before you integrate it with the K2 Pathfire capture service.

Use procedures later in this section as appropriate to satisfy prerequisites.

Considerations for the Pathfire capture service

When you are configuring and using the K2 Pathfire capture service, bear in mind the following considerations:

- You must be logged in with administrator privileges on the stand-alone K2 system or the K2 Media Server as well as having the appropriate security permissions to access the watched folder.

- If using the Pathfire capture service on a K2 SAN, the K2 Capture Services utility and the watched folder 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.

- 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 from the Pathfire system to the watched folder must be 100% complete before the K2 Pathfire capture service begins the import into K2 media storage.

- Imports are serialized. For example, if you drop two clips of Pathfire-delivered content into the watched folder, the Pathfire 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.

- Pathfire 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 Pathfire-delivered content into the watched folder, the import triggered by the Pathfire capture service becomes the fifteenth clip in the transfer queue.

- When the Pathfire-delivered content becomes a K2 clip, it is given 16 audio tracks by default. If the original Pathfire-delivered content has less than 16 audio tracks, the remaining audio tracks of the K2 clip are silent.

Configuring the Pathfire capture service

To configure the K2 Pathfire capture service, follow these steps:

NOTE: Once configured, the service deletes files in the watched folder (source directory) that are older than the specified cleanup frequency.

1. From the **Start** menu, access the **Programs** menu and select **Grass Valley | K2 Capture Services**.

   If the write filter is enabled, a message appears that informs you about the write filter and prompts you to restart.

2. If the write filter is enabled, restart as prompted, then repeat previous steps.

   The K2 Capture Services utility dialog box is displayed.

3. Click on the Pathfire tab.

   If you have not yet licensed the Pathfire 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.
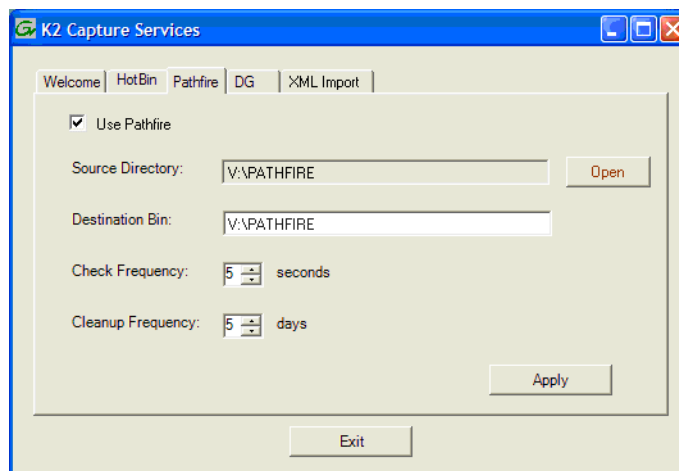
4. Select **Use Pathfire**.

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 a file is placed in this directory, the Pathfire capture service automatically imports it into the K2 media storage.

   NOTE: The directory you configure here as the Source Directory must be configured as a destination for Pathfire-delivered content.

   • Destination Bin — The clip bin in the K2 media storage that receives the media imported by the K2 Pathfire 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 files are imported to it.

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 Pathfire capture service settings are complete, click **Apply**.

9. A success message displays. Click **OK**. The Pathfire capture service starts up and continues to run after you exit.

    A message appears that informs you about the write filter and prompts you to restart.

10. Click **OK**.

    The K2 system restarts.

    The service immediately checks the source directory for any files that are beyond the specified cleanup age and deletes them from the directory.

Testing the Pathfire capture service

1. In the Pathfire application, drag Pathfire-delivered content onto the K2 system.

2. On the K2 System, open Windows Explorer, browse to the watched folder and verify that the files have arrived from Pathfire. The transfer from Pathfire must be 100% complete before the K2 Pathfire capture service triggers the import into K2 media storage.

3. Open AppCenter and use Transfer Monitor to verify that the transfer into K2 media storage is underway.

4. After the transfer into K2 media storage completes, verify that the media appears in the destination bin.

5. Playout the media to verify that the import was successful.

Pathfire capture service components

The following table describes the components that support K2 Pathfire capture service functionality.

Name	Description
Grass Valley Pathfire Bin service	This is the Pathfire capture service. It is the service that does the automatic import from the watched folder (source directory) to 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 a file is placed in this directory, the Pathfire capture service automatically imports it into the K2 media storage. By default, the location of the source directory is `V:\PATHFIRE`.
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.

Name	Description
Destination bin	The clip bin in the K2 media storage that receives the media imported by the K2 Pathfire capture service. The destination bin is in the K2 media database and appears in AppCenter as a media bin. By default, it location is `V:\PATHFIRE`.
DMGtransfer.exe	A program installed with Pathfire Transfer Service software. It appears only in the Windows operating system Task Manager.
Pathfire EsdClient service	A service installed with Pathfire Transfer Service software. It appears in the Windows operating system Services control panel. Its status should be Started, with startup type Automatic.
Pathfire logs	Find Pathfire logs at C:\Program Files\pathfire\logs.
Catch server	A generic term for a server dedicated to the purpose of downloading, capturing, and managing media content as it arrives via a specific distribution mechanism at a broadcast or media production facility. Examples of catch servers are a Pathfire DMG Server and a DG Spot Box.

Pathfire capture service procedures

Use the following procedures as necessary to support the operation of the Pathfire capture service in your facility.

Recovery after a failed Pathfire transfer

If the transfer of the Pathfire-delivered content into the watched folder fails, the Pathfire system manages the failure and reports errors. For some failure modes, such as a network outage, there might be some *.tmp files remaining in the watched folder as a result of the failed transfer. These files do not cause problems with subsequent transfers. Once you correct the problem that caused the original failure, if you restart the Pathfire transfer service and then transfer the same Pathfire-delivered content again, the transfer is successful. If the content is not transferred again, the *.tmp files persist until manually deleted.

Installing Pathfire Transfer Service software

To support K2 Capture Service features for automatically importing media from a Pathfire catch server, Pathfire software must be installed on a stand-alone K2 system or on a K2 Media Server. This software is Pathfire software, not Grass Valley software. Likewise, its license is a Pathfire license, not a Grass Valley license.

You must procure a license file for the Pathfire license. Follow the instructions on the Software License sheet that you received from Grass Valley. You must prepare a text file with unique system identifiers and send the text file to Grass Valley in order to received license files.

Refer to *K2 Release Notes* for information on the compatible version of Pathfire Transfer Service software.

NOTE: The Pathfire Transfer Service software install deletes files in C:\temp. If you have any files in C:\temp that you want to save, copy the files to a different location before proceeding.

To install Pathfire software, you must run multiple installation programs, as directed by the following procedures:

Install first DMG Master software

1. If installing on a K2 Summit Production Client or K2 Solo Media Server, disable the write filter.

2. If you have any files in *C:\temp* that you want to save, copy the files to a different location.

3. Make the contents of the Pathfire Transfer Service CD-ROM accessible to the K2 system.

4. Open *DMGMASTER40IT79.exe*. The name of this file might change slightly, depending on the version of Pathfire Transfer Service software.

   InstallShield Wizard opens and extracts files for two sets of data. The entire extracting process is less than 3 minutes. When the process completes, the Pathfire Digital Media Gateway Installation program opens and runs.

5. When the Welcome to the InstallShield Wizard for DMG window displays, click **Next** to progress through the wizard.

6. When you arrive at the License Agreement window, click **Yes**.

7. In the Installation Type window, select **Station Integration (3xx, 6xx)** and then click **Next**.

8. In the Enter Text window, enter the IP address of the Pathfire DMG Receive Server from which you are pulling content as input for the K2 Pathfire capture service.

   If an IP address is already entered, it is the IP address of the server as detected from a previous install.

9. Once the IP address of the Pathfire DMG Receive Server is correctly entered, click **Next**.

   A series of message boxes display for approximately twelve minutes as the necessary "skins" are installed. Once completed, the DMG Install Complete dialog box displays.

10. In the DMG Install Complete dialog box, respond as appropriate to restart and allow the K2 system to restart.

11. Continue with the next procedure "Install second DMG Master software".

Install second DMG Master software

Prerequisites for this procedure are as follows:

• The first DMG Master software is installed on the K2 system.

1. If installing on a K2 Summit Production Client or K2 Solo Media Server, disable the write filter.

2. If you have any files in *C:\temp* that you want to save and you have not already done so, copy the files to a different location.

3. If you have not already done so, make the contents of the Pathfire Transfer Service CD-ROM accessible to the K2 system.

4. Open *DMGMASTER.exe*.

   InstallShield Wizard opens and extracts files.

   The Pathfire Digital Media Gateway Installation program opens and runs installation processes. This takes approximately two minutes. When installation processes are complete, the DMG Install Complete dialog box displays.

5. In the DMG Install Complete dialog box, respond as appropriate to restart and allow the K2 system to restart.

6. Continue with the next procedure "Install DMG Transfer Service software".

Install DMG Transfer Service software

Prerequisites for this procedure are as follows:

• The first DMG Master software and the second DMG Master software is installed on the K2 system.

Transfer Service has the capability to transfer HD content and SD content. However, HD does not transfer to a SD destination nor does SD transfer to a HD destination. Therefore, if both types of content flow through the Transfer Service process, they each require their own destination.

1. If installing on a K2 Summit Production Client or K2 Solo Media Server, disable the write filter.

2. If you have any files in *C:\temp* that you want to save and you have not already done so, copy the files to a different location.

3. If you have not already done so, make the contents of the Pathfire Transfer Service CD-ROM accessible to the K2 system.

4. Open *DMGTRANSFER.exe*.

   InstallShield Wizard opens and extracts files, then the Pathfire Digital Media Gateway Installation program opens.

5. In the Information window, click **Next**.

6. In the Type window, select **Server Connect for Programming** and then click **Next**.

7. In the Destinations window, select **Configure destination one** and then click **Next**.

   If SD and HD destinations are required, configure the SD first.

8. In the Enter Text window, type the name of the K2 system on which you are now installing the Pathfire software.

   This name does not have to match any DNS names or computer names. However, it should be a name that is recognized when working in the Destinations window of the Pathfire DMG application.

9. In the Destinations window, click **Next**.

10. In the next Enter Text window, type a description that applies to the K2 system on which you are now installing the Pathfire software, and then click **Next**.

11. In the Transfer Engine window, select **DirectConnect** and then click **Next**.

12. In the Video Resolution window, select the video resolution for this destination. If SD and HD destinations are required, configure destination one for SD and

destination two for HD. Then click **Next**.

The Enter default output directory window dialog box opens.

13.Enter the path that specifies the K2 Pathfire capture service watched folder and then click **OK**.

In the K2 Capture Services utility, this watched folder is labeled the Source Directory.

14.In the Destinations window, do one of the following:

- If you require another destination (such as the HD destination), select **Configure destination two** and click **Next**. Repeat previous steps to configure the destination.

- If all your required destinations are configured, select **Done** and then click **Next**.

After a few seconds of inactivity, a series of install windows flash.

When the install is complete the installation programs close and the Windows desktop appears.

15.Restart (boot) the K2 system using the Windows operating system restart procedure.

16.Continue with the next procedure .

Licensing Pathfire Transfer Service software

There are two licenses required for operation of the Pathfire capture service, as follows:

- The Pathfire Transfer Service license, as explained in this section. The license for Pathfire Transfer Service software is a Pathfire license, not a Grass Valley license. You must license the Pathfire software on the stand-alone K2 system or the K2 Media Server.

- The K2 Pathfire capture service license, which is a Grass Valley license. Refer to .

Prerequisites for this procedure are as follows:

- The first DMG Master software, the second DMG Master software, and the DMG Transfer Service is installed on the K2 system.

- You have procured the license file. Follow the instructions on the Software License sheet that you received from Grass Valley. You must prepare a text file with unique system identifiers and send the text file to Grass Valley in order to received license files.

1. If installing on a K2 Summit Production Client or K2 Solo Media Server, disable the write filter.

2. Copy the license file to *C:\Program Files\pathfire\dmg\skippy\dat*.

3. Click **Start | All Programs | StartUp | Transfer**.

4. Press **Ctrl + Alt + Delete**. The Windows Security dialog box opens.

5. Click **Task Manager**. Windows Task Manager opens.

6. In Task Manager, confirm that **DMGTransfer.exe** is running.

7. Restart (boot) the K2 system using the Windows operating system restart procedure.

The Pathfire software is installed and licensed.

Using the DG capture service

The following sections provide information for the K2 DG capture service.

- "About the DG capture service"
- "Prerequisites for using the DG capture service"
- "Configuring the DG capture service"
- "Testing the DG capture service"
- "DG capture service procedures"
- "DG capture service components"

About the DG capture service

The K2 DG capture service provides a way to have DG spots automatically imported into a K2 system. The DG capture service watches for DG spots as they become available on DG Spot Box. When an operator on the DG Spot Box assigns a house ID to a DG spot, the spot is detected by the K2 DG capture service. The capture service then goes into action and does the necessary processing to import the spot into the K2 media storage. This is similar to what happens when you manually import media using K2 AppCenter import features. The spot is then available as a K2 clip, ready for playout.

The K2 DG capture service controls transfers and manages house IDs for spots. In order to track house IDs, the K2 capture service creates two instances in the K2 media database for each spot. One instance is in the destination bin. The other instance is in a tracking bin. Playout and other normal media operations take place from the destination bin. The tracking bin is used internally by the DG capture service for house ID tracking purposes. The tracking bin is not available for normal operations.

The DG capture service must run on a K2 system that hosts the K2 FTP interface, as follows:

- A stand-alone K2 system — The K2 DG capture service imports DG spots into the internal media storage or direct-connect media storage of the K2 system.
- A K2 Media Server with role of FTP server — The K2 DG capture service imports DG spots into the shared media storage of the K2 SAN.

Prerequisites for using the DG capture service

Before you can configure and use the DG capture service, the following requirements must be satisfied:

- K2 system software must be at a version that supports the DG capture service. Refer to *K2 Release Notes* for information on DG capture service support.
- The DG capture service must be licensed on the stand-alone K2 system or K2 Media Server. This is a Grass Valley software license.
- The DG system in your facility must be installed and operating correctly before you can integrate it with the K2 DG capture service.

Use procedures later in this section as appropriate to satisfy pre-requisites.

Configuring the DG capture service

When configuring the K2 DG capture service, bear in mind the following considerations:

- You must be logged in with administrator privileges on the stand-alone K2 system or the K2 Media Server.

- If using the DG 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.

- Imports are serialized. For example, if two clips become available on the DG Spot Box, the DG capture service does not queue the second clip for import until the first clip is finished importing. This is different than the ordinary K2 transfer process.

- DG capture service imports are serialized with other K2 transfers. For example, if fourteen items are already queued up from ordinary K2 transfers, and a DG spot becomes available for import, the import triggered by the DG capture service becomes the fifteenth clip in the transfer queue.

To configure the DG capture service, follow these steps:

1. From the **Start** menu, access the **Programs** menu and select **Grass Valley | K2 Capture Services**.

   If the write filter is enabled, a message appears that informs you about the write filter and prompts you to restart.

2. If the write filter is enabled, restart as prompted, then repeat previous steps.

   The K2 Capture Services utility dialog box is displayed.

3. Click on the DG tab.

   If you have not yet licensed the DG 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.
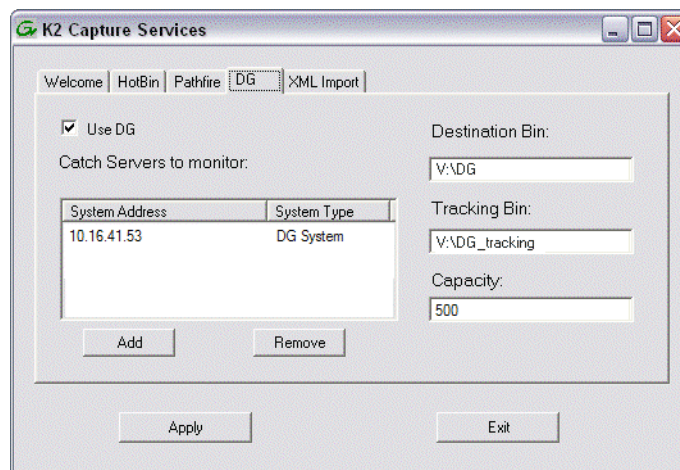
4. Select **Use DG**.

5. Enter the paths to the destination bin and the tracking bin, which are defined as follows:

   • Destination Bin — This is the clip bin in the K2 media storage that receives the media imported by the DG capture service. The destination bin is defined by the K2 media database and appears in AppCenter as a media bin. The bin must be on the K2 system's V: drive.

   • Tracking Bin — This is another clip bin in the K2 media storage. This bin is used by the K2 capture service. It stores a second instance of each spot, for the purpose of tracking house IDs. You do not use it for normal K2 media operations. The bin must be on the K2 system's V: drive. If you specify a bin name that does not yet exist, the K2 system creates it when files are imported to it.

6. Set the Capacity, which specifies the maximum number of DG spots retained in K2 media storage. When this maximum number is reached, the DG capture service deletes the five oldest spots from the K2 media storage. Set the capacity to be larger than the capacity of the DG Spot Box.

7. Click **Add**. The New Server Information dialog box opens.
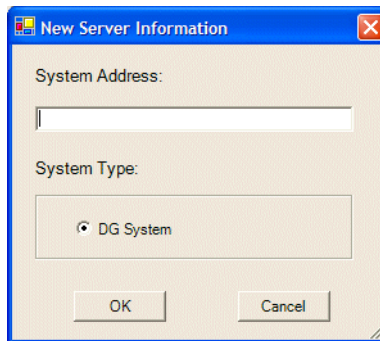
8. Enter the IP address of the DG Spot Box and click **OK**.

9. When your DG capture service settings are complete, on the K2 Capture Services utility dialog box, click **Apply**.

10. A success message displays. Click **OK**. The DG capture service starts up and continues to run after you exit.

   A message appears that informs you about the write filter and prompts you to restart.

11. Click **OK**.

   The K2 system restarts.

Testing the DG capture service

1. On the DG Spot Box, assign a house ID to a spot.

2. On the K2 system, open AppCenter and verify that the media has been imported into the destination bin.

3. Playout the media to verify that the import was successful.

DG capture service procedures

Use the following procedures as necessary to support the operation of the DG capture service in your facility.

Deleting a spot

If you want to delete a spot, you must delete for all instances of the spot in the proper sequence so that no references to the house ID remain. Use the following procedure:

1. In AppCenter, delete the spot from the destination bin.

2. In AppCenter, delete the spot from the tracking bin.

3. On the DG Spot Box, delete the spot.

DG capture service components

The following table describes the components that support K2 DG capture service functionality.

Name	Description
Grass Valley DG Capture service	This is the DG capture service. It is the service that does the automatic import of DG spots to the K2 media storage.
K2 Capture Services utility	Configures K2 capture services.
Destination Bin	This is the clip bin in the K2 media storage that receives the media imported by the DG capture service. The destination bin is in the K2 media database and appears in AppCenter as a media bin. The bin must be on the K2 system's V: drive. By default, the location is V:\DG.
Shallow Copy Bin	This is another clip bin in the K2 media storage. This bin is used by the K2 capture service. It stores a second instance of each spot, for the purpose of tracking house IDs. You do not use it for normal K2 media operations. The bin must be on the K2 system's V: drive. By default, the location is V:\DG_Tracking.
Capacity	The maximum number of DG spots retained in K2 media storage. When this maximum number is reached, the DG capture service deletes the five oldest spots from the K2 media storage.
Catch server	A generic term for a server dedicated to the purpose of downloading, capturing, and managing media content as it arrives via a specific distribution mechanism at a broadcast or media production facility. Examples of catch servers are a Pathfire DMG Server and a DG Spot Box.

Using the XML Import capture service

The following sections provide information for the K2 XML Import capture service.

- "About the XML Import capture service"
- "Prerequisites for using the XML Import capture service"
- "Considerations for the XML Import capture service"
- "Configuring the XML Import capture service"
- "Testing the XML Import capture service"
- "XML Import capture service components"

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.

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 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 *K2 Release Notes* 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 procedures in this section as appropriate to satisfy prerequisites.

Considerations for 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 stand-alone K2 system or the K2 Media Server as well as having the appropriate security permissions to access the watched folder.

- If using the XML Import capture service on a K2 SAN, the K2 Capture Services utility and the watched folder 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.

- After the capture service creates the clip in the 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

To configure the K2 XML Import capture service, follow these steps:

NOTE: Once configured, the service deletes files in the watched folder (source directory) that are older than the specified cleanup frequency.

1. From the **Start** menu, access the **Programs** menu and select **Grass Valley | K2 Capture Services**.

   If the write filter is enabled, a message appears that informs you about the write filter and prompts you to restart.

2. If the write filter is enabled, restart as prompted, then repeat previous steps.

   The K2 Capture Services utility dialog box is displayed.

3. Click on the **XML Import** tab.
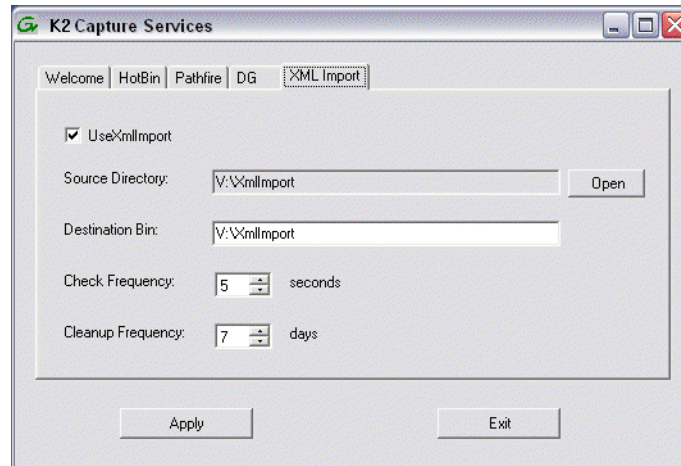
4. Select **Use XmlImport**.

   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. Make sure the write filter is disabled.

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 media files, then a valid XML file, are placed in this directory, the XML Import 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 K2 XML Import 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 XML Import capture service settings are complete, click **Apply**.

   A message appears that informs you about the write filter and prompts you to restart.

9. Click **OK**.

   The K2 system restarts.

   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 the files have completed the transfer. The transfer must be 100% complete before proceeding.

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. Playout the media to verify that the clip was successfully created.

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 the XML Import 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, then a valid XML file, are placed in this directory, the XML Import 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 K2 XML Import 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 Import capture service

The following sections provide information for the K2 P2 Import capture service.

- "About the P2 Import capture service"
- "Prerequisites for using the P2 Import capture service"
- "Considerations for the P2 Import capture service"
- "Configuring the P2 Import capture service"
- "Testing the P2 Import capture service"
- "P2 Import capture service components"

About the P2 Import capture service

The K2 P2 Import capture service provides a way to have P2 media automatically imported into a K2 system. 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.

The watched folder receives the nested directories that define P2 media for one clip or multiple clips. After all the directories/files are finished being transferred to the watched folder, the capture service goes into action and validates the P2 media to make sure it has the proper structure. 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 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 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 Import capture service

Before you can configure and use the P2 Import capture service, the following requirements must be satisfied:

- The K2 system must support AVC-Intra. This requires that the AVC-Intra codec card be installed.

- K2 system software must be at a version that supports the P2 Import capture service. Refer to *K2 Release Notes* 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.

Use procedures in this section as appropriate to satisfy prerequisites.

Considerations for the P2 Import 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 stand-alone K2 system or the K2 Media Server as well as having the appropriate security permissions to access the watched folder.

- If using the P2 Import capture service on a K2 SAN, the K2 Capture Services utility and the watched folder 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.

- 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 creates the clip in the 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 K2 P2 Import 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 (AVC-Intra and DV) 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

Configuring the P2 Import capture service

To configure the K2 P2 Import capture service, follow these steps:

NOTE: Once configured, the service deletes files in the watched folder (source directory) that are older than the specified cleanup frequency.

1. From the **Start** menu, access the **Programs** menu and select **Grass Valley | K2 Capture Services**.

   If the write filter is enabled, a message appears that informs you about the write filter and prompts you to restart.

2. If the write filter is enabled, restart as prompted, then repeat previous steps.

    The K2 Capture Services utility dialog box is displayed.

3. Click on the **P2 Import** tab.
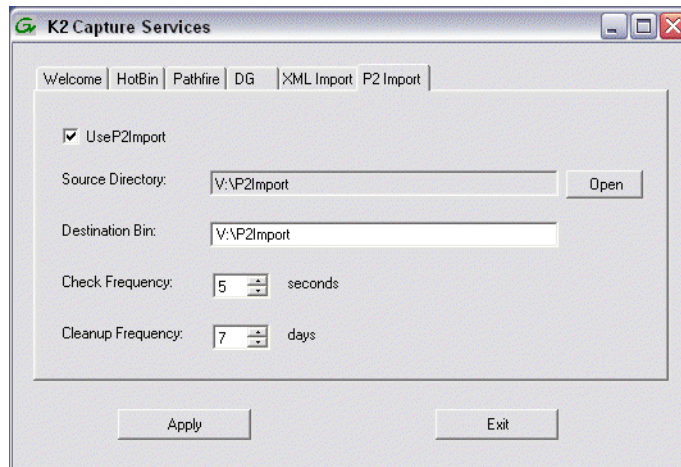
4. Select **Use P2Import**.

    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. Make sure the write filter is disabled.

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 P2 directories/ files are placed in this directory, the P2 Import 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 K2 P2 Import 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 P2 Import capture service settings are complete, click **Apply**.

    A message appears that informs you about the write filter and prompts you to restart.

9. Click **OK**.

The K2 system restarts.

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 Import 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 P2 directories/files have completed the transfer. The transfer must be 100% complete before the K2 P2 Import 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. Playout the media to verify that the clip was successfully created.

P2 Import 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 the P2 Import 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 P2 Import 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 K2 P2 Import 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`.

Licensing K2 capture service software

Licensing is required for K2 capture service software as follows:

• To use the Pathfire capture service, you must obtain a Pathfire capture service license from Grass Valley.

• To use the DG capture service, you must obtain a DG capture service license from Grass Valley.

• 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.

Licenses are requested through the K2 License Wizard and managed through the SabreTooth License Manager, which are installed with K2 system software.

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. 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.

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 following sections:

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.

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.

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.

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.

Whenever a DV, AVC-Intra, XDCAM-EX, XDCAM-HD, XDCAM-HD 422, or IMX format simple clip is created on a K2 system, K2 software creates a corresponding QuickTime 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. 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.

Connection types are as follows:

- Fibre Channel – This is a connection as a client to a Fibre Channel K2 SAN. The connection requires a K2 FCP Connect license and supporting software on the Macintosh system. The connection uses the K2 SAN's Fibre Channel network.

- 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.

- CIFS – This is a basic CIFS connection. You can access files on K2 SAN storage or K2 stand-alone storage with this type of connection. The connection uses a basic 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 Fibre Channel, file copy over iSCSI, file copy over CIFS, 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 Fibre Channel, iSCSI, or CIFS connections.

- Flip4Mac – This is a Telestream product that supports FTP file transfer of K2 media to the Macintosh system. It is a Final Cut Pro plug-in.

Connections, access, and software apply to K2 storage and versions as follows:

K2 storage/version	Connection type	Access method	Software
K2 SAN and stand-alone K2 Media Client software version 3.2 and higher	CIFS	File transfer	Flip4Mac recommended
Stand-alone K2 Media Client software version 3.3 and higher, and stand-alone K2 Summit Production Client software version 7.1 and higher	CIFS	All	K2 FCP Connect recommended
K2 SAN (K2 Media Client) software version 3.3 and higher, and K2 SAN (K2 Summit Production Client) software version 7.1 and higher	All	All	K2 FCP Connect recommended for CIFS, required for iSCSI and Fibre Channel SAN.

For detailed instructions refer to documentation as follows:

- Fibre Channel, iSCSI, or CIFS connection with K2 FCP Connect – 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

- Basic CIFS connection without K2 FCP Connect – Refer to topics later in this manual.

Install and configure Macintosh Final Cut Pro systems on K2 storage

Read the following topics to get systems connected and media access operational.

Final Cut Pro CIFS mount to K2 storage quick start installation checklist

Use the following sequence of tasks to set up Final Cut Pro access to K2 storage via CIFS mount without a K2 FCP Connect license. This applies to the following K2 systems:

- K2 SAN and stand-alone K2 Media Client software version 3.2 and higher

- K2 SAN and stand-alone K2 Summit Production Client software version 7.1 and higher

This checklist assumes that the K2 system has been installed/commissioned and is fully operational.

On the K2 system

	Task	Instructions	Comment
☐	Configure hosts files on the K2 system	Add Macintosh systems to the K2 hosts file	Enter Macintosh IP address and name in hosts files.
☐	Create a Macintosh user account. This is the account that the Macintosh system uses to log on to the K2 system.	Use standard Windows operating system procedures.	This is not necessary if the Macintosh system logs on with the default K2 administrator account (administrator/adminK2)
☐	Optional: Enable Access Control Lists, if desired.	Topic "Enable Access Control Lists on the K2 system"	This is optional. If you do this task, you must also configure Active Directory Domain on the Macintosh systems.
☐	Share V: drive as *default/gvfs_hostname*.	Use standard Windows operating system procedures. Set permissions to read only.	On a K2 SAN, create the share on the primary K2 Media Server. Do not create the share on a SAN connected K2 client.

On all Macintosh client computers

	Task	Instructions	Comment
☐	Install Final Cut Pro, if not already installed.	Final Cut Pro documentation	—
☐	Install Flip4Mac, if necessary for your workflow.	Flip4Mac documentation	This software is optional
☐	Cable network connections.	Connect the Macintosh system to the K2 system's control network.	Only the control network connection is necessary.
☐	Configure for control network, if not already done.	Topic "Configure Macintosh systems for control network"	—
☐	Optional: Configure Active Directory Domain	Topic "Configure Macintosh systems for Active Directory Domain"	This is optional. If you do this task, you must also enable Access Control Lists on the K2 system.
☐	Mount the K2 system's volume *default*.	Topic "Connecting via SAMBA/CIFS"	In the Name field, enter <K2_name>/<username>.

Final tasks

	Task	Instructions	Comment
☐	If used, verify Access Control Lists.	Topic "Verify Access Control Lists"	—
☐	If desired, configure HotBin on the K2 system to receive finished Final Cut Pro files.	Topics "Configure HotBin" and "About QuickTime import delay"	—

Enable Access Control Lists on the K2 system

Prerequisites for the K2 system are as follows:

- Current compatible versions of the Windows operating system and SNFS software.

- Standard C:, D:, E: and V: disk volumes.

- SNFS has been configured with Grass Valley's Storage Utility.

- The SNFS configuration file is located 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.

Configure Macintosh systems for control network

Configure each Macintosh system as follows:

1. Open System Preferences, Network settings.

2. Set Ethernet 1 to configure manually (static IP).

3. Configure IP address, subnet mask, and other settings as required for the control network.

Configure Macintosh systems for Active Directory Domain

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

1. In the *Applications/Utilities* folder, open the **Directory Utility**.
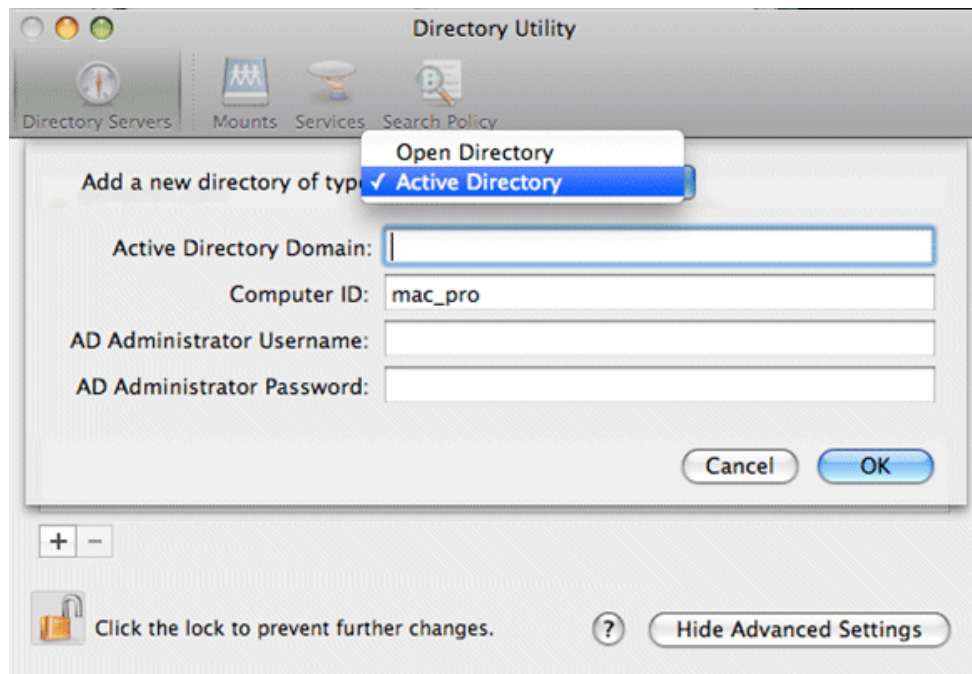
2. Click the **Directory Servers** tab.

3. Click the **+** icon in the lower left, above the padlock icon, to add a new domain binding.

4. In the **Add a new directory of type** drop-down list, select **Active Directory**.
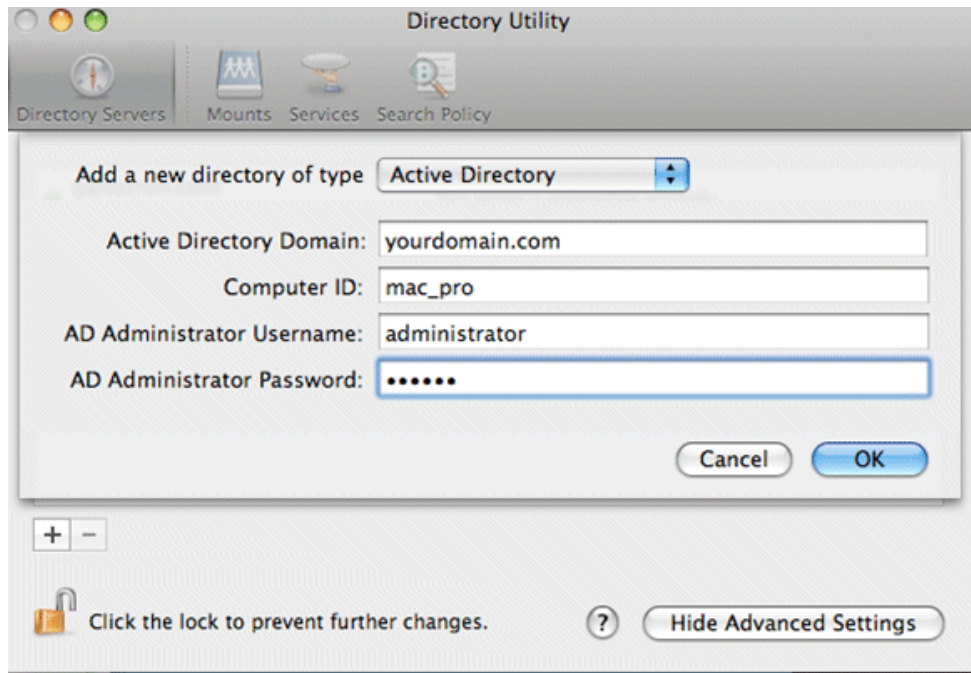
5. Fill in the Active Directory information for the domain administrator account.

    The administrator account is only needed at the time of binding. Once the computer is bound to a domain, all users of the domain can be used to log in to the Macintosh system.

6. Click **OK**.

    The Macintosh computer goes through the binding process. If successful, the domain name is listed with the status message, "This server is responding normally".

7. Click **Services**.
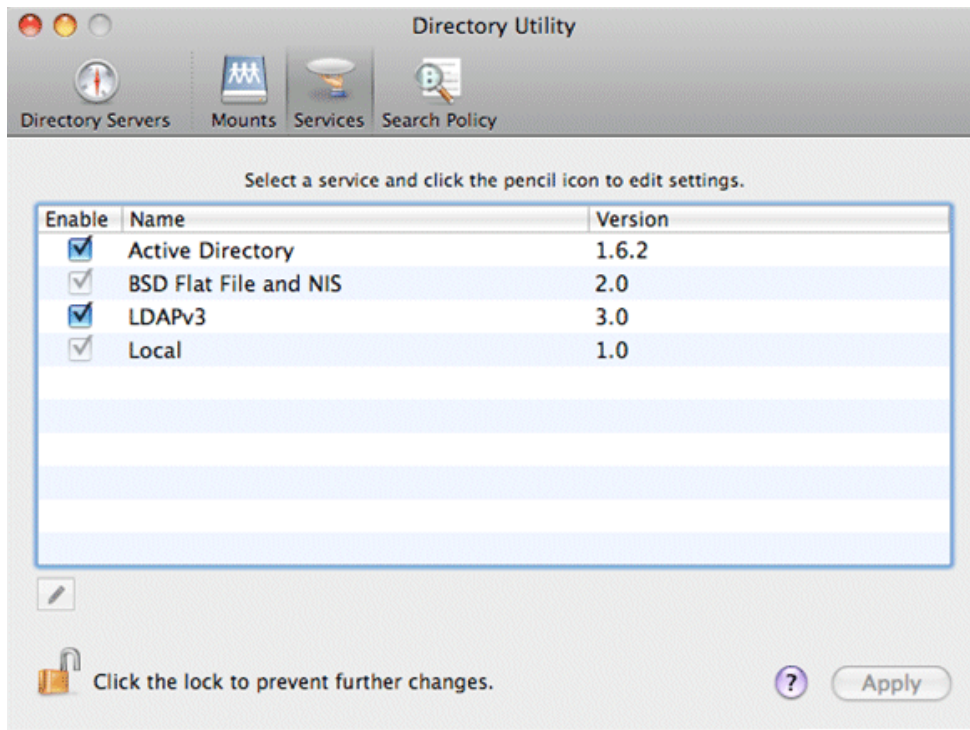
8. Verify that the Active Directory option is checked.

   If you need to change options, first double-click the padlock icon on the lower left hand corner and authenticate as administrator.

9. If desired, add AD accounts or groups as administrators of the Macintosh computer as follows:

   a. In the **Services** tab, double-click on the **Active Directory** name.

   b. Open the advanced options and click on the **Administrative** tab.
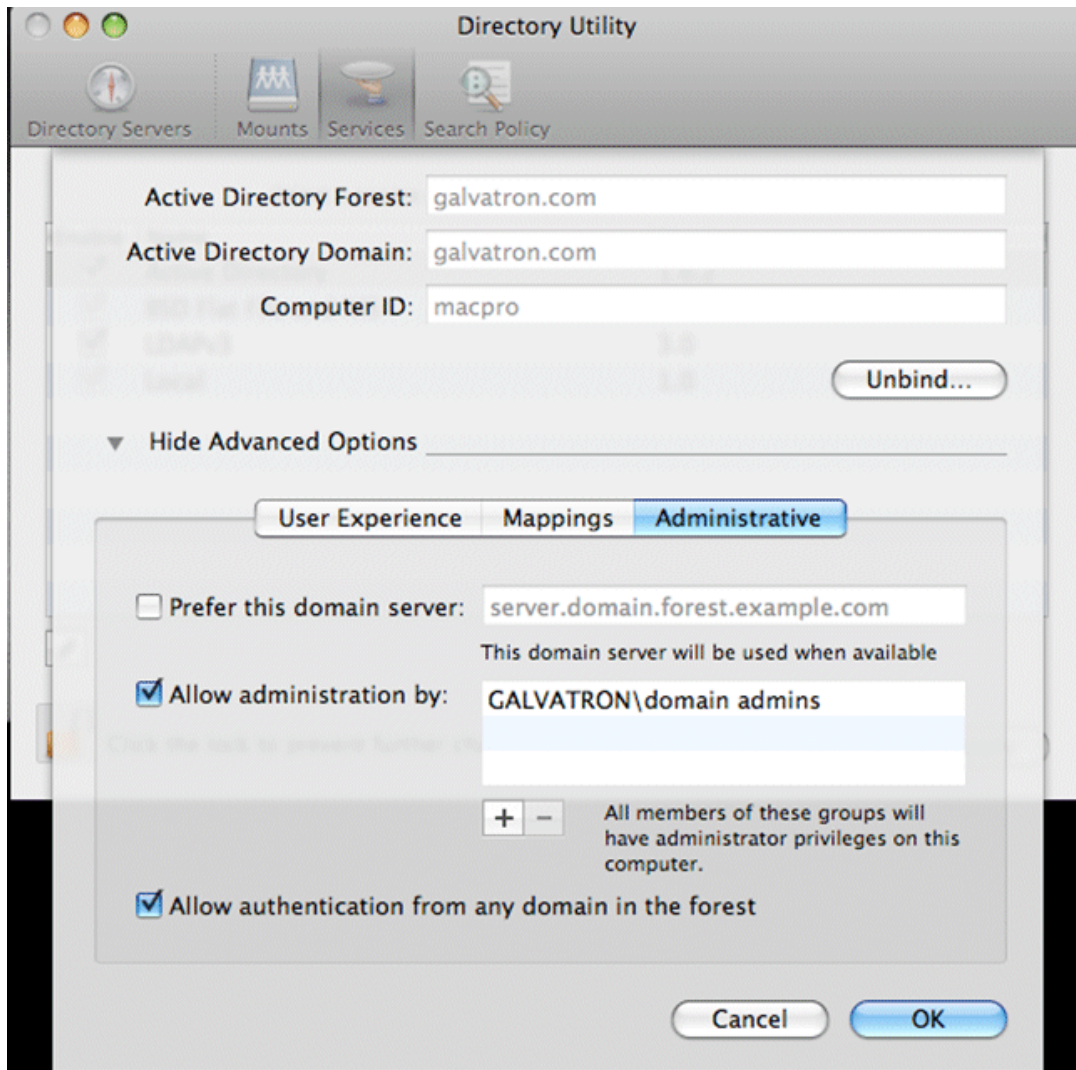
      c. Verify that **Allow administration by:** checkbox is checked.

      d. Add any AD user or group of the domain to the list.

          You must type the user or group name, then a backslash, before the domain name.

Connecting via SAMBA/CIFS

   Use this method to connect to the SNFS volume via CIFS. Once the Macintosh computer has been bound to a domain it can then connect to any domain controlled, shared volume via SAMBA. If connecting via SAMBA, XSan software does not need to be installed or configured.

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

    The Connect to Server dialog box opens.
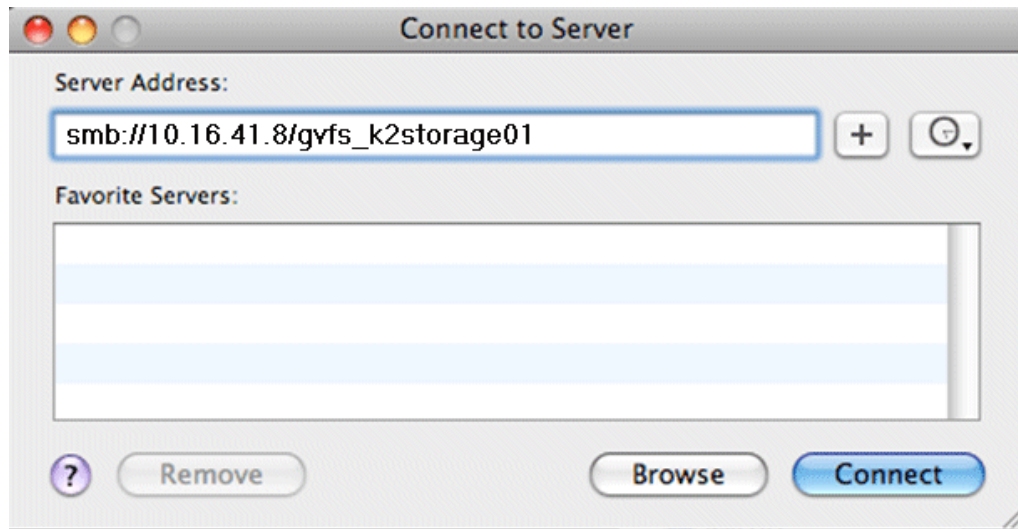
2. In the Server Address field, type `smb://`, then type the IP or DNS name of the
server to which you are connecting, slash, then type the volume name.

3. Click **Connect**.

You are prompted to authenticate.

In the **Name** field, make sure you enter the name of the K2 system (shown here as

"yourdomain"), then a backslash, then the username.

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

Verify Access Control Lists

Prerequisites:

- 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.
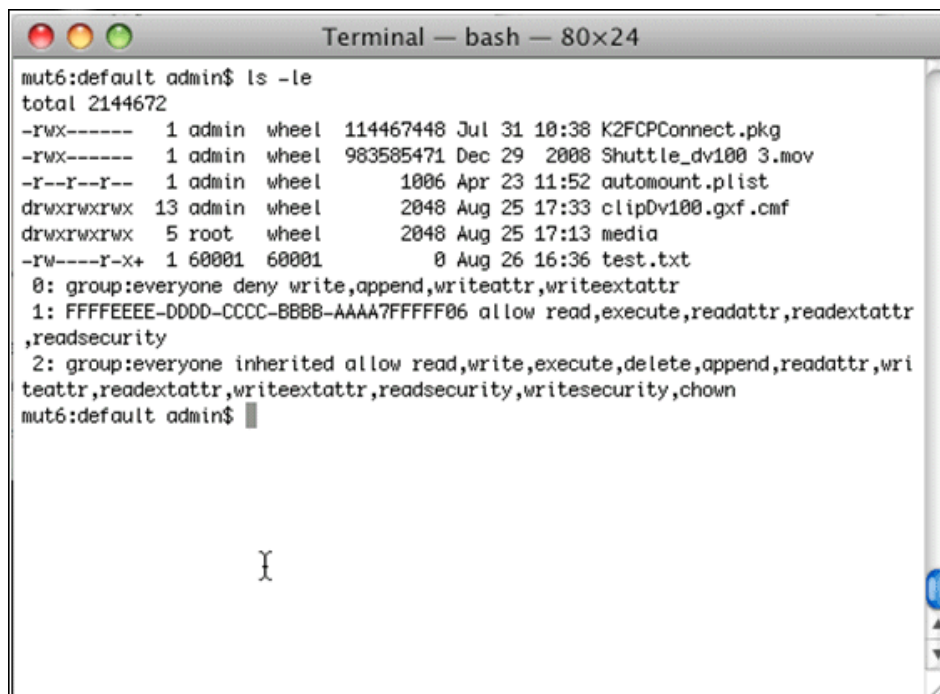
      If the SNFS file system is named "default" type the following and press **Enter**:

      ```
      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
```

```
mut6:default admin$ ls -le
total 2144672
-rwx------   1 admin  wheel  114467448 Jul 31 10:38 K2FCPConnect.pkg
-rwx------   1 admin  wheel  983585471 Dec 29  2008 Shuttle_dv100 3.mov
-r--r--r--   1 admin  wheel       1006 Apr 23 11:52 automount.plist
drwxrwxrwx  13 admin  wheel       2048 Aug 25 17:33 clipDv100.gxf.cmf
drwxrwxrwx   5 root   wheel       2048 Aug 25 17:13 media
-rw----r-x+  1 60001  60001          0 Aug 26 16:36 test.txt
 0: group:everyone deny write,append,writeattr,writeextattr
 1: FFFFEEEE-DDDD-CCCC-BBBB-AAAA7FFFFF06 allow read,execute,readattr,readextattr
,readsecurity
 2: group:everyone inherited allow read,write,execute,delete,append,readattr,wri
teattr,readextattr,writeextattr,readsecurity,writesecurity,chown
mut6:default admin$
```

    e. Verify that there is a "+" next the text file, plus a list of permissions below. If this is true then cross-platform ACLs are enabled.

    f. Open the Finder, go to the default volume and try to edit the text file. This should fail as the file should not be writeable.

    g. In the Finder, go to the folder you created earlier in this procedure and create a text file in the folder. This operation should be successful.

    h. Log out and then log back in as userB.

    i. In the Finder, go to the folder you created earlier in this procedure and try to create a text file in the folder. This operation should fail.

Configure HotBin

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.

Using Final Cut Pro on a K2 storage

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

Operation guidelines

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

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

Media access

1. From the Macintosh system on which you are running Final Cut Pro, access K2 media as follows:

   - If your access method is file transfer via Flip4Mac (FTP), in Final Cut Pro click **File | Import | Grass Valley...**.

   - If your access method is file transfer via direct file copy, open the Macintosh Finder.

   - If your access method is edit-in-place, in Final Cut Pro click **File | Open**.

2. Browse to the location of the media in your K2 bin structure.

   The QuickTime reference path/file is named according to the convention *\<bin name>\<clip name>\<clip name>.mov*.

   If accessing media on a K2 version 7.x system, all the files associated with the clip are in the *\<bin name>\<clip name>* directory.

3. Do one of the following:

   - If your access method is file transfer via Flip4Mac (FTP), transfer the QuickTime reference file to the local Macintosh system, then open the file in Final Cut Pro and Save As to the location of your work in progress.

- If your access method is file transfer via direct file copy, copy all the files associated with the clip to the local Macintosh system, then open the QuickTime reference file in Final Cut Pro and Save As to the location of your work in progress.

- If your access method is edit-in-place, open the QuickTime reference file in Final Cut Pro.

4. Edit the file as desired.

5. When you have finished material that you have created in Final Cut Pro, export it to the K2 system.

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.

Connecting RS-422

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:
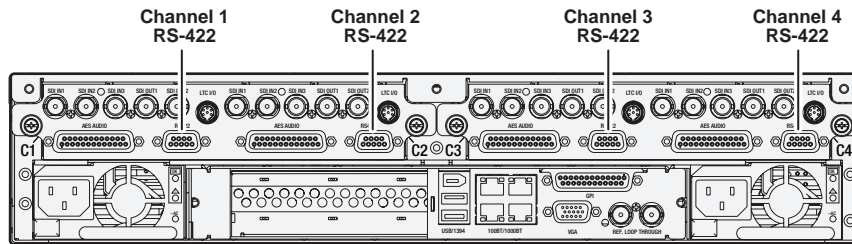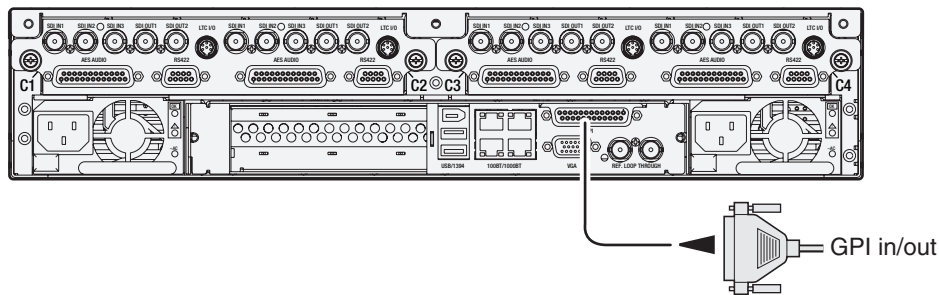
Refer to the following for more information about RS-422 and protocol control:

- Appendix A, *Remote control protocols*

- *K2 AppCenter User Manual* to configure the K2 system for remote control.

Connecting GPI

The K2 system provides 12 GPI inputs, and 12 GPI outputs on a single DB-25 rear panel connector, as illustrated.

GPI in/out

Also see the following related sections of this manual:

- "GPI I/O specifications" on page 197

- "GPI I/O connector pinouts" on page 235

Refer to the *K2 AppCenter User Manual* for GPI configuration procedures.

Chapter **4**

Managing Stand-alone Storage

Topics in this chapter include the following:

- "About the internal storage system"
- "About the direct-connect storage system"
- "Using Storage Utility"

Also refer to *K2 Summit Transmission Server Package* for information unique to that product.

About the internal storage system

A K2 Summit Production Client with internal drives for media storage or a K2 Solo Media Server is a self-contained, stand-alone unit, with no external devices for storage, audio, or video connections required.

K2 Summit Production Client internal storage system

The storage system on an internal storage K2 Summit Production Client includes the following:

Compact Flash — The Compact Flash boot media serves as the system drive of the K2 Summit Production Client. The Windows operating system, applications, and other standard computer software components reside on the system drive.

RAID drives — There are slots for eight 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 Summit Production Clients 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. Media drives can be RAID 1 or RAID 0. 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 or in NetCentral 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 of the K2 Solo Media Server. 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 can not 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 — 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.

About the direct-connect storage system

A K2 Summit Production Client 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 an internal storage K2 Summit Production Client includes the following:

Compact Flash — The Compact Flash boot media serves as the system drive of the K2 Summit Production Client. The Windows operating system, applications, and other standard computer software components reside on the system drive.

Fibre Channel card — The direct-connect K2 Summit Production Client has a direct Fibre Channel connection to external K2 RAID. The K2 Summit Production Client 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 Summit Production Client.

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 or in NetCentral 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 includes the following topics:

- "About Storage Utility"
- "Opening Storage Utility"
- "Overview of Storage Utility"
- "Checking storage subsystem status"
- "Checking controller microcode"
- "About identifying disks"
- "Get controller logs"
- "Check disk mode pages"
- "Disabling a disk"
- "Forcing a disk to rebuild"
- "Unbind LUN"
- "Bind Luns"
- "Changing RAID type for internal storage"
- "Making a new media file system on a K2 Summit/Solo"
- "Checking the media file system"
- "Cleaning unreferenced files and movies"
- "Downloading controller microcode"
- "Downloading disk drive firmware"
- "Placing the K2 system into online mode"

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. Also refer to "Storage Utility" on page 36 for a general description of Storage Utility.

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.

To open Storage Utility through AppCenter, do the following:

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. Refer to "About identifying disks" on page 114.

Opening Storage Utility Independently

Do not open Storage Utility independently unless there is a problem that prevents you from opening it through AppCenter.

To open Storage Utility independently, do the following:

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.
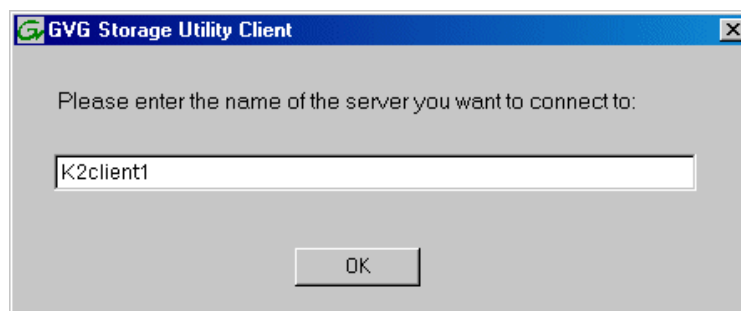
2. Enter the name or IP address of the K2 system for which you intend to use Storage

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.
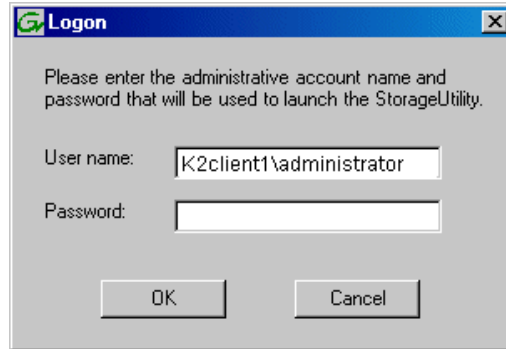
3. Logon to Storage Utility. Make sure you log in with appropriate privileges. Administrator-level permission is necessary for most Storage Utility operations. For user name, you might need to enter the machine name as the domain to successfully log in.

    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. Refer to "About identifying disks" on page 114.

Overview of Storage Utility
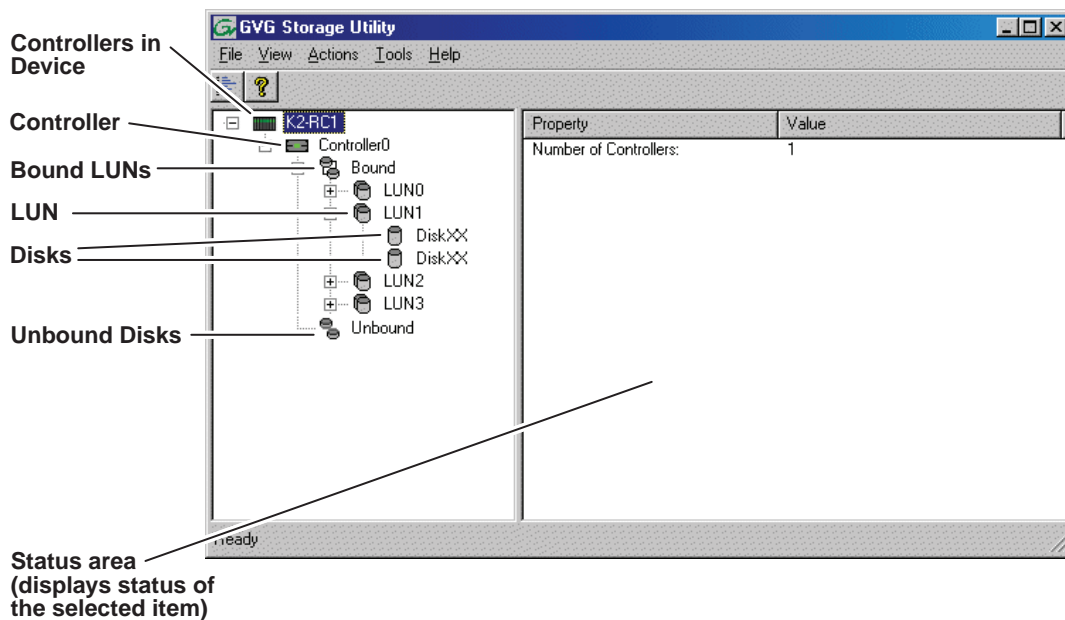
The Storage Utility user interface includes a tree view in the left-hand pane, and a status information area displayed in the right-hand pane. The tree view displays the hardware that makes up the storage system connected. The context menus in the tree view are used to configure storage. The right-hand 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

To identify internal storage RAID disks do the following:

1. Open Storage Utility and in the tree view expand all nodes so that all disks are displayed. Disks are configured as RAID 1 (shown as for Summit) or RAID 0.
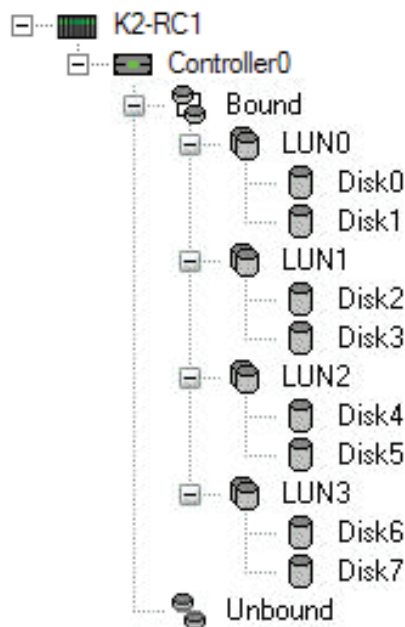
2. On the K2 Summit Production Client, remove the front bezel assembly. On the K2 Solo Media Server, disk LEDs are visible without removing the bezel.

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 product chassis. Compare the drive number positions and the disk numbering displayed in Storage Utility to identify drive locations.

• K2 Summit Production Client

Disk2	Disk4	Disk7
Disk1	Disk3	Disk6
Disk0		Disk5

• K2 Solo Media Server

Disk0
Disk1

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. 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. 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 system at *C:\logs*:

   • MegaRaidDriveFailureLog.txt

   • MegaRaidNVRAMLog.txt

   • tty.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.*

For a direct-connect storage, refer to "Setting up direct-connect RAID storage" on page 173.

To unbind a LUN, do the following:

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.
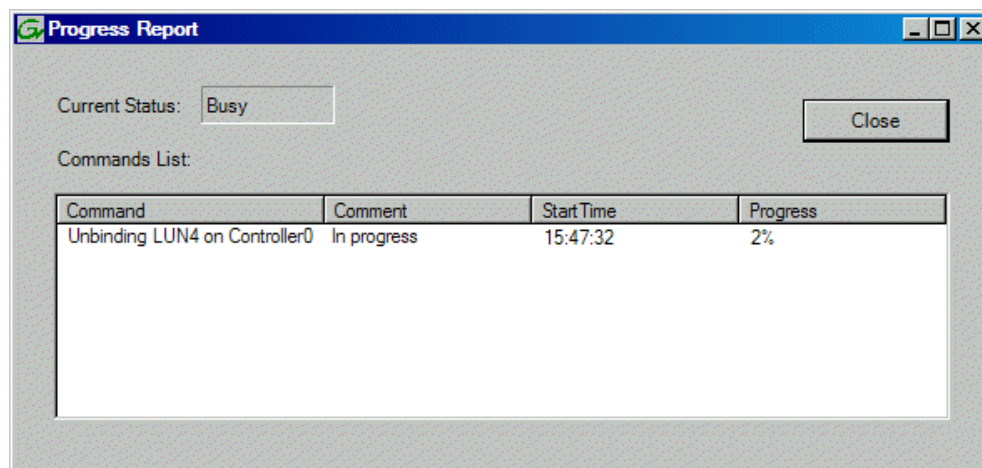
5. When progress reports 100% complete, the LUN is unbound.

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.

For a direct-connect storage, refer to .

To bind a LUN, do the following:

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.
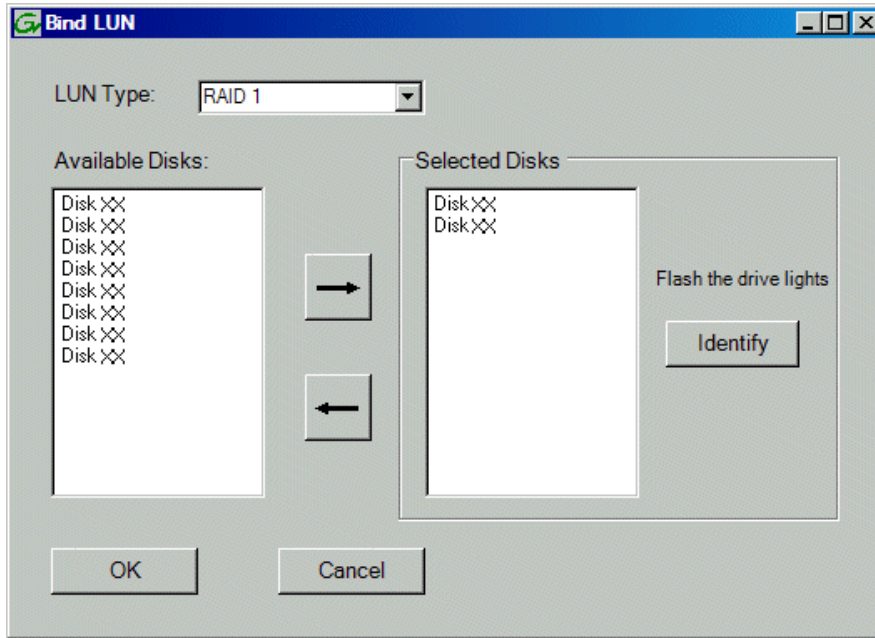
3. In the LUN Type drop-down list, for internal storage select either RAID 0 or RAID 1. For direct-connect storage select RAID 5. Then proceed as follows:

- RAID 0 — 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 — 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 — 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, as explained in "Making a new media file system on a K2 Summit/Solo" on page 120.

Changing RAID type for internal storage

You can change the media storage on an internal storage K2 Media Client or K2 Summit Production Client to be either RAID 1 or RAID 0, as follows:

- RAID 1 — Recommended for the "full" media drive option, which is ten drives on a K2 Media Client and eight drives on a K2 Summit Production Client. 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 — Can be used with any media drive option. 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.

To change internal storage RAID-type configuration, do the following:

1. If you need to retain media, transfer it to another K2 system or otherwise back it up.

2. Unbind all media LUNs, as instructed in "Unbind LUN" on page 116. On a K2 Media Client, do not unbind LUN 0, as this is the system drive.

3. Restart.

4. Bind media drives, using the procedure "Bind Luns" on page 117, 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, as explained in "Making a new media file system on a K2 Summit/Solo" on page 120.

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.
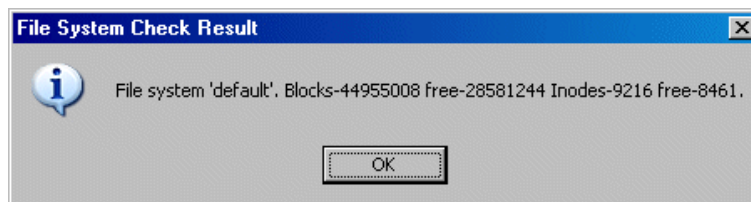
1. Click **Tools | Make New File System**.

2. If a message informs you about the write filter, restart as prompted to disable the write filter. After restart, repeat previous steps and then continue.

3. 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.

4. 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.

5. When a message "Succeeded to make the new file system. The server will be restarted now" appears, click **OK** to restart. The write filter is enabled on restart.

6. 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

This procedure checks the media file system but retains current media files.

1. 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.

File System Check Result

File system 'default'. Blocks-44955008 free-28581244 Inodes-9216 free-8461.

OK

4. Click **OK** to dismiss the results.

    Your file system has been checked.

Cleaning unreferenced files and movies

Check your *K2 Release Notes* for the latest information on this feature.

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.

To clean unreferenced files, do the following:

1. Click **Tools | Clean Unreferenced Files**.

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 "…searching…Please wait". Observe progress.

4. 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.

To clean unreferenced movies, do the following:

1. Click **Tools | Clean Unreferenced Movies**.

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 "…searching…Please wait". Observe progress.

4. 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.

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.

To download controller microcode, do the following:

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.

To download disk drive firmware, do the following:

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.

Chapter **5**

Managing stand-alone K2 systems with SiteConfig

This chapter contains the following topics:

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	—

	Task	Comment
☐	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	—
☐	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 control point PC

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

Requirements	Comments
Operating system	Microsoft Windows (Must be a U.S. version): XP Professional Service Pack 2, Server 2003, or Vista Enterprise Service Pack 1.
RAM	Minimum 512 MB, 1 GB recommended
Graphics acceleration	Must have at least 128 MB memory
Processor	Pentium 4 or higher class, 2 GHz or greater
Hard disk space	400 MB
Microsoft .NET Framework	Version 2.0
Java JRE	1.3.1_12 and 1.4.2_05 or higher. Required for the HP Ethernet Switch configuration interface, which is used for K2 Storage Systems (shared storage).
XML	Microsoft XML 4 Service Pack 2 is required. You can install it from the msxml4sp2 file on the K2 System Software CD.

About installing SiteConfig

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

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

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

Installing/upgrading SiteConfig

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

1. Procure SiteConfig installation files from the Grass Valley website or 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**.
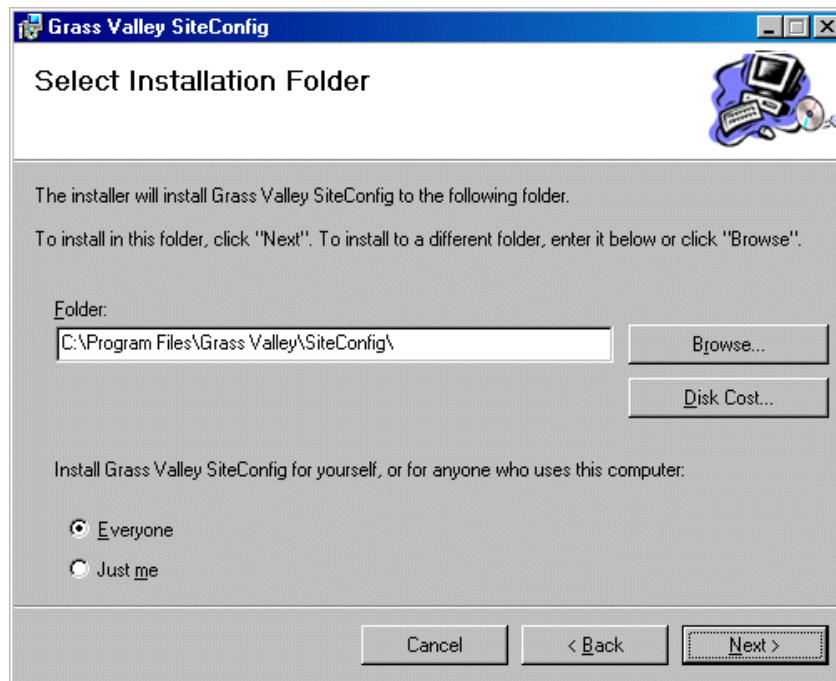
If the PC does not have the appropriate version of Microsoft .NET, the SiteConfig installation programs installs it.

5. Open the Windows operating system Services control panel on your Control Point PC and look for an entry called " ProductFrame Discovery Agent".

The Discovery Agent must be installed on the control point PC so that the control point PC can be discovered by SiteConfig and added to the system description as a managed device. This is necessary to ensure name resolution in SiteConfig's hosts file.

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 control point PC with a valid Ethernet IP address for the LAN using Windows Network Connections.

8. If you are not going to be using SiteConfig to manage system hosts files, put the system hosts file on the control point PC.

Creating a system description for stand-alone K2 clients

Do not do this task if:

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

Do this task if:

- You do not yet have a system description appropriate for managing your stand-alone K2 clients.

1. Open SiteConfig and proceed as follows:

   - If a dialog box opens that gives you the choice of creating or importing a system description, it means SiteConfig does not have access to a system description file. Click **Create**.

   - If the SiteConfig main window opens, click **File | New**.

   The Create New System Description dialog box opens.

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

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

3. Click **OK**.

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

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

   The New Site Wizard opens.
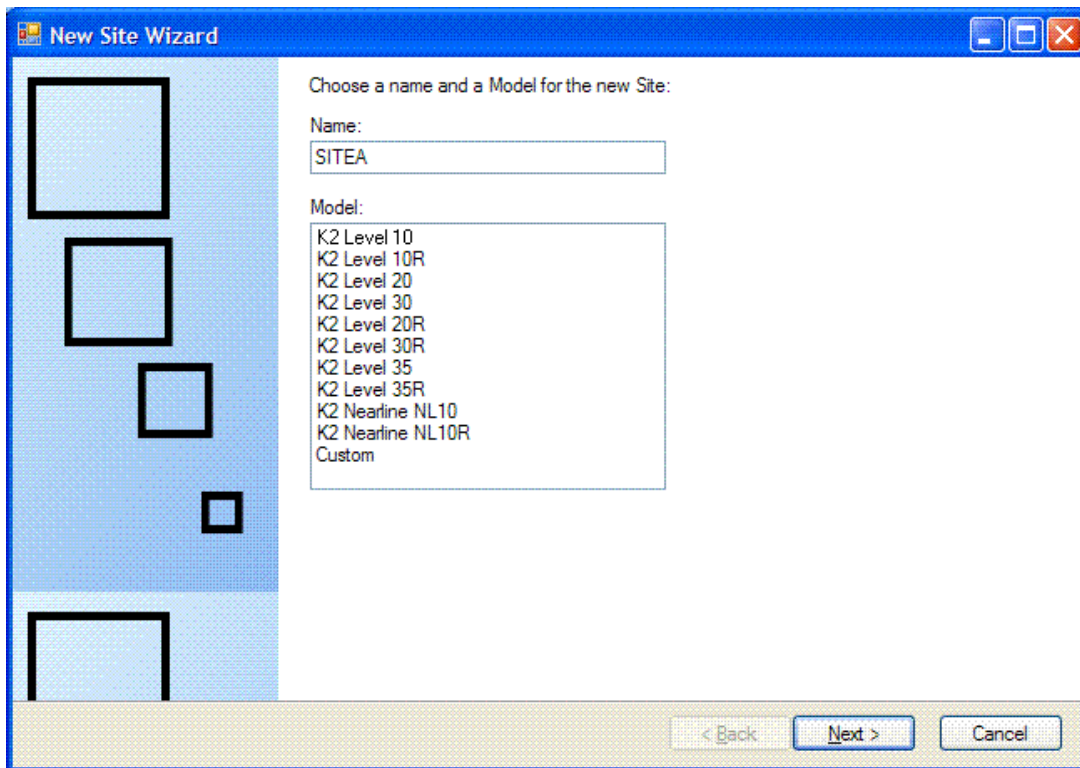
5. Enter a name for the site you are creating, considering the following:

- Keep the site name short, as it becomes the root identifier that is the default prefix for device and network names.

- Sites in the tree view are automatically sorted alphabetically.

6. Select **Custom** and click **Next**.

7. Click **Finish** to create the site.

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

Creating the control network for stand-alone K2 clients

1. In the **Network Configuration | Networks** tree view, select a System node or a Site node.

2. Proceed as follows:

- To add a network under the currently selected node, in the tree view right-click the node and select **Add Network**.

The Network Settings dialog box opens.
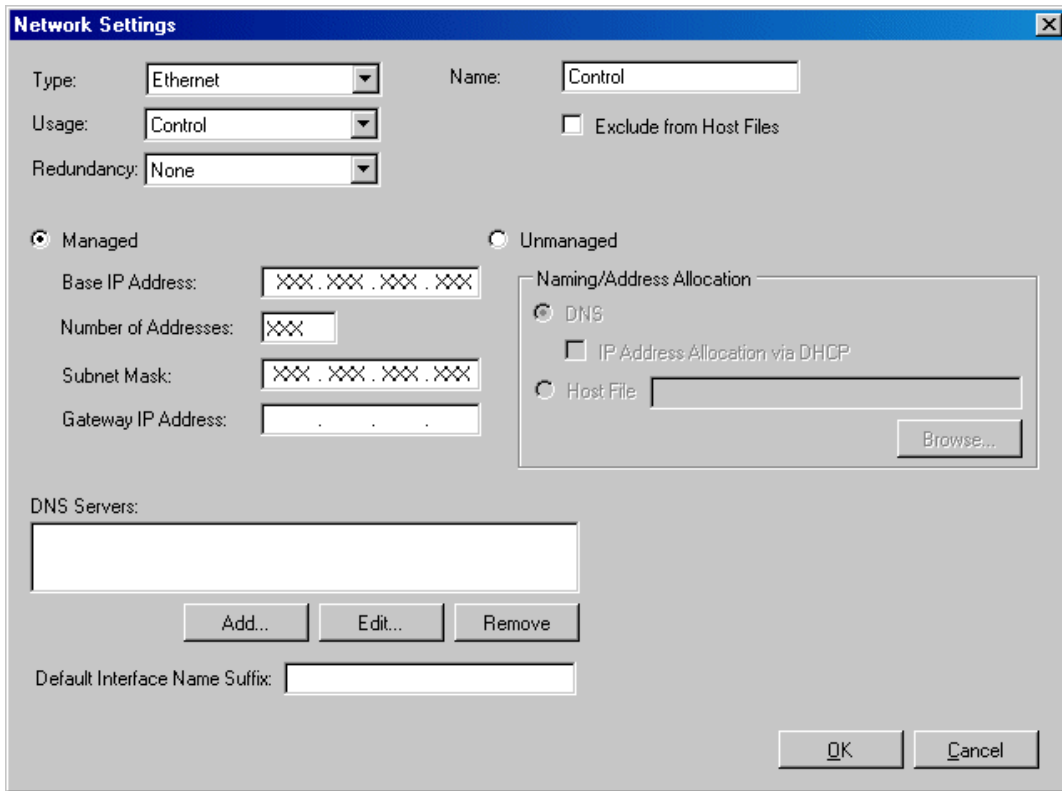
3. Configure the settings for the network as follows:

| Setting...	For control network
Type	*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

Prerequisites for this task are as follows:

• The system description contains a group.

1. In the **Network Configuration | Devices** tree view, right-click a group and select **Add Device**.
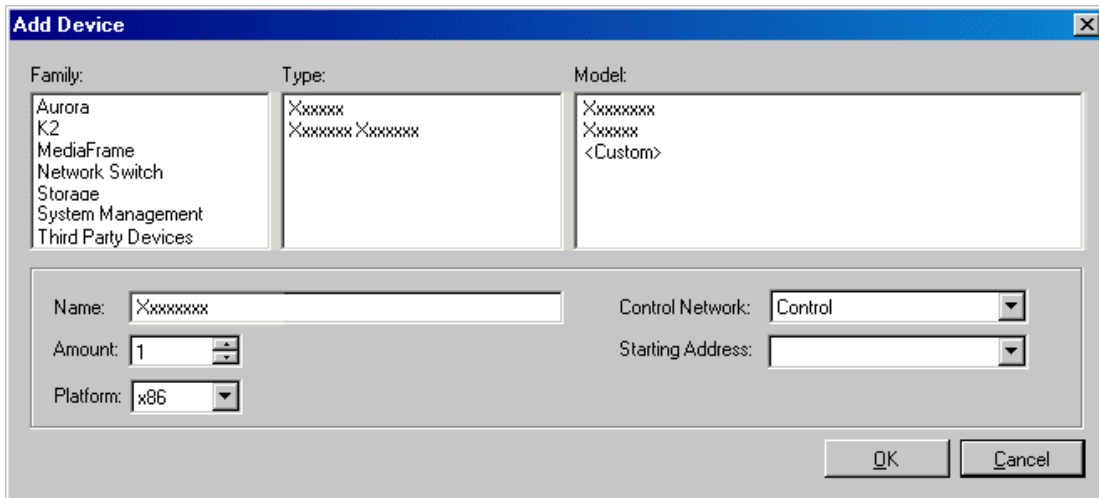
2. Configure settings for the device you are adding as follows:

- 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

Prerequisites for this task are as follows:

- The system description has a stand-alone K2 client that is a placeholder device.

- The placeholder device has a one or more unmanaged network interfaces.

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

- K2 Summit Production Client

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

   The interfaces for that device are displayed in the interfaces list view.
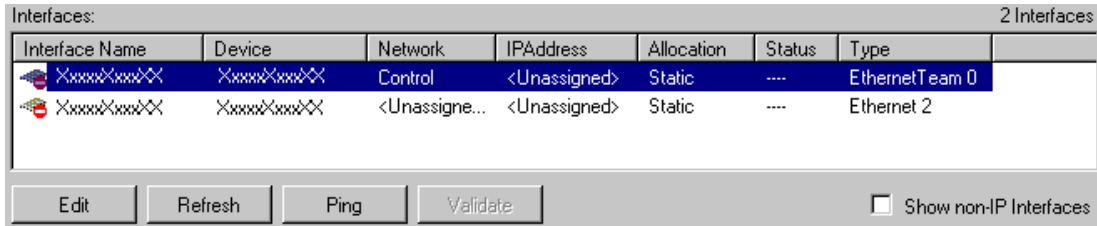
Edit the control network interface first.

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

   The Unmanaged Network Interface Details dialog box opens.
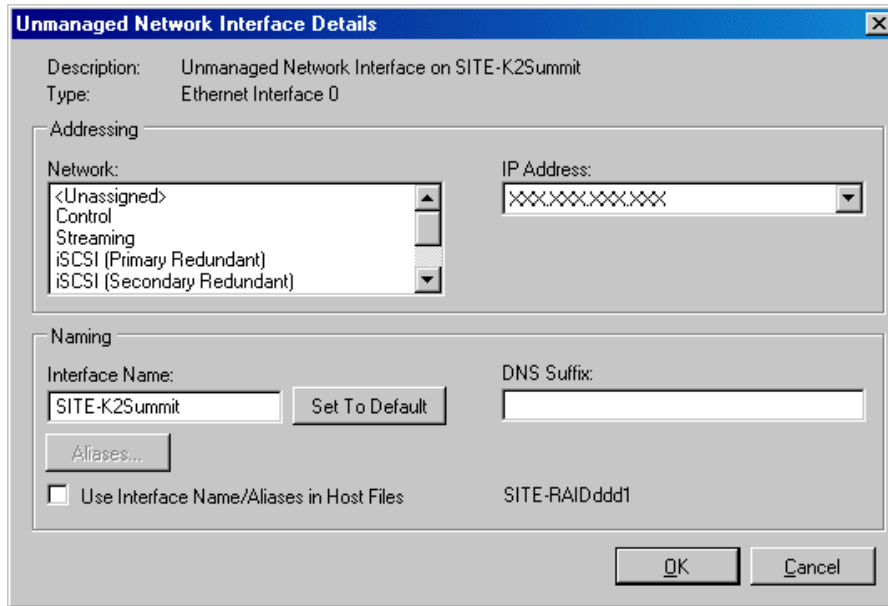
3. Configure the settings for the interface as follows:

Setting...	For control network interface
Network	*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.

Setting...	For control network interface
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

Prerequisites for this task are as follows:

• The Ethernet switch or switches that the support the control network are configured and operational. If multiple switches, ISLs are connected and trunks configured.

• The control point PC is communicating on the control network.

• There are no routers between the control point PC and the devices to be discovered.

• Devices to be discovered are Windows operating system devices, with SiteConfig support installed.

• Devices are cabled for control network connections.

1. Open SiteConfig on the control point PC.

2. In the toolbar, click the discover devices button. 🔎

   The Discover Devices dialog box opens.
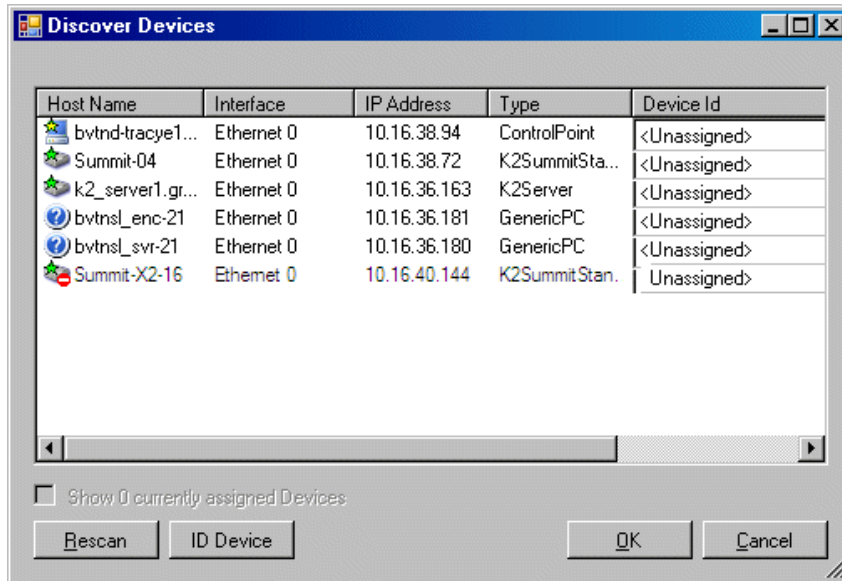
   A list of discovered devices is displayed.

3. Click **Rescan** to re-run the discovery mechanism. You can do this if a device that you want to discover has its network connection restored or otherwise becomes available. Additional devices discovered are added to the list.

Assigning discovered devices

Prerequisites for this task are as follows:

- Devices have been discovered by SiteConfig

- Discovered devices are not yet assigned to a device in the system description

- The system description has placeholder devices to which to assign the discovered devices.

1. If the Discovered Devices Dialog box is not already open, click the discover

   devices button 🔎.

   The Discover Devices dialog box opens.

2. Identify discovered devices.

   - If a single device is discovered in multiple rows, it means the device has multiple network interfaces. Choose the interface that represents the device's currently connected control connection. This is typically Ethernet ... 0.

   - If necessary, select a device in the list and click **ID Device**. This triggers an action on the device, such as flashing an LED or ejecting a CD drive, to identify the

device.

3. To also view previously discovered devices that have already been assigned to a device in the system description, select **Show … currently assigned devices**.

The currently assigned devices are added to the list. Viewing both assigned and unassigned devices in this way can be helpful to verify the match between discovered devices and placeholder devices.

4. In the row for each discovered device, view items on the Device Id drop-down list to determine the match with placeholder devices, as follows:

- If SiteConfig finds a match between the device-type discovered and the device-type of one or more placeholder devices, it displays those placeholder devices in the list.

- If SiteConfig does not find a match between the device-type discovered and the device-type of a placeholder device, no placeholder device is displayed in the list.

5. In the row for a discovered device, click the Device Id drop-down list and select the placeholder device that corresponds to the discovered device.

If there is no corresponding placeholder device currently in the system description, you can select **Add** to create a new placeholder device and then assign the discovered device to it.

6. When discovered devices have been assigned, click **OK** to save settings and close.

7. In the **Network Configuration | Devices** tree view, select each of the devices to which you assigned a discovered device.

Modifying stand-alone K2 client managed network interfaces

Prerequisites for this task are as follows:

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

- SiteConfig has communication with the device.

- The device is defined in the system description with an appropriate network interface.

Use this task to modify managed network interfaces on stand-alone K2 client models as follows:
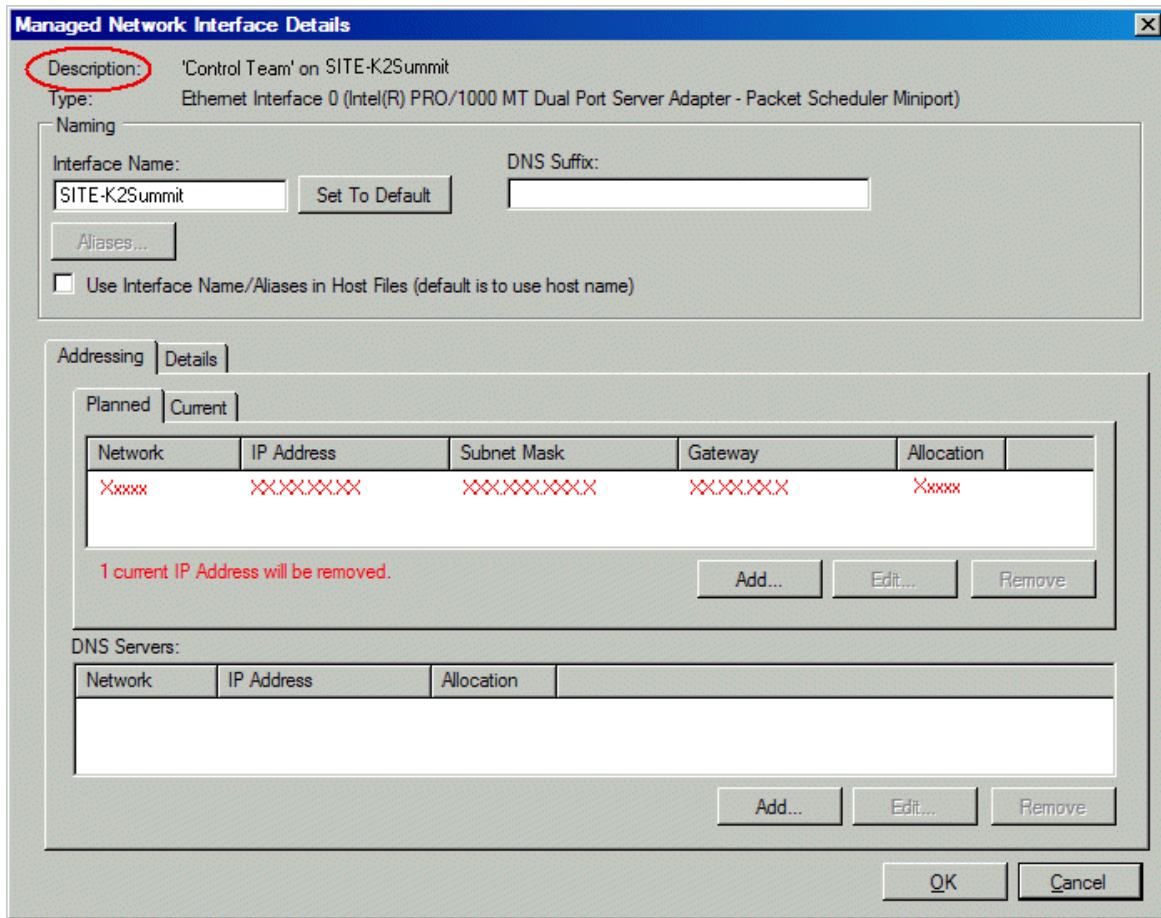
- K2 Summit Production Client

1. In the tree view select a K2 client, then in the Interfaces list view, identify interfaces as follows:

- For a stand-alone K2 Summit Production Client, the control network interface is a team. Modify the control team interface first. The control team is comprised of two individual interfaces, one for Control Connection #1 and one for Control Connection # 2. If these individual interfaces are displayed, do not modify them.

- A stand-alone K2 client's other interface is for FTP/streaming. If you have a FTP/streaming network, you can configure and use this interface if desired.

2. In the Interfaces list view determine the interface to configure, as follows:

- Identify the interface with which SiteConfig is currently communicating, indicated by the green star overlay icon. This should be the control network interface.

- Verify that the interface over which SiteConfig is currently communicating is in fact the interface defined for the control network in the system description. If this is not the case, you might have the control network cable connected to the wrong interface port.

- Configure the control network interface first before configuring any of the other interfaces.

- After you have successfully configured the control network interface, return to this step to configure each remaining interface.

3. In the Interfaces list view, check the icon for the interface you are configuring.

   If the icon has a red stop sign overlay, it indicates that current settings and planned settings do not match or that there is some other problem. Hover over the icon to read a tooltip with information about the problem.

   For the K2 Summit Production Client, make sure that the device is unlocked in SiteConfig before proceeding. This disables the write filter.

4. In the Interfaces list view, right-click the interface you are configuring and select **Edit**.

   The Managed Network Interface Details dialog box opens.

Managed Network Interface Details

Description: 'Control Team' on SITE-K2Summit
Type: Ethernet Interface 0 (Intel(R) PRO/1000 MT Dual Port Server Adapter - Packet Scheduler Miniport)

Naming

Interface Name:
SITE-K2Summit   Set To Default

DNS Suffix:

Aliases...

☐ Use Interface Name/Aliases in Host Files (default is to use host name)

Addressing | Details

Planned | Current

Network	IP Address	Subnet Mask	Gateway	Allocation	
X.xxxx	XX.XX.XX.XX	XX.XX.XX.X	XX.XX.XX.X	X.xxxx	

1 current IP Address will be removed.   Add...   Edit...   Remove

DNS Servers:

Network	IP Address	Allocation	

Add...   Edit...   Remove

OK   Cancel

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

- Identify Ethernet LAN adapters by their "Description" name. This is the Windows connection name. SiteConfig reads this name from the device and displays it at the top of this dialog box. This is the most accurate way to identify the network adapter on the discovered device that you are configuring.

- For a K2 Summit Production Client, when you configure its first interface, make sure you are configuring the 'Control Team' interface.

6. Configure naming settings as follows:

Setting...	For network interface Control Team
Interface Name	The device host name. Required.
Set To Default	Not recommended
DNS Suffix	Allowed, if applicable to the network. The DNS suffix is added to the interface name.
Aliases	Not allowed

Setting...	For network interface Control Team
Use Interface Name/Aliases in Host Files	*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.
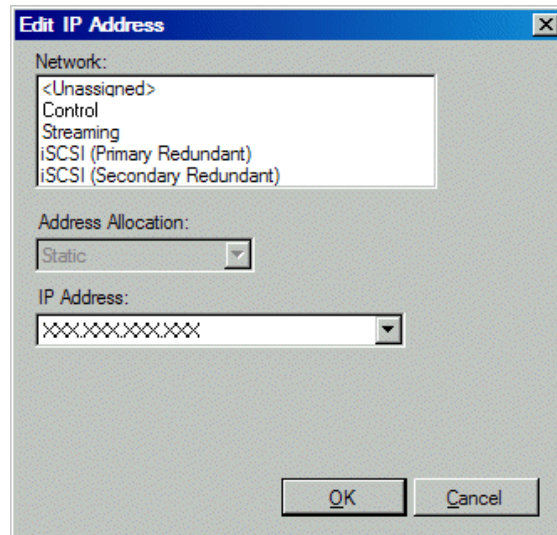
   b. Edit IP address settings as follows:

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.

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

Adding a control point PC placeholder device to the system description

Prerequisites for this task are as follows:

• The system description contains a group.

1. In the **Network Configuration | Devices** tree view, right-click a group and select **Add Device**.
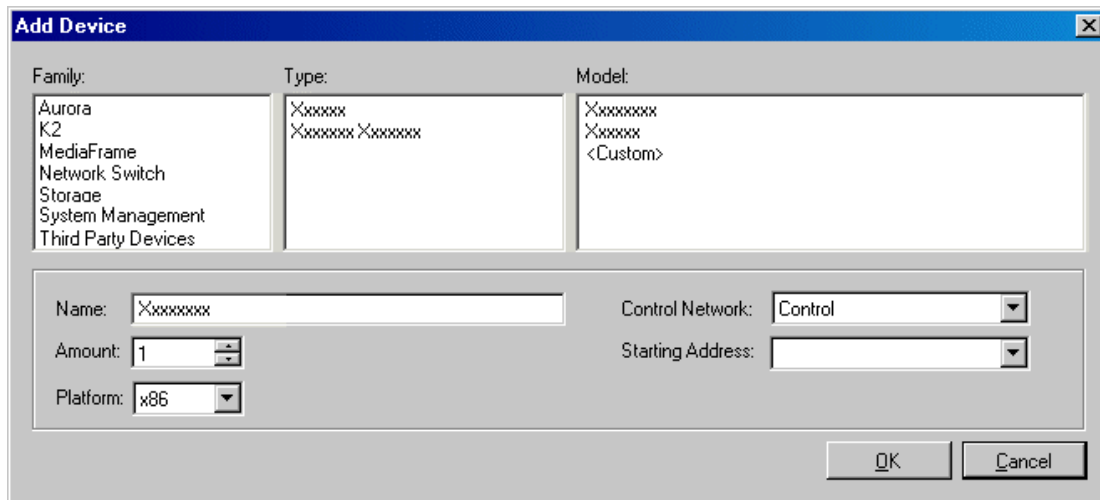
The Add Device dialog box opens.

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

Prerequisites for this task are as follows:

- The SiteConfig control point PC has 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 contains a control point PC placeholder device.

- The placeholder's control network interface is configured with the control network IP address that is currently on the actual control point PC.

- The device name of the control point PC placeholder is same as the host name of the actual control point PC.

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

1. Open SiteConfig on the control point PC.

2. Discover devices and identify the control point PC discovered device.

3. Assign the discovered device to the control point PC placeholder.

4. In the **Network Configuration | Devices** tree view, select the control point PC.

5. In the Interfaces list view, right-click the control network interface and select **Edit**.

   The Managed Network Interface Details dialog box opens.

6. Evaluate IP settings as follows:

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

- If both a Current tab and a Planned tab are displayed, it means the planned settings you configured on the placeholder device are not identical to those on the actual control point PC. If this is the case, do not apply planned settings. Doing so overwrites IP settings on the actual control point PC, which stops network communication. Instead, select the **Planned** tab and click **Remove**.

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

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

Making the host name the same as the device name

1. Verify that the current device name, as displayed in the SiteConfig tree view, is the same as your desired host name.

2. In the **Network Configuration | Devices | Device** list view, right-click the device and select **Edit**.

   The Edit Device dialog box opens.

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

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

4. Click **OK**.

Pinging devices from the control point PC

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

1. In the **Network Configuration** | **Networks** tree view, select a network, site, or system node.

2. In the Devices list view, select one or more devices. Use Ctrl + Click or Shift + Click to select multiple devices.

3. Right-click the selected device or devices and select **Ping**.

   The Ping Devices dialog box opens and lists the selected device or devices.

The Ping Devices dialog box reports the progress and results of the ping command per device.

About hosts files and SiteConfig

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

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

• If you do not want SiteConfig to manage your host table information, you can manage it yourself. This is typically the case if your facility has an existing hosts file that contains host table information for devices that are not in the SiteConfig system description. In this case, you can have SiteConfig generate a single hosts file that contains the host table information for the devices in the system description. You can then copy the desired host table information out of the SiteConfig hosts file and copy it into your facility hosts file. You must then distribute your facility hosts file to devices using your own mechanisms.

• If you want SiteConfig to manage all information in hosts files on devices, you can have SiteConfig copy its hosts file to devices. In so doing, SiteConfig overwrites the existing hosts files on devices. Therefore, this requires that all devices that have name resolution through the hosts file be configured accordingly in the SiteConfig system description.

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

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

Generating host tables for devices with SiteConfig

Prerequisites for this task are as follows:

• Planned control network settings are applied to control network interfaces and devices are communicating on the control network as defined in the system description.

• Interfaces for networks that require name resolution via the hosts file, such as the FTP/streaming network, have settings applied and are communicating.

• You have viewed host names, as currently defined in the system description, and determined that they are correct.

• The control point PC is added to the system description so that it is included in the host tables generated by SiteConfig.

1. In the **Network Configuration | Networks** tree view, select a network, site, or system node.

2. Click **View Hosts file**.

   A Hosts File Contents window opens that displays the contents of the hosts file as currently defined in the system description.

3. Verify the information in the hosts file.

4. Do one of the following:

- If you are managing host table information yourself, click **Save As** and save a copy of the hosts file to a location on the control point PC. Then open the copy of the hosts file, copy the desired host table information from it, and paste it into your facility hosts file as desired. Then you can use your own process to distribute the facility hosts file to devices. Remember to distribute to the control point PC so that SiteConfig and other management applications such as K2Config can resolve network host names.

- If SiteConfig is managing hosts files, do the following:

Writing hosts files to multiple devices consumes system resource and network bandwidth. Therefore it is recommended that you wait and do this after the system is complete and fully implemented, rather than updating hosts files incrementally as you discover/assign devices.

a. In the **Network Configuration | Devices | Devices** list view, right-click a device to which you intend to write the hosts file and select **View Current Host File**.

A Host File Contents window opens that displays the contents of the hosts file that is currently on that actual device.

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

c. In the **Network Configuration | Devices | Devices** list view, right-click a device or use Ctrl + Click to select multiple devices, and select **Update Host File**.

The current hosts file is overwritten with the hosts file as defined in the system description.

Configuring deployment groups

Prerequisites for this procedure are as follows:

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

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

A deployment group appears in the tree view.

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

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

The Add Target Device(s) wizard opens.
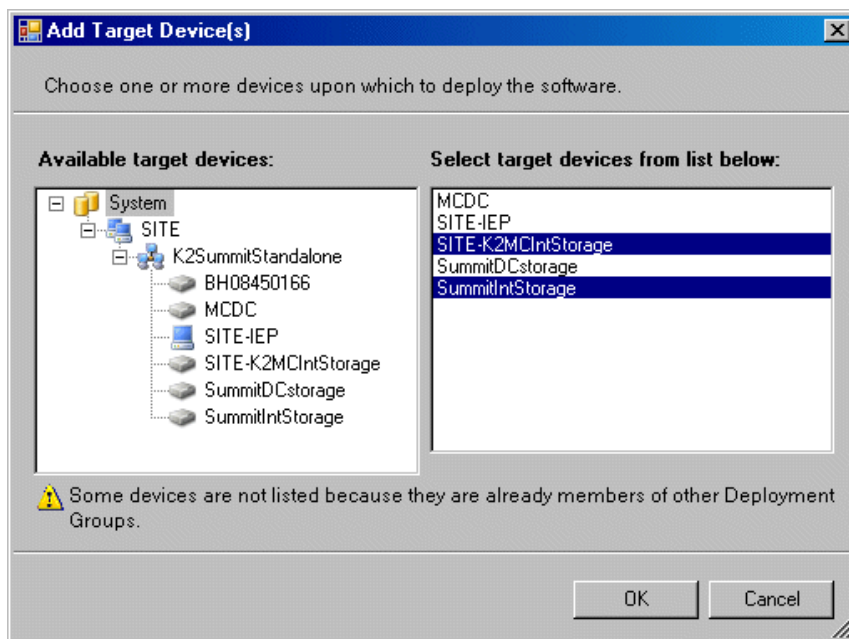
4. In the Available Target Devices tree view, select the node that displays the devices that you are combining as a deployment group.

5. In the right-hand pane, select the devices that you are combining as a deployment group.

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

6. Click **OK**.

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

About deploying software for stand-alone K2 clients

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

Chapter *6*

Managing K2 system software

This chapter contaK2 Edge Transmission Serverins the following topics:

- "About K2 system software"
- "Installing Control Point software"
- "Installing K2 software"
- "Backup and recovery strategies"

About K2 system software

Check *K2 Release Notes* for the latest information about software.

At the time of this writing, the primary software installations for the K2 Summit Production Client and K2 products are as follows:

This software…	Is distributed on…	With the installation file located at…	Which is installed on…	And is described as follows:
K2 Client	The K2 System Software CD and via download	..\K2Client\setup.exe	K2 Summit Production Clients and K2 Media Clients	Provides core functionality for all K2 clients models.
K2 Server	The K2 System Software CD and via download	..\K2Server\setup.exe	K2 Media Servers	Provides core functionality for all K2 Media Servers in all roles.
Control Point	The K2 System Software CD and via download	..\ControlPoint\setup.exe	Control Point PCs	Provides remote control and configuration of K2 clients (both internal and external storage) as well as the K2 SAN.
Media File System (SNFS)	The K2 System Software CD and via download	..\snfs\gvSnfsxxSetupK2.bat	K2 Media Servers, stand-alone K2 clients, and shared storage (SAN) K2 clients	Provides a dedicated file system for access to media data. Install only as instructed by release notes.
NetCentral	The NetCentral Manager CD	..\ServerSetup.exe	The NetCentral server PC (this can be a Control Point PC)	Provides remote monitoring of all K2 products.

In addition, the following software is installed in special cases:

- Multi-Path I/O software — You must install this software on K2 Summit Production Clients and K2 Media Clients that are part of a redundant K2 SAN and

on K2 Summit Production Clients and K2 Media Clients with direct-connect storage.

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.
	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. Refer to . Then install software and configure as follows:

1. Set up Windows user accounts according to your site's security policies. The accounts and the case-sensitive passwords that match the factory default accounts on K2 systems are as follows:

   - Administrator:adminK2

   - K2Admin:K2admin

   - K2User:K2user

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 the K2 System Software CD.

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 the K2 System Software CD.

   - Adobe Acrobat Reader, for reading documentation from the K2 Documentation CD.

5. Install SiteConfig. It is recommended that you use SiteConfig to manage stand-alone K2 clients. It is required that you use SiteConfig to manage K2 SANs.

6. Install NetCentral and its supporting software, such as the following:

   - NetCentral Manager

   - Basic IIS 6.0 package

   - SNMP (Windows Components)

   Refer to NetCentral manuals for complete installation and configuration instructions.

   NetCentral is required and included as part of the product for shared storage K2 clients and the K2 SAN. NetCentral is optional but recommended for stand-alone K2 clients.

7. Create a backup image.

Installing K2 software

Except as noted in the preceding sections, when you receive your K2 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 system, refer to the *K2 Release Notes* 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 clients to the same software version. Upgrade K2 Media Servers first, then K2 clients. Refer to *K2 Release Notes* 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 *K2 Release Notes* 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 Summit Production Client	K2 Summit Production Client 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 client Service Manual

Chapter **7**

Administering and maintaining the K2 system

This chapter contains the following topics:

Also refer to Chapter 9, *K2 Summit Transmission Server Package* for information unique to that product.

About the write filter

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

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

To enable the write filter, the K2 system must be restarted. Likewise, to disable the write filter, the K2 system must be restarted. You can enable/disable the write filter remotely using the SiteConfig lock/unlock feature on one K2 system at a time or on a group of K2s all at once. You can also enable/disable the write filter from a local K2 system.

Enabling the write filter

Prerequisite:

• K2 software must be installed on the K2 system.

1. If you have not already done so, log in to the K2 system with administrator privileges.

2. From the Windows desktop click **Start | All Programs | Grass Valley | Write Filter Utility**.

   FBWF Manager opens.

3. Under Filter Settings, set Filter to **Enable**.

4. Under Protected Volumes, set C: to **Protected**.

5. Click **OK**.

6. When prompted, restart the K2 system.

Disabling the write filter

Prerequisite:

• K2 software must be installed on the K2 system.

1. If you have not already done so, log in to the K2 system with administrator privileges.

2. From the Windows desktop click **Start | All Programs | Grass Valley | Write Filter Utility**.

   FBWF Manager opens.

3. Under Filter Settings, set Filter to **Disable**.

4. Click **OK**.

5. When prompted, restart the K2 system.

Committing a file to disk with write filter enabled

Prerequisite:

• K2 software must be installed on the K2 system.

You can over-ride the write filter for an individual file and permanently save the file to disk.

1. If you have not already done so, log in to the K2 system with administrator privileges.

2. From the Windows desktop click **Start | All Programs | Grass Valley | Write Filter Utility**.

   FBWF Manager opens.

3. Under Exclusions, click **Browse**.

4. Browse to the file that you want to save permanently, select the file and click **OK**.

Files in directories that exist on the Compact Flash can be created. New directories cannot be created. You cannot commit deletions of files.

5. Click **Commit**.

6. Click **OK**.

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 includes the following topics:

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 settings in the Windows operating system. Refer to the next section "Security and user accounts" on page 161.

- 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. Refer to the next section "Security and user accounts" on page 161.

- 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. Refer to "AppCenter operations and media access security" on page 163.

  - 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. Refer to "FTP and media access security" on page 163.

  - 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. Refer to "Protocol control of channels and media access security" on page 164.

- Channel access — 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. Refer to "Configuring channel access security" on page 165.

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.	"Security and user accounts" on page 161
Configure a "userA" account and a "userB" account on the local K2 client.	Use standard Windows procedures
Log on to AppCenter with K2 administrator permissions.	"Security and user accounts" on page 161
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 161

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 161

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.	"Security and user accounts" on page 161
Configure a "userA" account and a "userB" account on the local K2 client.	Use standard Windows procedures
Log on to AppCenter with K2 administrator permissions.	"Security and user accounts" on page 161

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
	"Configuring channel access security" on page 165

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
	"Configuring channel access security" on page 165

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.	—

Security and user accounts

To provide a basic level of security, the K2 system ships from the factory with three pre-configured Windows operating system user accounts, with login usernames Administrator, K2Admin, and K2User. From these accounts, the K2 system enforces security levels, as shown in the following table.

	Windows administrator	K2 administrator	K2 user	Unknown user (a login that is not one of the default accounts)
Login	Administrator	K2Admin	K2User	N/A[a]
Password (case sensitive)	adminK2	K2admin	K2user	N/A
AppCenter Configuration Manager	Full access	Full access	Can view	Can't access
AppCenter	Full access	Full access	Full access; requires an account on the K2 system(s)	Can view channel suites, channel status, on-line help and System Status pane. Can export logs.
Storage Utility	Full access[b.]	Full access	Can't access	Can't access
K2 System Configuration application	Full access[b]	Full access	Can't access	Can't access
Windows Operating System	Full access	Limited access (based on Windows login privileges)	Limited access (based on Windows login privileges)	Limited access (based on Windows login privileges)

[a.] The unknown user, like all others who access the K2 system, must have a valid Windows login for the K2 system or the control point PC through which the K2 system is being accessed.

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

Using standard Windows operating system procedures and the Microsoft Management Console, you can set up additional local users and groups, as well as domain users and groups. Once these are set up, they are available to K2 security features. In this way you can set up a security framework to match your site's unique security requirements.

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* and *mxfmovie* 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.
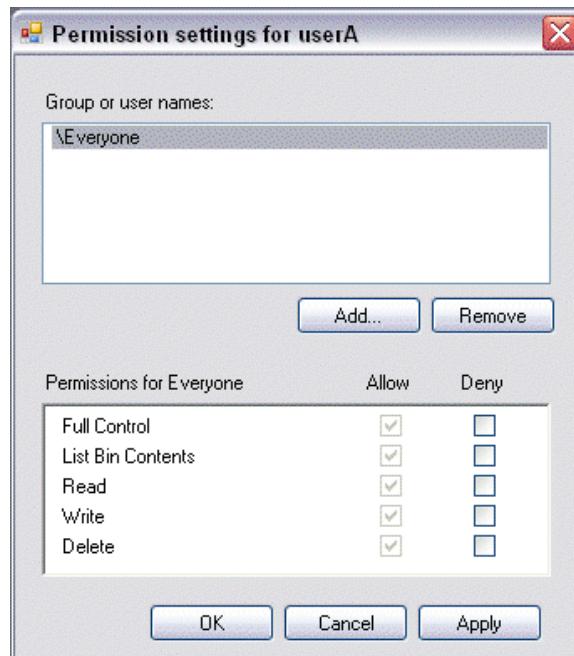
5. Add users and groups to the access control list and set permissions as follows:

    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 compatibility FTP access conventions, accounts for user *movie* or user *mxfmovie* are provided on the K2 system. 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. To simplify account setup and maintenance, you can use domain users and groups rather than local users and groups.

If you use local users and groups, to support media access security you must have those same exact local accounts set up on each K2 client and K2 Media Server within the K2 SAN. However, you don't need to set up security via AppCenter on each K2 client. When you modify permissions on a shared storage bin from one K2 client, then permissions are enforced similarly on all of the K2 clients in the 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.

To associate a protocol channel with a user account, do the following:

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.

Configuring 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, set up a channel access control list, 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. 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.
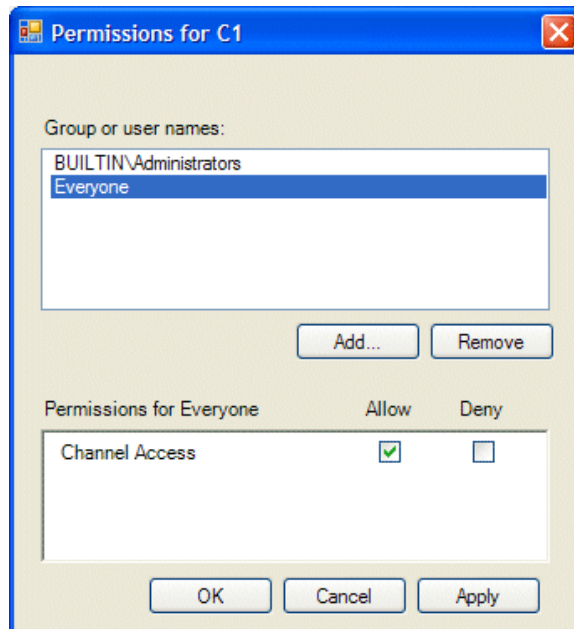
7. Add users and groups to the access control list and set permissions as follows:

   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 NetCentral security considerations

When using K2 with NetCentral, bear in mind that NetCentral has its own levels of security. Grass Valley recommends mapping the NetCentral administrator with the K2 administrator level application access. You need Windows administrator privileges to add or modify a user's privileges.

Mapping a NetCentral administrator to the K2 administrator level

The following procedure uses K2Admin as an example of a user name. You may want to modify the administrator accounts to bring them in line with your site's security policies.

A user who belongs to a group has all the rights and permissions granted to that group. To be able to use NetCentral and K2, you need to create a local K2Admin user account and add it to the NCAdministrator group on the NetCentral Server PC. (This could also be the Control Point PC.)

1. Create the user named K2Admin:

   a. Open Computer Management.

   b. In the console tree, right-click on the Users folder.

   c. Select New User.

   d. In the New User dialog box, enter the user name **K2Admin** and the password **K2admin**.

   e. Select or clear the check boxes, as desired, for:

      - User must change password at next logon

      - User cannot change password

      - Password never expires

      - Account is disabled

   f. Click Create, and then click Close.

2. Add the NCAdministrator group to the K2Admin user:

   a. Open Computer Management.

   b. In the console tree, click Users.

c. Right-click the K2Admin user and select Properties.

d. Select the Member Of tab and click Add.

e. Enter the group name `NCAdministrator` and click OK.
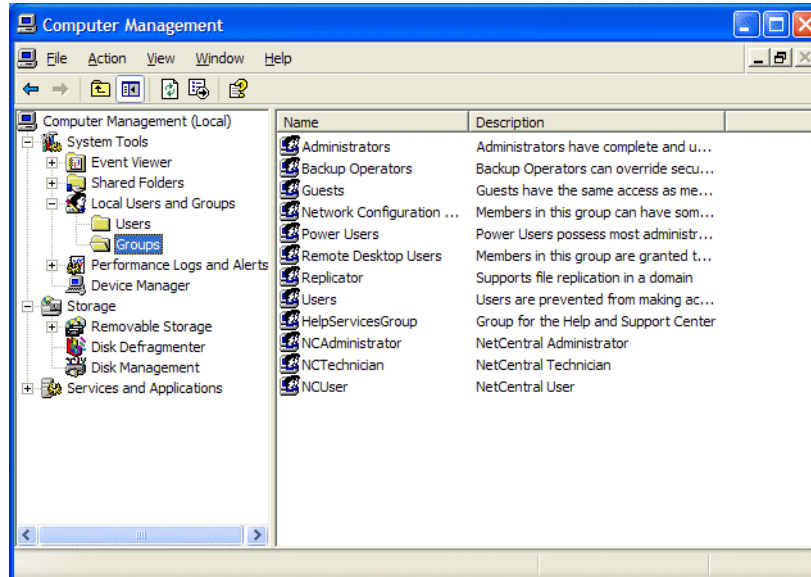
For more information on NetCentral security, see the NetCentral on-line Help.

Microsoft Windows updates

The K2 Summit Production Client or K2 Solo Media Server operating system is Microsoft Windows XP Embedded. Publicly available Microsoft Windows updates do not apply to the Microsoft Windows Embedded operating systems. Do not attempt to install a Microsoft Windows update on a K2 Summit Production Client or K2 Solo Media Server except as specifically instructed by product documentation or by Grass Valley Support.

Other Grass Valley products, such as the K2 Media Server, have a non-embedded Windows operating system. Grass Valley recognizes that it is essential to be able to deploy Microsoft security patches to these Windows-based products as quickly as possible. As Grass Valley systems are used to meet the mission-critical requirements of your environment, we feel it is imperative that systems be kept up to date in order to maintain the highest level of security available. To that end, we encourage you to install all high priority operating system 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 our products to properly function with the Microsoft update in question.

Please note that this policy applies to "High Priority" updates only. There are countless other updates not classified as "High Priority" which are made available by Microsoft. If you feel that one or more of these other updates must be applied, we request that you contact Grass Valley prior to installation.

You should exercise common sense when applying these updates. Specifically, updates should not be downloaded or installed while a Grass Valley product is being used for mission critical purposes such as play to air.

Virus scanning policies

The K2 system is based on the Microsoft Windows operating system. It is important to defend this system against virus or SpyWare attacks. Grass Valley supports the scanning of the K2 system drives (the disk drives or drive partition used to house the operating system and installed application software) from a PC that is running the scanning program while the K2 system is being used to record or play video to air. The anti-virus package executing on the PC can be scheduled to scan the system drives of multiple K2 systems.

The following strategies are recommended for virus scanning:

- Run the scanning software on a dedicated PC that connects to the K2 system via a network mount. Do not run scanning software locally on the K2 system.

- Connect to the K2 system via 100BaseT network. This constrains the bandwidth and system resources consumed, so as to not interfere with media operations. Do not connect and scan via Gigabit Ethernet.

- Grass Valley does not support the running of anti-virus programs on a K2 system. This includes K2 Media Server, K2 Media Client, K2 Summit Production Client, and K2 Solo Media Server.

With these recommended strategies, you should be able to scan the K2 system without interrupting media access.

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.

- If operating with an Aurora Browse system, ports should allow incoming packets so requests to the Proxy NAS can be properly processed. The port that needs to be open is port 445 for TCP and UDP for Windows and SAMBA shares. If your site's policies require that these port numbers change, contact Grass Valley support for assistance.

- Access to the K2 system should be controlled in order to limit the likelihood of malicious or unintended introduction of viruses.

- The front and rear USB ports of the K2 system should normally be disabled; they should only be used by Windows administrators. (If a K2 system has USB RS-422 cards, be careful not to disable the RS-422 USB.) For more information, see "Enabling and disabling the USB ports" on page 170.

Enabling and disabling the USB ports

Grass Valley recommends that the front and rear USB ports be disabled. This protects the K2 system from exposure to unauthorized files. If a K2 system has USB RS-422 cards, do not disable the RS-422 USB. As an example, the following illustration shows which USB ports should be disabled in Windows Device Manager on a K2 system.
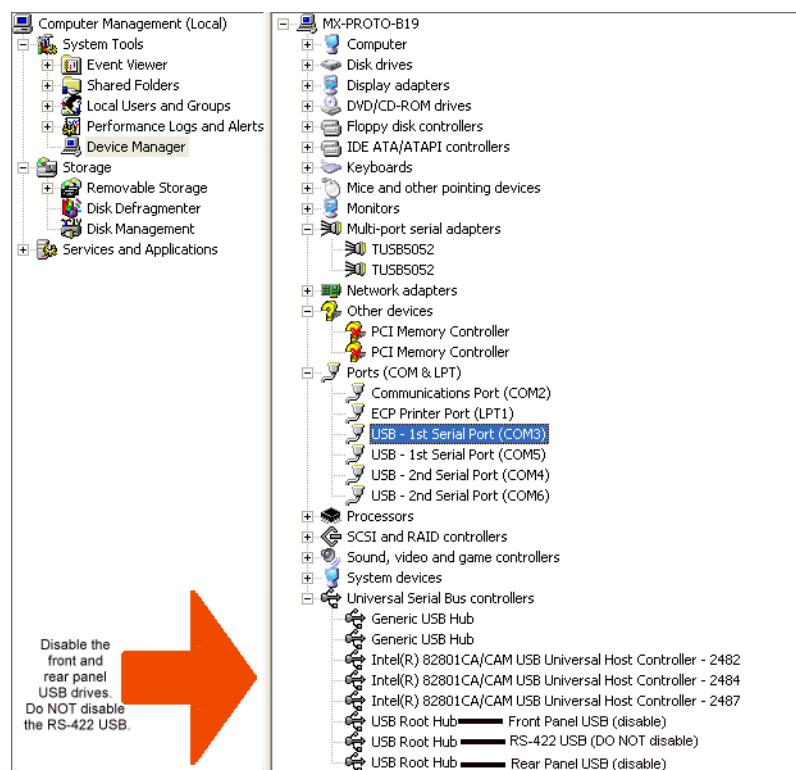
Only the Windows administrator, working locally, can enable or disable USB ports. To enable a USB port, right-click on the USB device in Windows Device Manager and select **Enable**. You cannot enable the a K2 system USB port via a control point PC.

To transfer to or from a USB drive on an internal storage K2 system, the Windows administrator should first enable the USB port. When the transfer is complete, the Windows administrator should then disable the USB port to prevent unauthorized use. Transferring to and from a USB drive is supported on a local internal storage K2 system only. USB drive transfers on shared storage K2 clients, K2 Media Servers, 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.

Configuring 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 Windows 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 Windows XP, 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 "Regional and Language Options", you can make settings on the "Regional Options" tab and on the "Languages" tab as desired. K2 AppCenter supports these settings and displays dates, times, and other values as appropriate. However, there are special requirements for the settings on the "Advanced" tab to support FTP transfers. Do not change settings on the "Advanced" tab. Refer to "FTP internationalization" on page 55 and "Internationalization" on page 214 for more information.

Chapter **8**

Direct Connect Storage

Use the following topics to install direct-connect storage for a K2 Summit Production Client or K2 Media Client:

- "Setting up direct-connect RAID storage" on page 173
- "Powering up K2 RAID" on page 177

Setting up direct-connect RAID storage

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 has one type of optional Fiber Channel card, the 4 Gb/s LSI Fibre Channel card.

A K2 Media Client has two types of optional Fibre Channel cards. The type of card installed can be identified from the rear panel, as follows:

- The 2 Gb/s GVG SCSI Fibre Channel card. The exposed plate of the card has vent holes and there are no LEDs on the card.
- The 4 Gb/s LSI Fibre Channel card. The exposed plate of the card is solid (no vent holes), and there are LEDs on the card.

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.

Prerequisites for the following procedure are as follows:

- If a 2 Gb/s GVG SCSI Fibre Channel card on a K2 Media Client, RAID controllers must be configured for 2 Gb/s. Contact Grass Valley Support for information about this configuration.
- If a 4 Gb/s LSI Fibre Channel card on a K2 Media Client or K2 Summit Production Client, RAID controllers must be configured for 4 Gb/s. This is the default configuration as shipped from Grass Valley.

To set up media storage for a direct connect RAID K2 client, do the following:

1. Connect the K2 client and RAID devices as shown in the following illustrations. Use the illustration appropriate for the K2 client model.

K2 Media Client
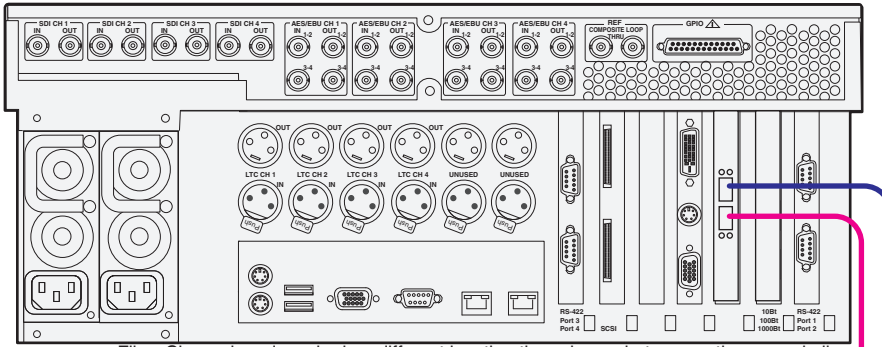
Fibre Channel card can be in a different location than shown, but connections are similar.

To K2 RAID
Controller

To K2 RAID
Controller

K2 Summit Production Client
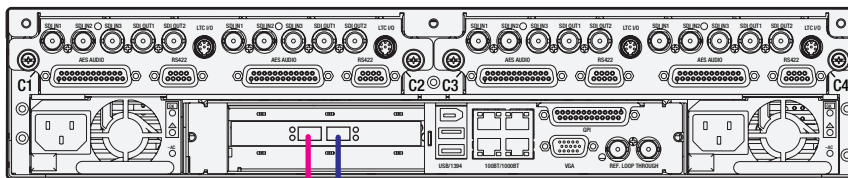
To K2 RAID
Controller

To K2 RAID
Controller
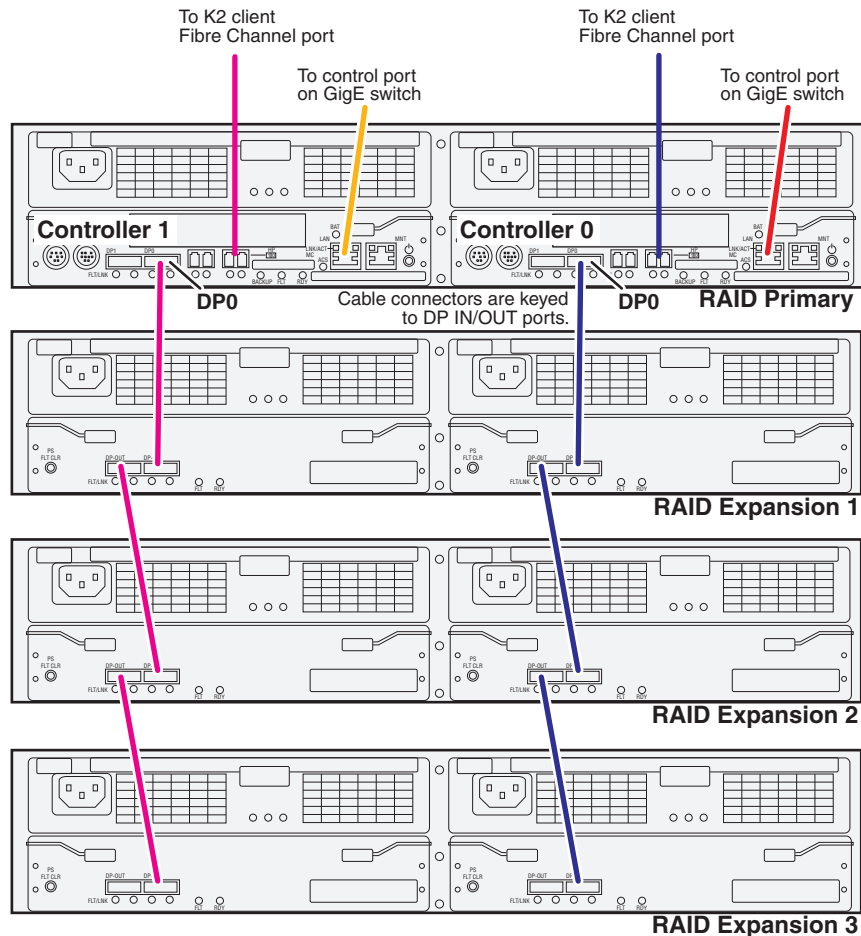
Connect K2 client Fibre Channel ports to RAID controllers. Connect Fibre Channel port 1 to RAID controller 0. If you have the redundant controller, connect Fibre Channel port 2 to RAID controller 1.

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 up 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 follows:

   a. On the K2 client, from the Windows desktop click **Start | Run**, type cmd and press **Enter**. The MS-DOS command prompt window opens.

   b. From the command prompt, navigate to the *C:\profile\mpio* directory.

   c. Type the following at the command prompt:

   ```
   gdsminstall.exe -u C:\profile\mpio gdsm.inf Root\GDSM
   ```

   d. Press **Enter**.

   The MPIO software is uninstalled.

9. Restart the K2 client and 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.

   b. Bind the disks in the external RAID. Bind in groups of six disks as RAID 5.

   NOTE: On a K2 Media Client, do not attempt to unbind or otherwise configure the RAID 1 system drive, which is made up of the two RAID disks in the K2 Media Client chassis.

   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 follows:

   a. From the Windows desktop click **Start | Run**, type cmd and press **Enter**. The MS-DOS command prompt window opens.

   b. From the command prompt, navigate to the *C:\profile\mpio* directory.

   c. Type the following at the command prompt:

   ```
   gdsminstall.exe -i c:\profile\mpio gdsm.inf Root\GDSM
   ```

   d. Press **Enter**.

   The MPIO software is installed.

17. Restart the K2 client and log in to Windows.

18. To verify that the software is installed, on the Windows desktop right-click **My Computer** and select **Manage**. The Computer Management window opens.
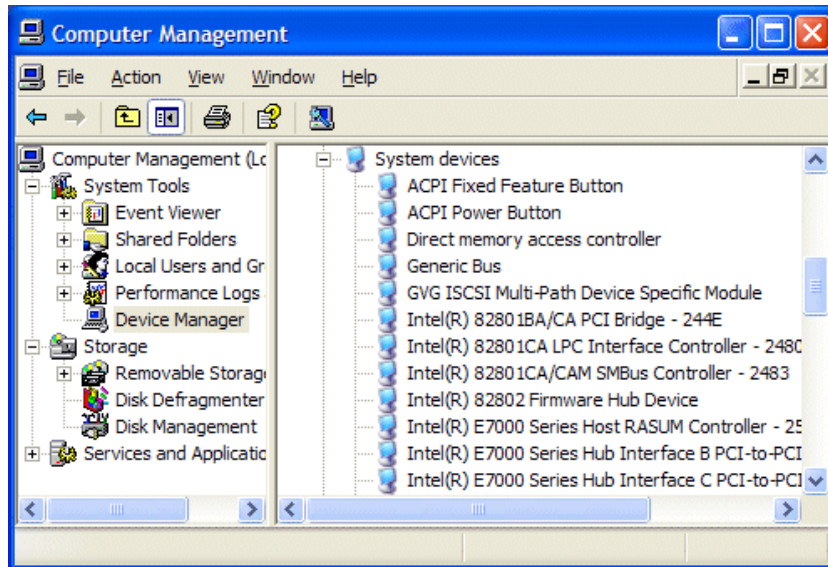
19. In the left pane select **Device Manager**.

20. In the right pane open the **System devices** node and verify that **GVG ISCSI Multi-Path Device Specific Module** is listed.

21. In Storage Utility, make a new file system

    If you get a "…failed to remove the media database…" message, you can safely proceed.

22. Restart the K2 client and log in to Windows.

23. Open AppCenter and manually remove all clips and bins except the default bin and the recycle bin.

24. 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.

25. As you install K2 Client software, when you arrive at the Specify Target Type page, select **K2 with local storage**.

26. Restart the K2 client.

27. On a K2 Media Client, from the Windows desktop system tray, open SQL Server Service Manager and verify that **Auto-start service when OS starts** is selected. (This is not required on a K2 Summit Production 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.

Powering up K2 RAID

To power up K2 RAID devices, do the following:

1. Verify power and cabling.

2. Press and hold down the power button on the controller, as shown.
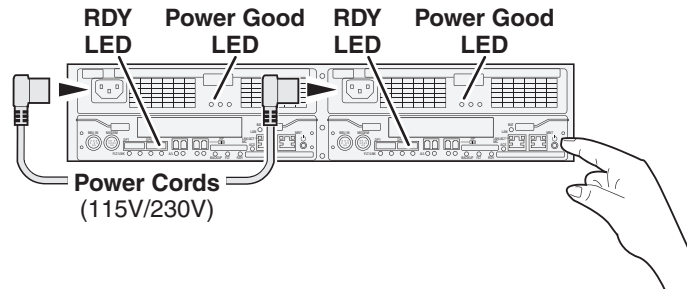
If the RAID chassis has two controllers, you can press the power button on either controller. You do not need to press both power buttons.

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.

Chapter **9**

K2 Summit Transmission Server Package

Topics in this chapter include the following:

- "K2 Summit Transmission Server Package features"
- "K2 Summit Transmission Server Package requirements and restrictions"
- "Storage Utility procedures for the K2 Summit Transmission Server Package"

This chapter contains information that is unique to the K2 Summit Transmission Server Package. Refer to other chapters for information that applies to all K2 Summit Production Client systems, including the K2 Summit Transmission Server Package.

K2 Summit Transmission Server Package features

The K2 Summit Transmission Server Package is an internal storage K2 Summit Production Client configured especially for high capacity. To support this high capacity, the K2 Summit Transmission Server Package is restricted to a subset of K2 Summit Production Client bit rates, formats, and other features.

Features are as follows:

- Eight 1 TB 7.2K RPM SAS internal storage media drives, configured as RAID 1 for 4 TB usable storage.
- Supports SD formats. Support for HD formats available with license.
- Records video bit rates up to 50Mbps, with 16 channels of audio at 24bits/sample.
- Supports MPEG-2 formats and DVCPRO formats at 50Mbps or less.
- Supports FTP bandwidth up to 30 MB/second.

The K2 Summit Transmission Server Package has one bi-directional recorder/player channel and three player channels. The channels can be configured for use as follows:

0x4 channels

Channel	DV record	DV play	MPEG-2 record	MPEG-2 play
1		X		X
2		X		X
3		X		X
4		X		X

1x3 channels

Channel	DV record	DV play	MPEG-2 record	MPEG-2 play
1	X	X	X	X
2		X		X

Channel	DV record	DV play	MPEG-2 record	MPEG-2 play
3		X		X
4		X		X

To identify a K2 Summit Transmission Server Package, open Storage Utility and view drive capacities. If 1 TB drives, the system is a K2 Summit Transmission Server Package.

K2 Summit Transmission Server Package requirements and restrictions

- DVCPRO HD not supported

- MPEG-2 data rates above 50 Mbps not supported

- AVC-Intra format not supported

- Transition effects not supported

- ChannelFlex Suite inputs and outputs are not supported..

- Mobile environment not supported.

Storage Utility procedures for the K2 Summit Transmission Server Package

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 1 TB 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. Refer to "Using Storage Utility" on page 109.

Appendix **A**

Remote control protocols

This section provides information for using remote control protocols to operate K2 clients and K2 Solo Media Servers. It is intended for use by installers, system integrators, and other persons responsible for setting up automation systems at a customer site. Topics are provided as follows:

- "Using AMP protocol to control K2 systems"

- "Using VDCP protocol to control K2 systems"

- "Using BVW protocol to control K2 systems"

- "Special considerations for automation vendors"

- "RS-422 connections on the K2 Summit Production Client or K2 Solo Media Server"

- "Security and protocol control"

For information about configuring AppCenter to enable protocol control of a K2 channel, refer to the *K2 AppCenter User Manual.*

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 (DV/MPEG/AVC-Intra). For same compression format playout, preroll is 10 frames.

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 client 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.

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.

Controlling transfers with AMP

Remote control automation applications can initiate transfers via AMP. The AMP command must be sent to the K2 client or K2 Solo Media Server, not the K2 Media Server. This applies to both stand-alone and shared storage K2 clients.

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 Summmit Production Client or K2 Solo Media Server, the first port maps to the first channel, the second port maps to the second channel, and so on.

Internationalization

AMP supports UTF-8. 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 (DV/MPEG/AVC-Intra). For same compression format playout, preroll is 10 frames.

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 client 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 client 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 client 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.

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).

Controlling transfers with VDCP

Remote control automation applications can initiate transfers via VDCP. The VDCP command must be sent to the K2 client or K2 Solo Media Server, not the K2 Media Server. This applies to both stand-alone and shared storage K2 clients.

If you are using VDCP to perform video network transfers, you must configure the K2 client 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.

Internationalization

VDCP does not support UTF-8 or Unicode, so use ASCII only for clip names and bin names.

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 client 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.
Back To Back Rec	Unchecked	Unchecked	K2 does not support this feature.

RS-422 connections on the K2 Summit Production Client or K2 Solo Media Server

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. (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 the *K2 AppCenter User Manual* 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. Refer to "Protocol control of channels and media access security".

Appendix A   Remote control protocols

Appendix **B**

Specifications

Specifications in this chapter:

- "AC power specification"
- "Environmental specifications"
- "Mechanical specifications"
- "Electrical specifications"
- "Operational specifications"
- "MIB specifications"

Also refer to Chapter 9, *K2 Summit Transmission Server Package* for information unique to that product.

AC power specification

The K2 Summit Production Client specification is shown in the following table.

Characteristic	Specification
Power supply	Dual, redundant
Mains Input Voltage	90 to 260V auto-range, 47-63Hz
Power consumption	450W typical (standalone) 300W typical (SAN client) Maximum AC current 4.5A @ 115VAC, 2.3A@230VAC

The K2 Solo Media Server specification is shown in the following table.

Characteristic	Specification
Power supply	Single
Mains Input Voltage	100-240V, 50/60 Hz
Power consumption	180W typical Maximum AC current 4.5A @ 115VAC, 2.3A@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 Production Client and K2 Solo Media Server 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 -5 to +45 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

Characteristic	Specification
Random Vibration	Operational: 0.27 GRMS (5-500Hz) Non-Operational: 2.38 GRMS overall .0175 g^2/Hz (5-100Hz) .009375 g^2/Hz (200-350Hz) .00657 g^2/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.

Mechanical specifications

The 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[a]	24.3 in (617 mm) total 23.0 in (585 mm) rack depth
Weight:	53.0 lbs (24.0 kg) maximum

a. Adjustable rack-mounting ears accommodate different rack depth limitations.

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)

Electrical specifications

The following sections describe the electrical specifications:

Serial Digital Video (SDI)

The K2 Summit Production Client and K2 Solo Media Server 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

Parameter	Specification
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 Production Client and K2 Solo Media Server 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	Not supported

System Timing

The K2 Summit Production Client and K2 Solo Media Server specification is shown in the following table

Characteristic	Description[a]
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 274M-5)
	    Frames: 0 to +1
	    Lines: 0 to +1124
	    Pixels: 0 to +2199

	720p at 59.94 FPS (SMPTE 296M-2)
	    Frames: 0 to +1
	    Lines: 0 to +749
	    Pixels: 0 to +1649

	1080i at 25 FPS (SMPTE 274M-6)
	    Frames: 0 to +1
	    Lines: 0 to +1124
	    Pixels: 0 to +2639

	720p at 50 FPS (SMPTE 296M-3)
	    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.

[a.] All delay values shown are relative to Black Reference.

AES/EBU Digital Audio

The K2 Summit Production Client and K2 Solo Media Server 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.

Parameter	Specification
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 Production Client and K2 Solo Media Server 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 Production Client and K2 Solo Media Server 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

The RS-422 interface conforms to ANSI/SMPTE 207M-1997 standard (SMPTE 422).

The K2 Summit Production Client and K2 Solo Media Server 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 Production Client and K2 Solo Media Server 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 risetimes approximately 625ns Typical falltimes approximately 400ns

Operational specifications

- "Video codec description K2 Summit/Solo"
- "Playout of multiple formats"
- "Active Format Description (AFD) specifications"
- "VBI/Ancillary/data track specifications"
- "Internationalization"
- "Naming specifications for assets and bins"
- "Video network performance"
- "Supported file input/output formats on K2 Summit/Solo/SAN"
- "MXF export behavior on K2 Summit/Solo"
- "Media file system performance on K2 systems"
- "Transition effects formats supported"
- "Protocols supported"
- "Transfer compatibility with K2 Summit/Solo"
- "Control Point PC system requirements".

Video codec description K2 Summit/Solo

K2 Summit 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 (720x480/576)	4:1:1/ 4:2:0	29.97, 25	28.8 Mbps	Conforms to IEC 61834
DVCPRO25 (720x480/576)	4:1:1	29.97, 25	28.8 Mbps	Conforms to SMPTE 314M
DVCPRO50 (720x487.5/585)	4:2:2	29.97, 25	57.6 Mbps	Conforms to SMPTE 314M
DVCPRO HD (960x720p, 1280x1080i59.94, 1440x1080i50)	4:2:2	29.97, 25	100 Mbps	Conforms to SMPTE 370M

MPEG-2 formats

Format	Sampling	Frame Rate	Data Rate (Mbps)	Other
720x480	4:2:0	29.97	2-15	I-frame and long GoP
720x480	4:2:2	29.97	4-50	I-frame and long GoP
720x512	4:2:2	29.97	4-50	I-frame and long GoP
720x576	4:2:0	25	2-15	I-frame and long GoP
720x576	4:2:2	25	4-50	I-frame and long GoP
720x608	4:2:2	25	4-50	I-frame and long GoP
D10/IMX (720x512)	4:2:2	29.97	30, 40, 50 CBR	I-frame only
D10/IMX (720x608)	4:2:2	25	30, 40, 50 CBR	I-frame only
1920x1080	4:2:0	29.97, 25	20-80	I-frame and long GoP[a]
1920x1080	4:2:2	29.97, 25	20-100	I-frame and long GoP
1280x720	4:2:0	29.97, 25	12-80	I-frame and long GoP
1280x720[b]	4:2:2	29.97, 25	20-100	I-frame and long GoP
XDCAM-HD (1440x1080)	4:2:0	29.97, 25	18 VBR, 25 CBR, 35 VBR	Long GoP
XDCAM-HD422 (1920x1080)	4:2:2	29.97, 25	50 CBR	Long GoP
XDCAM-HD422 (1280x720)	4:2:2	59.94	50 CBR	Long GoP

Format	Sampling	Frame Rate	Data Rate (Mbps)	Other
XDCAM-EX (1920x1080)	4:2:0	29.97, 25	35 VBR	Long GoP
XDCAM-EX (1280x720)	4:2:0	59.94, 50	25 CBR, 35 VBR	Long GoP

a. Decode of lower bit rate is possible

b. Includes playout of HDV, which is available only via transfer to the K2 system.

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 (1440x1080)	4:2:0	29.97, 25	50 Mbps	
AVC-Intra 50 (960x720)	4:2:0	29.97, 25	50 Mbps	
AVC-Intra 100 (1920 x 1080)	4:2:2	29.97, 25	100 Mbps	
AVC-Intra 100 (1280 x 720)	4:2:2	29.97, 25	100 Mbps	

Playout of multiple formats

The K2 client 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 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. Refer to .

The K2 Summit Production Client and K2 Solo Media Server supports mixed clips with uncompressed and compressed (PCM, AC3, and Dolby) audio on the same timeline.

25/50 fps conversions on HD K2 system models

The following specifications apply to the HD-00 K2 Media Client, the K2 Solo Media Server, and to K2 Summit Production Client channels with the XDP (HD) license.

| | | Converted SD format | Converted HD formats | |
		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 formats	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
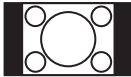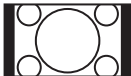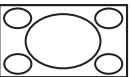
29.97/59.95 fps conversions on HD K2 client models

The following specifications apply to the HD-00 K2 Media Client, the K2 Solo Media Server, and to K2 Summit Production Client channels with the XDP (HD) license.

| | | Converted SD format | Converted HD formats | |
		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 formats	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 the HD-00 K2 Media Client, the K2 Solo Media Server, and to K2 Summit Production Client 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	
		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 only applies to K2 Summit Production Clients, and K2 Solo Media Servers.

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 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)

To see the full list of AFD input/output settings, refer to .

NOTE: Bar data is not supported on the K2 system.

Storing AFD in the K2 Summit Production Client and K2 Solo Media Server

The K2 Summit Production Client and K2 Solo Media Server stores clip metadata in clip properties and uses this data throughout the workflow. You can modify the AFD setting in AppCenter. For more information on applying AFD settings in the UI, see .

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. If present, the AFD setting from two seconds into the file is copied into the clip properties. (If selected, the ANC data is copied into the K2 data track.)

AFD input/output settings

The following table shows the various AFD input settings, and the resulting output values.

Input and Settings				Output AFD Value					
AFD set in the clip properties	AFD already in the data Track	ARC Performed	AFD in Config Mgr setting	AFD set in Clip property	Translated from the clip property according to the ARC performed[a]	Same as data track settings	Translated from AFD values on the data track[a.]	No AFD	Default AFD[b]
n/a	Y	n/a	Never			X			
Y	n/a	N	Always or When Known	X					
Y	n/a	Y	Always or When Known		X				
N	Y	N	Always or When Known			X			
N	Y	Y	Always or When Known				X		
N	N	n/a	Always						X
N	N	n/a	When Known					X	
n/a	N	n/a	Never					X	

a. For a list of supported AFD conversions, see "Supported conversions from SD to HD using AFD" on page 209 and "Supported conversions from HD to SD using AFD" on page 209.

b. For a list of default AFD settings, see "Default generated AFD values" on page 205.

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.

File transfer AFD priority	
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.
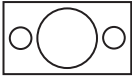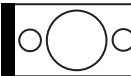
Default generated AFD values

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
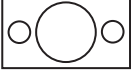
Under these conditions, default AFD is generated and inserted, based on ARC performed and the source material format. Default generated AFD settings are described in the table below.
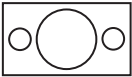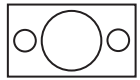
Default generated AFD values when up-converting to HD

Source aspect ratio	Presumed[a] 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 16:9 HD "bars"	

a. Source image is presumed based on the conversion that has been selected.
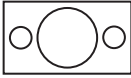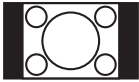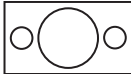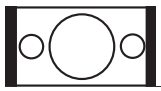
Default generated AFD values when down-converting to SD

Source aspect ratio	Presumed[a] source image	Conversion option	Converted AFD and aspect ratio	Converted image
4:3 SD		No conversion	AFD = 1001 AR = 4:3 SD	
16:9 SD		No conversion (only if ARC set to 'stretch')	AFD = 1010 AR = 16:9 SD	

Source aspect ratio	Presumed[a] 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"	
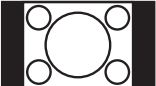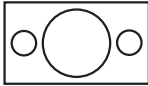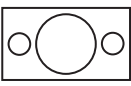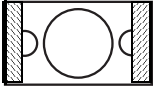
a.   Source image is presumed based on the conversion that has been selected.

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 = 1001[a] AR 4:3 SD		Scale up pillarbox	AFD = 1001 AR 16:9 HD	
AFD = 1010[a.] AR 16:9 SD		Scale up	AFD = 1010[a.] AR 16:9 HD	
AFD = 1011 AR = 4:3 SD		Scale up Crop vertical pillarbox	AFD = 1011 AR 16:9 HD	

[a.] The SMPTE standard describes two valid AFD codes. The K2 system uses the second value.

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 = 1010[a] AR = 16:9		Scale down letterbox	AFD = 1010 AR = 4:3	
AFD = 1001 AR = 16:9		Scale down crop horizontal	AFD = 1001 AR = 4:3	
AFD = 1010[a.] AR = 16:9		Scale down	AFD = 1010[a.] AR = 16:9	
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	

[a.] The SMPTE standard describes two valid AFD codes. The K2 system uses the second value.

VBI/Ancillary/data track specifications

This section contains the following topics:

- "Definitions"
- "Luma/Chroma VBI support on K2 Summit/Solo"
- "VBI data support on K2 Summit/Solo"
- "Data track support on K2 Summit/Solo SD channels"
- "Data track support on K2 Summit/Solo HD channels"
- "Captioning system support"
- "Data bridging of VBI information on K2 Summit/Solo HD channels"

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.

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 supported, as native to DVCAM.	—
MPEG-2 525 line (NTSC)	Supported as 16 lines per field. Range: 7–22	Not supported	CC supported and always on. Not selectable.	—
MPEG-2 625 line (PAL)	Supported as 16 lines per field. Range: 7–22	Not supported	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 suppported 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.

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[a] 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.
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.

a. UserData CC packets always on. If CC exists, it is recorded and played back. MPEG UserData can be played out but not recorded.

Internationalization

When you enable internationalization on a K2 system, you can name your media assets in a local language. The K2 system supports the local language name as specified in the following table.

System	Internationalization support
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:\PDR) remain unchanged, but are Unicode. • Elementary streams remain as GUIDs, but are Unicode.
K2 Media Client applications	• Movie assets are described in Unicode. • Application user interfaces are Unicode compliant.
Protocols	Refer to Appendix A, Remote control protocols, in the K2 System Guide.
FTP transfers	Refer to "FTP internationalization" in the K2 System Guide.

Names of media assets and bins must conform to the "Naming specifications for assets and bins".

Naming specifications for assets and bins

Names of media assets and bins must conform to the following specifications.

Characters not allowed in asset and bin names

Position	Character	Description
Anywhere in name	\	backward slash
	/	forward slash
	:	colon
	*	asterisk
	?	question mark
	<	less than
	>	greater than
	%	percent sign
	|	pipe
At beginning of name	"	double quote
	~	tilde

Asset and bin name limitations

The maximum number of characters in an asset path name, including the bin name, is 259 characters. This includes parts of the path name that are not visible in AppCenter.

	Asset name, bin name, and path (up to 259[a] characters, including separators such as \\)			
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

a. 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.

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
```

Video network performance

K2 systems support streaming transfers to and from K2 Summit Production Clients, K2 Solo Media Servers, 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 system	Up to 50 MBytes per second	—
Transfer bandwidth per Level 2 K2 Storage	50 MBytes per second	—
Transfer bandwidth per Level 3 K2 Storage	80 MBytes per second	Additional K2 Media Servers dedicated as FTP servers add 80 MBytes per second each
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	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.	—

Supported file input/output formats on K2 Summit/Solo/SAN

The K2 Solo Media Server, K2 Summit Production Client, and K2 SAN can send and receive files of various formats using import, export, and transfer mechanisms. Formats supported are as follows:

Streaming file format	Video elementary format	Audio elementary format	File based[a] Import	Export	FTP stream Import	Export	Other information
GXF	DVCPRO25 DVCPRO50 DVCPRO HD[b] DVCAM MPEG-2[c] AVC-Intra	48 kHz, 16 bit, or 24 bit PCM, Dolby-E, or AC-3	Yes	Yes	Yes	Yes	Streaming between online K2 Systems supports complex movies and agile playlists of mixed format.
MXF[d]	DVCPRO25 DVCPRO50 DVCPRO HD[b.] DVCAM D10[e] MPEG-2[c.] AVC-Intra	48 kHz, 16 bit, or 24 bit PCM, Dolby-E, or AC-3	Yes	Yes	Yes	Yes	MXF OP 1A. See "MXF export behavior on K2 Summit/Solo" on page 218
AVI[d.]	DVCPRO25 DVCPRO50 DVCPRO HD DVCAM	48 kHz, 16 bit, or 24 bit PCM	Yes	Yes	No	No	Type-2 (non-interleaved) DV video only. Audio tracks handled as stereo pairs.

Streaming file format	Video elementary format	Audio elementary format	File based[a]		FTP stream		Other information
			Import	Export	Import	Export	
QuickTime[d.]	DVCPRO25 DVCPRO50 DVCPRO HD[b.] DVCAM AVC-Intra D10/IMX XDCAM-HD XDCAM-EX XDCAM-HD4 22	48 kHz, 16 bit, or 24 bit PCM	Yes	Yes	No	No	Audio tracks handled as stereo pairs on export
MPEG	MPEG-2	48kHz MPEG-1 (layer 1 & 2) SMPTE 302M AES3 LPCM AC-3 DVD/VOB LPCM DVD/VOB AC-3	Yes	No	Yes	No	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.
WAV audio	NA	48 kHz 16 bit stereo PCM	Yes	No	No	No	Audio tracks handled as stereo pairs

a. Based on a file that is visible from the operating system. For example, AppCenter import/export features are file based.

b. Super Slo-Mo requires software version 7.1. x or higher

c. Includes all MPEG-2 formats (IMX, XDCAM, etc.) that can be stored on a K2 system.

d. 3D/Video + Key not supported

e. A D10 MXF stream is handled as an eVTR style D10AES3 stream. Uncompressed audio only. Maximum 8 channels audio. If you want to export clips with more than 8 audio tracks, export as GXF

MXF export behavior on K2 Summit/Solo

The following sections specify how a K2 system handles file formats when they are exported as MXF.

Behavior on MXF export from K2 systems

Upon MXF export the K2 system checks media for specifications as they apply to industry standard formats such as XDCAM. If specifications match, the media is exported as the appropriate format.

The K2 system allows you to alter clips so that they no longer match the specifications for the industry-standard format. For example, you can add audio tracks to exceed the "# of Audio Tracks" specification for XDCAM. If you alter a clip in this way, on MXF export the K2 system exports the clip but it is not compatible with the industry-standard format.

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 playing out the same clip on another channel. Live play mode is available only on the K2 Solo Media Server and the K2 Summit Production Client 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.

Stand-alone K2 Summit Production Client or K2 Solo Media Server

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 Production Client
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 Production Client	Record-to play on different K2 Summit Production Clients
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 Production Client	Record-to play on different K2 Summit Production Clients
All formats	10 seconds	20 seconds

Other media file system specifications

Parameter	Stand-alone K2 system	K2 SAN
Maximum number of clips[a]	20,000	50,000
Maximum length continuous record	24 hours	24 hours
Off-speed play range for audio scrub	-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

[a]. 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.

Transition effects formats supported

Transition (mix) effects between formats are supported as follows:

	DV	AVC-Intra	MPEG-2 I-frame	MPEG-2 long GoP
DV	Yes	No	No	No

	DV	AVC-Intra	MPEG-2 I-frame	MPEG-2 long GoP
AVC-Intra	No	Yes	No	No
MPEG-2 I-frame	No	No	Yes	No
MPEG-2 long GoP	No	No	No	No

Protocols supported

AMP, VCDP, and BVW protocols are supported. Refer to Appendix A, Remote control protocols in the *K2 System Guide* for more information.

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
From K2 Media Client to K2 Summit/Solo	All types of material supported, according to the SD and/or HD capability.	

Transfer compatibility with Turbo iDDR

Transfer	Material transferred	Compatibility
From K2 Summit/Solo to Turbo iDDR	DVCPRO25, DVCPRO50, DVCPRO HD	Not supported.
	SD MPEG 4:2:0 long GoP clips up to 15 Mbps. HD MPEG 1920x1080 and 1280x720 4:2:0 long GoP clips up to 25 Mbps.	Playout supported.
	SD clips above 15 Mbps. HD clips above 25 Mbps. D10, XDCAM-HD, HDV formats.	Supported for storage only. Transfer is successful but playout not supported. Avoid transfer of clips with ancillary data. These clips include data that cannot be played or deleted.
	AVC-intra	Not supported
From Turbo iDDR to K2 Summit/Solo	Half-rate material, such as 720p at frame rates 25 or 29.97, not supported. All other types of material supported, according to the SD and/or HD capability of the model. For example, ancillary data in SD not supported.	

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
	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
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 Summit Production Client or a K2 Solo Media Server, 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	
SD MPEG-2	Any data recorded with Profile compatible setting.[a]	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.

[a.] When Record ancillary data = No or when Record Uncompressed VBI and captioning data to track = No

Control Point PC system requirements

If you are building your own Control Point PC, the machine you chose must meet the following requirements. These requirements assume that the PC is dedicated to its function as the control point for the K2 system and that no other applications run 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): XP Professional Service Pack 2, Server 2003, or Vista Enterprise Service Pack 1.
RAM	Minimum 512 MB, 1 GB recommended
Graphics acceleration	Must have at least 128 MB memory
Processor	Pentium 4 or higher class, 2 GHz or greater
Hard disk space	400 MB
Microsoft .NET Framework	Version 1.1, Version 1.1 hotfix, Version 3.5 SP1
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&displayl ang=en

- http://www.apple.com/quicktime/download/

- http://get.adobe.com/reader/

To fix the screen resolution problem seen with NetCentral on the Grass Valley Control Point PC, do the following:

1. Go to Display properties (right mouse selection of properties on the display area)

2. Select Settings tab

3. Select the Advanced button

4. In the General tab, set the DPI setting to Normal size (96 DPI)

5. Restart the PC

MIB specifications

This section specifies Management Information Base (MIB) information for monitoring K2 devices with the Simple Network Management Protocol (SNMP). 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.

MIBs specified in this section are as follows:

- "K2 client MIBs"
- "K2 Media Server MIBs"
- "K2 Appliance (Generic Windows computer based) MIBs"

K2 client 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 - 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
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

Appendix B   Specifications

Appendix **C**

Connector Pinouts

This appendix contains the following topics:

- "K2 Summit Production Client connector pinouts"
- "K2 Media Client connector pinouts"
- "K2 Media Server connector pinouts"

K2 Summit Production Client connector pinouts

The following sections describe K2 Summit Production Client rear panel connector pinouts.

AES Audio

Pinouts for each channel's AES Audio DB25 connector are as follows:
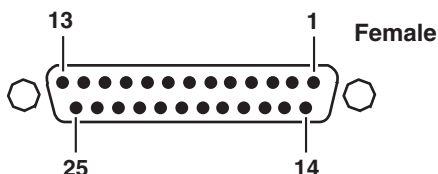
Pin #	Signal	Description
1	IN_P<0>	Channel Input 1&2 positive
2	IN_P<1>	Channel Input 3&4 positive
3	IN_P<2>	Channel Input 5&6 positive
4	IN_P<3>	Channel Input 7&8 positive
5	OUT_P<0>	Channel Output 1&2 positive
6	OUT_P<1>	Channel Output 3&4 positive
7	OUT_P<2>	Channel Output 5&6 positive
8	OUT_P<3>	Channel Output 7&8 positive
9	NO_C	NO_C
10	GND	GND
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:
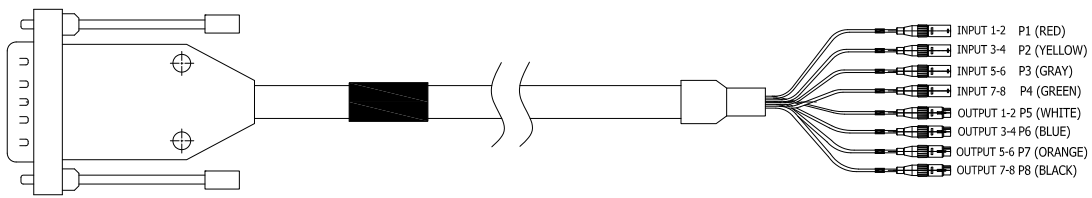
RS-422 connector pinouts

The K2 Summit Production Client RS-422 interface conforms to ANSI/SMPTE 207M-1997 standard (SMPTE 422).

Pinouts for the individual DB9 connectors are as follows:
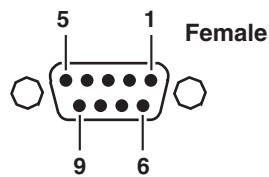
Pin #	Signal	Description
1	GND	Frame Ground
2	-TXD	Differential Transmit Data (low)
3	+RXD	Differential Receive Data (high)
4	GND	Transmit Signal Common
5	NC	Spare
6	GND	Receive Signal Common
7	+TXD	Differential Transmit Data (high)
8	-RXD	Differential Receive Data (low)
9	GND	Signal Ground

LTC connectors pinouts

The K2 Summit Production Client LTC panel connector provides balanced linear timecode input and output connections. The interface conforms to SMTPE 12M Linear Timecode.

On the K2 Summit Production Client there is one 6 pin Switchcraft TRA6M Mini-XLR male connector for each channel. Pinouts are as follows:
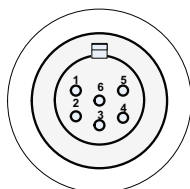
Pin #	Signal	Description
1	IN_P<0>	
2	IN_N<0>	
3	GND	Frame Ground
4	OUT_P<0>	
5	OUT_N<0>	
6	GND	Frame Ground

The mini-XLR to XLR LTC cable has connections as follows:
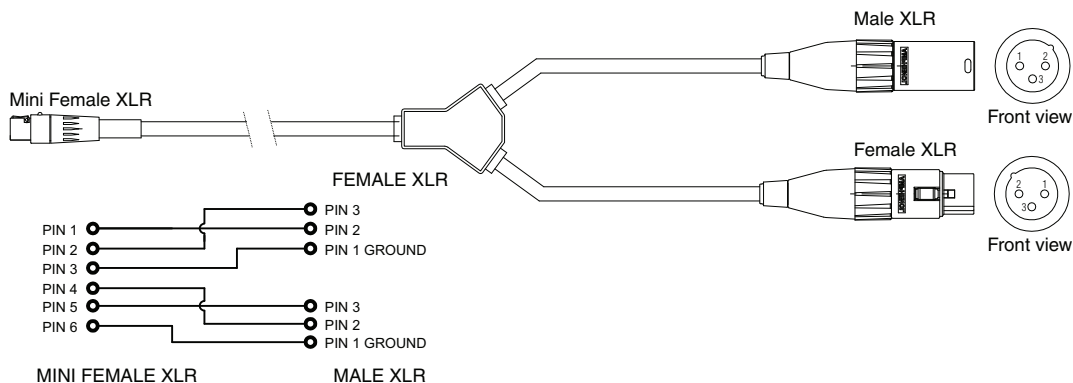
GPI I/O connector pinouts
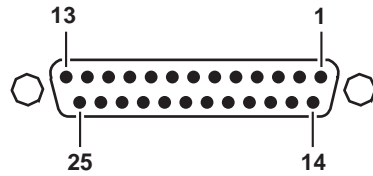
Pin	Signal		Pin	Signal
1	Output 1		14	Input 1
2	Output 2		15	Input 2
3	Output 3		16	Input 3
4	Output 4		17	Input 4
5	Output 5		18	Input 5
6	Output 6		19	Input 6
7	Output 7		20	Input 7
8	Output 8		21	Input 8
9	Output 9		22	Input 9
10	Output 10		23	Input 10
11	Output 11		24	Input 11
12	Output 12		25	Input 12
13	Ground			

K2 Media Client connector pinouts

The following sections describe K2 Media Client rear panel connector pinouts.

RS-422 connector pinouts

K2 Media Clients have been manufactured with two types of RS-422 configurations, as follows:

- A K2 Media Client can have two RS-422 adapters. Each adapter is connected via an internal USB cable to the motherboard, so while a RS-422 adapter does occupy a rear panel slot, it does not plug into a PCI bus. Each adapter provides two RS-422 ports for connecting equipment for remote control of the K2 Media Client.

- A K2 Media Client can have one RS-422 adapter. The adapter is connected via PCI slot to the motherboard. The adapter includes an external interface with eight ports. On the external interface, ports 1–4 are active. This provides the four ports for connecting equipment for remote control of the K2 Media Client.

The RS-422 interface conforms to ANSI/SMPTE 207M-1997 standard (SMPTE 422).

Pinouts for the individual DB9 connectors are as follows:
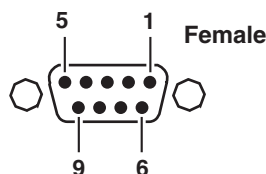
Pin #	Signal	Description
1	GND	Frame Ground
2	-TXD	Differential Transmit Data (low)
3	+RXD	Differential Receive Data (high)
4	GND	Transmit Signal Common
5	NC	Spare
6	GND	Receive Signal Common
7	+TXD	Differential Transmit Data (high)
8	-RXD	Differential Receive Data (low)
9	GND	Signal Ground

Pinouts for the DB25 connector on the PCI RS-422 board are as follows:
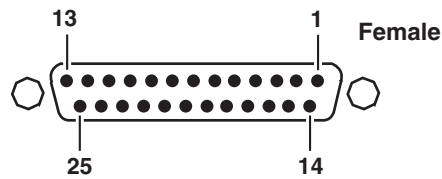
Pin #	Signal	Description
1–6	Not Used	
7	GND	
8–14	Not Used	
15	+RXD	
16	Not Used	
17	-RXD	
18	Not Used	
19	+TXD	
20–24	Not Used	
25	-TXD	

LTC connectors pinouts
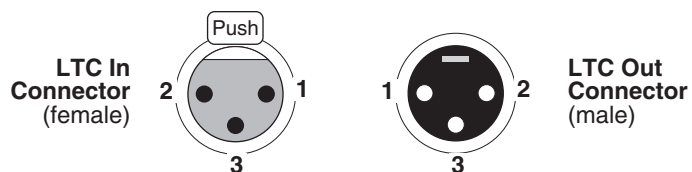
Pin #	LTC In	Pin #	LTC Out
1	Signal Ground	1	Signal Ground
2	(+)	2	(+)
3	(-)	3	(-)

GPI I/O connector pinouts
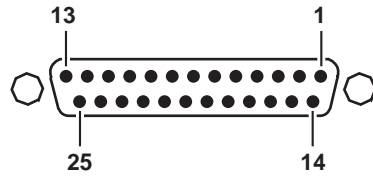
Pin	Signal		Pin	Signal
1	Output 1		14	Input 1
2	Output 2		15	Input 2
3	Output 3		16	Input 3
4	Output 4		17	Input 4
5	Output 5		18	Input 5
6	Output 6		19	Input 6
7	Output 7		20	Input 7
8	Output 8		21	Input 8
9	Output 9		22	Input 9
10	Output 10		23	Input 10
11	Output 11		24	Input 11
12	Output 12		25	Input 12
13	Ground			

K2 Media Server connector pinouts

The following sections describe K2 Media Server rear panel connector pinouts.

Redundant server heartbeat 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

Appendix **D**

Rack mounting

This section contains the following topics:

- "Rack-mount considerations"
- "Rack mount hardware shipped with the K2 system"
- "Mounting the Rack Slides"
- "Installing the K2 system on the rack mount rails"
- "Making Rack Slide Adjustments"

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. See "Environmental specifications" on page 190 for details.

- 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 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 hardware shipped with the K2 system

Your K2 system rack mount kit comes with rack mounting hardware as shown.

Rear

Flat Nut Bar

Locking bracket

NOTE: The locking brackets should
be toward the rear when slides are
in place.
(The left-hand rail is shown above.)

PNH
screws

Front
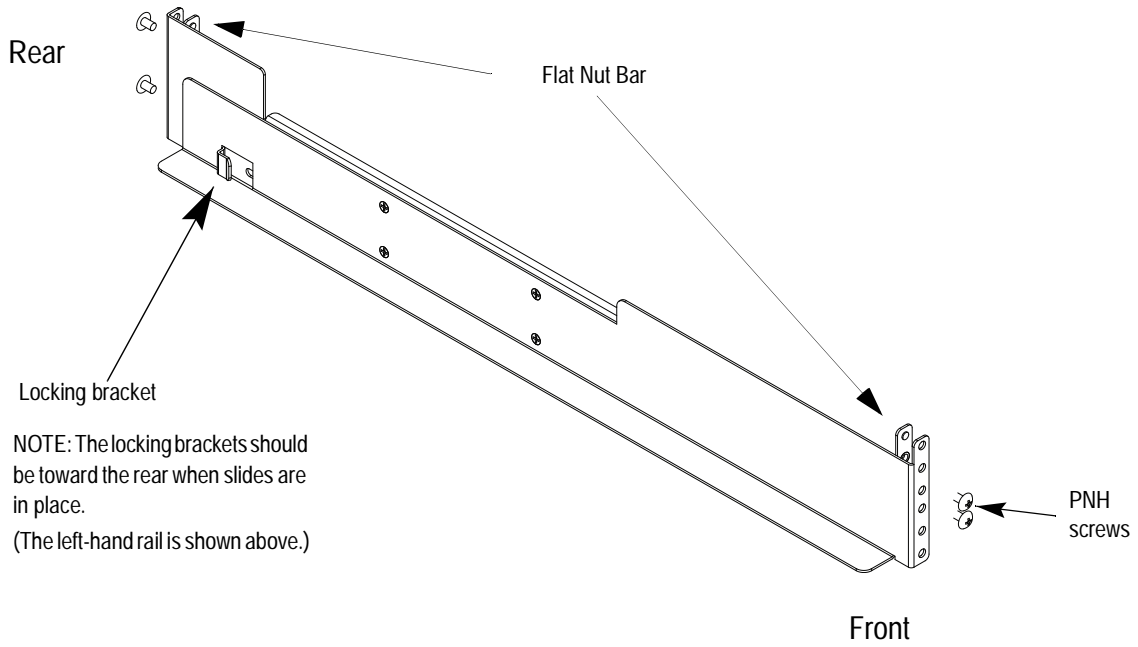
Mounting the Rack Slides

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.

MIL STD 189 SPACING   "UNIVERSAL" SPACING EIA RS310, RETMA

1.250 in

1.250 in

1.250 in

0.500 in

0.625 in

0.625 in
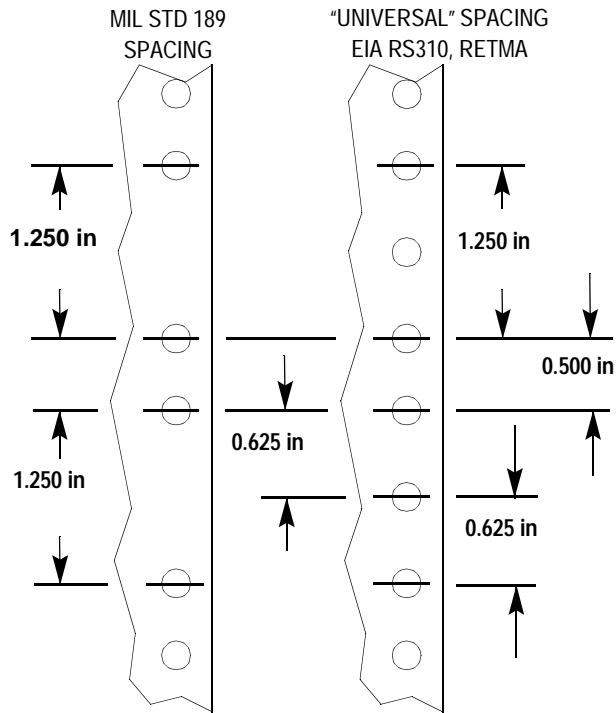
Front and rear rack rail mounting hardware is provided with the rack mount kit. Mount the rails using the enclosed hardware. Make sure the stationary sections are horizontally aligned and are level, as well as parallel to each other.

NUT BAR
(Use if the front rail is not tapped)

Because the system is 1 RU, the two front screws must align with the mounting holes as shown.

FRONT RACK RAIL

Locking bracket
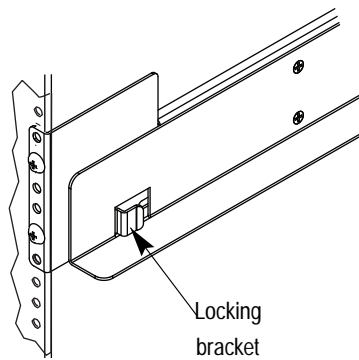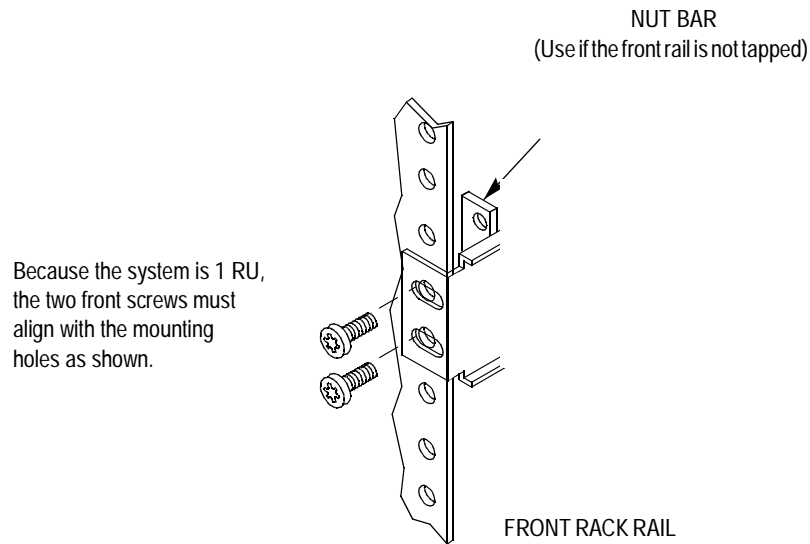
REAR RACK RAIL   (Nut bar not visible)

Installing the K2 system on the rack mount rails

To install 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.

Index

Symbols

_he0, using in a host table 48

Numerics

100BaseT 169

A

AC power, specification 190
adapter
    network loopback 46
administrative share on SiteConfig control point
        PC 128
administrator
    mapping NetCentral administrators with
            K2 167
    password 161
AES audio connector K2 Summit Client
        pinout 232
AES/EBU audio
    specification 194
AMP
    channel designations 182
    protocol settings 182
    transfers 182
ancillary data specifications 210
anti-virus 169
AppCenter
    channel access security 165
    user access 161
application system
    architecture 27
    software 27
aspect ratio
    HD-00 202
    SD-00 200
assets and bins, naming limitations 214
audio
    digital audio specification 194
    Dolby 200
audio scrub off-speed play range specification 219
auto logon 171
AVI, supported formats 216

B

backup, strategies 154

binding LUNs 117
bins, configuring security 161
board
    XLR 27
BVW
    protocol settings 185

C

cable
    redundant server heartbeat 239
    requirements, Ethernet connections 43
captions 212
channels
    security 165
cleaning unreferenced files and movies 121
clips, maximum number 218
clips, maximum number specification 219
closed captioning 210
commands, FTP 59
configuration
    auto logon 171
    channel access security 165
    customizing 34
    K2 Summit Production Client security 158
    loading defaults 34
    media access security for K2 bins 161
    opening 33
    protocol security 164
    sample K2 Summit Production Client hosts
            file 50
    saving and restoring 33
configuration file 36
Configuration Manager, description 33
connect kit
    SiteConfig 129
connections
    GPI 106
    RS-422 105, 187
connector pinouts
    GPI 238
    GPI, K2 Summit Production Client 235
    LTC connector 234, 237
    RS-422 239
    RS-422, K2 Media Client 236
    RS-422, K2 Summit Client 233
continuous record

router
    and SiteConfig 128
RS-422
    connector pinout 236, 239
    connector pinout, K2 Summit Client 233
    rear panel connections 105, 187
    specification 196
    USB port 170

S

SAMBA shares 169
SCSI board
    description 107, 108
SD-00
    aspect ratio formats 200
    loop through 29
SDI 192
security
    AppCenter operations 163
    configuring
        channel access 165
        FTP security 163
        K2 bins 161
        K2 SANs security 164
        protocol security 164
    mapping NetCentral administrators with K2 167
    Microsoft Windows updates 168
    NetCentral 167
    overview 158
    passwords 161
    user accounts 161
site wizard
    SiteConfig 130
SiteConfig
    description 38
SiteConfig Network Configuration Connect Kit 129
SNFS, see media file system
software
    SiteConfig on K2 SAN 149
specification
    AC power 190
    AES/EBU 194
    electrical 192
    environmental 190
    external storage, media file system 218
    genlock 193
    GPI 197
    LTC 196
    mechanical 192
    media file system performance 218
    operational 198
    RS-422 196
    system timing 194
    transferring 216
    VBI/ancillary data 210
    VITC 196
SpyWare 169
storage system, description 28
Storage Utility 35, 36
    checking subsystem status 113
    description 110
    opening through AppCenter 110
    overview 112
streaming
    see transferring
stripe
    group 107, 108
    media 107, 108
subsystem status, checking with Storage Utility 113
subtitles 212
switch Ethernet
    and SiteConfig 128
synchronizing the media file system 121
system description
    file 39
system timing 194
System Tools, K2 Summit Production Client 33

T

TCP ports 169
third-party FTP access 54
transferring
    between a K2 and a non-K2 system 53
    compatibility considerations 221
    K2 FTP interface 54
    mechanically or automatically 53
    remote control protocols 54
    specification 216
    supported formats 216
    using Internet Explorer 56
    using third-parties 54
transfers
    VDCP 183