



K2

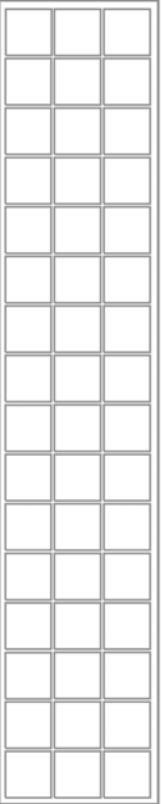
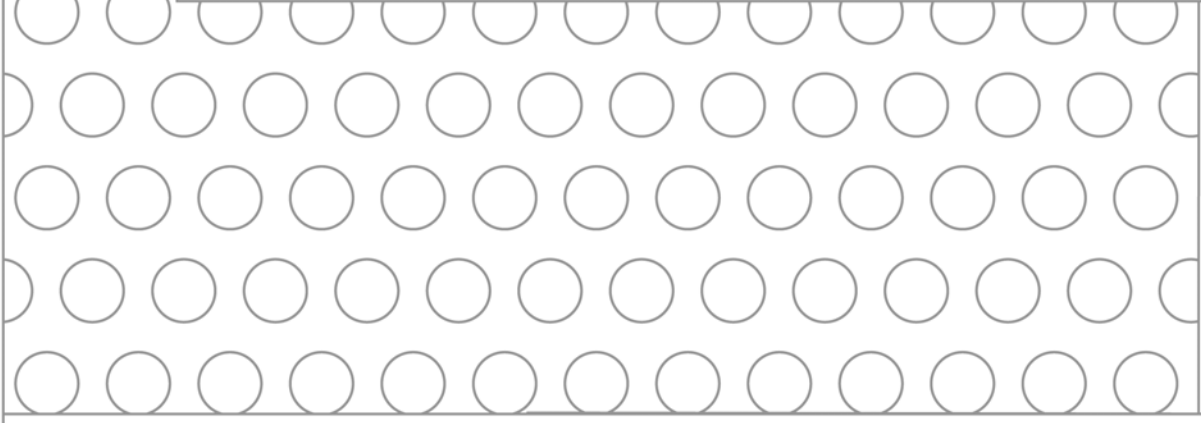
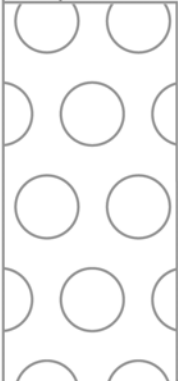
MEDIA PLATFORM FOR SUMMIT CLIENTS

System Guide



SOFTWARE VERSION 7.0

86231160
MARCH 2009



Copyright

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

Disclaimer

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

U.S. Government Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7013 or in subparagraph c(1) and (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19, as applicable. Manufacturer is Grass Valley, Inc., P.O. Box 59900, Nevada City, California 95959-7900 U.S.A.

Trademarks and Logos

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

Other trademarks and logos used in this document are either registered trademarks or trademarks of the manufacturers or vendors of the associated products, such as Microsoft® Windows® operating system, Windows Media® player, Internet Explorer® internet browser, and SQL Server™. QuickTime and the QuickTime logo are trademarks or registered trademarks of Apple Computer, Inc., used under license therefrom.



Revision Status

Rev Date	Description
November 23, 2005	Initial release of the K2 Media Client System Guide — 071-8460-00
September 7, 2006	Update information for 3.1 release — 071-8460-01
July 3, 2007	Update information for 3.2 release — 071-8460-02
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

Contents

	Finding Information	7
	Grass Valley Product Support	10
	Telephone Support	11
Chapter 1	Product Description	
	K2 Summit Production Client features	14
	Features of internal storage models	14
	Features of external storage models	14
	Product identification	15
	Front panel indicators	16
	Rear panel view	17
	Considerations for first startup out of box	17
	K2 Summit Production Client system overview	18
	Application System	18
	Real Time System	18
	Media control and processing	18
	Loop through, E to E, and feeds	19
	Ports used by K2 services	21
	RAID drive numbering	22
Chapter 2	Using K2 system tools	
	Configuration Manager	23
	Accessing Configuration Manager	23
	Saving and restoring Configuration Manager settings	23
	Restoring default Configuration Manager settings	24
	K2 System Configuration	24
	Storage Utility	26
	NetCentral	27
	Windows Remote Desktop Connection	27
Chapter 3	System connections and configuration	
	About networks	30
	Control network description	30
	Streaming/FTP network description	30
	Media (iSCSI) network description	30
	Network connections	31
	Cable requirements	31
	About network ports	31
	Making network connections	32
	Network configuration	33
	About network functionality	33
	About modifying or restoring network settings	34
	Configure network settings for a stand-alone K2 Summit Production Client	34
	Streaming video between K2 systems	36
	Using FTP for file transfer	41
	About the K2 FTP interface	41
	Limitations with complex media types	41
	Transferring between different types of systems	42
	Transfer mechanisms	42
	FTP access and configuration	42
	FTP access by automation	43
	FTP security	43
	FTP internationalization	43
	FTP access by Internet Explorer	44
	FTP commands supported	47
	Using FTP on a K2 Nearline SAN	48
	Using the HotBin service	49

	About the HotBin service.....	49
	Prerequisite for using the HotBin service	50
	Configuring the HotBin service	50
	HotBin service components.....	53
	Using the XML Import capture service	54
	About the XML Import capture service	54
	Prerequisites for using the XML Import capture service.....	54
	Considerations for the XML Import capture service	55
	Configuring the XML Import capture service	55
	Testing the XML Import capture service.....	57
	XML Import capture service components.....	57
	Licensing K2 capture service software.....	57
	QuickTime and Final Cut Pro support	58
	Connecting RS-422.....	59
	Connecting GPI.....	59
Chapter 4	Managing Stand-alone Storage	
	About the internal storage system.....	61
	About the direct-connect storage system	61
	Using Storage Utility.....	63
	About Storage Utility.....	64
	Opening Storage Utility	64
	Overview of Storage Utility	66
	Checking storage subsystem status.....	67
	Checking controller microcode	67
	About identifying disks.....	68
	Identifying K2 Summit Production Client internal disks	68
	Get controller logs	69
	Check disk mode pages	69
	Disabling a disk	69
	Forcing a disk to rebuild	70
	Unbind LUN.....	70
	Bind Luns	71
	Changing RAID type for internal storage.....	73
	Making a new media file system on a K2 Summit Client.....	73
	Making a new media file system on a K2 Media Client	74
	Checking the media file system.....	74
	Cleaning unreferenced files and movies	75
	Downloading disk drive firmware.....	75
	Storage Utility operation not supported	76
	Placing the K2 Media Client into online mode	76
Chapter 5	Managing K2 system software	
	About K2 system software	77
	Software components installed	78
	Installing Control Point software.....	78
	Installing K2 software	80
	Pre-installed software.....	80
	Backup and recovery strategies.....	80
Chapter 6	Administering and maintaining the K2 system	
	About the write filter	81
	Enabling the write filter	82
	Disabling the write filter	82
	Committing a file to disk with write filter enabled	82
	Licensing	83

	Software version licenses	83
	Licensable options	83
	Configuring K2 security	84
	Overview of K2 security features	85
	Example: Setting up user access to bins	86
	Example: Setting up user access to channels	86
	Security and user accounts	87
	Configuring media access security for K2 bins	87
	AppCenter operations and media access security	89
	FTP and media access security	89
	K2 SANs and media access security	90
	Protocol control of channels and media access security	90
	Configuring channel access security	91
	K2 and NetCentral security considerations	93
	Mapping a NetCentral administrator to the K2 administrator level	93
	Microsoft Windows updates	94
	Virus scanning policies	95
	Network and firewall policies	95
	Enabling and disabling the USB ports	96
	Configuring auto log on	97
	Regional and language settings	97
Chapter 7	Direct Connect Storage	
	Setting up direct-connect RAID storage	99
	Powering up K2 RAID	102
	Unbinding/binding direct-connect storage LUNs	103
Appendix A	Remote control protocols	
	Using AMP protocol to control the K2 Summit Production Client	106
	Using VDCP protocol to control the K2 Summit Production Client	107
	Using BVW protocol to control the K2 Summit Production Client	109
	Special considerations for automation vendors	110
	Harris settings	110
	RS-422 connections on the K2 Summit Production Client	111
	Security and protocol control	111
Appendix B	Specifications	
	AC power specification	114
	Environmental specifications	114
	Mechanical specifications	115
	Electrical specifications	115
	Serial Digital Video (SDI)	115
	Genlock Reference	116
	System Timing	117
	AES/EBU Digital Audio	117
	LTC Input/Output	119
	VITC Input/Output	119
	RS-422 specification	119
	GPI I/O specifications	120
	Operational specifications	121
	Video codec description – K2 Summit Production Client	122
	Layout of multiple formats	123
	VBI/Ancillary/data track specifications	126
	Internationalization	128
	Video network performance	128
	Supported file input/output formats on K2 Summit Production Client and K2 SAN	129

Media file system performance on K2 Summit Production Client and K2 SAN.....	129
Live Play mode specifications	130
Protocols supported	130
Transfer compatibility with K2 Summit Production Client.....	131
Control Point PC system requirements	132
MIB specifications	133
K2 client MIBs	134
K2 Media Server MIBs	135
K2 Appliance (Generic Windows computer based) MIBs.....	136
Appendix C Connector Pinouts	
K2 Summit Production Client connector pinouts.....	140
AES Audio	140
RS-422 connector pinouts.....	141
LTC connectors pinouts	142
GPI I/O connector pinouts	143
K2 Media Client connector pinouts	144
RS-422 connector pinouts.....	144
LTC connectors pinouts	145
GPI I/O connector pinouts	146
K2 Media Server connector pinouts	147
Redundant server heartbeat cable	147
Appendix D Rack mounting	
Rack-mount considerations	149
Rack mount hardware shipped with the K2 system	150
Mounting the Rack Slides.....	151
Installing the K2 system on the rack mount rails	152
Making Rack Slide Adjustments	153
Index	155

Finding Information

This manual describes K2™ server system 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 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 lists the chapters 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 5, *Managing K2 system software*](#)

[Chapter 6, *Administering and maintaining the K2 system*](#)

[Chapter 7, *Direct Connect Storage*](#)

[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 client with internal storage

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

	Find this document...	In these locations...	In these formats:
1	K2 Release Notes	K2 client shipping box	Printed
		Grass Valley Website	PDF file
2	K2 Media Client Quick Start Guide or K2 Summit Production Client Quick Start Guide	K2 client 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 client shipping box	Printed
		Grass Valley Website	PDF file
2	K2 Direct Connect Storage Quick Start Guide	K2 RAID shipping box	Printed
		K2 Documentation CD	PDF file
		Grass Valley Website	PDF file
2	K2 Media Client Quick Start Guide or K2 Summit Production Client Quick Start Guide	K2 client 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 client shipping box	Printed
		Grass Valley Website	PDF file
2	K2 SAN Cabling Guide, for your level of K2 SAN.	K2 RAID shipping box	Printed
		K2 Documentation CD	PDF file
		Grass Valley Website	PDF file
2	K2 Media Client Quick Start Guide and/or K2 Summit Production Client Quick Start Guide	K2 client 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 Summit Production Client. The Quick Start Guide provides step-by-step installation instructions for basic installation and operation of your K2 Summit Production Client, 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.

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 Summit Production Client.

The K2 Documentation CD includes the following documents:

- **Quick Start Guides** — A Quick Start Guide provides step-by-step installation instructions for basic installation and operation of a K2 client model, including recording and playing clips.
- **K2 AppCenter User Manual** — Describes the K2 Summit Production Client and provides instructions for operating the product in a variety of applications.
- **K2 System Guide** — This guide provides all the information you need to go beyond

factory default settings and customize your system's configuration to meet your site-specific needs.

- **K2 Summit Production Client Service Manual** — Contains information for solving common setup problems, as well as information on servicing and maintenance.
- **K2 SAN Installation and Service Manual** — Contains installation and configuration procedures for shared storage options. Also includes administrative and maintenance procedures.
- **K2 SAN Cabling Guide** — Contains diagrams for cabling the devices of the K2 SAN.
- **RAID Storage Instruction Manuals** — Contains procedures for troubleshooting and servicing the different level RAID storage devices.

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**.

Thomson 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.thomsongrassvalley.com>.

Grass Valley Product Support

For technical assistance, to check on the status of a question, or to report new issue, 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.thomsongrassvalley.com/support/>
Technical Support E-mail Address: gvgtechsupport@thomson.net.

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 Thomson Grass Valley Product Support (<http://www.thomsongrassvalley.com/support/contact/phone/>).

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

Region	Country	Telephone
Asia	China	+861 066 0159 450
	Hong Kong, Taiwan, Korea, Macau	+852 2531 3058
	Japan	+81 3 5484 6868
	Southeast Asia - Malaysia	+603 7805 3884
	Southeast Asia - Singapore	+65 6379 1313
	Indian Subcontinent	+91 11 515 282 502 +91 11 515 282 504
Pacific	Australia, New Zealand	+61 1300 721 495
Central America, South America	All	+55 11 5509 3440
North America	North America, Mexico, Caribbean	+1 800 547 8949 +1 530 478 4148

Region	Country	Telephone
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, Tadjhikistan, Ukraine, Uzbekistan	+7 095 258 09 20 +33 (0) 2 334 90 30
	Nordics (Norway, Sweden, Finland, Denmark, Iceland)	+45 40 47 22 37
	Southern Europe – Italy	+39 02 24 13 16 01 +39 06 87 20 35 42
	Southern Europe – Spain	+34 91 512 03 50
	Middle East, Near East, Africa	Middle East
Near East and Africa		+800 80 80 20 20 +33 1 48 25 20 20



END-OF-LIFE PRODUCT RECYCLING NOTICE

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

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

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

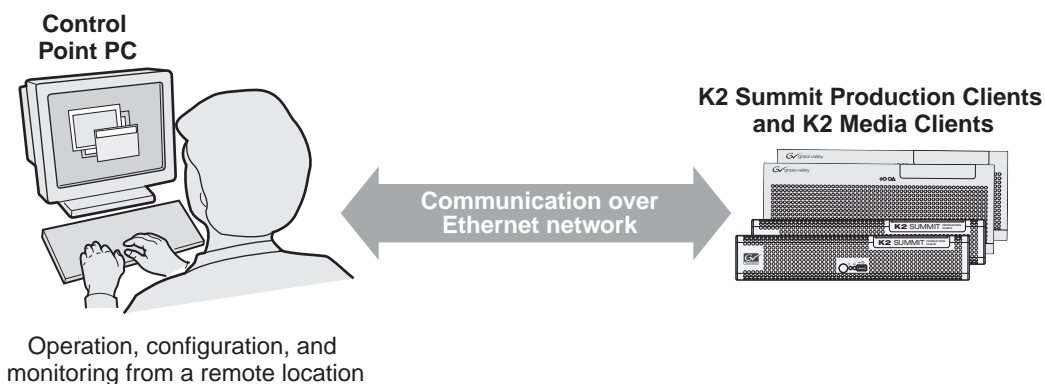


For further information on the Grass Valley product take back system please contact Grass Valley at + 800 80 80 20 20 or +33 1 48 25 20 20 from most other countries. In the U.S. and Canada please call 800-547-8949 or 530-478-4148, and ask to be connected to the EH&S Department. Additional information concerning the program can be found at: www.thomsongrassvalley.com/environment



Product Description

The K2 Summit Production Client is a cost-effective Broadcast Enterprise Server that incorporates IT server platform and storage technologies to deliver a networked solution to facilities for ingest, playout, news integration, sports, and media asset management. It is a comprehensive platform that provides a suite of user applications and system tools.



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

The K2 Summit Production Client product is further described in the following sections:

- [“K2 Summit Production Client features” on page 14](#)
- [“Product identification” on page 15](#)
- [“Front panel indicators” on page 16](#)
- [“Rear panel view” on page 17](#)
- [“K2 Summit Production Client system overview” on page 18](#)

K2 Summit Production Client features

The following features are common to all K2 Summit Production Client models:

- 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

The K2 Summit Production Client has 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. All channels support Standard Definition (SD) video and, if licensed, each pair of channels can also support High Definition (HD) video.

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.

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. Compact Flash serves as the system drive. This makes the internal storage K2 Summit Production Client 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 Summit Production Client via Gigabit Ethernet. You can also export media to a mapped drive or USB-attached storage.

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:

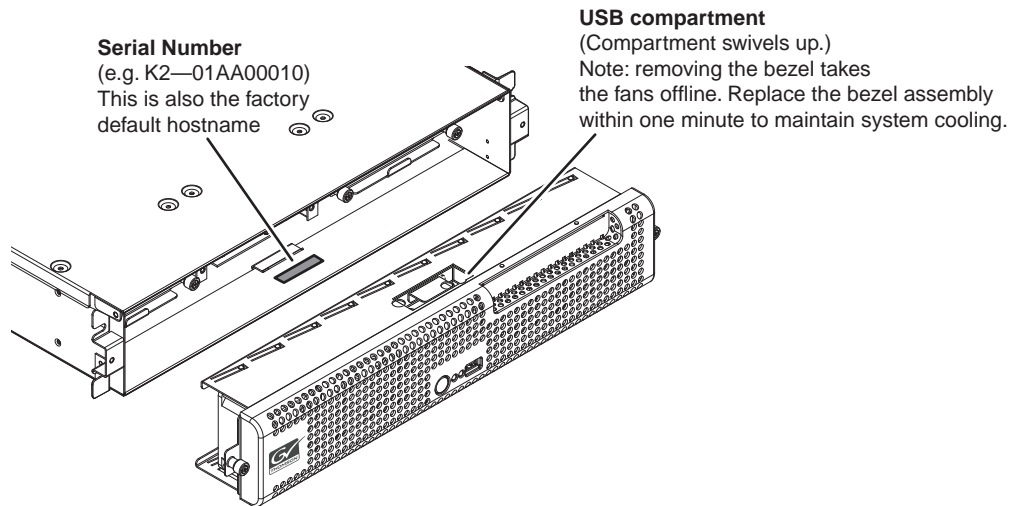
- Shared storage — Multiple external storage K2 Summit Production Clients

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.

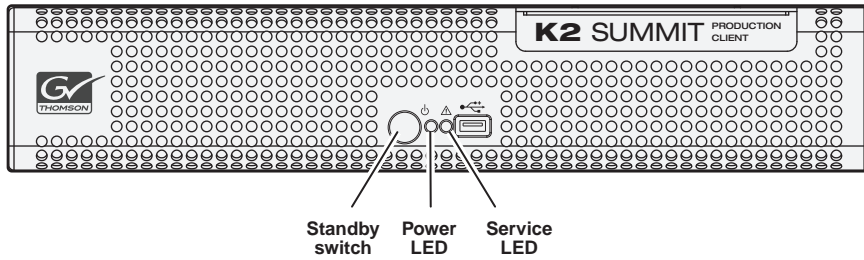
Product identification

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



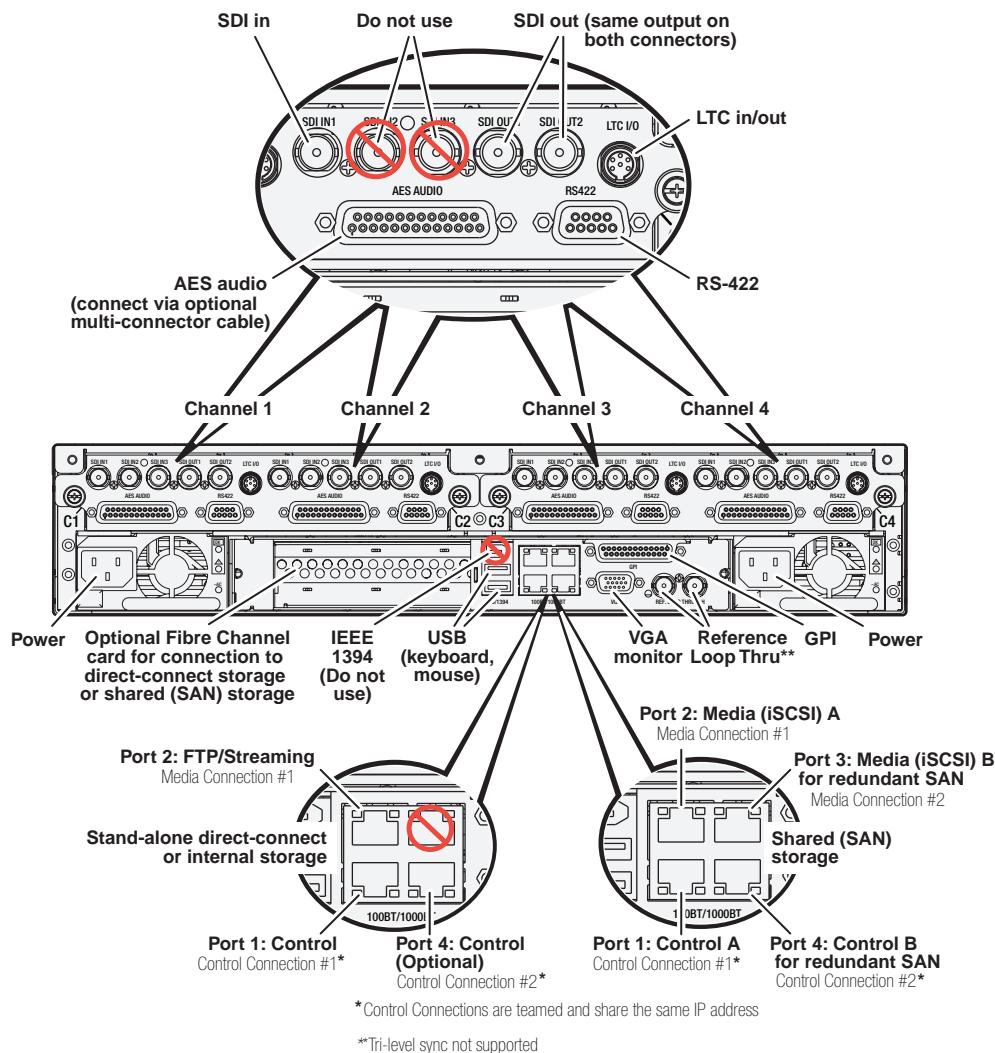
Front panel indicators

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 *K2 Summit Production Client Service Manual*.



Rear panel view

The following drawings identify the rear panel connectors and components.



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 system overview

The K2 Summit Production Client is a purpose-built client 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 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, one PCIe board slot for expansion, built in Ethernet, and USB ports.

The Application system uses a Windows XP embedded operating system upon which all K2 Summit Production Client 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 Summit Production Client.

Media control and processing

The following section explains how the Application system and the Real Time system work together to provide K2 Summit Production Client 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 Summit Production Client 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 Summit Production Client. 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, and the K2 Summit Production Client 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 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 Production Client, 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 the K2 Summit Production Client 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
3389	TCP	Remote Desktop	Used by SiteConfig.
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 Summit Production Client 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.
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 Disk1	When configured as RAID 1, these two RAID drives make up LUN 0.
Disk2 Disk3	When configured as RAID 1, these two RAID drives make up LUN 1.
Disk4 Disk5	When configured as RAID 1, these two RAID drives make up LUN 2.
Disk6 Disk7	When configured as RAID 1, these two RAID drives make up LUN 3.

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 correlate with the position of drives in the chassis. However, regardless of the RAID type and/or order of drives displayed in Storage Utility, an individual drive number in Storage Utility always correlates with that individual drive's labeling on the chassis.

Using K2 system tools

Topics in this chapter include the following:

- [“Configuration Manager”](#)
- [“K2 System Configuration”](#)
- [“Storage Utility”](#)
- [“NetCentral”](#)
- [“Windows Remote Desktop Connection”](#)

Configuration Manager

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

Configuration Manager settings are stored in a database. When the K2 Summit Production Client 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.

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 either the local K2 Summit Production Client 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:

- You can restore some individual settings or groups of settings by selecting the **Default** button which appears below the settings in the configuration screen.
- You can 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.

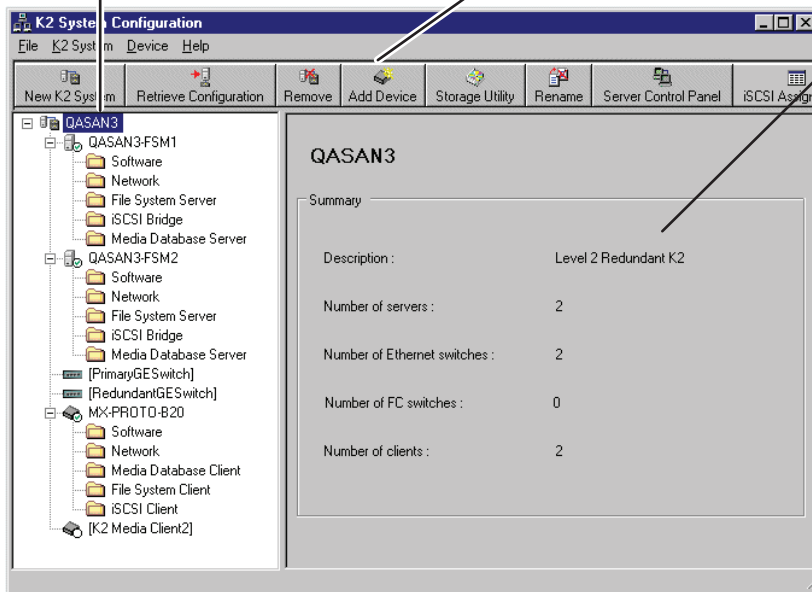
To open the K2 System Configuration application do the following:

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

You should be aware that there are two versions of Storage Utility:

- Storage Utility for the K2 SAN.
- Storage Utility for stand-alone K2 clients with their own storage

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 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. The K2 Summit Production Client 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 K2 client with stand-alone only. NetCentral is required if you are using a K2 SAN.

Windows Remote Desktop Connection

You can connect to a K2 client 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.

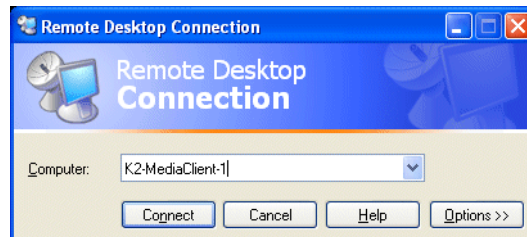
To access the Remote Desktop Connection, follow these steps:

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.

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 XML Import capture service”
- “Licensing K2 capture service software”
- “QuickTime and Final Cut Pro support”
- “Connecting RS-422”
- “Connecting GPI”

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”](#)

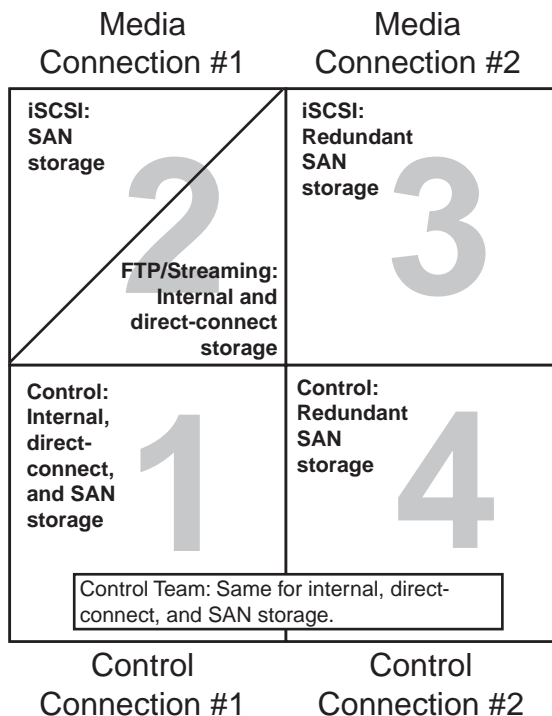
Cable requirements

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

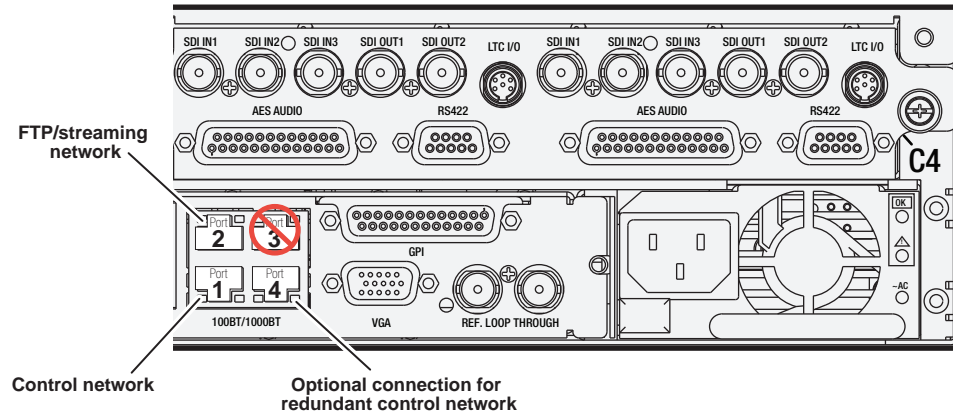
When you receive a K2 Summit Production Client from the factory, it has a specific network configuration, including a loopback adapter and two of the four Gigabit Ethernet ports configured as a teamed pair. The Gigabit Ethernet ports, as viewed when looking at the rear panel, are represented in the following illustration.



Making network connections

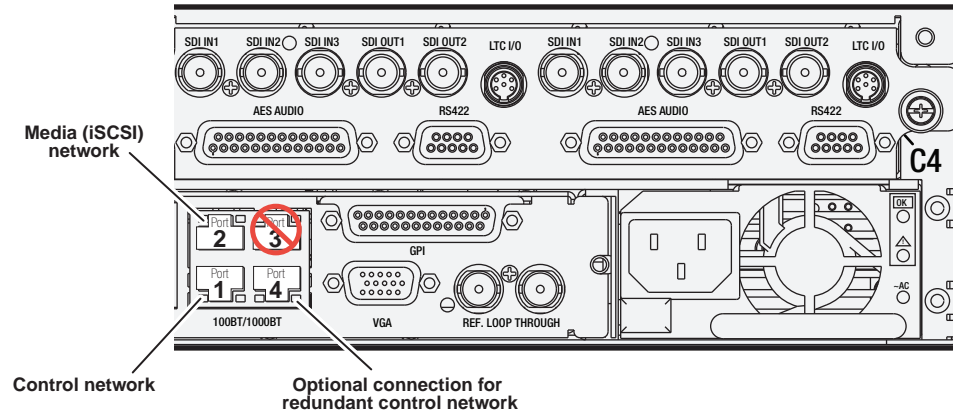
Connect network ports as appropriate for the K2 Summit Production Client storage option, as follows:

Stand-alone storage K2 Summit Production Client network connections



On an internal storage 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.

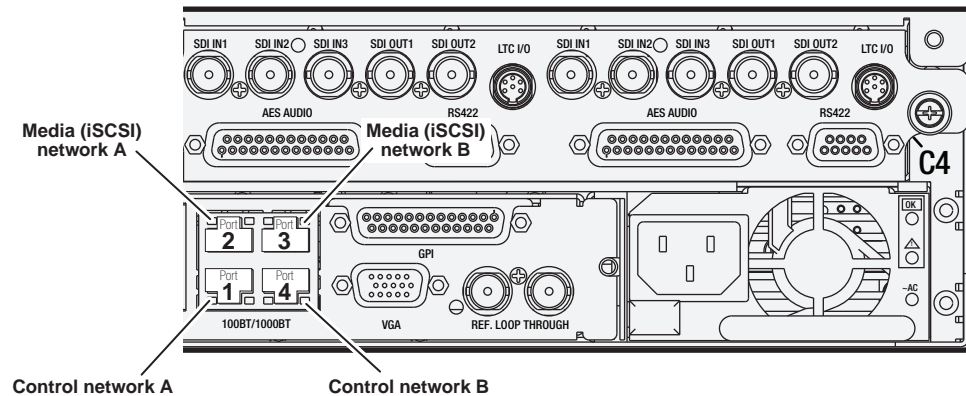
Basic shared storage (SAN) K2 Summit Production Client network connections



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 Summit Production Client”](#)
- [“Streaming video between K2 systems”](#)

About network functionality

K2 networks support the following:

- Remote control and configuration of the K2 Summit Production Client using AppCenter from a Control Point PC.
- Remote control of the K2 Summit Production Client using devices and applications software developed for the K2 Summit Production Client 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 Summit Production Client has a write filter that must be disabled before making a network configuration change. Refer to [“About the write filter” on page 81](#).
- Loopback adapter — When you receive a K2 Summit Production Client or a K2 Media Client from the factory, it has a loopback adapter installed. The loopback adapter allows the media file system to continue operating if an Ethernet cable is disconnected. Do not modify the loopback adapter. If you need to restore the loopback adapter, refer to the *Service Manual* for your 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 Summit Production Client 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 Summit Production Client



CAUTION: *The K2 Summit Production Client 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 K2 Summit Production Client 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 K2 Summit Production Client 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 K2 Summit Production Client need to be configured, you must have Windows administrator security privileges on the K2 Summit Production Client.

To configure network settings on a stand-alone K2 Summit Production Client, do the following:

1. If you have not already done so, disable the write filter. Refer to [“Disabling the write filter” on page 82](#).
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 K2 Summit Production Client 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 K2 Summit Production Client 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 K2 Summit Production Client.

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 K2 Summit Production Client 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 82](#).

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 K2 Summit Production Clients or K2 Media Clients, the K2 client 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 37](#).
- The host name of all peer K2 systems, M-Series iVDRs, 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 38](#). 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 82](#).
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 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.

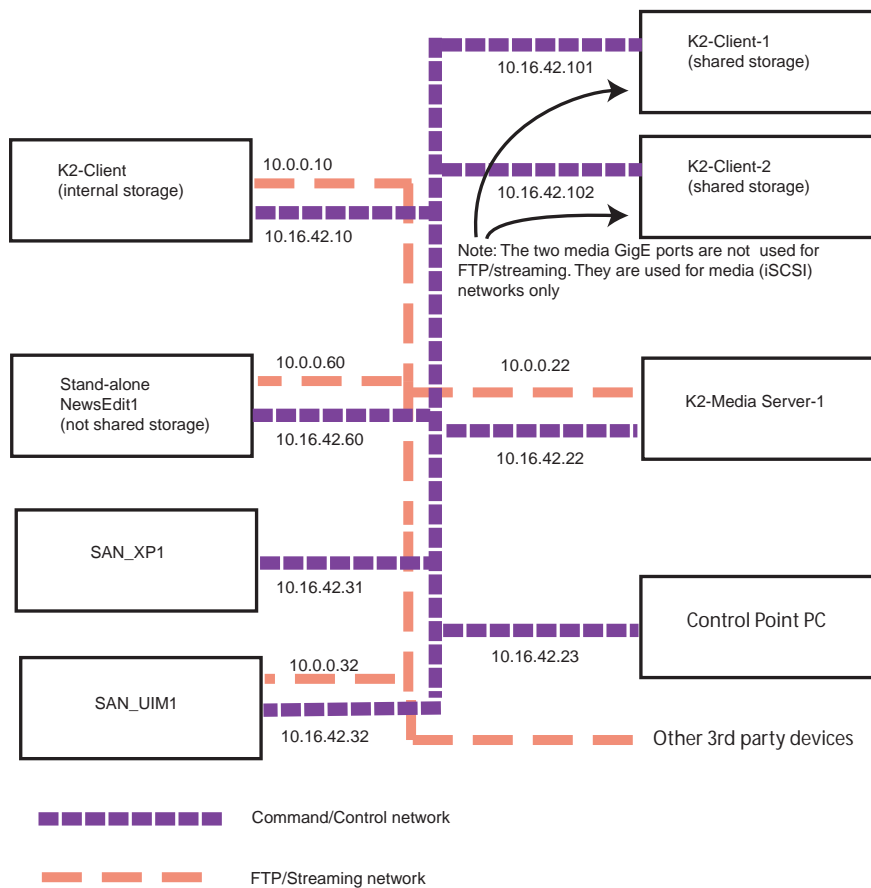
Remember to disable the write filter on all K2 Summit Production Clients.

8. Enable the write filter. Refer to “Enabling the write filter” on page 82.

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 client with stand-alone storage, K2 clients with shared (SAN) storage, and other Grass Valley systems.



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

All lines beginning with a # are comments and can be ignored or deleted.

```
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# For example:
# 102.54.94.97 rhino.acme.com # source server
# 38.25.63.10 x.acme.com # x client host
```

127.0.0.1	localhost
10.16.42.10	K2-Client
10.0.0.10	K2-Client_he0
10.16.42.101	K2-Client-1
10.16.42.102	K2-Client-2
10.16.42.22	K2-MediaServer-1
10.0.0.22	K2-MediaServer-1_he0
10.16.42.23	ControlPointPC
10.16.42.60	NewsEdit1
10.0.0.60	NewsEdit1_he0
10.16.42.31	SAN_XP1
10.0.0.32	SAN_XP1_he0 SAN_UIM1_he0
10.16.42.32	SAN_UIM1

Add host names to AppCenter to enable streaming

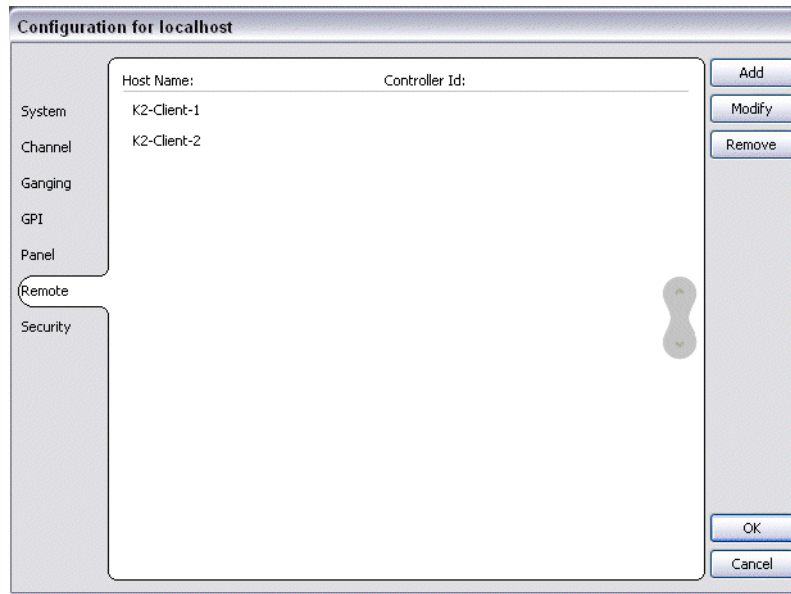
In K2 AppCenter, you must add the host names of all peer K2 systems on the network that support streaming transfers. Adding host names is required to allow selection of networked K2 systems in the AppCenter user interface and to provide a successful network connection for streaming. The host names added appear in the “Import” and “Send to” dialog boxes.

NOTE: By default, the K2 system host name is the same as the Windows 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”.

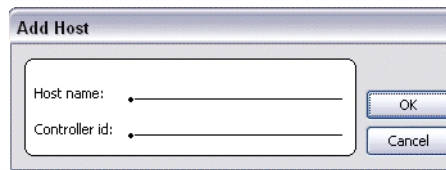
To add network host names:

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 client model 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 44](#) for examples.

The K2 FTP server runs on K2 Media Servers that have the role of FTP server. While it also runs on 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 84](#).

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 K2's 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 113](#).

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 43](#).
 - 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 clients. 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
- M-Series iVDR
- 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 89.

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.

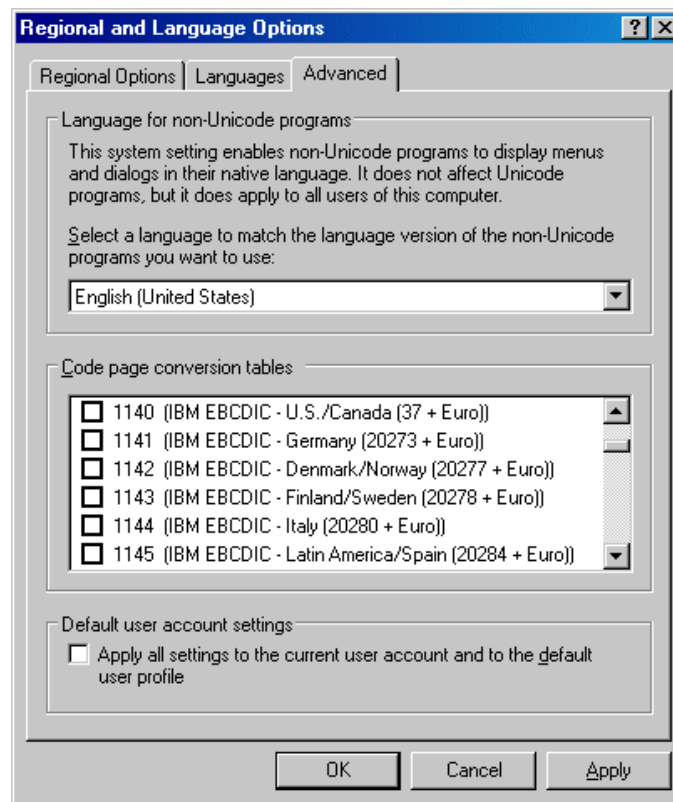
Also refer to [“Internationalization”](#) on page 128.

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 both a K2 Media Server and a stand-alone K2 client, as they both 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 82](#).
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 82](#).

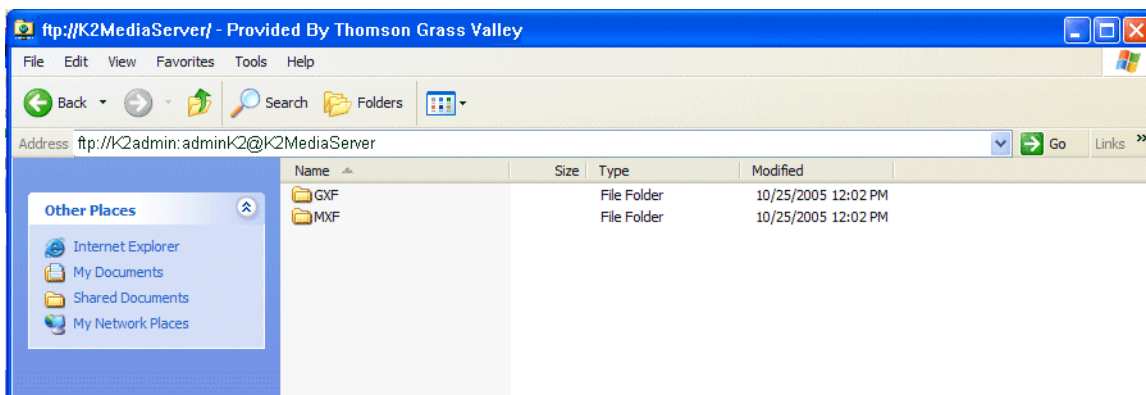
FTP access by Internet Explorer

You can use Internet Explorer to transfer files via FTP between a PC and the FTP interface on a stand-alone K2 client 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 89 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.



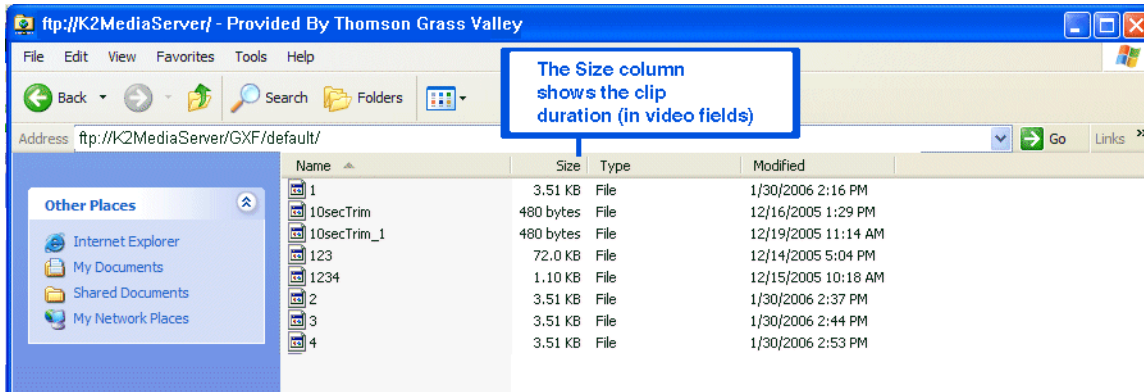
GXF — General Exchange Format (SMPTE 360M). This is the standard Grass Valley file interchange format. Refer to specifications later in this manual for media types supported.

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 client 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 K2 client 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
SYST	System	Supported
SIZE	Size of file (clip)	Supported. Reports size in Bytes.
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 113](#).

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.

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 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 Summit Production Client, a stand-alone K2 Media Client, 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.
- 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 a K2 client (Stand-alone)

1

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



K2 client (stand-alone)

2

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



3

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

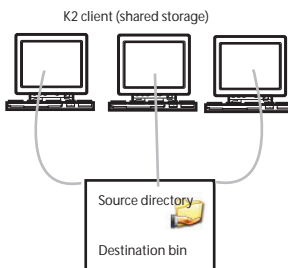
4

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

Using the HotBin service with a K2 SAN

1

On the K2 Media Server, make the source directory a shared folder.



K2 Media Server

2

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



3

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

4

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.

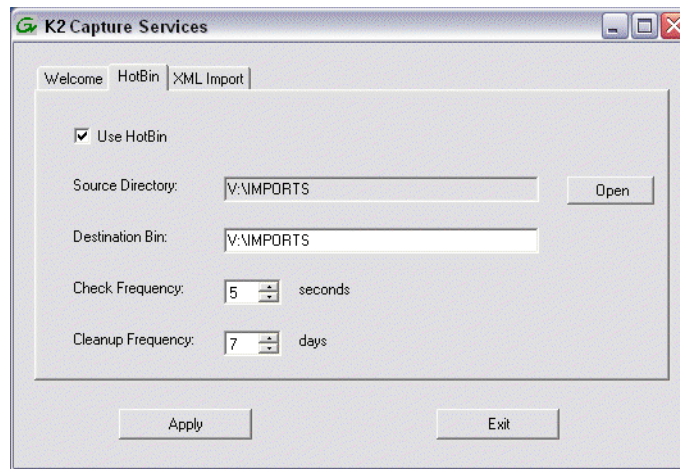
If your source directory is on:	... and the source directory is on a shared folder on a mapped drive, you need:
Another Windows system	<ul style="list-style-type: none"> • Administrator privileges for the K2 system • A user account with log-in service rights for your system
Macintosh operating system	<ul style="list-style-type: none"> • 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.
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. Click **Apply**.

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

9. Click **OK**.

The K2 client 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.

10. 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 <code>V: / IMPORTS</code> .
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, <code>V: / IMPORTS</code> .

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 Summit Production Client or stand-alone K2 Media Client — 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 client. The watched folder must be on the K2 client’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 Summit Production Client, stand-alone K2 Media Client, 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 client 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.*

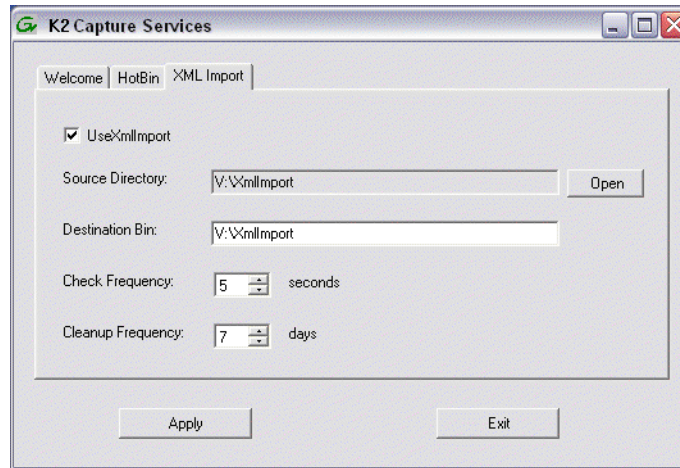
1. From the **Start** menu, access the **Programs** menu and select **Grass Valley | K2 Capture Services**.

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** tab.



4. Select **Use Xmllmport**.

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 client 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 <code>V:\XmlImport</code> .
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 <code>V:\XmlImport</code> .

Licensing K2 capture service software

Licensing is required for K2 capture service software as follows:

- To use the XML Import capture service, you must obtain a XML Import capture service license from Grass Valley.

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.

QuickTime and Final Cut Pro support

Whenever a new, simple, DV-format 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 Summit Production Client is not supported.

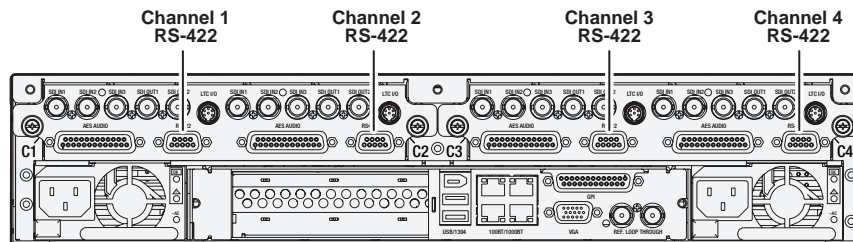
The QuickTime reference file is created when the K2 clip's record or import operation is complete. QuickTime related files are stored next to the media in your V: bin structure. Subsequent modifications to the K2 clip do not affect the QuickTime reference file.

The following procedure outlines the supported workflow for accessing and using the QuickTime files. Do not attempt other workflows, such as attempting to edit the files and saving the changes to the *V:\default* share on the K2 system.

1. Share *V:\default*. Use standard Windows operating system procedures and set permissions to read only. Create the share as follows:
 - If the files are on a stand-alone K2 client, on that K2 client create the *V:\default* share.
 - If the files are on a K2 SAN, on the primary file system/metadata K2 Media Server create the *V:\default* share. Do not create the share on a SAN connected K2 client.
2. To open a QuickTime reference file, from the system on which you are running your QuickTime tool, access the *V:\default* share. Use standard Macintosh operating system procedures.
3. Browse to the location of the media in your bin structure. The QuickTime reference file is named according to the following convention:
`<bin name>\<clip name>\<clip name>.mov.`
4. Open the file in your QuickTime tool and then **Save As** to the location of your work in progress. This is now your master file.
5. Edit the master file as desired.
6. When you have finished material that you have created in your QuickTime tool, export it to the K2 system via FTP.

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:

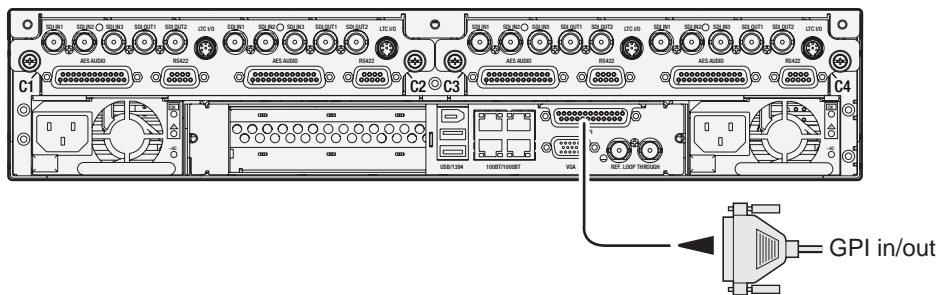


Refer to the following for more information about RS-422 and protocol control:

- [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.



Also see the following related sections of this manual:

- [“GPI I/O specifications” on page 120](#)
- [“GPI I/O connector pinouts” on page 143](#)

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

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”](#)

About the internal storage system

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

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.

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 Client”](#)
- [“Checking the media file system”](#)
- [“Cleaning unreferenced files and movies”](#)
- [“Downloading disk drive firmware”](#)
- [“Storage Utility operation not supported”](#)
- [“Placing the K2 Media Client into online mode”](#)

About Storage Utility

You can use Storage Utility for general maintenance tasks on a stand-alone K2 client. Refer to the K2 Service Manual for the K2 client model for repair procedures, such as those required to replace a failed drive. Also refer to “Storage Utility” on page 26 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 client or from a Control Point PC. In both cases the Storage Utility’s primary functionality is hosted by the K2 client. The Storage Utility uses the connection to the RAID disks for access and configuration.

The K2 Media Client runs in either an online mode or an offline mode. These modes are required for Storage Utility operations on a K2 Media Client. On a K2 Summit Production Client, Storage Utility does not require online/offline modes.

On a K2 Media Client, online/offline modes are as follows?

- Online mode — This is the K2 Media Client’s normal operating mode. When the K2 Media Client 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 K2 Media Client channels are disconnected and all media access operations are disabled. You are prompted to put the K2 Media Client into offline mode when you select an operation that configures the storage system. When the K2 Media Client 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 K2 Media Client 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 client, 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 into Storage Utility separately.

If you are running AppCenter on the local K2 client, as Storage Utility opens it connects to the storage system of that K2 client. If you are running AppCenter on a control point PC, as Storage Utility opens it connects to the storage system of the K2 client 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 client or on the control point PC and logon.
Make sure you logon to AppCenter with appropriate privileges, as this logon is passed to Storage Utility. Administrator-level permission is necessary for most Storage Utility operations. If you log in with user-level permissions, the Storage Utility menu item is disabled.
2. If you are running AppCenter from a control point PC and you have channels from multiple K2 clients in your channel suite, select a channel from the stand-alone K2 client whose storage you intend to configure with Storage Utility. This is important as Storage Utility automatically connects to the K2 client that hosts the currently selected channel.

NOTE: Make sure you are connecting to a stand-alone K2 client. 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 client. To verify this, use the Identify feature to flash the disks on the K2 client. Refer to [“About identifying disks” on page 68](#).

Opening Storage Utility Independently

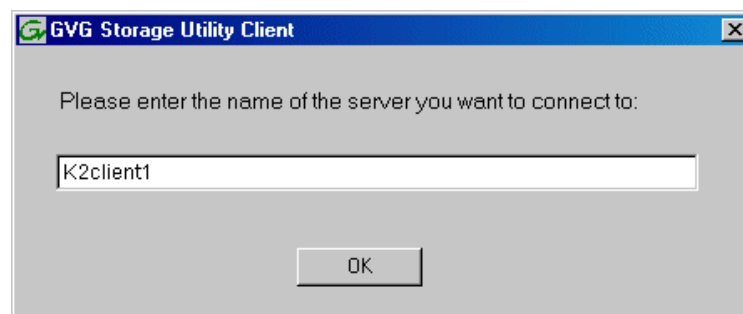
Do not open Storage Utility independently unless there is a problem that prevents you from opening it through AppCenter.

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.

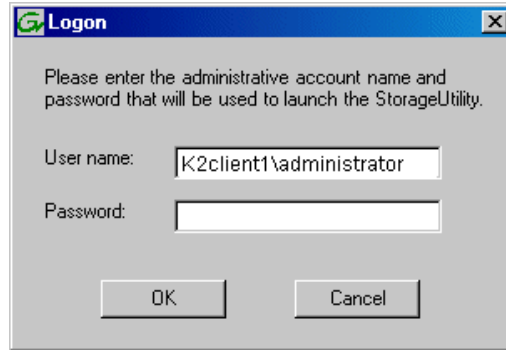
NOTE: Make sure you are connecting to a stand-alone K2 client. You should never connect Storage Utility directly to a K2 client that uses shared storage.



2. Enter the name or IP address of the K2 client for which you intend to use Storage Utility. If you are opening Storage Utility on a local K2 client, enter the name of

that K2 client. Click **OK**.

The Storage Utility logon dialog box opens.

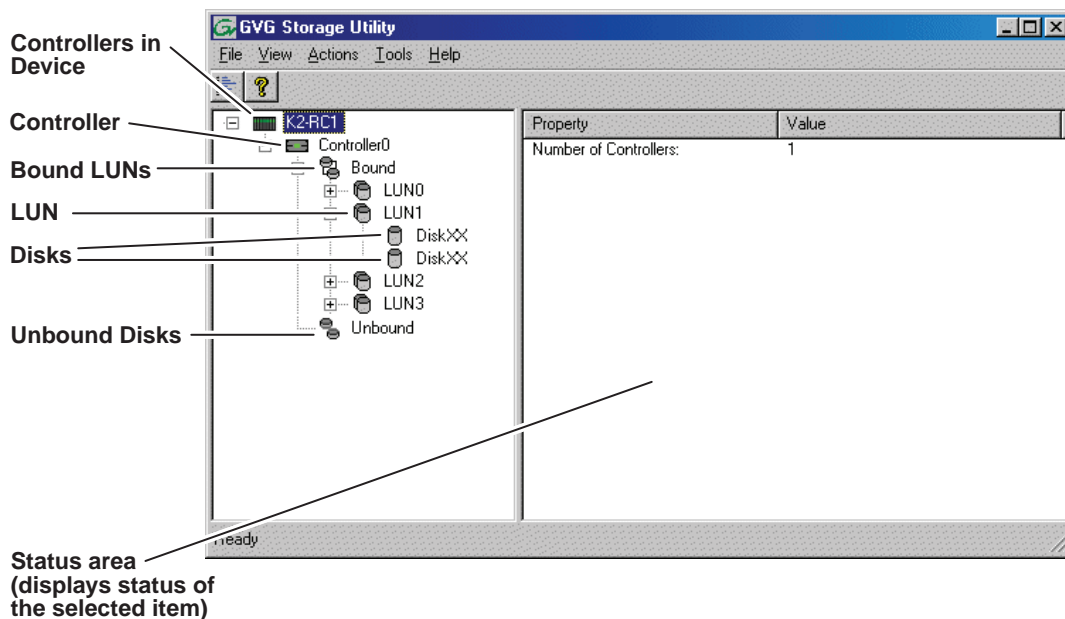


3. Logon to Storage Utility. Make sure you logon with appropriate privileges. Administrator-level permission is necessary for most Storage Utility operations. For User name, you might need to enter the machine name as the domain to successfully log on.

Storage Utility opens.

4. If you are connecting from a control point PC, you should verify that you are connected to the correct K2 client. To verify this, use the Identify feature to flash the disks. Refer to [“About identifying disks”](#) on page 68.

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

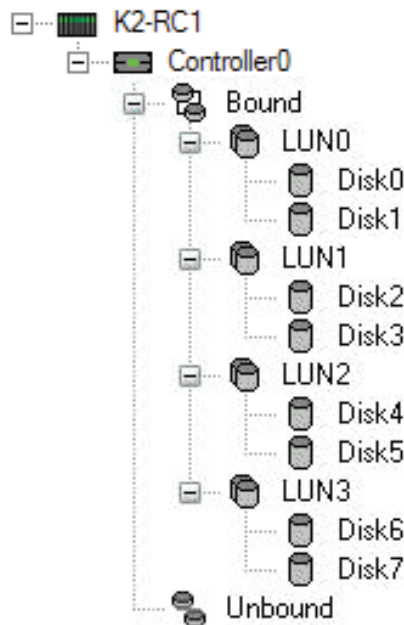
The Identify feature allows you to flash the disk LEDs so that you can physically locate a specific disk module or group of disk modules that make up a LUN. Always use the disk identify feature before removing and replacing a failed disk module. Accidentally removing the wrong disk module can destroy all data on the disk drives.

You can also use this feature to verify the K2 client to which you are currently connected.

Identifying K2 Summit Production Client internal disks

To identify 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) or RAID 0.



2. Remove the front bezel assembly from the K2 Summit Production Client chassis.

NOTE: Replace the bezel assembly within one minute to maintain system cooling.

3. The table below illustrates the position of drives as numbered in the K2 Summit Production Client chassis. Compare the drive number positions and the disk numbering displayed in Storage Utility to identify drive locations.

Disk2	Disk4	Disk7
Disk1	Disk3	Disk6
Disk0		Disk5

4. Position yourself so you can see the RAID drive LEDs. In normal operation LEDs are red.
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 on the internal storage disk or disks 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

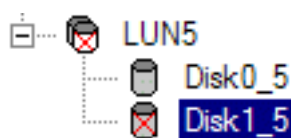
1. In the tree view, select the controller.
2. Click **Actions | Get Controller Logs**.
3. A message informs you of the location of the logs.
4. Find the following files on the local K2 client at `C:\logs`:
 - MegaRaidDriveFailureLog.txt
 - MegaRaidNVRAMLog.txt
 - tty.log

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 client 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 client 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.

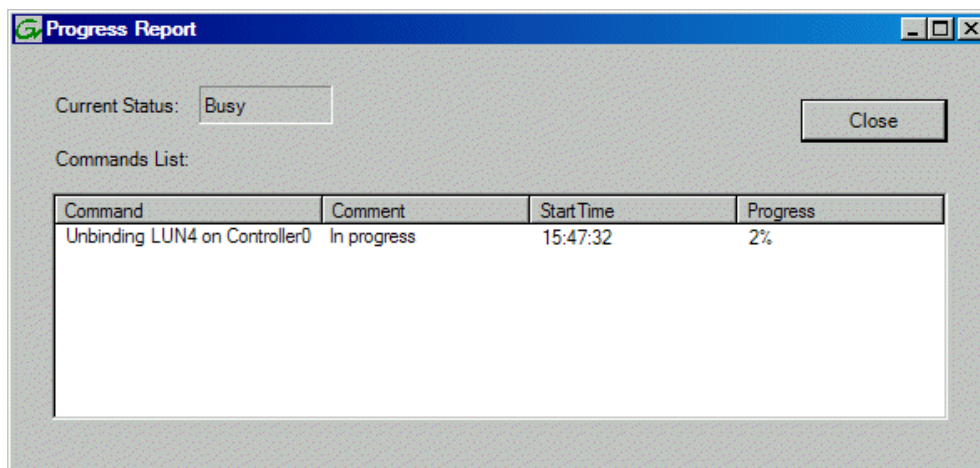


CAUTION: *Unbinding destroys all data stored on disk modules.*

For a direct-connect storage, refer to [“Unbinding/binding direct-connect storage LUNs” on page 103](#).

To unbind a LUN, do the following:

1. In the tree view, right-click the LUN and select **Unbind LUN**.
2. If a K2 Media Client and online, messages appear “...offline mode now?” and “...continue?”. Click **Yes** to put the K2 Media Client 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 client.

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

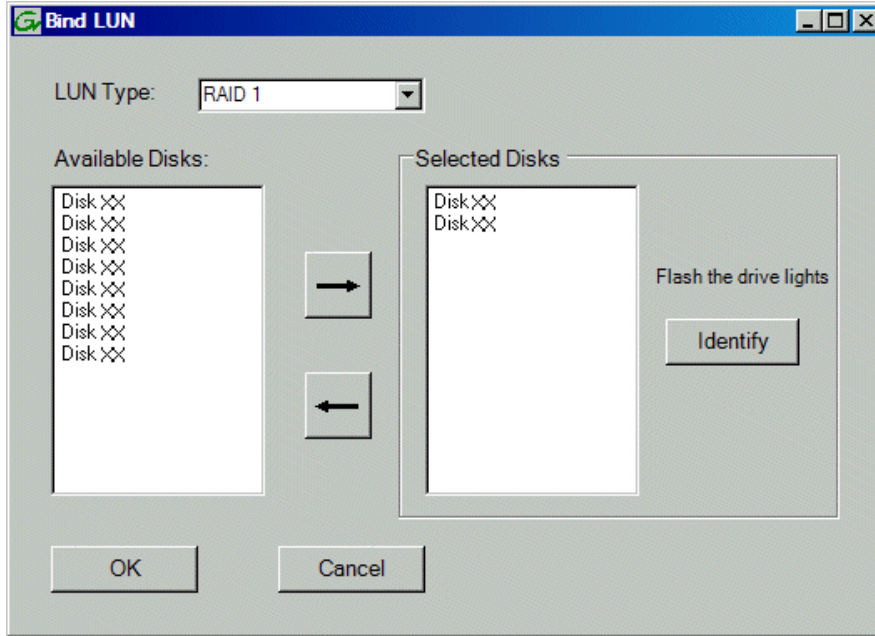
When you bind a LUN, you select one or more unbound disks and create a new LUN. The Storage Utility places this new LUN at the bottom of the list and numbers it accordingly. However, with internal storage, disk numbers are enforced by the chassis slot in which the disk resides. Therefore, depending on 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 client 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 [“Unbinding/binding direct-connect storage LUNs” on page 103](#).

To bind a LUN, do the following:

1. In the tree view, right-click the **Unbound** node and select **Bind LUN**.
2. If a K2 Media Client and online, messages appear “...offline mode now?” and “...continue?”. Click **Yes** to put the K2 Media Client 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.
 - 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 client.

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 Client” on page 73](#).

Changing RAID type for internal storage

You can change the media storage on an internal storage K2 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. 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 70](#). 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 71](#), 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 Client” on page 73](#).
7. If you backed up your media, you can now transfer it back.

Making a new media file system on a K2 Summit Client

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.

The Configuration File window opens.

3. You can view media file system settings, but do not attempt to change them. Click **Accept**.

A “Making new file system. Please wait” message box displays progress.

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

Making a new media file system on a K2 Media Client

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

2. If the K2 client is online, messages appear “...offline mode now?” and “...continue?”. Click **Yes** to put the K2 Media Client in offline mode.

AppCenter channels go offline. The Configuration File window opens.

3. You can view media file system settings, but do not attempt to change them. Click **Accept**.

A “Making new file system. Please wait” message box displays progress.

4. When a message “Succeeded to make the new file system. The server will be restarted now” appears, click **OK** to restart the K2 Media Client.

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 a K2 Media Client and online, messages appear “...offline mode now?” and “...continue?”. Click **Yes** to put the K2 Media Client in offline mode.

AppCenter channels go offline.

3. A message box appears “Checking media file system. Please wait”. Observe progress.

If problems are discovered they are reported. If the check process passes, when the process is complete a message appears to confirm success.



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

Your file system has been checked.

Cleaning unreferenced files and movies

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 a K2 Media Client and online, messages appear "...offline mode now?" and "...continue?". Click **Yes** to put the K2 Media Client 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 a K2 Media Client and online, messages appear "...offline mode now?" and "...continue?". Click **Yes** to put the K2 Media Client 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 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 a K2 Media Client and online, messages appear "...offline mode now?" and "...continue?". Click **Yes** to put the K2 Media Client 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.
5. 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.

6. Repeat this procedure on each drive.
7. When finished, exit Storage Utility. If a K2 Media Client, put AppCenter channels back online. Restart.

Storage Utility operation not supported

The following option is displayed in the Storage Utility menu system, but the operation is not supported for internal storage.

- Expand File System by Capacity

Placing the K2 Media Client into online mode

If the K2 Media Client is in offline mode and you have completed your storage system configuration tasks, you have the following options to return the K2 Media Client 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 Media Client, close and reopen AppCenter.

- **Restart the K2 Media Client** — Restarting automatically resets the K2 Media Client to online mode. When you log into AppCenter channels connect and come up online.

Managing K2 system software

This chapter contains 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.
SiteConfig	The K2 System Software CD and via download	..\SiteConfig\setup.exe	Control Point PCs	Manages K2 clients and devices of the K2 SAN for network configuration and software deployment.
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 “[Control Point PC system requirements](#)” on page 132. 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 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 Product Client	K2 Summit Production Client Service Manual
K2 Media Client	K2 Media Client Service Manual
K2 Media Server	K2 SAN Installation and Service Manual
Control Point PC	Use procedures from a K2 client Service Manual

Administering and maintaining the K2 system

This chapter contains the following topics:

[“Licensing” on page 83](#)

[“About the write filter” on page 81](#)

[“Enabling the write filter” on page 82](#)

[“Disabling the write filter” on page 82](#)

[“Committing a file to disk with write filter enabled” on page 82](#)

[“Configuring K2 security” on page 84](#)

[“K2 and NetCentral security considerations” on page 93](#)

[“Microsoft Windows updates” on page 94](#)

[“Virus scanning policies” on page 95](#)

[“Enabling and disabling the USB ports” on page 96](#)

[“Configuring auto log on” on page 97](#)

[“Regional and language settings” on page 97](#)

About the write filter

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

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

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

Enabling the write filter

Prerequisite:

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

Disabling the write filter

Prerequisite:

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

Committing a file to disk with write filter enabled

Prerequisite:

- K2 software must be installed on the K2 Summit Production Client.

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 on to the K2 Summit Production Client 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” on page 85](#)
- [“Example: Setting up user access to bins” on page 86](#)
- [“Example: Setting up user access to channels” on page 86](#)
- [“Security and user accounts” on page 87](#)
- [“Configuring media access security for K2 bins” on page 87](#)
- [“AppCenter operations and media access security” on page 89](#)
- [“FTP and media access security” on page 89](#)
- [“K2 SANs and media access security” on page 90](#)
- [“Protocol control of channels and media access security” on page 90](#)
- [“Configuring channel access security” on page 91](#)

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 87](#).
- 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 87](#).
- 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 89](#).
 - 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 89](#).
 - 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 90](#).
- Channel access — You can set user permissions for each channel. Then, depending on the current AppCenter logon, permission is granted or denied to operate the channel. Refer to [“Configuring channel access security” on page 91](#).

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
<input type="checkbox"/> Log on to the local K2 client with Windows administrator permissions.	“Security and user accounts” on page 87
<input type="checkbox"/> Configure a “userA” account and a “userB” account on the local K2 client. Do not assign these users to the administrators group.	Use standard Windows procedures
<input type="checkbox"/> Log on to AppCenter with K2 administrator permissions.	“Security and user accounts” on page 87
<input type="checkbox"/> Create a “userA_private” bin and a “userB_share” bin on the local K2 client.	<i>K2 AppCenter User Manual</i>
<input type="checkbox"/> For bin “userA_private” configure an access control list with permissions as follows: - Everyone: Remove this group from the access control list - BUILTIN/Administrators: Deny Full Control - userA: Allow Full Control	“Configuring media access security for K2 bins” on page 87
<input type="checkbox"/> For bin “userB_share” configure an access control list with permissions as follows: - Everyone: Remove this group from the access control list - userA: Allow Full Control - All accounts except userA: Allow Explore Bin, Deny Rename Clips, Deny Delete Clips	“Configuring media access security for K2 bins” on page 87
<input type="checkbox"/> Log on to AppCenter as userA. Test userA access to bins. Log off.	—
<input type="checkbox"/> 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
<input type="checkbox"/> Log on to the local K2 client with Windows administrator permissions.	“Security and user accounts” on page 87
<input type="checkbox"/> Configure a “userA” account and a “userB” account on the local K2 client. Do not assign these users to the administrators group.	Use standard Windows procedures
<input type="checkbox"/> Log on to AppCenter with K2 administrator permissions.	“Security and user accounts” on page 87
<input type="checkbox"/> For channels 1 and 2, configure access control lists with permissions as follows: - Everyone: Remove this group from the access control list - userA: Allow	“Configuring channel access security” on page 91
<input type="checkbox"/> For channels 3 and 4, configure access control lists with permissions as follows: - Everyone: Remove this group from the access control list - userB: Allow	“Configuring channel access security” on page 91
<input type="checkbox"/> Log on to AppCenter as userA. Test userA access to channels. Log off.	—
<input type="checkbox"/> 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 client(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 client 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.

Security on K2 bins is enforced through the media database. It is not enforced through the Windows file system. Even though the configuration for permissions on K2 bins appears similar to that for Windows folders, do not confuse the two types of security. Do not use Windows procedures to configure file system security on a folder and

expect it to be enforced as a part of K2 media access security. Likewise, do not configure K2 media access security and expect it to affect Windows file system operations.

You can set permissions on a K2 bin as follows:

- Rename — Allow or deny access to rename any of the clips located in the bin.
- Delete — Allowed or deny access to delete any of the clips located in the bin.
- Explore Bin — 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.

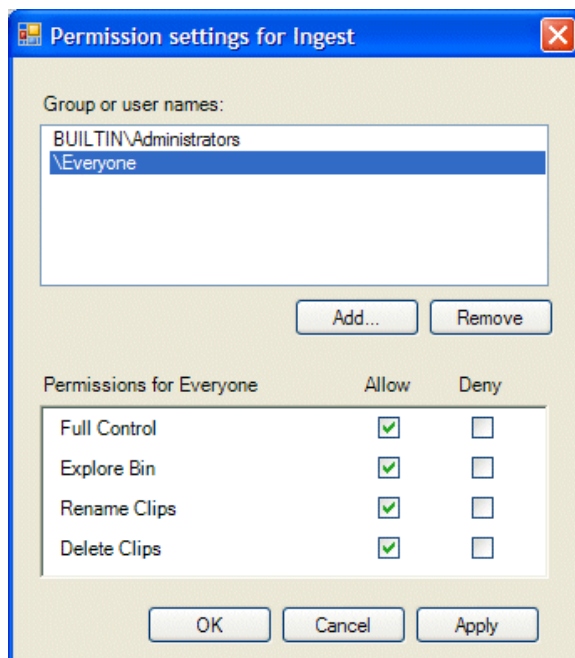
As you configure permissions, take the following into account:

- 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.
- You can remove the “Everyone” group from the access control list. In most cases this gives you better control for selectively allowing and denying permissions.
- The *BUILTIN\Administrators* account retains the ability to modify permissions, even if you set the permission for this account to deny Full Control.

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 Summit Production Client or K2 Media Client.
- 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 explore 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 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.

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 client, permissions for all four local channels are based on the single user logged on. Therefore channel permissions are enforced for just one user at a time across the four 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 client, 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.

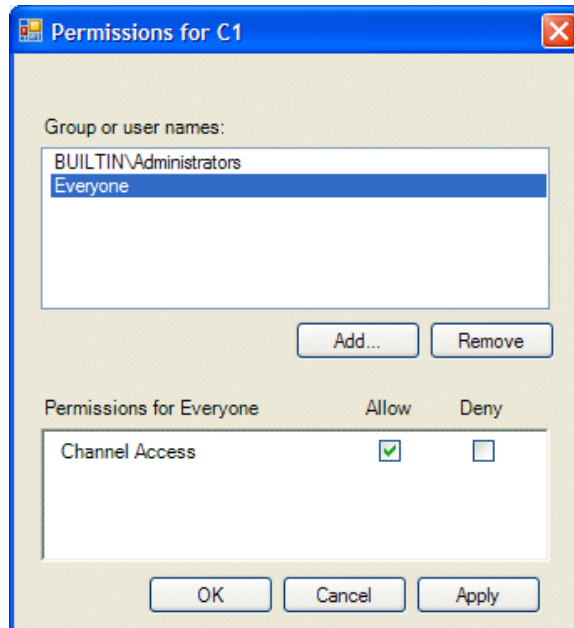
Once permissions are granted based on the current logon account, those permissions remain in place until that account logs off of AppCenter.

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.

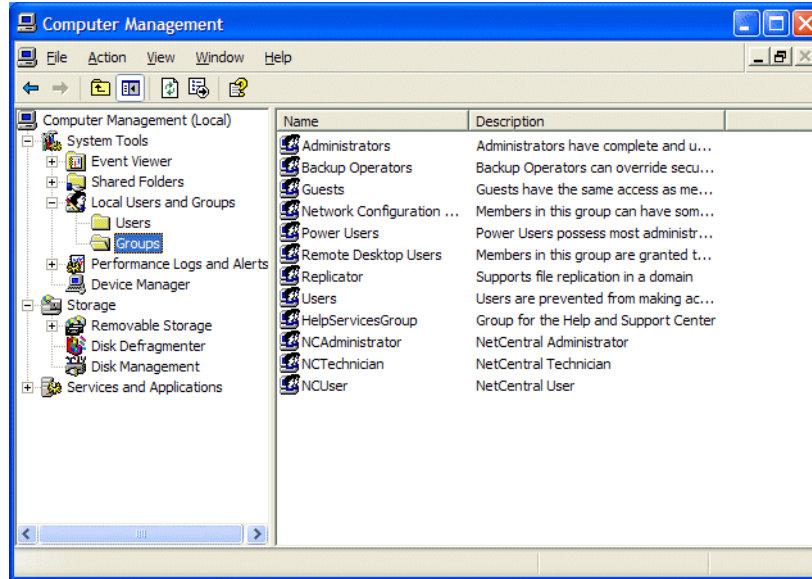
Mapping a NetCentral administrator to the K2 administrator level

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 operating system is Microsoft Windows XP Embedded. 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.

Other Grass Valley products, such as the K2 Summit Production Client and 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 itself at the same time the system is being used to record or play video to air.

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

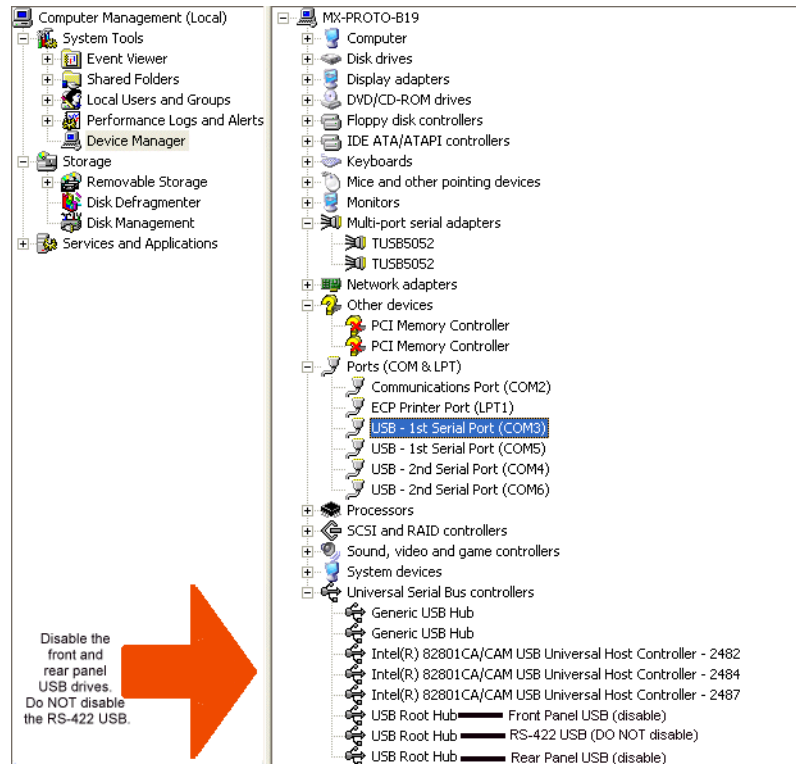
Network and firewall policies

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 client 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 96.](#)

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 client 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 client.



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 client USB port via a control point PC.

To transfer to or from a USB drive on an internal storage K2 client, 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 client 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 or a K2 Summit Production Client to automatically log on to Windows at startup, AppCenter honors this setting. This means that at startup AppCenter bypasses its log on dialog box and opens automatically. For more information about how to turn on automatic logon 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 Client, K2 Media Clients, 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 43](#) and [“Internationalization” on page 128](#) for more information.

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 99](#)
- [“Powering up K2 RAID” on page 102](#)

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 intended 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. Also refer to [“Using Storage Utility” on page 63](#).

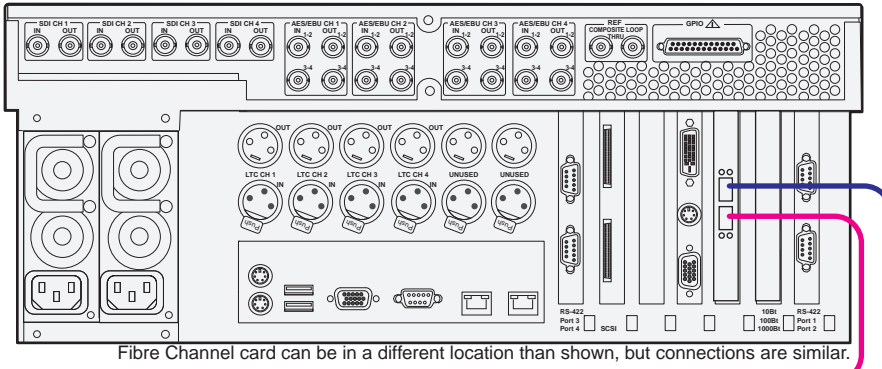
Prerequisites for the following procedure are as follows:

- 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

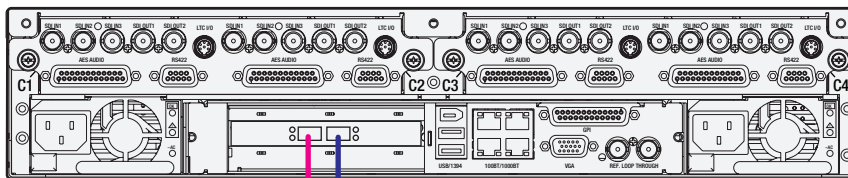


Fibre Channel card can be in a different location than shown, but connections are similar.

To K2 RAID Controller

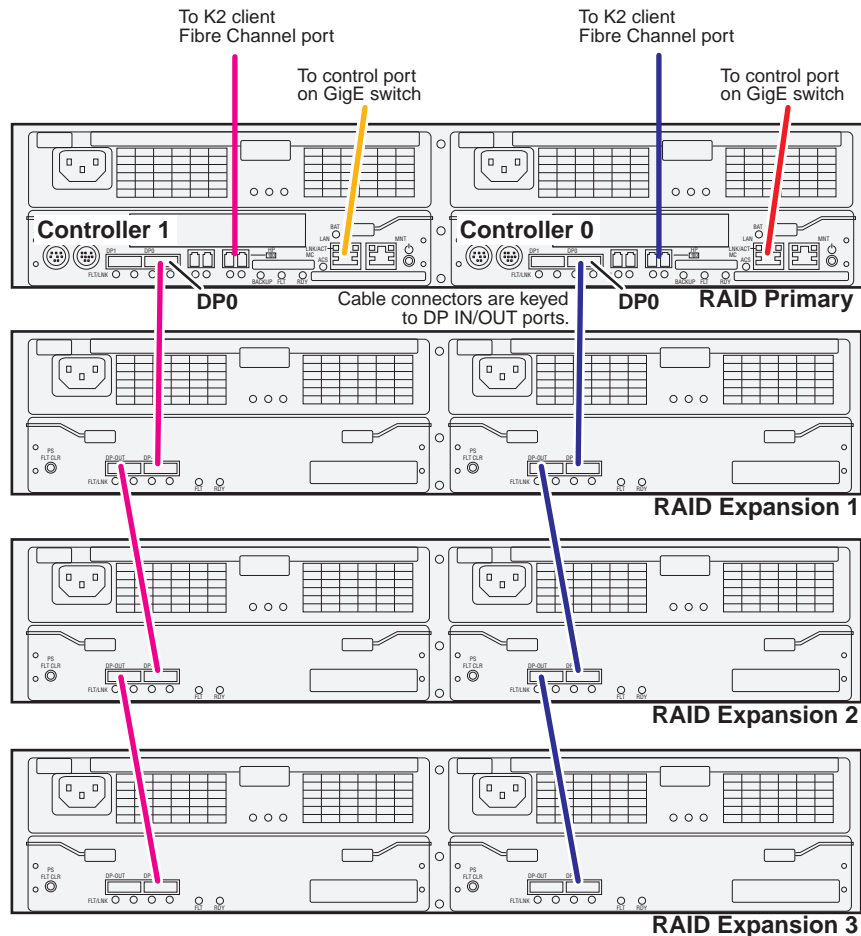
To K2 RAID Controller

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

6. Restart the K2 client.
7. 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.)
8. On the K2 client, open Storage Utility.
9. 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.

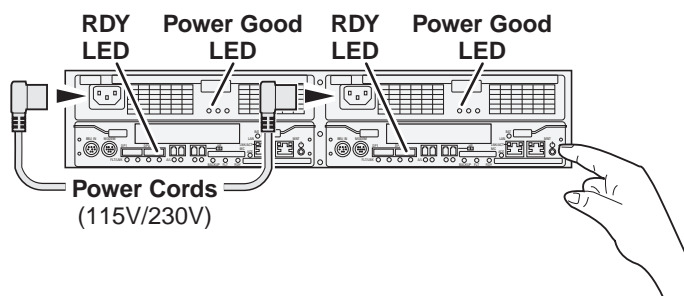
- c. When the binding process completes, restart the K2 client.
- d. In Storage Utility, make a new file system. If you get a "...failed to remove the media database..." message, you can safely proceed.
- e. Restart the K2 client.

The K2 client is now ready for record/play operations.

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.

Unbinding/binding direct-connect storage LUNs

Once you have LUNs bound and your direct-connect storage is operational, special procedures are required for subsequent unbinding and/or binding, as follows:

1. Unbind all LUNs.
2. Disconnect all Fibre Channel cables from the K2 client.
3. Restart the K2 client.
4. On the K2 client, from the Windows desktop click **Start | Run**, type `cmd` and press **Enter**. The MS-DOS command prompt window opens.
5. From the command prompt, navigate to the `C:\profile\mpio` directory.
6. Type the following at the command prompt:

```
gdsminstall.exe -u C:\profile\mpio gdsminf Root\GDSM
```
7. Press **Enter**. The Multi-Path I/O (MPIO) software is uninstalled.
8. Restart the K2 client.
9. Reconnect Fiber Channel cables.
10. Restart the K2 client.
11. On the K2 client, open Storage Utility.
12. 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, restart the K2 client.
 - d. In Storage Utility, make a new file system. If you get a "...failed to remove the media database..." message, you can safely proceed.
 - e. Restart the K2 client.
 - f. On a K2 Media Client, open AppCenter and manually remove all clips and bins except the default bin and the recycle bin.
13. On the K2 client, from the Windows desktop click **Start | Run**, type `cmd` and press **Enter**. The MS-DOS command prompt window opens.
 14. From the command prompt, navigate to the `C:\profile\mpio` directory.

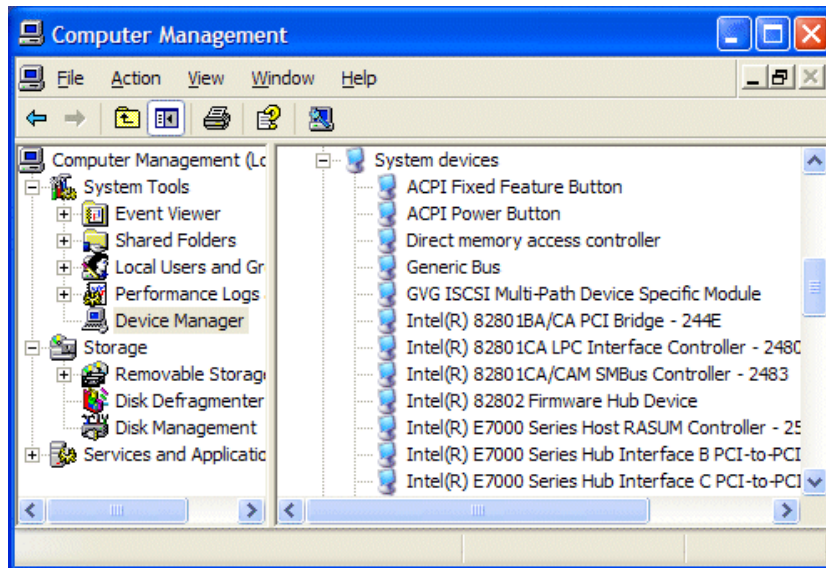
15. Type the following at the command prompt:

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

16. Press **Enter**. The software is installed.

17. Restart the K2 client.

18. After restart, to verify that the software is installed, on the Windows desktop right-click **My Computer** and select **Manage**. The Computer Management window opens.



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.

Remote control protocols

This section provides information for using remote control protocols to operate K2 clients. 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 the K2 Summit Production Client”
- “Using VDCP protocol to control the K2 Summit Production Client”
- “Using BVW protocol to control the K2 Summit Production Client”
- “Special considerations for automation vendors”
- “RS-422 connections on the K2 Summit Production Client”
- “Security and protocol control”

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

Using AMP protocol to control the K2 Summit Production Client

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.

The AMP's socket interface uses IANA assigned port number 3811 for both TCP and UDP.

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. 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 Summit Production Client, 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 the K2 Summit Production Client

Video Disk Control Protocol (VDCP) commands are available via RS-422 serial ports.

The automation setting for preroll should be at least 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 Summit Production 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. 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. Refer to ["Add host names to AppCenter to enable streaming" on page 39](#).

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 the K2 Summit Production Client

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	Value	Comments
Disk Prerolls	10 frames	—
Frames to send Play early (Preroll Play)	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)	10 frames	
Disk Port Comm Timeout	60 frames	This is the minimum required by K2. Do not use the Harris default value, which is 10.
Back To Back Rec	Unchecked	K2 does not support this feature.

RS-422 connections on the K2 Summit Production Client

You can control the K2 Summit Production Client 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 K2 Summit Production Client 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 **B**

Specifications

AC power specification

The K2 Summit Production Client AC power 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



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

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
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

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.

Electrical specifications

The following sections describe the electrical specifications:

Serial Digital Video (SDI)

Parameter	Specification
Video Standard	SD: 525 Line or 625 Line component HD: 720p or 1080i
Number of Inputs	1 per channel
Number of Outputs	2 per channel
Data format	Conforms to SMPTE 259M (SD) and 292M (HD)
Number of bits	10bits
Embedded Audio Input	SD data format conforms to SMPTE 259M (48kHz, 20bits) HD data format conforms to SMPTE 299. 48 kHz (locked to video) and 16- or 24- bit PCM Compatible with AC-3 and Dolby-E
Embedded Audio Output	Output data format is 48 kHz 24-bit User can disable embedded audio on SDI output
Connector	BNC, 75 ohm, No loop-through
nominal Amplitude	800mV peak-to-peak terminated
DC Offset	0 ±0.5V
Rise and Fall Times	SD: 400 - 1500ps; measured at the 20% and 80% amplitude points HD: <270ps
Jitter	<0.2UI peak-to-peak
Max Cable Length	SD 300 meters HD 125 meters
Return Loss	≥15db, 5Mhz to 1.485Ghz

Genlock Reference

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	≥36 dB to 6MHz
Tri-level sync	Not supported

System Timing

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 ^b	The video, AES, and LTC inputs pass to the output connectors as loop through.

^a. All delay values shown are relative to Black Reference.

^b. Also refer to “Loop through and E to E” in the [“Loop through, E to E, and feeds”](#) on page 19.

AES/EBU Digital Audio

Parameter	Specification
Standard	AES3
Audio Inputs	4 Channels per video input/output Shar 50 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.

Appendix B Specifications

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

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

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).

Characteristic	Description
Number of Inputs/Outputs	1 per channel
Connector type	Female DB9 pin

GPI I/O specifications

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

Topics include:

- “Video codec description – K2 Summit Production Client”
- “Playout of multiple formats”
- “VBI/Ancillary/data track specifications”
- “Internationalization”
- “Video network performance”
- “Supported file input/output formats on K2 Summit Production Client and K2 SAN”
- “Media file system performance on K2 Summit Production Client and K2 SAN”
- “Live Play mode specifications”
- “Protocols supported”
- “Transfer compatibility with K2 Summit Production Client”
- “Control Point PC system requirements”

Video codec description – K2 Summit Production Client

Format	Other
DVCAM (720x480/576)	Conforms to IEC 61834
DVCPRO25 (720x480/576)	Conforms to SMPTE 314M
DVCPRO50 (720x487.5/585)	Conforms to SMPTE 314M
DVCPRO100 ^a (960x720p, 1280x1080i59.94, 1440x1080i50)	Conforms to SMPTE 370M

^a. Requires XPD (HD) license.

Playout of multiple formats

The K2 Summit Production Client automatically handles material of various types and formats as specified in the following sections:

Playout on K2 Summit Production Client

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 table “[Video codec description – K2 Summit Production Client](#)” earlier in this section for a list of the supported formats

On channels with the XPD (HD) license, for similar frame rates (25/50 fps or 29.97/59.95 fps), SD material transferred or recorded into the K2 Summit Production Client 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 “[Aspect ratio conversions on HD K2 client models](#)” on page 1.

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

25/50 fps conversions on HD K2 client models

The following specifications apply to the HD-00 K2 Media Client and to K2 Summit Production Client channels with the XPD (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
	1080i at 25 fps	Down-convert HD to SD	No conversion	Cross-convert from 1080i to 720p
Source HD formats	720p at 50 fps	Down-convert HD to SD	Cross-convert from 720p to 1080i	No conversion


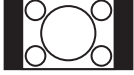


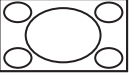
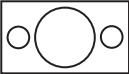




29.97/59.95 fps conversions on HD K2 client models

The following specifications apply to the HD-00 K2 Media Client and to K2 Summit Production Client channels with the XPD (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
	1080i at 29.97 fps	Down-convert HD to SD	No conversion	Convert HD to HD
Source HD formats	720p at 59.94 fps	Down-convert HD to SD	Convert HD to HD	No conversion

Aspect ratio conversions on HD K2 client models

The following specifications apply to the HD-00 K2 Media Client and to K2 Summit Production Client channels with the XPD (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	

VBI/Ancillary/data track specifications

This section contains the following topics:

- [“Definitions”](#)
- [“Data track support on K2 Summit Production Client HD channels”](#)
- [“Subtitling system support”](#)
- [“Data compatibility between K2 Summit Production Client and PVS models”](#)

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.

Data track support on K2 Summit Production Client HD channels

On K2 Summit Production Client channels with the XPD (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.

Video format	Data	Supported as follows:
DVCPRO100	Ancillary timecode	<p>For record, selectable to use VITC or LTC ancillary timecode as timecode source.</p> <p>For playout, selectable to insert recorded timecode track as ancillary data VITC or LTC timecode packets.</p> <p>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.</p> <p>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.</p>

Subtitling system support

An API is provided for access to subtitling data, allowing Closed Captioning and Teletext systems to produce timecode correlated subtitles for an existing K2 clip.

Data compatibility between K2 Summit Production Client and PVS models

When material is transferred between a PVS Profile XP Media Platform and a K2 Summit Production Client, data is supported as follows:

Source device	Source format	Source data	Destination device	Data support: SD Playout	Data support: HD Playout
PVS	DVCPRO25, DVCPRO50	Closed captioning	K2 Summit Client	Yes	No
		Ancillary data	K2 Summit Client	No	No
	DVCPRO50	Compressed VBI	K2 Summit Client	Yes	No
K2 Summit Client	DVCPRO25, DVCPRO50	Any supported on K2 Summit Client	PVS	Yes	NA
	DVCPRO100	Any supported on K2 Summit Client	PVS	NA	NA

Internationalization

When you enable internationalization on a K2 Summit Production Client, you can name your media assets in a local language. The K2 Summit Production Client supports the local language name as specified in the following table:

System	Internationalization support
Media database	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 Summit Production Client applications	<ul style="list-style-type: none"> Movie assets are described in Unicode. Application user interfaces are Unicode compliant.
Protocols	Refer to Appendix A, Remote control protocols, in the K2 Media Client System Guide.
FTP transfers	Refer to “FTP internationalization” in the K2 Media Client System Guide.

Video network performance

K2 systems support streaming transfers to and from K2 Summit Production Clients, K2 Media Clients, K2 SANs, M-Series iVDRs, 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 client	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	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 Production Client and K2 SAN

The 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		FTP stream		Other information
			Import	Export	Import	Export	
GXF	DVCPRO25 DVCPRO50 DVCPRO100 DVCAM	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. See “Transfer compatibility with K2 Summit Production Client” on page 1.
MXF	DVCPRO25 DVCPRO50 DVCPRO100 DVCAM	48 kHz, 16 bit, or 24 bit PCM, Dolby-E, or AC-3	Yes	Yes	Yes	Yes	MXF OP 1A. Standard Definition and High Definition supported.
AVI	DVCPRO25 DVCPRO50 DVCPRO100 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.
QuickTime	DVCPRO25 DVCPRO50 DVCPRO100 DVCAM	48 kHz, 16 bit, or 24 bit PCM	Yes	Yes	No	No	Audio tracks handled as stereo pairs on export
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.

Media file system performance on K2 Summit Production Client and K2 SAN

NOTE: For performance specifications on Live Play, see [“Live Play mode specifications”](#)

Parameter	Internal Storage Specification	Shared Storage Specification
Maximum number of clips ^a	20,000	50,000
Minimum delay between start record and start playout when record and play is on the same K2 Summit Production Client.	6 seconds	6 seconds ^b
Minimum delay between start record and start playout when record and play is on different K2 Summit Production Clients	NA	8 seconds ¹ .

Parameter	Internal Storage Specification	Shared Storage Specification
Maximum length continuous record	24 hours	24 hours

- 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.
- b. Qualified at up to 48 channels. Performance with larger systems is not tested.

Live Play mode specifications

Live Play mode is available only on the K2 Summit Production Client with the AppCenter Pro license. When using Live Play mode, specifications are as follows:

Parameter	Internal Storage Specification	Shared Storage Specification
Minimum delay between start record and start playout when record and play is on the same K2 Summit Production Client.	Less than 0.5 seconds	Less than 0.5 seconds
Maximum length continuous record	24 hours	24 hours

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 of media with mixed format 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.

Transfer compatibility with K2 Summit Production Client

When transferring material between a K2 Summit Production Client and other Grass Valley products, you must consider the specifications of the different products. The following table illustrates some of these considerations:

Source device	Destination device	Material transferred	Compatibility
K2 Summit Production Client	K2 Media Client, Turbo iDDR, M-Series iVDR, Profile XP Media Platform	DVCPRO25, DVCPRO50	Playout supported.
		DVCPRO100	Not supported
K2 Media Client, Turbo iDDR, M-Series iVDR, Profile XP Media Platform	K2 Summit Production Client	DVCPRO25, DVCPRO50	Playout supported.
		MPEG	Not supported

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 <i>msxml4sp2</i> file on the K2 System Software CD.
Quicktime	Version 7 or higher
Acrobat Reader	Version 8 or higher

Find software at Internet locations such as the following:

- <http://msdn.microsoft.com/en-us/netframework/default.aspx>
- <http://java.sun.com/javase/downloads/index.jsp>
- <http://www.microsoft.com/downloads/details.aspx?FamilyId=3144B72B-B4F2-46DA-B4B6-C5D7485F2B42&displaylang=en>
- <http://www.apple.com/quicktime/download/>
- <http://get.adobe.com/reader/>

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

Connector Pinouts

This appendix contains the following topics:

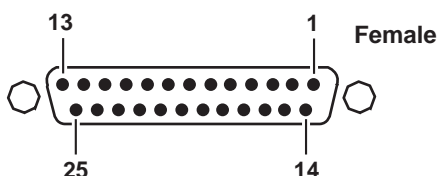
- [“K2 Summit Production Client connector pinouts”](#)
- [“K2 Media Client connector pinouts”](#)
- [“K2 Media Server connector pinouts”](#)

K2 Summit Production Client connector pinouts

The following sections describe K2 Summit Production Client rear panel connector pinouts.

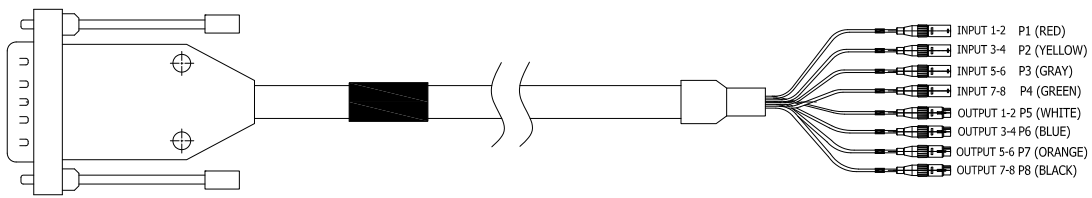
AES Audio

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

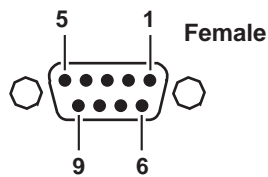
The optional audio cable has connections as follows:



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:

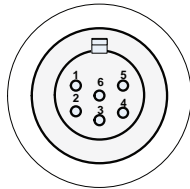


Pin #	Signal	Description
1	GND	Frame Ground
2	-TXD	Differential Transmit Data (low)
3	+RXD	Differential Receive Data (high)
4	GND	Transmit Signal Common
5	NC	Spare
6	GND	Receive Signal Common
7	+TXD	Differential Transmit Data (high)
8	-RXD	Differential Receive Data (low)
9	GND	Signal Ground

LTC connectors pinouts

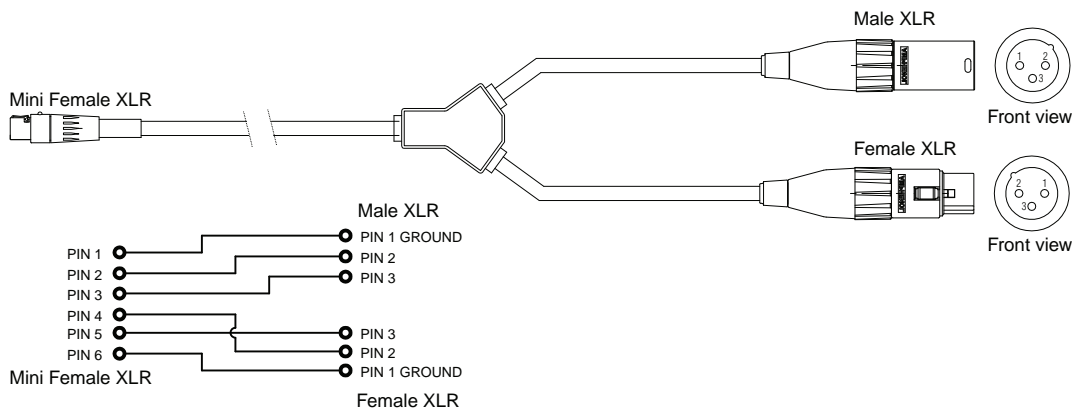
The K2 Summit Production Client LTC panel connector provides balanced linear timecode input and output connections. The interface conforms to SMTPE 12M Linear Timecode.

On the K2 Summit Production Client there is one 6 pin Switchcraft TRA6M Mini-XLR male connector for each channel. Pinouts are as follows:

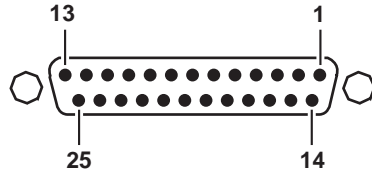


Pin #	Signal	Description
1	IN_P<0>	
2	IN_N<0>	
3	GND	Frame Ground
4	OUT_P<0>	
5	OUT_N<0>	
6	GND	Frame Ground

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.

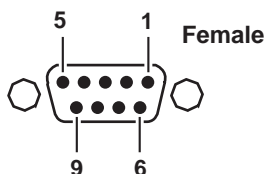
RS-422 connector pinouts

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.

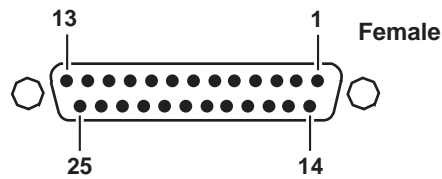
The RS-422 interface conforms to ANSI/SMPTE 207M-1997 standard (SMPTE 422).

Pinouts for the individual DB9 connectors are as follows:



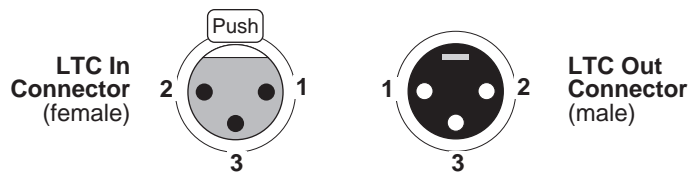
Pin #	Signal	Description
1	GND	Frame Ground
2	-TXD	Differential Transmit Data (low)
3	+RXD	Differential Receive Data (high)
4	GND	Transmit Signal Common
5	NC	Spare
6	GND	Receive Signal Common
7	+TXD	Differential Transmit Data (high)
8	-RXD	Differential Receive Data (low)
9	GND	Signal Ground

Pinouts for the DB25 connector on the PCI RS-422 board are as follows:



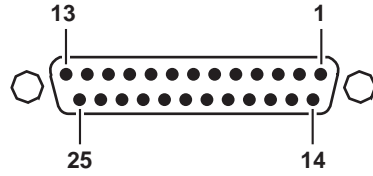
Pin #	Signal	Description
1-6	Not Used	
7	GND	
8-14	Not Used	
15	+RXD	
16	Not Used	
17	-RXD	
18	Not Used	
19	+TXD	
20-24	Not Used	
25	-TXD	

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

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

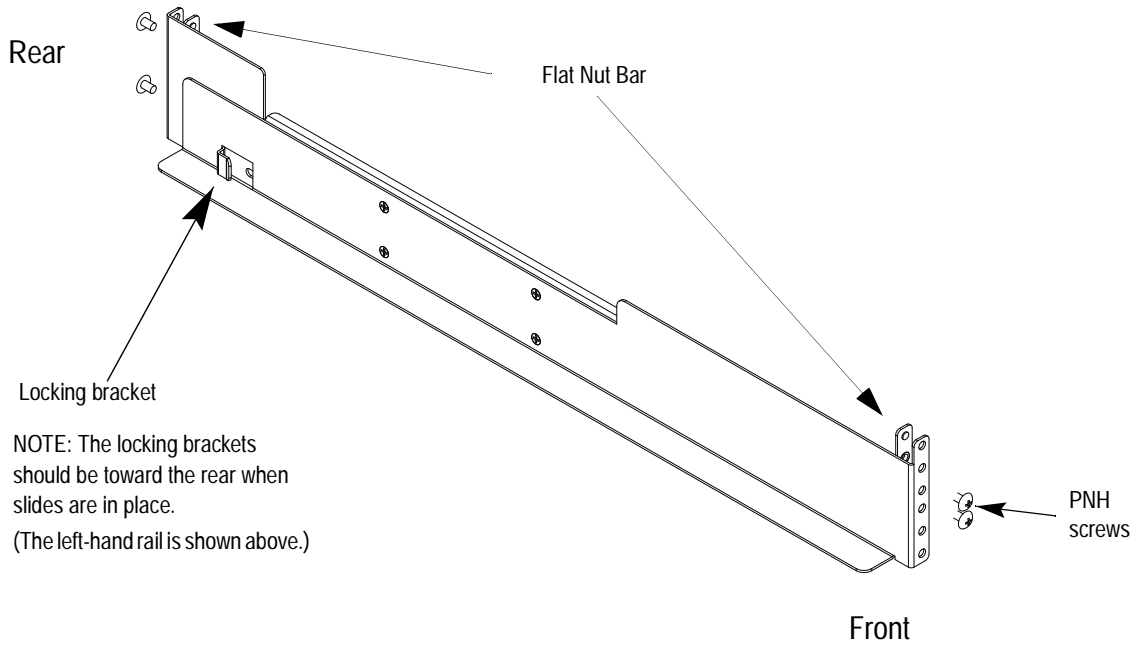
When planning the placement of equipment in your equipment rack, bear in mind the following:

- 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 114](#) 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.

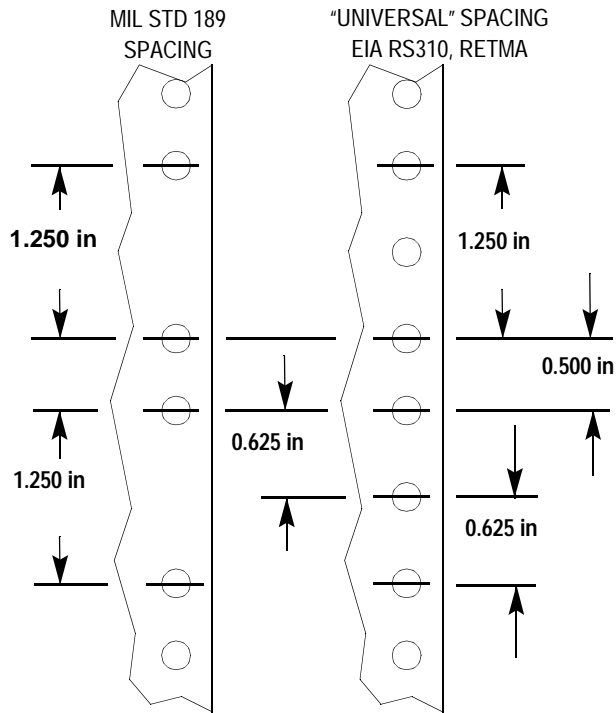
Rack mount hardware shipped with the K2 system

Your K2 system rack mount kit comes with rack mounting hardware as shown.

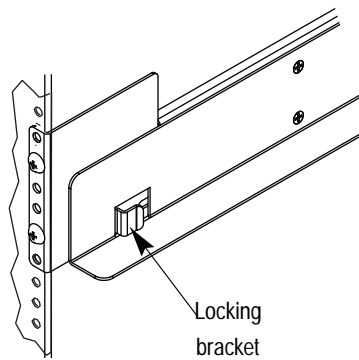
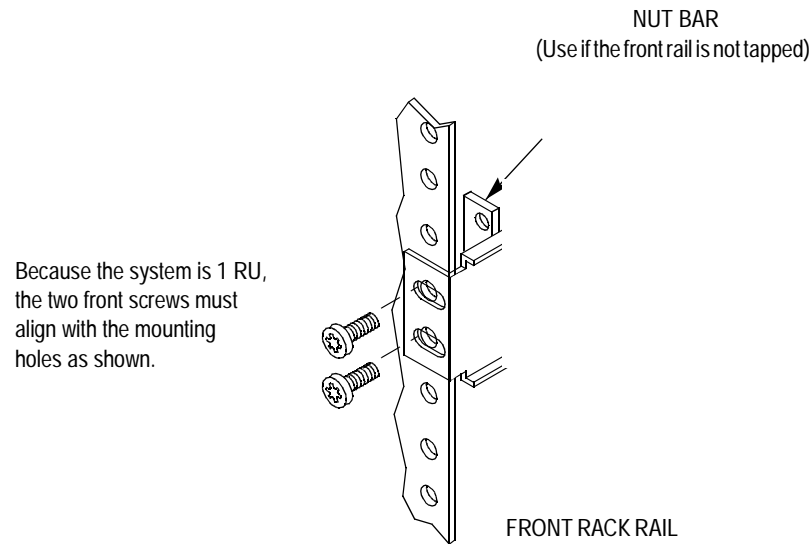


Mounting the Rack Slides

Choose the proper set of rail mounting holes on the rack. Notice that the hole spacing can vary with the rack type. When mounting the slides in racks with EIA spacing, make sure that the slides are attached to the 0.5-inch spaced holes.



Front and rear rack rail mounting hardware is provided with the rack mount kit. Mount the rails using the enclosed hardware. Make sure the stationary sections are horizontally aligned and are level, as well as parallel to each other.



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 36

A

AC power, specification 114

adapter

network loopback 34

administrator

mapping NetCentral administrators with
K2 93

password 87

AES audio connector K2 Summit Client

pinout 140

AES/EBU audio

specification 117

AMP

channel designations 106

protocol settings 106

transfers 106

ancillary data specifications 126

AppCenter

channel access security 91

user access 87

application system

architecture 18

software 18

aspect ratio

HD-00 125

SD-00 123

audio

digital audio specification 117

Dolby 123

auto logon 97

AVI, supported formats 129

B

backup, strategies 80

binding LUNs 71

bins, configuring security 87

board

XLR 18

BVW

protocol settings 109

C

cable

redundant server heartbeat 147

requirements, Ethernet connections 31

channels

security 91

cleaning unreferenced files and movies 75

clips, maximum number 129

closed captioning 126

commands, FTP 47

configuration

auto logon 97

channel access security 91

customizing 23

K2 Summit Production Client security 84

loading defaults 24

media access security for K2 bins 87

opening 23

protocol security 90

sample K2 Summit Production Client hosts
file 38

saving and restoring 23

configuration file 26

Configuration Manager, description 23

connections

GPI 59

RS-422 59, 111

connector pinouts

GPI 146

GPI, K2 Summit Production Client 143

LTC connector 142, 145

RS-422 147

RS-422, K2 Media Client 144

RS-422, K2 Summit Client 141

continuous record

maximum length 129

Control Point PC

installing software 78

screen resolution problem with
NetCentral 132

software components 78

system requirements 132

where software is installed 77

controller

microcode, checking 67

obtaining logs 69

corrupt movies 41

D

database, description 18

delay, minimum 129

direct-connect storage

 K2 client 61, 99

disk

 checking disk mode pages 69

 disabling 69

 downloading firmware PFR 700 75

 identifying 68

 rebuilding forcibly 70

disk controller board

 description 61

drive

 disabling 69

 numbering RAIDs 22

 striping media 61

DV, creating DV-format clips 58

E

electrical specification 115

environmental specification 114

Ethernet

 cable requirements 31

exporting, supported formats 129

external storage

 specification, media file system 129

F

features

 external storage 14

 internal storage 14

 K2 Summit Production Client 14

file system, description 18

files, cleaning unreferenced 75

firewall policies 95

formats, supported 129

fps conversions on HD-00 models 123

front panel

 enabling and disabling USB ports 96

 indicators 16

FTP

 access and configuration 42

 accessing with Internet Explorer 44

 automated access 43

 clips with gaps 41

 internationalization 43

 K2 FTP server 41

 specifying language 44

 streaming from a K2 SAN 37

 streaming ports 36

 streaming transfer network requirements 36

 supported commands 47

 using for file transfer 41

G

genlock, specification 116

GPI

 connector pinout 146

 connector pinout, K2 Summit Production
 Client 143

 electrical specification 120

 inputs 59

GXF

 description 45

 supported formats 129

H

hardware

 rack mount 150

Harris settings, protocol 110

HD-00

 aspect ratio conversions 125

 fps conversions 123

host name

 adding 39

 problems when changing 34

hosts file

 editing 37

 K2 Summit Production Client sample 38

 using _he0 36

HotBins, about 49

HTTP 21

I

identify

 disks 68

importing, supported formats 129

indicators, front panel 16

installing

 Control Point software 78

internal storage

- changing RAID types 73
- K2 Summit Production Client 61
- internationalization
 - AMP 106
 - FTP 43
 - K2 Summit Production Client 128
 - VDCP 108
- Internet Explorer, FTP access 44

K

- K2 client
 - administrator 87
 - auto logon 97
 - changing RAID types 73
 - connecting remotely 27
 - connector pinouts 140
 - direct-connect storage 99
 - direct-connect storage system, description 61
 - installing software 80
 - pre-installed software 80
 - security considerations with NetCentral 93
 - software components 78
 - user 87
 - user accounts 87
 - virus scanning 95
 - where software is installed 77
- K2 FTP
 - interface 42
 - internationalization 43
 - security 89
 - specifying language 44
 - supported commands 47
- K2 FTP server 41
 - configuration with M-Series iVDR 43
 - configuration with Profile XP 43
- K2 Media Client
 - connector pinouts 144
 - FTP configuration 43
 - modes, online and offline 64
 - network loopback adapter 34
 - returning to online mode 76
- K2 Media Server
 - connecting remotely 27
 - connector pinouts 147
 - security considerations with NetCentral 93
 - software components 78
 - where software is installed 77
- K2 SAN

- security 90
- K2 Summit Production Client
 - configuring security 84
 - description 13
 - features 14
 - FTP configuration 43
 - identifying specific client-types 15
 - internal storage system, description 61
 - internationalization 128
 - licensing 83
 - network and firewall policies 95
 - network loopback adapter 34
 - playout formats 123
 - rack mounting 149
 - sample configuration and hosts file 38
 - streaming transfers 128
 - supported transfer formats 129
 - system overview 18
 - system tools, using 23
- K2 System Configuration 24
- K2admin 87
- K2Config, see K2 System Configuration
- K2user 87

L

- language
 - AMP 106
 - K2 Summit Production Client support 128
 - restrictions in Internet Explorer 45
 - specifying in K2 FTP 44
 - VDCP 108
- language and regional settings 97
- licensing
 - description 83
 - options 83
- logs, obtaining controller 69
- loop through
 - description 19
 - SD models 20
- loopback adapter
 - network IP address 34
- LTC
 - connector pinouts 145
 - input/output 119
 - K2 Summit Client 142
- LUN
 - binding 71
 - unbinding 70

M

making new media file system 73, 74
 mechanical specifications 115
 media
 access security for AppCenter 89
 access security for FTP 89
 access security for K2 bins, configuration 87
 access security for K2 SANs 90
 access security for protocols 90
 changing RAID types 73
 control and processing 18
 limitations with complex types 41
 making new media file system 73, 74
 naming disk drive 67
 striped data 61
 transferring mixed formats 42
 media file system
 checking 74
 description 18
 performance 129
 software location
 MIB 133
 microcode, checking controller 67
 Microsoft Windows
 see Windows
 minimum between start of record and playout 129
 mode
 checking disk mode pages 69
 online and offline 64
 online, returning K2 Media Client 76
 movie
 cleaning unreferenced 75
 corrupt 41
 MPEG, supported formats 129
 M-Series iVDR
 FTP configuration with K2 FTP server 43
 transfer compatibility 131
 transferring to K2 Summit Production Client 128
 MXF
 implemented in K2 45
 supported formats 129

N

NetCentral 27
 mapping administrators with K2 93
 screen resolution problem with Control Point PC 132

security considerations 93
 software location

network
 100BaseT, setup 33
 adding host names
 FTP/streaming transfer requirements 36
 host file, setup 37
 modifying settings 34
 policies 95
 video performance 128

O

offline mode, description 64
 online mode
 description 64
 returning K2 Media Client 76

P

passwords 87
 permissions
 AppCenter 89
 channel access 91
 FTP 89
 K2 bins 87
 K2 SANs 90
 protocols 90
 PFR700, downloading disk firmware 75
 pinouts
 AES audio connector, K2 Summit Client 140
 K2 Media Client 144
 K2 Summit Client 142
 RS-422 141
 playout
 minimum delay between start of record 129
 ports
 enabling and disabling USB 96
 used by K2 services 21
 Profile XP
 FTP configuration with K2 FTP server 43
 transfer compatibility 131
 transferring to K2 Summit Production Client 128
 protection, network and firewall 95
 protocol
 AMP channel designations 106
 associating with a user account 91
 Harris settings 110
 remote control, transferring 42

security 91

Q

QuickTime

reference file 58
supported formats 129

R

rack mounting 149

adjusting 153
hardware 150
rails 152
slides 151

RAID

binding LUNs 71
changing type 73
checking disk mode pages 69
disabling disks 69
drive numbering 22
drives, description 61
identifying disks 68
rebuilding disks forcibly 70
unbinding LUNs 70

real time system

components 18
description 19

rear panel

connector pinouts 140, 144
enabling and disabling USB ports 96
GPI 59
RS-422 connections 59, 111
view 17

rebuilding disks forcibly 70

record, maximum length of continuous 129

recovery, strategies 80

redundant server heartbeat cable 147

reference file, QuickTime 58

regional and language settings 97

remote control protocols

controlling with RS-422 59, 111
transferring 42

remote desktop 27

requirements

Control Point PC system 132
FTP/streaming 36

restrictions

AppCenter 89
channel access 91

FTP 89

K2 bins 87

K2 SANs 90

NetCentral and K2 security considerations 93
protocols 90

RS-422

connector pinout 144, 147
connector pinout, K2 Summit Client 141
rear panel connections 59, 111
specification 119
USB port 96

S

SCSI board

description 61

SD-00

aspect ratio formats 123
loop through 20
video codec specification 122

SDA-00

video codec specification 122

SDI 115

security

AppCenter operations 89

configuring

channel access 91
FTP security 89
K2 bins 87
K2 SANs security 90
protocol security 90

mapping NetCentral administrators with
K2 93

Microsoft Windows updates 94

NetCentral 93

overview 84

passwords 87

user accounts 87

SNFS, see media file system

specification

AC power 114
AES/EBU 117
electrical 115
environmental 114
external storage, media file system 129
genlock 116
GPI 120
LTC 119
mechanical 115

- media file system performance 129
- operational 121
- RS-422 119
- SDA-00 and SDA-00 video codec 122
- system timing 117
- transferring 128
- VBI/ancillary data 126
- VITC 119
- storage system, description 19
- Storage Utility 25, 26
 - checking subsystem status 67
 - description 64
 - opening through AppCenter 64
 - operation not supported 76
 - overview 66
- streaming
 - see transferring
- stripe
 - group 61
 - media 61
- subsystem status, checking with Storage Utility 67
- subtitles 126
- synchronizing the media file system 75
- system timing 117
- System Tools, K2 Summit Production Client 23

T

- third-party FTP access 43
- transferring
 - between a K2 and a non-K2 system 42
 - compatibility considerations 131
 - K2 FTP interface 42
 - mechanically or automatically 42
 - M-Series iVDRs 128
 - remote control protocols 42
 - specification 128
 - supported formats 129
 - using Internet Explorer 44
 - using third-parties 43
- transfers
 - VDCP 107
- Turbo iDDR
 - transfer compatibility 131

U

- unbinding LUNs 70
- Unicode, UTF-8

- AMP 106
- VDCP 108
- USB, enabling and disabling ports 96
- user
 - accounts, passwords 87
 - associating protocols with an account 91
 - names 87

V

- V drive 19, 61
- VBI
 - ancillary data specifications 126
 - compression 126
 - Line 21 data services 126
- VDCP
 - Harris settings 110
 - protocol settings 107
 - transfers 107
- view
 - front panel 16
 - rear panel 17
- Virus scanning policies 95
- VITC input/output 119

W

- WAV, supported formats 129
- web site, for Thomson Grass Valley 10
- Windows
 - high priority updates
 - Remote Desktop, using 27
 - system description 18

X

- XLR board 18
- XML 23
- XML import capture service 54