grass valley

Aurora Edit and LD

FAST-TURN PRODUCTION TOOLS

Installation Manual

Software Version 7.0

www.grassvalley.com

071-8501-04
April 2010

Affiliate with the N.V. KEMA in The Netherlands

CERTIFICATE

Certificate Number: 510040.001
The Quality System of:

Thomson Inc, and its worldwide Grass Valley division affiliates DBA GRASS VALLEY

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

15655 SW Greystone Ct.
Beaverton, OR 97006
United States

10 Presidential Way
Suite 300
Woburn, MA 01801
United States

Kapittelweg 10
4827 HG Breda
The Nederlands

7140 Baymeadows Way
Ste 101
Jacksonville, FL 32256
United States

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

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

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

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

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

Spinnereistrasse 5
CH-5300 Turgi
Switzerland

Brunnenweg 9
D-64331 Weiterstadt
Germany

Carl-Benz-Strasse 6-8
67105 Schifferstadt
Germany

Including its implementation, meets the requirements of the standard:

ISO 9001:2008

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

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

H. Pierre Sallé
President
KEMA-Registered Quality

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

Experience you can trust.

KEMA-Registered Quality, Inc.
4377 County Line Road
Chalfont, PA 18914
Ph: (215)997-4519
Fax: (215)997-3809

Accredited By:
ANAB

CRT 001 073004

grass valley

Aurora Edit and LD

FAST-TURN PRODUCTION TOOLS

Installation Manual

Software Version 7.0

www.grassvalley.com

071-8501-04
April 2010

Copyright

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

Revision Status

Rev Date	Description
March 28, 2005	Initial release, part number 071-8294-00
Nov. 21, 2005	Release 071-8294-01 for Software Version 5.5
June 30, 2006	Release 071-8501-00 for Software Version 6.0
October 26, 2006	Release 071-8501-01 for Software Version 6.0a
Sept. 20, 2007	Release 071-8501-02 for Software Version 6.3
Nov. 25, 2008	Release 071-8501-03 for Software Version 6.5
April 15, 2010	Release 071-8501-04 for Software Version 7.0

Contents

Grass Valley Product Support

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

Web Technical Support

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

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

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

Telephone Support

Use the following information to contact Product Support by phone.

International Support Centers

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

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

Authorized Local Support Representative

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

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

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

Region	County	Telephone
Asia	China	+86 10 5883 7575
	Hong Kong, Taiwan, Korea, Macau	+852 2531 3058
	Japan	+81 3 6848 5561
	Southeast Asia - Malaysia	+603 7492 3303
	Southeast Asia - Singapore	+65 6379 1313

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

Chapter 1

Preparing for installation

This section contains the following topics:

- *Aurora Edit installation checklists*

Aurora Edit installation checklists

Use the following sequence of checklists to guide the overall task flow of installing and commissioning an Aurora Edit system.

Optional equipment checklist

Use items in this checklist as appropriate for the optional equipment you are installing in your Aurora Edit workstation.

	Task	Instructions	Comment
□	Install video board and breakout box		
□	Connect audio/video cables to breakout box		
□	Connect audio mixer		
□	Connect video tape recorder		
□	Connect jog/shuttle controller		
□	Connect motorized fader or effects controller		
□	Assign Com Port (Windows)		
□	Assign Com Port (Aurora Edit)		
□	Next: Network setup and implementation checklist		

Network setup and implementation checklist

	Task	Instructions	Comment
□	If you have not already done so, add your storage, either K2 SAN or NAS, to the system description		Modify your existing system description.
□	If you have not already done so, configure your storage, either K2 SAN or NAS, and verify that it is operational.	Refer to the *K2 SAN Installation and Service Manual*. For NAS, follow procedures for K2 Nearline SAN.	—

	Task	Instructions	Comment
□	If you have Aurora Edit LD systems on the corporate LAN, add the corporate LAN to system description		Modify your existing system description.
□	Add a group for your Edit devices to the system description		—
□	Add a placeholder device to the system description for each of your actual Edit devices		—
□	Configure the names of the placeholder devices		—
□	Configure the network interfaces of the placeholder devices		Specify IP address ranges and other network details
□	Install SiteConfig support on devices if necessary.		
□	Set credentials on devices if necessary.		
□	Discover your Edit devices		—
□	Assign each discovered device to its placeholder device		—
□	For each discovered and assigned device, edit each network interface. Specify network settings and apply them to the device.		If a device connects to multiple networks, set the control network interface IP address first. Also set the hostname.
□	If you have Aurora Edit LD systems on the corporate LAN, add them to the system description and set credentials.		
□	If not already set correctly, set the hostname of discovered devices		Make sure the device name is correct, then make the hostname the same as the device name.
□	Ping each Edit device to test network communication		—

	Task	Instructions	Comment
□	Generate host table information and distribute to hosts files on each device and on the control point PC		Make sure you have completed network configuration of all network interfaces across all devices to ensure complete and valid host table information. You can use SiteConfig to copy hosts files to devices, or you can manage hosts files yourself.
□	Next: Software update checklist		

Software update checklist

	Task	Instructions	Comment
□	Add/remove software roles	—	Make sure software roles match the software that should be installed on each device, according to your system design.
□	Add Edit devices to the deployment group	—	
□	Place software on control point PC	—	
□	Create a deployment group		Procure the correct version of software installation files and prerequisite files.
□	Check software on devices		Refer to the release notes for your product.
□	Add software to deployment group		
□	Set deployment options		
□	Upgrade/install software to devices from control point PC		
□	If using Final Cut Pro with Aurora Edit, install and license K2-FCP-Connect.	*K2 FCP Connect Installation Manual*	These tasks are not supported by SiteConfig. Do them manually, at each local device.
□	Next: Configuration checklist		

Configuration checklist

	Task	Instructions	Comment
□	Set up media files for sharing		
□	Add video sources to Aurora Edit		
□	Set Options (Tools/Options)		
□	Configure Smartbins		
□	Configure Conform Server		
□	Design Aurora Security Schema		
□	If K2 FCP Connect is installed and licensed, configure Macintosh systems on K2 storage.	*K2 FCP Connect Installation Manual*	
□	If using K2 FCP Connect, configure Aurora Edit for using Final Cut Pro.		
□	Next:		

Chapter 2

Installing Aurora Edit Hardware

This section contains the following topics:

- *Aurora Edit Components*
- *Installing Optional Equipment*

Aurora Edit Components

The Aurora Edit application is part of the Aurora Suite of products that consists of several components that comprise a total digital news production system. All Aurora Edit applications run on the Aurora Edit platform. For a list of system specifications for customer-supplied hardware qualified for use with Aurora Edit, refer to the Version Compatibility section. This information is also included in the *Aurora Edit Release Notes* on the CD-ROM where the most recent information is always included.

Refer to the *Aurora Edit Release Notes* for the most updated information for the following:

- System Specifications for qualified laptops, desktop computers, and workstations
- HP Workstation Board Assignments
- Compatible DSM Components
- Compatible Grass Valley Products
- Compatible Third Party Products

Workstation Components

The Aurora Edit application is provided on a CD-ROM and installed on a customer-supplied laptop, desktop computer, or workstation depending on the editing application needed. When you order your system, you will choose the components needed for your facility based on your system design.

NOTE: For a list of supported hardware configurations, see the latest Aurora Edit Release Notes included on the CD and online for the most up-to-date information on system specifications and software updates.

System components can include:

- Keyboard and Mouse

  A keyboard and mouse can be used to control the Aurora Edit and Aurora Edit LD functions. The keyboard and mouse are customer-supplied. Included with each Aurora Edit application CD-ROM is a set of keyboard stickers that are applied to the standard keyboard to make the key strokes compatible with the current Aurora Edit software version. A customer-supplied laptop computer can also use the keyboard stickers in the same manner to control Aurora Edit or Aurora Edit LD.

- Monitor

  Aurora Edit workstations support either one or two monitors. In a dual-monitor configuration, one monitor is typically used to display bins while the other displays other Aurora Edit application components.

- Breakout Box (BOB)

Aurora Edit supports an option that includes an I/O board that connects to a rackmountable Breakout Box (BOB) to provide multiple analog and SDI video and audio inputs and outputs.

- External Control Devices

  Standard USB jog/shuttle controllers are acceptable. For an officially qualified list of devices used on Aurora Edit check with your sales representative when you plan your system design or contact customer support.

Storage Options

The Aurora Edit system provides three options for storing files:

Local (standalone) on a workstation, computer, or laptop not tied to a shared strorage solution.

NOTE: In Local mode, no DSM or Smartbins are possible, as well as other network-required functionality.

NAS (Network Attached Storage) network, a shared storage network consisting of:

- A NAS Server to manage the network file systems
- RAID arrays to provide media storage
- Database System Manager (DSM) to host the News database and (optionally) the SmartBins Service

NAS networks support Gigabit Ethernet networking.

K2, a shared storage network, consisting of these components:

- A K2 Media Server to manage network file systems
- RAID arrays to provide media storage
- Gigabit Ethernet Switches to connect the K2 Media Server to Aurora Edit clients
- A Control Point PC to K2 Configuration application
- A Database System Manager (DSM) to host the News database and (optionally) the SmartBins Service

K2 networks use Gigabit Ethernet networking.

Installing Optional Equipment

Aurora Edit allows you to connect a variety of specialized optional equipment to enhance your editing capabilities. This includes an optional AJA Video Breakout Box (BOB) and video board. Other interfaces include customer-supplied external controllers such as a jog shuttle, motorized fader, and effects controllers.

Optional Breakout Box and Video I/O Board

Qualified Aurora Edit workstations can be equipped with an optional rack-mountable AJA Video Breakout Box (BOB) with an I/O video board that installs in a slot in the Aurora workstation.

This option provides additional high-quality analog and digital audio and analog, component, and SDI video sources, in addition to one HDMI (High Definition Multimedia Interface) input and one HDMI output. It allows interfacing to various external devices such as tape decks and cameras as well as HDMI sources. When the I/O Video board is installed in the workstation during initial installation, the necessary software components for this option will be installed when the Aurora Edit software is deployed using the SiteConfig application.

Installing the Video I/O Board and Connecting to the Breakout Box (BOB)

Install the video I/O board in the workstation, then connect it to the rear of the Breakout Box (BOB) as described below.

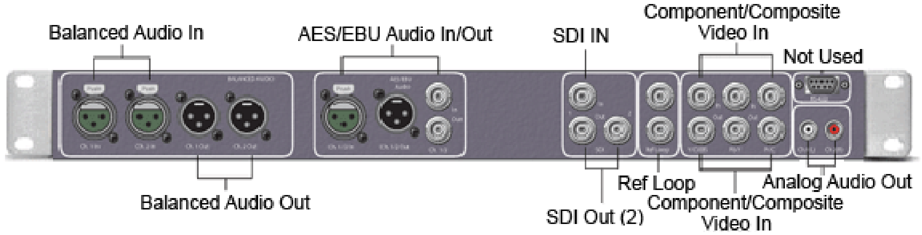
NOTE: The previous version Breakout Box (BOB) and video I/O board had three SDI BNC connectors and no HDMI connectors and had a differenct breakout cable. Cable it in the same manner by following the labeled cables.

1. Install the video I/O board in the correct workstation slot.
2. Connect the video board to the rear of the breakout box (BOB) using the two cables provided. One end of the cables attaches to the video board and the other to the back of the BOB. The cables included are listed below and labeled clearly for installation:
   a) Connect the 60-pin to 60-pin cable to the 60-pin connector on the video board installed in the workstation and J1 on the rear of the Breakout Box (BOB).
   b) Connect the breakout cable with two BNCs labeled SDI OUT to J5 and SDI IN to J4 on the BOB and in the same order (OUT, IN) to the video card, installed in the workstation, then connect the two HDMI connectors Iabeled HDMI OUT to J3 and HDMI IN to J2 on the BOB and in the same order (OUT, IN) to the video board in the workstation.

Connecting Cables to the Breakout Box

The following illustrations and table detail how to connect video and audio cables to the breakout box to interface external equipment to your Aurora Edit system.

The image below illustrates the previous version of the HDR Breakout Box (BOB) with three SDI connectors (one IN and two OUT) and no HDMI connectors. This BOB requires a specific video board and cable set as specified in the option model.



The image below shows the latest version AJA Breakout Box (BOB) that is identical to the older version except it now has two SDI connectors and two HDMI connectors. This BOB requires a specific video board and cable set as specified in the option model.

The table below gives cabling information from the AJA Breakout Box (BOB) to external devices.

NOTE: This table assumes VTRs are operating in playout to tape mode.

Input	From	To	Cable Type
Analog Audio (without mixer)	VTR Channel 1 output	BOB Balanced IN left channel	XLR-female to XLR-male
	VTR Channel 2 output	BOB Balanced IN right channel	XLR-female to XLR-male
	BOB Balanced Left Out	VTR Channel 1 input	XLR-male to XLR-female
	BOB Balanced Right Out	VTR Channel 2 input	XLR-male to XLR-female
	BOB Unbalanced Left Out	Left desktop speaker	RCA-male to XLR or 1/4" male
	BOB Unbalanced Right Out	Right desktop speaker	RCA-male to XLR or 1/4" male
Digtial Audio	VTR AES/EBU Channels 1&2 Output	BOB AES/EBU Channels 1&2 Input	XLR-male to XLR-male
	BOB AES/EBU Channels !&2 Output	VTR AES/EBU Channels 1&2 Input	XLR-male to XLR-female
	BOB Unbalanced Left Out	Left desktop speaker	RCA-male to XLR or 1/4" male
	BOB Unbalanced Right Out	Right desktop speaker	RCA-male to XLR or 1/4" male

Input	From	To	Cable Type
Video	VTR SDI Output	BOB SDI Input	Single BNC-BNC
	BOB SDI Output	VTR SDI Input	Single BNC-BNC
	VTR Composite Output	BOB Composite Input	Single BNC-BNC
	BOB Composite Output	VTR Composite Input	Single BNC-BNC
	VTR Component Output	BOB Component Input	Tri BNC-BNC harness
	BOB Component Output	VTR Component Input	Tri BNC-BNC harness
HDMI 1.3a	HDMI Device Output	BOB HDMI Input	HDMI Audio/Video cable
	BOB HDMI Output	HDMI Monitor	HDMI Audio/Video Cable

Controlling a Video Tape Recorder

Machine control of external devices such as VTRs/camcorders and other control devices is done through an RS-422 remote serial interface or a USB port. Check the specifications for your specific workstation for RS-422 connector requirements. In some cases, the workstation must have an optional RS-422 PCI card installed. You may also use the local RS-232 port on the workstation with an RS-422 adapter for tape deck serial control applications.

Once cabling is complete, the workstation port must be configured in the Aurora Edit application to control the external device. Also configure the port on the Controller card for DCE (controller).

NOTE: The serial interface to the Aurora system is made to a connection on the rear of the workstation. Do not use the Breakout Box (BOB) Machine Control connection.

Connecting External Controllers to Aurora Edit

Aurora Edit supports three types of external controllers: the Motorized Fader Controller, the Jog/Shuttle Controller, and the Effects Controller as described in the table below. Control connections for these devices are USB or RS-422 depending on the device. An optional PCI board with an RS-422 machine control port must be installed in the workstation for correct RS-422 control. Check the specifications for your workstation type in Appendix B, Workstation Slot Map, for slot installation location of the optional PCI RS-422 board.

Controller	Description
Jog Shuttle	Assists editing with a jog/shuttle wheel for convenient searching, buttons to minimize keyboard strokes, and a backlit LCD timecode display.
Motorized Fader	Assists audio mixing with four touch-sensitive, motorized faders, 16 channel switches, 4 function keys, and bank shift buttons.
Effects	Assists effects editing with a 3–axis joystick mechanism, five rotary encoders, and 10 switches.

Connecting a Jog/Shuttle Controller

Your workstation should be powered down for this task.

1. Plug the controller’s 9-pin connector into the RS-422 port on the optional PCI board on the back of the Aurora Edit workstation (COM4). The port should be set for DTE (Device).
2. Plug the controller’s power connector into a DC power adapter connection.
3. Verify that the following information appears on the controller’s display when it powers up:

   Grass Valley

   Aurora Edit

   Rev x.xx

4. Turn on your Aurora Edit workstation.

Connecting a Motorized Fader or Effects Controller

Your workstation should be powered down for this task.

1. Plug the controller’s USB connector into one of the two available USB ports on the back of your Aurora Edit workstation (usually COM5 for the Motorized Fader Controller and COM6 for the Effects Controller).
2. If you are connecting the Motorized Fader Controller, plug the controller’s power connector into a DC power adapter connection.

   The Effects Controller is powered via the USB cable.
3. Turn on your Aurora Edit workstation.
4. When the **New Hardware Wizard** appears, follow the directions on the screen.
5. When asked for the controller’s driver, insert the Aurora Edit CD and navigate to **\Drivers\JLC USB Drivers**.
6. Finish the new hardware installation.

Assigning a COM Port (Windows)

To verify that the COM port is set correctly in the Windows Device Manager:

1. Right-click on **My Computer** and select **Properties**.
2. Click the **Hardware** tab on the **System Properties** window and then click **Device Manager**.
3. Click the * symbol next to the Ports item.
4. Click on **JLCooper USB to Serial (COM#)** and select **Properties**.
5. Click the Port Settings tab on the Properties tab and click **Advanced**.
6. Select the correct **COM Port Number**.
7. Click **OK** to close the **Advanced** window, and again to close the **Properties** window.

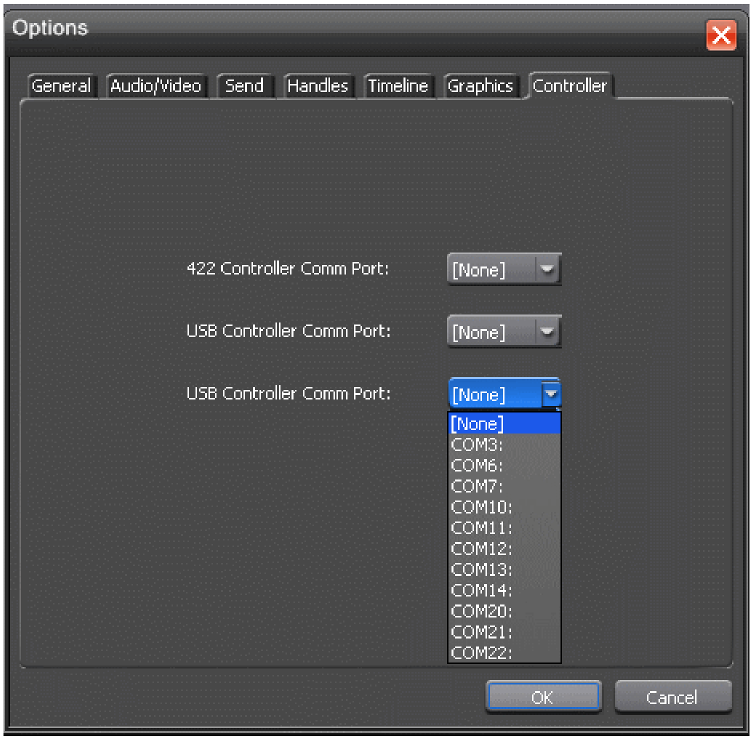
Assigning a COM Port (Aurora Edit)

To use any of the controllers, you need to assign a specific Aurora Edit COM port for the controller. Aurora Edit has pre-configured COM ports as follows:

COM Port		
1	GPIO	Aurora Playout GPIO
2		
3	RS-422	Video Tape Recorder (VTR)
4	RS-422	Jog/Shuttle Controller
5	USB	Motorized Fader Controller
6	USB	Effects Controller

To assign a COM port:

1. In the Aurora Edit application, choose the **Tools | Options | Controller** pulldown to bring up the Controller window.



422 Controller Comm Port: [None]

USB Controller Comm Port: [None]

USB Controller Comm Port: [None]

2. For the Jog/Shuttle Controller, select the correct COM port from the **422 Controller Comm Port** drop-down list; for the other controllers, select the correct COM port from the **USB Controller Comm Port** drop-down lists.

   The COM port needs to match the number of the USB port where you connected the controller.

3. Click **OK**.

You can now use the controller to control features on Aurora Edit.

Chapter 3

Configuring the network

This section contains the following topics:

Network setup and implementation checklist

	Task	Instructions	Comment
□	If you have not already done so, add your storage, either K2 SAN or NAS, to the system description		Modify your existing system description.
□	If you have not already done so, configure your storage, either K2 SAN or NAS, and verify that it is operational.	Refer to the *K2 SAN Installation and Service Manual*. For NAS, follow procedures for K2 Nearline SAN.	—
□	If you have Aurora Edit LD systems on the corporate LAN, add the corporate LAN to system description		Modify your existing system description.
□	Add a group for your Edit devices to the system description		—
□	Add a placeholder device to the system description for each of your actual Edit devices		—
□	Configure the names of the placeholder devices		—
□	Configure the network interfaces of the placeholder devices		Specify IP address ranges and other network details
□	Install SiteConfig support on devices if necessary.		
□	Set credentials on devices if necessary.		
□	Discover your Edit devices		—
□	Assign each discovered device to its placeholder device		—
□	For each discovered and assigned device, edit each network interface. Specify network settings and apply them to the device.		If a device connects to multiple networks, set the control network interface IP address first. Also set the hostname.

	Task	Instructions	Comment
□	If you have Aurora Edit LD systems on the corporate LAN, add them to the system description and set credentials.		
□	If not already set correctly, set the hostname of discovered devices		Make sure the device name is correct, then make the hostname the same as the device name.
□	Ping each Edit device to test network communication		—
□	Generate host table information and distribute to hosts files on each device and on the control point PC		Make sure you have completed network configuration of all network interfaces across all devices to ensure complete and valid host table information. You can use SiteConfig to copy hosts files to devices, or you can manage hosts files yourself.
□	Next: Software update checklist		

About NewsShare

NewsShare allows Aurora Edit to share a common news database and media volume, making the editing workflow easier to create and maintain.

NewsShare allows Aurora Edit to share a common news database and media volume, making the editing workflow easier to create and maintain. You can configure NewsShare for NAS storage or K2 storage.

About K2 networks

NewsShare allows Aurora Edit to share a common news database and media volume, making the editing workflow easier to create and maintain. You can configure NewsShare for NAS storage or K2 storage.

Before creating a NewsShare environment, you first need to install and configure a K2 Media Server. Refer to the *K2 SAN Installation and Service Manual*.

Many K2 network components, particularly the StorNext File System (SNFS), require all clients and servers to use fixed IP addresses. If your network uses a DHCP server, you must create address reservations or a fixed address subnet.

Complete IP connectivity must exist between all DSMs, K2 Media Servers, and Aurora Edit workstations for a particular K2 network. You might find it convenient to assign all machines on a K2 network to the same Workgroup.

About SiteConfig

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

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

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

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

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

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

About developing a system description

The topics in this manual assume that you are modifying an existing system description. Your system description is typically developed using one of the following taskflows:

- For a system in which all devices are new from Grass Valley with one or more K2 SANs, you first create a system description for your K2 SAN or SANs, then add Browse/MediaFrame, Edit, Ingest, and Playout devices as appropriate. Refer to the *K2 SAN installation and Service Manual* for instructions on creating the system description.
- For a system in which all devices are new from Grass Valley with one or more stand-alone K2 systems, you first create a system description and add your

stand-alone K2 systems, than add other devices as appropriate. Refer to the *K2 System Guide* for instructions on creating the system description and adding your stand-alone K2 systems.

- For a system with existing devices running earlier software, you must first migrate the system to become a SiteConfig managed system. Refer to *SiteConfig Migration Instructions* for instructions on migrating your devices to be SiteConfig managed devices.

If you are using a different taskflow, use the topics in this manual as appropriate and refer to the *SiteConfig User Manual* or *SiteConfig Help Topics* for additional information.

Your devices must be in a SiteConfig system description in order to be managed by SiteConfig. When you already have a system description in place, you should use SiteConfig to modify this system description and add your devices. You can do this in your planning phase, even before you have devices installed or cabled. Your goal is to have the SiteConfig system description accurately represent all aspects of your devices and networks before you begin actually implementing any networking or other configuration tasks for those devices.

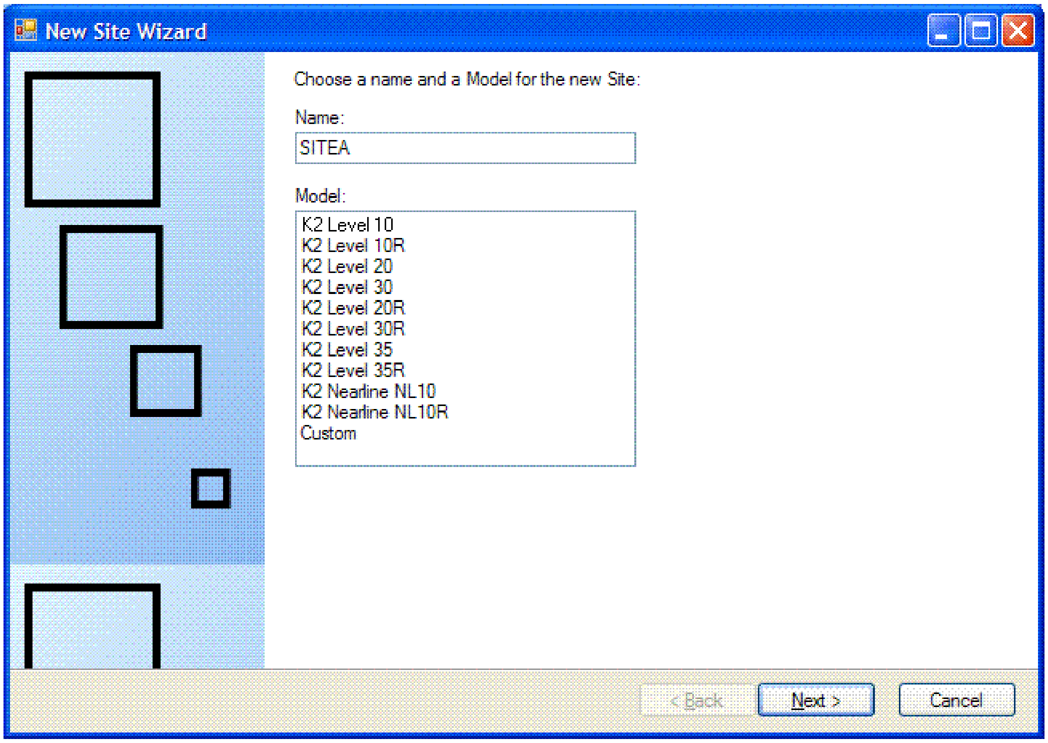
Adding NAS to system description

The NAS is a K2 nearline SAN, so instructions for cabling, networking, and configuration are in the *K2 SAN Installation and Service Manual*. If the NAS is not already included in the SiteConfig system description, add it as follows.

1. In the **Network Configuration | Devices** tree view, right-click the **Site** node that includes your K2 SAN and other connected devices and select **Add Site**.

   In this context, "Site" is a distinct system, such as a K2 SAN or an Aurora Browse system.

   The New Site Wizard opens.



Choose a name and a Model for the new Site:

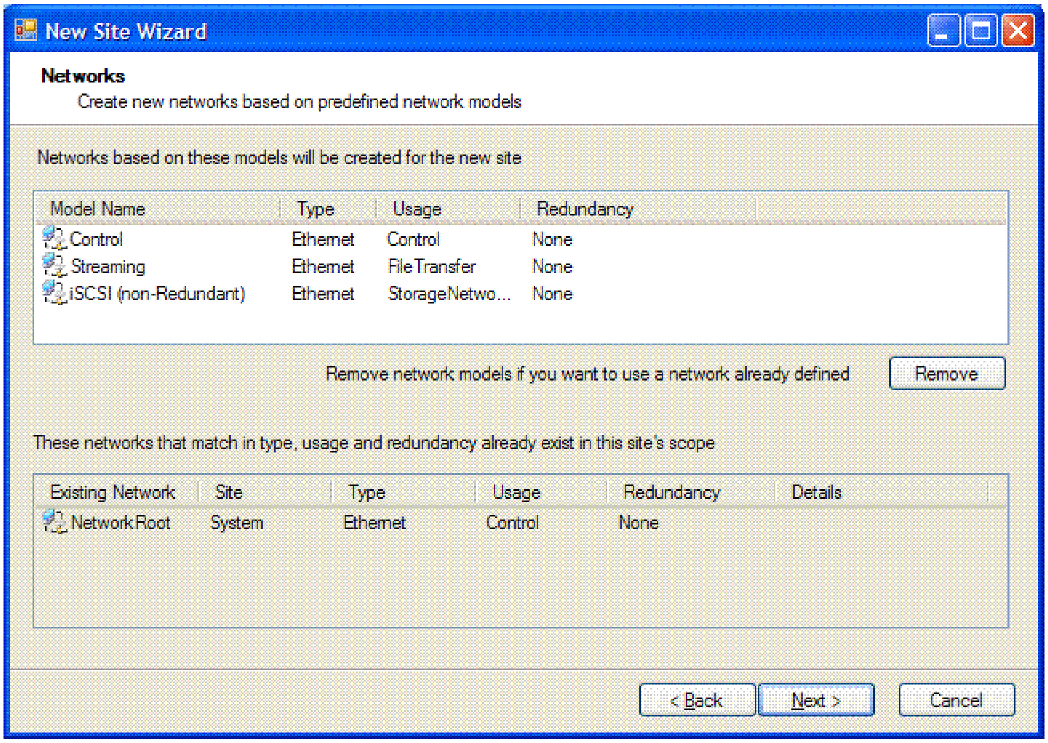
Name: SITEA

Model:

- K2 Level 10
- K2 Level 10R
- K2 Level 20
- K2 Level 30
- K2 Level 20R
- K2 Level 30R
- K2 Level 35
- K2 Level 35R
- K2 Nearline NL10
- K2 Nearline NL10R
- Custom

2. Enter a name for the NAS, considering the following:
   - Keep the site name short, as it becomes the root identifier that is the default prefix for device and network names.
   - Sites in the tree view are automatically sorted alphabetically.
3. Select the appropriate K2 Nearline model.
   - If the K2 RAID chassis has one controller, select K2 Nearline NL10
   - If the K2 RAID chassis has two controllers, select K2 Nearline NL10R
4. Click **Next**.

   The Networks page opens.



Networks

Create new networks based on predefined network models

Networks based on these models will be created for the new site

Model Name	Type	Usage	Redundancy
Control	Ethernet	Control	None
Streaming	Ethernet	FileTransfer	None
iSCSI (non-Redundant)	Ethernet	StorageNetwo...	None

Remove network models if you want to use a network already defined

These networks that match in type, usage and redundancy already exist in this site's scope

Existing Network	Site	Type	Usage	Redundancy	Details
NetworkRoot	System	Ethernet	Control	None	

The Networks page displays a list of networks that are defined for the selected site model. Each of these networks is based on a network model that defines the type, usage and redundancy of the network. When the New Site Wizard creates a network, it is based on this model.

5. Remove the control network and the streaming network.

   Since child sites inherit the networks defined at their parent(s), if the site you are creating has a parent site that already contains one of the displayed networks, then it is not necessary to include that network here.

   The parent site of the NAS is the site that contains your K2 SAN, and it already has a control network and a streaming network.

6. Click **Next**.

   The Devices page opens.

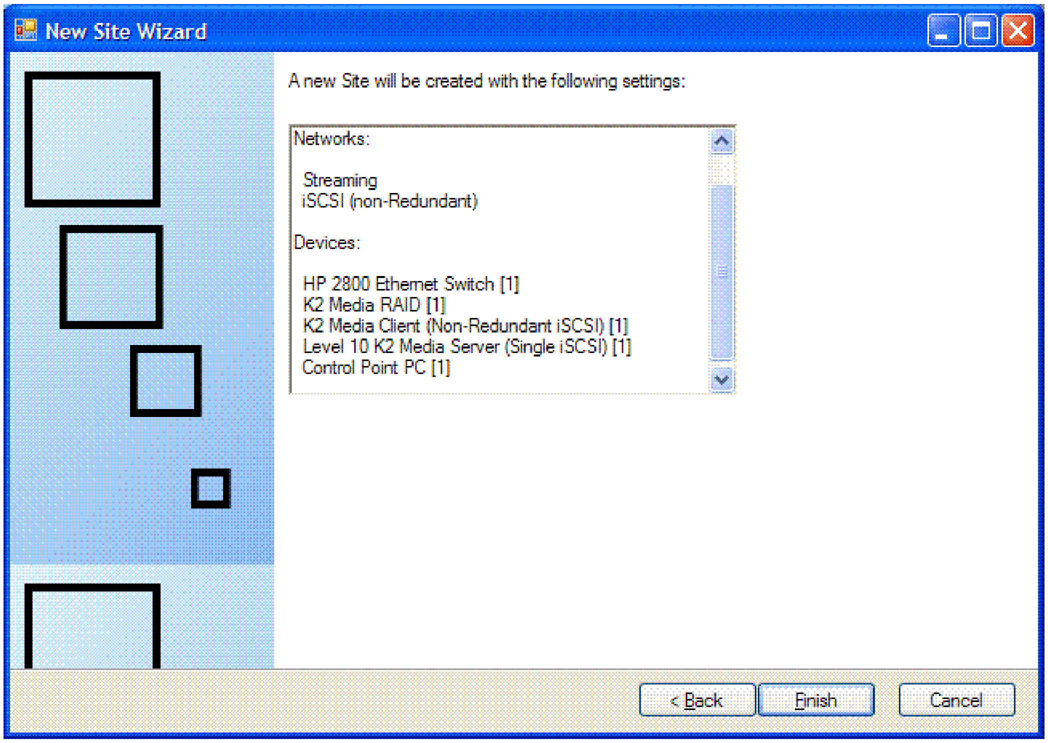
   The Devices page shows you the device models that typically comprise a site based on the model you chose in the first page of the New Site Wizard. The New Site Wizard creates these devices as part of the site. You can then modify, remove, or you add devices, including device models that are not shown on this page.

7. You can select a device model and do one or more of the following:

- Specify the number of devices of that model for the site. If the control is disabled, it means that the number of devices is constrained by the site model. For example, a site model might be constrained to have one Ethernet switch only.
- Specify the starting IP address of a set of devices of that model. SiteConfig automatically assigns IP addresses from this range. If you require a different sequence of IP addresses, you can modify them on each device after the New Site Wizard completes.

8. Click **Next**.

   The "...Site will be created..." page opens.



A new Site will be created with the following settings:

Networks:

Streaming
iSCSI (non-Redundant)

Devices:

HP 2800 Ethernet Switch [1]
K2 Media RAID [1]
K2 Media Client (Non-Redundant iSCSI) [1]
Level 10 K2 Media Server (Single iSCSI) [1]
Control Point PC [1]

   This is the last page and summarizes what the New Site Wizard adds to the tree view.

9. Click **Finish** to create the site.
10. Add additional K2 Media Servers as necessary for the NAS.

About the corporate LAN

Some devices, such as the MediaFrame server or Aurora Edit LD workstations, are on the corporate LAN, which is considered an unmanaged network in SiteConfig. You can configure your system description to include the corporate LAN for the following purposes:

- If a device, such as the MediaFrame server, is on the corporate LAN yet is a SiteConfig managed device, then SiteConfig needs to know the connection for each network interface on the device, including the corporate LAN connection. Otherwise, SiteConfig displays error messages.
- If a device uses a DNS server on the corporate LAN for name resolution, SiteConfig needs to reference that DNS server.
- If a device has software that SiteConfig supports and the devices is on the corporate LAN, such as Aurora Edit LD workstations, you can use SiteConfig to deploy software to the device via the corporate LAN.

If the device is on the corporate LAN and is not on a network that is managed by SiteConfig, you cannot configure network settings on the device.

Related Links

Configuring the corporate LAN on page 35

About software deployment on the corporate LAN

If you have Aurora Edit LD workstations that are on a network that SiteConfig does not manage, such as your corporate LAN, you can configure your system description to allow software deployment to those devices. This method uses SiteConfig as a software deployment tool only, as you cannot configure network settings on the device or manage the device's network. With this method you create an unmanaged network in SiteConfig, add the DNS server(s) to the control point PC, then when you add the PC, edit the control interface and set it to the unmanaged network. This allows communication with the Aurora Edit LD workstations. Then add a placeholder device for each of your Aurora Edit LD workstations. With this method you do not use SiteConfig device discovery, and it is not necessary to install a discovery agent on the Aurora Edit LD workstation. Rather, you configure SiteConfig to look up the address via DNS or hosts file. This allows the Aurora Edit LD workstation to communicate as if it was a discovered device. SiteConfig can then deploy software to the device.

If necessary, get help from your IT department to ensure that the SiteConfig PC is configured to communicate with the Aurora Edit LD workstations on the corporate network. If SiteConfig can ping it, it can deploy software.

Related Links

Installing and configuring SiteConfig support for Aurora Edit LD on page 45

Adding Aurora Edit LD workstations for software deployment on page 53

Configuring the corporate LAN

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

The networks under that node are displayed in the list view.

2. Proceed as follows:

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

   The Network Settings dialog box opens.

3. Configure the settings for the network as follows:

   - Type – Select Ethernet
   - Usage – Select Control
   - Redundancy – Select None
   - Name – Enter a name to identify the network in the system description
   - Exclude from Host Files – Select the checkbox
   - Unmanaged – Select this option, then select DNS and select the checkbox for IP Address Allocation via DHCP.
   - Base IP Address – Do not configure
   - Number of IP Addresses – Do not configure
   - Subnet Mask – Do not configure
   - DNS Servers – Servers providing DNS for name resolution. These DNS server can be for both managed and unmanaged networks.
   - Default Interface Name Suffix – The suffix added to the end of host names to identify interfaces on this network.

4. Click **OK** to save settings and close.
5. If you added a network, it appears in the **Network Configuration | Networks** tree view at the bottom of the list.

Related Links

About the corporate LAN on page 34

Adding a group

1. In the **Network Configuration | Networks** tree view, right-click a site node and select **Add Group**.

   The group appears in the tree view.

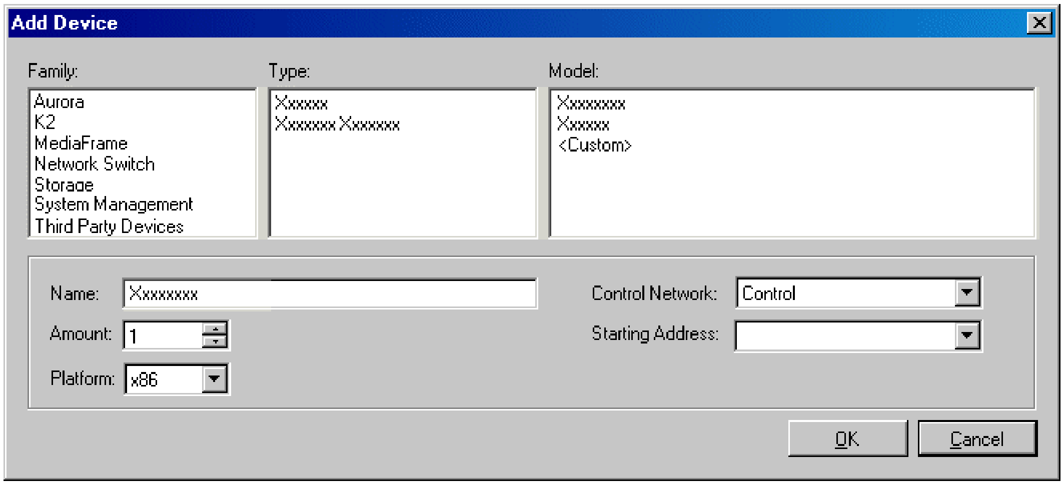
2. Right-click the group and select **Rename**.
3. Enter the desired name for the group.

Adding a device to the system description

Prerequisites for this task are as follows:

- The system description contains a group.

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



Name: Xxxxxxxx

Amount: 1

Platform: x86

Control Network: Control

Starting Address:

The Add Device dialog box opens.

2. Configure settings for the device you are adding as follows:
   - Family – Select **Aurora**.
   - Type – Select the appropriate type of Aurora device.
   - Model – Select the appropriate model.
   - Name – This is the device name, as displayed in the SiteConfig device tree view and device list view. This name can be different than the host name (network name). You can accept the default name or enter a name of your choice. Devices in the tree view are sorted alphabetically.
   - Amount – You can add multiple devices, as currently defined by your settings in the Add Device dialog box. An enumerator is added to the name to create a unique name for each device added.
   - Control network – Select the control network.
   - Starting Address – Select from the list of available addresses on the selected control network. If adding multiple devices, this is the starting address, with addresses assigned sequentially to each device added.

3. Click **OK** to save settings and close.
4. Repeat these steps for each of your devices.

About device and host names

In SiteConfig, a device can have different names, as follows:

- Device name — This is a name for display in SiteConfig only. It is stored in the SiteConfig system description, but not written to the actual device. It is displayed in the device tree view and in the device list view. It can be a different name than the device's host name.
- Host name — This is the network name of the device. SiteConfig has a default naming convention for host names which you can use or override with your own host names.

In most cases it is recommended that the Device name and Host name be the same. This avoids confusion and aids troubleshooting.

The Device name can serve as a placeholder as a system is planned and implemented. During the install/commission process, when you reconcile a device's current and planned network interface settings, the Host name as configured in the system description can be overwritten by the host name on the actual device. However, the Device name configured in the system description is not affected. Therefore it is recommended that in the early planned stages, you configure the Device name to be the desired name for the device, but do not yet configure the Host name. Then, after you have applied network interface settings, you can change the Host name to be the same as the Device name. This changes the host name on the actual device so that then all names are in sync.

SiteConfig does not allow duplicate device names or host names.

Items in the tree view are automatically sorted alphabetically, so if you change a name the item might sort to a different position.

Modifying a device name

1. In the **Network Configuration | Devices** tree view, right-click a device and select **Rename**.
2. Type in the new name.

   Note that this does not change the hostname on the physical device. If you want the hostname to match the device name, you must also modify the hostname.

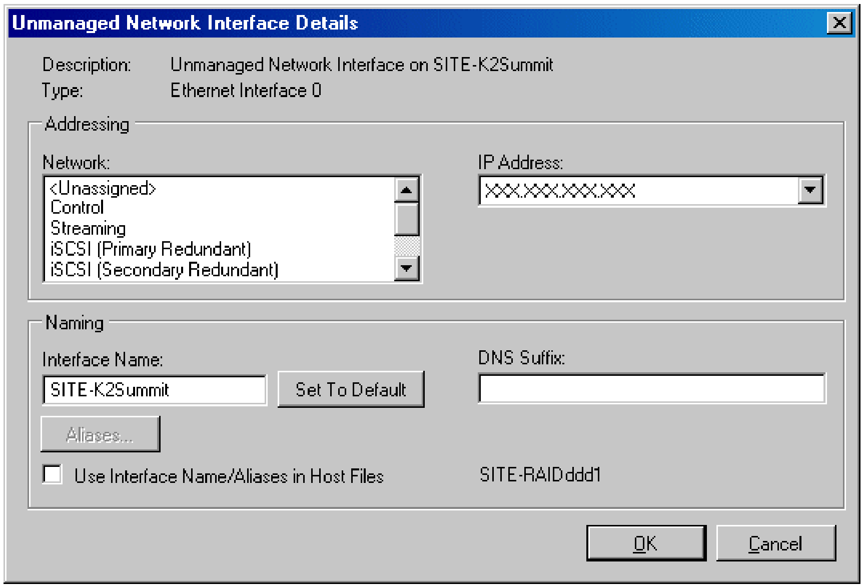
About IP configuration of network interfaces on devices

You can perform IP configuration of network interfaces when working with a placeholder device prior to discovery. When you add a device and choose a particular model, the model defines the number, type and usage characteristics of network interfaces to expect on such a device.

You can view and edit each network interface and set up IP configuration selecting an appropriate IP from the network to which each interface connects. The process for editing IP configuration varies, depending on the device's phase.

Placeholder device IP configuration

On a placeholder device, you edit network interfaces using the Unmanaged Network Interfaces dialog box.


Unmanaged Network Interface Details

Description: Unmanaged Network Interface on SITE-K2Summit
Type: Ethernet Interface 0

Addressing

Network:
- <Unassigned>
- Control
- Streaming
- iSCSI (Primary Redundant)
- iSCSI (Secondary Redundant)

IP Address: xxx.xxx.xxx.xxx

Naming

Interface Name: SITE-K2Summit

DNS Suffix:

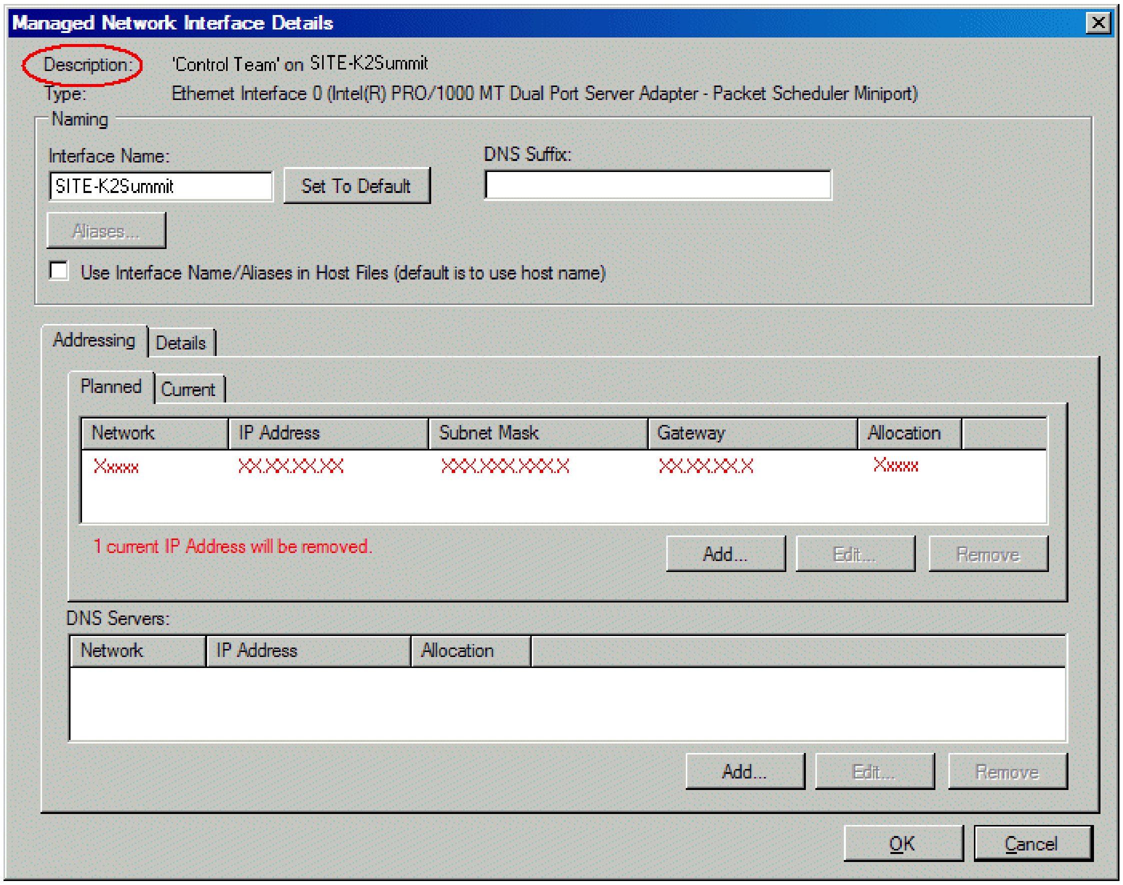
□ Use Interface Name/Aliases in Host Files

SITE-RAIDddd1

The Unmanaged Network Interfaces dialog box allows you only to save changes to the system description.

Discovered device IP configuration

On a discovered device, you edit network interfaces using the Managed Network Interfaces dialog box.



Managed Network Interface Details

Description: 'Control Team' on SITE-K2Summit

Type: Ethernet Interface 0 (Intel(R) PRO/1000 MT Dual Port Server Adapter - Packet Scheduler Miniport)

Naming

Interface Name: SITE-K2Summit

DNS Suffix:

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

Network	IP Address	Subnet Mask	Gateway	Allocation
Xxxxx	XX.XX.XX.XX	XXX.XXX.XXX.X	XX.XX.XX.X	Xxxxx

1 current IP Address will be removed.

DNS Servers:

Network	IP Address	Allocation

The Managed Network Interfaces dialog box allows you to edit and save changes to the device.

Modifying unassigned (unmanaged) network interfaces on Edit devices

Prerequisites for this task are as follows:

- The system description has one or more Aurora Edit devices that are placeholder devices.
- The placeholder device has a one or more unmanaged network interfaces.

Use this task to modify unmanaged network interfaces on Aurora Edit devices as follows:

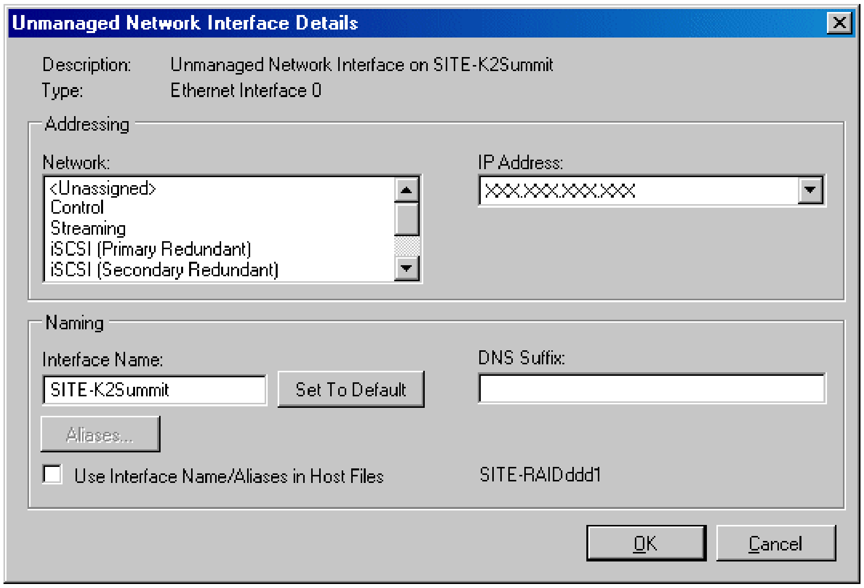
- Aurora Edit
- Conform Server
- DSM
- FTP Server
- SmartBin Server

1. In the **Network Configuration | Devices** tree view, select an Aurora Edit placeholder device.

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

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

   The Unmanaged Network Interface Details dialog box opens.



Unmanaged Network Interface Details

Description: Unmanaged Network Interface on SITE-K2Summit

Type: Ethernet Interface 0

Addressing

Network:

<Unassigned>
Control
Streaming
iSCSI (Primary Redundant)
iSCSI (Secondary Redundant)

IP Address: XXX.XXX.XXX.XXX

Naming

Interface Name: SITE-K2Summit

DNS Suffix:

□ Use Interface Name/Aliases in Host Files

SITE-RAIDddd1

3. Configure the settings for the interface as follows:

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

Setting...	For media (iSCSI) network interface
Network	If on a basic K2 SAN, *iSCSI (non-Redundant)* is required for the iSCSI interface.
	If on a redundant K2 SAN, *iSCSI (Primary Redundant)* is required for the iSCSI interface on devices connecting to the A side of the redundant K2 SAN
	If on a redundant K2 SAN, *iSCSI (Secondary Redundant)* is required for the iSCSI interface on devices connecting to the B side of the redundant K2 SAN
IP Address	The IP address for this interface on the network. Required.
Interface Name	Disabled, since names are excluded from the hosts file. Disregard.
Set to Default	Disabled, since names are excluded from the hosts file. Disregard.
Use Interface Name/Aliases in Host Files	Disabled, since names are excluded from the hosts file. Disregard.
Aliases	Disabled, since names are excluded from the hosts file. Disregard.
DNS Suffix	Disabled, since names are excluded from the hosts file. Disregard.

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

About SiteConfig support on Aurora Edit devices

Before SiteConfig can be used to discover or manage a device, the device must meet the following requirements:

- The device must be a Microsoft Windows operating system device.
- The device must have Microsoft .NET version 2.0 installed, as reported in the Windows Add/Remove Programs control panel.
- The ProductFrame Discovery Agent service must be running on the device, as reported in the Windows Services control panel.

For Aurora Edit devices shipped new from Grass Valley with software version 6.5 or higher, these requirements are pre-installed. These requirements are pre-installed on recovery images for these systems as well. Therefore, if you suspect a problem with these requirements, do not attempt to install SiteConfig support requirements. If you must restore SiteConfig support requirements, re-image the system.

For devices that you purchase and then install software and hardware to build an Aurora device, you must verify and install SiteConfig support requirements as necessary.

Software that meets these requirements is bundled in various components and installation programs, some of which are available at your SiteConfig install location as follows:

- The *`ConnectivityKit`* folder contains Microsoft .NET. You can copy the contents of this folder to a device and then run *`setup.exe`* to install the software.
- The *`DiscoveryAgent Setup`* folder contains the ProductFrame Discovery Agent. You can copy the contents of this folder to a device and then run *`setup.exe`* to install the software.

Installing SiteConfig support

Use this topic to verify and, if necessary, install SiteConfig support software so that the device can be discovered and managed by SiteConfig.

For Aurora Edit LD, do not use this topic. Instead, skip ahead and use the next topic.

1. Open the Windows Services Control Panel and look for the following required item:

   - ProductFrame Discovery Agent

2. Open the Windows Add\Remove Programs Control Panel and look for the following required item:

   - Microsoft .NET Framework 2.0 Service Pack 2

3. Proceed as follows:

   - On Aurora product devices, if the ProductFrame Discovery Agent at a version lower than 1.1.0.185 is installed, use the Windows Add\Remove Programs Control Panel and uninstall it. On these devices you must uninstall and then install version 1.1.0.185 or higher, as instructed in next steps.

     NOTE: The Discovery Agent can be named the ProductFrame Discovery Agent, the SiteConfig Discovery Agent, or the SiteConfig Network Configuration Connect Kit.

   - On other devices, if the ProductFrame Discovery Agent is already installed, you can leave it installed as is.
   - On all devices, if either the ProductFrame Discovery Agent or .NET is not installed, install the required software as instructed in next steps.

4. Navigate to your SiteConfig files or to the SiteConfig install location.
5. To install the ProductFrame Discovery Agent Service do the following:
   a) Copy the *`Discovery Agent Setup`* subdirectory to the device.
   b) In the *`Discovery Agent Setup`* directory, double-click the *`DiscoveryAgentServiceSetup.msi`* file.

The setup program launches to install the SiteConfig Discovery Agent.

c) Follow the setup wizard.

The setup wizard presents a list of devices types similar to the following:

- K2Server
- GigESwitch
- FCSwitch
- K2Client
- AuroraEdit
- MediaFrameServer
- ControlPoint
- K2Appliance
- K2Standalone
- K2SummitSanClient
- K2SummitStandaloneClient
- IEP
- DSM
- ProxyEncoder
- SmartBinServer
- FTPServer
- ConformServer
- AuroraEditLD
- GenericDevice
- RAIDBaseUnit
- AuroraPlayoutPlatform
- AuroraIngestPlatform

d) From the list, select the device type of the device on which you are installing the Discovery Agent.

e) Complete the setup wizard.

f) Restart.

The restart is required after the installation.

6. To install .NET 2.0 do the following:

Be sure that .NET is installed before installing the Discovery Agent.

a) From the directory at which the SiteConfig application is installed on the control point PC, copy the contents of the *`ConnectivityKit`* directory to the device.

b) Run *`setup.exe`* and install the software.

Installing and configuring SiteConfig support for Aurora Edit LD

Use this topic to install software and configure Aurora Edit LD workstations that are on the corporate LAN to prepare them for SiteConfig software deployment. You can do this using the following methods:

- Remotely from the SiteConfig control point PC, using a deployment preparation script that connects to each of your Aurora Edit LD workstations. This requires an appropriate domain admin account that can access all the devices remotely. Start with step 1 to use this method.
- Locally at each Aurora Edit LD workstation. This method is described in the last step of the procedure.

1. On the control point PC, create a text file that lists the hostnames of all the Edit LD devices you want to prep for SiteConfig software deployment, with one hostname per line. Name the text file *`EditLDdevices.txt`*.
2. Save the text file to the SiteConfig install directory. The default location is *`C:\Program Files\Grass Valley\SiteConfig`*.
3. Open the MS-DOS command prompt as follows.
   a) From the Windows desktop, click **Start | Run**.
   b) Type `cmd` and press **Enter**.

   The MS-DOS command prompt window opens.
4. From the MS-DOS command prompt, `cd` to the SiteConfig install directory. For example, type the following sequence of commands, pressing **Enter** after each command.
   a) `C:`
   b) `cd "Program Files"`
   c) `cd "Grass Valley"`
   d) `cd SiteConfig`
5. Run the batch file by typing the following and then pressing **Enter**:

   ```
   DeploymentPrep.bat {path to the text file} {domain admin
   user name}
   ```

   Example: `DeploymentPrep.bat "C:\Program Files\Grass Valley\SiteConfig\EditLDdevices.txt" CORP_LAN\Administrator`
6. Enter the domain admin password for the Aurora Edit LD devices when prompted. The assumes that the domain admin password is the same for all the devices.

   The script connects to each device with the admin user name specified. The script reports its activities on each device.

   If errors occur on a device, they are displayed. The script skips problem devices and continues on until it completes all devices in the text file list. When complete, the command prompt is displayed.

7. Restart each Aurora Edit LD device on which the script was successful.
8. For each Aurora Edit LD workstation on which the script was unsuccessful or for which the deployment preparation script is unsuitable, install the Connectivity Kit on the device and configure as follows:
   a) From the directory at which the SiteConfig application is installed on the control point PC, copy the contents of the `ConnectivityKit` directory to the device.
   b) Run `setup.exe` and install the software.
   c) Check firewall settings on the Aurora Edit LD device as follows and configure if necessary. The deployment preparation script configures the Windows firewall, so for devices using the Windows firewall on which you have run the script, these settings should already be configured.

      - Turn on the file and printer sharing ports - TCP 139, 445, UDP 137, 138.
      - Turn on remote desktop - TCP 3389.

   d) Restart the Aurora Edit LD workstation.

Related Links

Adding Aurora Edit LD workstations for software deployment on page 53
About software deployment on the corporate LAN on page 35

Set credentials

1. At each local device, view the Windows administrator user account and verify that the credentials are the same as those that SiteConfig uses to access the device.

   SiteConfig is pre-configured to use the following default credentials to access devices:

Device type	Username	Password
All K2 devices	Administrator	adminK2
All Aurora Browse (MediaFrame), Edit, Ingest, and Playout devices	Administrator	adminGV!

2. If necessary, change credentials so they match on the device and in SiteConfig, using one of the following methods:

   - Change the device's credentials to match the credentials that SiteConfig uses to access the device. This is recommended for most K2 and Aurora devices.
   - If your security policies prohibit changing the device's credentials, such as on Aurora Edit LD workstations on the corporate LAN, in SiteConfig change the credentials that SiteConfig uses to access the device.

Related Links

Setting credentials for a specific device on page 54

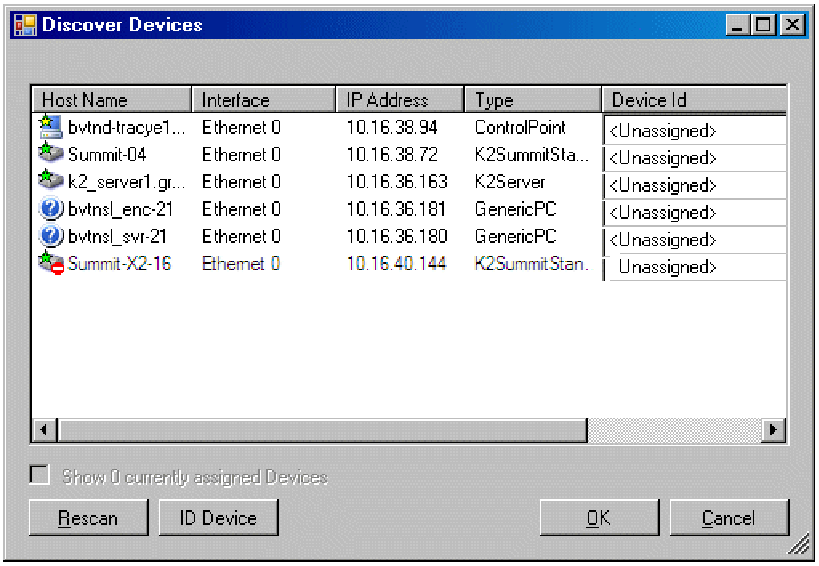
Discovering devices with SiteConfig

Prerequisites for this task are as follows:

- The Ethernet switch or switches that the support the control network are configured and operational. If multiple switches, ISLs are connected and trunks configured.
- The control point PC is communicating on the control network.
- There are no routers between the control point PC and the devices to be discovered.
- Devices to be discovered are Windows operating system devices, with SiteConfig support installed.
- Devices are cabled for control network connections.

1. Open SiteConfig on the control point PC.
2. In the toolbar, click the discover devices button. 🔍

   The Discover Devices dialog box opens.



Host Name	Interface	IP Address	Type	Device Id
bvtnd-tracye1...	Ethernet 0	10.16.38.94	ControlPoint	<Unassigned>
Summit-04	Ethernet 0	10.16.38.72	K2SummitSta...	<Unassigned>
k2_server1.gr...	Ethernet 0	10.16.36.163	K2Server	<Unassigned>
bvtnsl_enc-21	Ethernet 0	10.16.36.181	GenericPC	<Unassigned>
bvtnsl_svr-21	Ethernet 0	10.16.36.180	GenericPC	<Unassigned>
Summit-X2-16	Ethernet 0	10.16.40.144	K2SummitStan.	Unassigned>

   A list of discovered devices is displayed.

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

Assigning discovered devices

Prerequisites for this task are as follows:

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

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

   The Discover Devices dialog box opens.

2. Identify discovered devices.

   - If a single device is discovered in multiple rows, it means the device has multiple network interfaces. Choose the interface that represents the device's currently connected control connection. This is typically Ethernet ... 0.
   - If necessary, select a device in the list and click **ID Device**. This triggers an action on the device, such as flashing an LED or ejecting a CD drive, to identify the device.

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

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

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

   - If SiteConfig finds a match between the device-type discovered and the device-type of one or more placeholder devices, it displays those placeholder devices in the list.
   - If SiteConfig does not find a match between the device-type discovered and the device-type of a placeholder device, no placeholder device is displayed in the list.

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

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

6. When discovered devices have been assigned, click **OK** to save settings and close.
7. In the **Network Configuration | Devices** tree view, select each of the devices to which you assigned a discovered device.

Modifying Edit device managed network interfaces

Prerequisites for this task are as follows:

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

Use this task to modify managed network interfaces on a Aurora Edit devices as follows:

- Aurora Edit
- Conform Server
- DSM
- FTP Server
- SmartBin Server

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

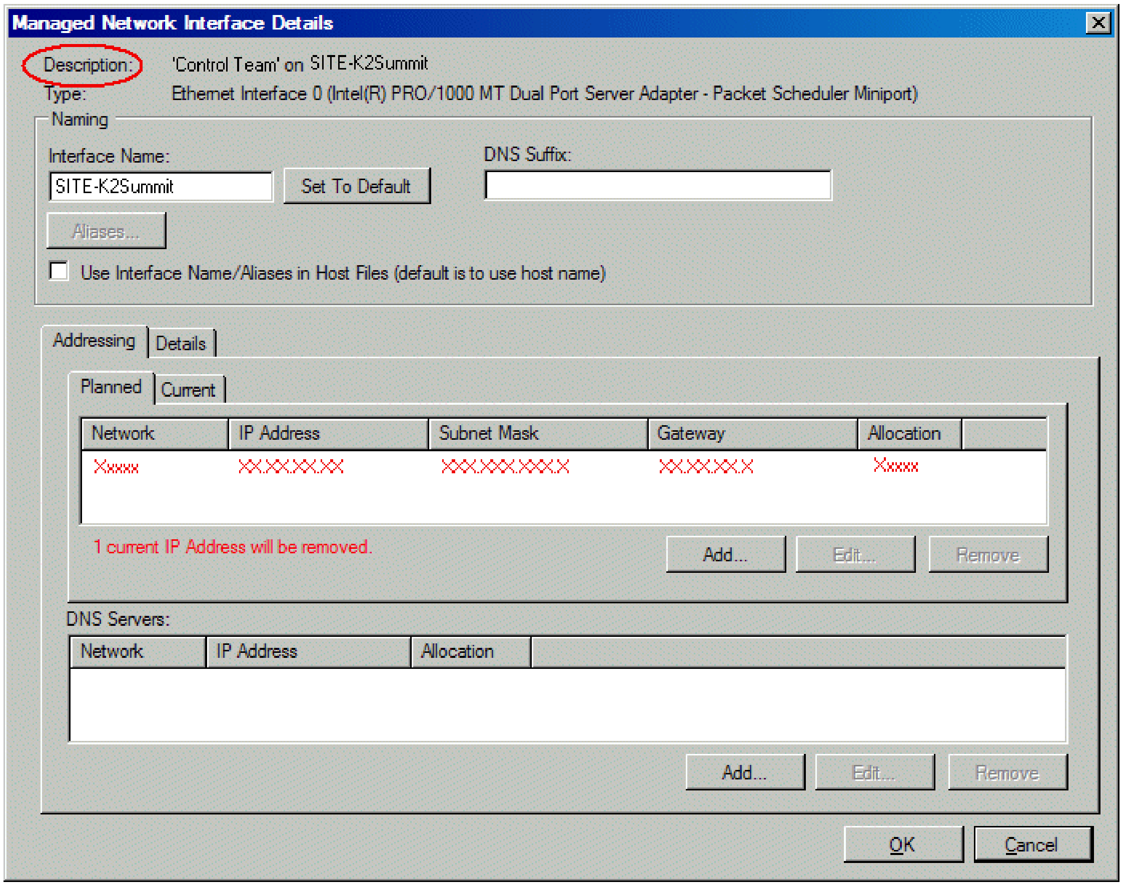
   - Identify the interface with which SiteConfig is currently communicating, indicated by the green star overlay icon. This should be the control network interface.
   - Verify that the interface over which SiteConfig is currently communicating is in fact the interface defined for the control network in the system description. If this is not the case, you might have the control network cable connected to the wrong interface port. The control connection should always be the first port on the motherboard, except when you have a loopback connection.
   - Configure the control network interface first before configuring any of the other interfaces.
   - After you have successfully configured the control network interface, return to this step to configure each remaining interface.

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

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

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

   The Managed Network Interface Details dialog box opens.



Description: 'Control Team' on SITE-K2Summit

Type: Ethernet Interface 0 (Intel(R) PRO/1000 MT Dual Port Server Adapter - Packet Scheduler Miniport)

Interface Name: SITE-K2Summit

DNS Suffix:

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

Network	IP Address	Subnet Mask	Gateway	Allocation
Xxxxx	XX.XX.XX.XX	XXX.XXX.XXX.X	XX.XX.XX.X	Xxxxx

1 current IP Address will be removed.

DNS Servers:

Network	IP Address	Allocation

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

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

Setting...	**For network interface Network Connection**
Use Interface Name/Aliases in Host Files	*Unselected* is required. Since not selected, the default behavior occurs, which is to use the device host name in the hosts file.

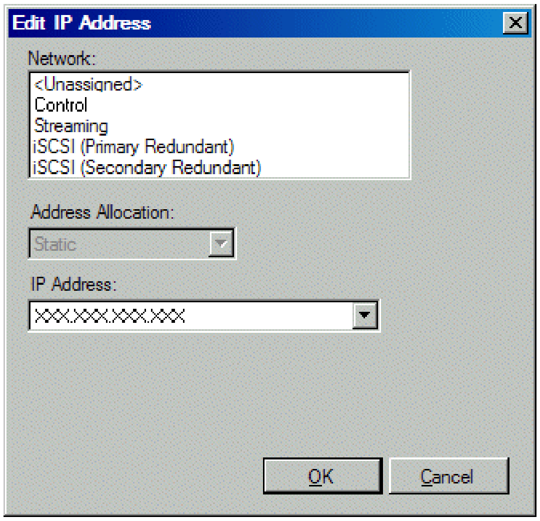
Setting...	**For any network interface of type iSCSI**
Interface Name	The text "Unused" is recommended. Displaying this text here serves as an aid in understanding SAN networks.The iSCSI network has no name resolution via the hosts file or otherwise, so the text you enter here is not actually use for name resolution.
Set To Default	Not allowed
DNS Suffix	Not allowed
Aliases	Not allowed
Use Interface Name/Aliases in Host Files	*Selected* is recommended. Since this interface's network has its names excluded from the hosts file, this setting has no affect. The interface name is excluded from the hosts file, regardless of settings here.

6. Evaluate settings on the Planned tab and change if necessary.
   - Compare settings on the Planned tab with settings on the Current tab.
   - If you want to keep the current settings as reported in the Current tab, click **Remove** to remove the planned settings.
   - Do not specify multiple IP addresses for the same interface. Do not use the Add button.

7. To modify planned settings, do the following:

   a) Select the network settings and click **Edit**.

   The Edit IP Address dialog box opens.


Edit IP Address

Network:

Address Allocation: Static

IP Address: xxx.xxx.xxx.xxx

b) Edit IP address settings as follows:

Setting...	For network interface Network Connection
Network	*Control* is required
Address Allocation	*Static* is recommended.
IP Address	The IP address for this interface on the network. Required.

Setting...	For basic SAN any network interface of type iSCSI
Network	*iSCSI (non-Redundant)* is required
Address Allocation	*Static* is required.
IP Address	The IP address for this interface on the network. Required.

Setting...	For redundant SAN A side any network interface of type iSCSI
Network	*iSCSI (Primary Redundant)* is required
Address Allocation	*Static* is required.
IP Address	The IP address for this interface on the network. Required.

Setting...	For redundant SAN B side any network interface of type iSCSI
Network	*iSCSI (Secondary Redundant)* is required
Address Allocation	*Static* is required.
IP Address	The IP address for this interface on the network. Required.

The networks listed in the Edit IP Address dialog box are those currently defined in the system description, with available settings restricted according to the network definition. If you require settings that are not available, you can close dialog boxes and go to the **Network Configuration | Networks** tab to modify network settings, then return to the Edit IP Address dialog box to continue.

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

   A Contacting Device message box reports progress.

9. After configuring control network settings, do the following

   a) If a message informs you of a possible loss of communication, click **OK**.

      This message is normal, since this is the network over which you are currently communicating.

   b) In the Device list view, observe the device icon and wait until the icon displays the green star overlay before proceeding.

      The icon might not display the green star overlay for several seconds as settings are reconfigured and communication is re-established.

   c) In the Interface list view, right-click the interface and select **Ping**.

      The Ping Host dialog box opens.

      If ping status reports success, the interface is communicating on the control network.

Adding Aurora Edit LD workstations for software deployment

If you have Aurora Edit LD workstations on the corporate LAN, use this topic to get the workstations communicating with SiteConfig in order to support software deployment. Do not attempt to use device discovery.

1. Add a placeholder device for an Aurora Edit LD workstation.
2. If necessary, set the placeholder device's credentials so that SiteConfig will use the correct credentials when it communicates with the device.
3. Select the placeholder device.
4. In the interfaces list view, right-click an interface and select **Edit**.

   The Unmanaged Network Interface Details dialog box opens.
5. Configure the settings for the interface as follows:
   - Network – If using DHCP or external hosts file, select the unmanaged network that you configured earlier in this procedure.
   - IP Address – Make no selection.
   - DNS Suffix – For communication on some networks, a suffix, such as `mycorp.com`, must be added to host names.
   - Remaining settings are irrelevant, as SiteConfig does not manage this device's network.
6. Configure for the device name as follows:

   a) In the tree-view select the placeholder device.

   b) In the Device list view right-click the device and select **Edit**.

   The Edit Device dialog box opens.

   c) Edit the hostname.

   d) If using DHCP, specify a domain name.

   e) Click OK to save settings and close.
7. Click **OK** to save settings and close.
8. From the control point PC, ping the Aurora Edit LD workstation to verify communication.

Related Links

Installing and configuring SiteConfig support for Aurora Edit LD on page 45

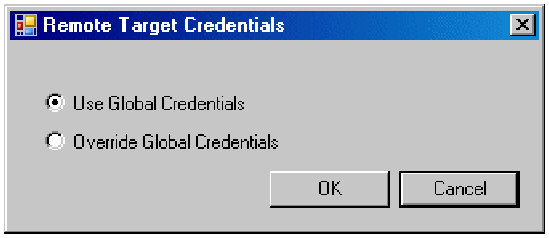
About software deployment on the corporate LAN on page 35

Setting credentials for a specific device

For Aurora Edit LD, override global credentials so that SiteConfig has access to the Aurora Edit LD workstation for software deployment.

1. In the tree view, right-click a device and select **Credentials**.

   The Remote Target Credentials dialog box opens.



2. Proceed as follows:

    - If you previously applied credentials to the device that were different than the global credentials and now you want to apply the global device type credentials, select **Use Global Credentials**.
    - If you want to apply credentials to the device that are different than the device-type credentials, select **Override Global Credentials**.

    The Set Device Logon Credentials dialog box opens.

3. Enter the user name and password for the device and click **OK**. To test the credentials, right-click on the device and choose **Remote Desktop** to start a session to the device.

Making the host name the same as the device name

1. Verify that the current device name, as displayed in the SiteConfig tree view, is the same as your desired host name.
2. In the **Network Configuration | Devices | Device** list view, right-click the device and select **Edit**.

    The Edit Device dialog box opens.

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

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

4. Click **OK**.

Pinging devices from the control point PC

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

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

2. In the Devices list view, select one or more devices. Use Ctrl + Click or Shift + Click to select multiple devices.
3. Right-click the selected device or devices and select **Ping**.

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

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

About hosts files and SiteConfig

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

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

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

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

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

Generating host tables for devices with SiteConfig

Prerequisites for this task are as follows:

- Planned control network settings are applied to control network interfaces and devices are communicating on the control network as defined in the system description.
- Interfaces for networks that require name resolution via the hosts file, such as the FTP/streaming network, have settings applied and are communicating.
- You have viewed host names, as currently defined in the system description, and determined that they are correct.
- The control point PC is added to the system description so that it is included in the host tables generated by SiteConfig.

1. In the **Network Configuration | Networks** tree view, select a network, site, or system node.
2. Click **View Hosts file**.

   A Hosts File Contents window opens that displays the contents of the hosts file as currently defined in the system description.
3. Verify the information in the hosts file.
4. Do one of the following:

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

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

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

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

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

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

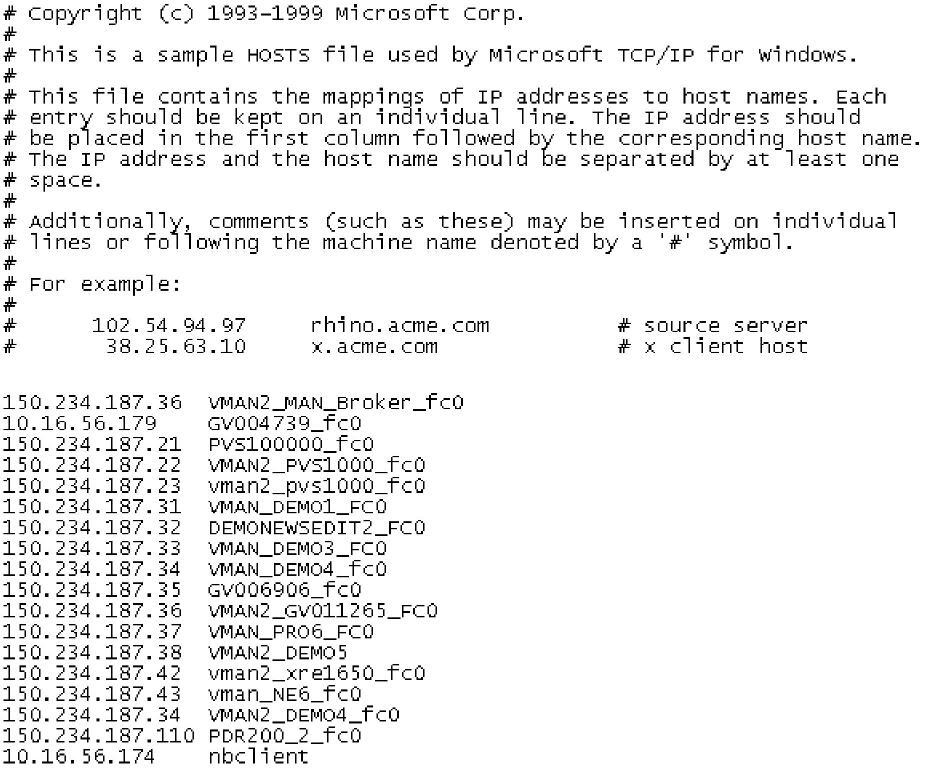
The current hosts file is overwritten with the hosts file as defined in the system description.

Setting Up the Host Table

The host table is a file that resides on the Aurora Edit workstation, which resolves the name of each Aurora Edit workstation with its IP addresses. Aurora Edit uses this file to verify that clips are sent across the proper network.

Use this topic if you choose to manage your hosts files manually.

A sample hosts file looks like this:



```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

150.234.187.36  VMAN2_MAN_Broker_fc0
10.16.56.179    GV004739_fc0
150.234.187.21  PVS100000_fc0
150.234.187.22  VMAN2_PVS1000_fc0
150.234.187.23  vman2_pvs1000_fc0
150.234.187.31  VMAN_DEMO1_FC0
150.234.187.32  DEMONEWSEDIT2_FC0
150.234.187.33  VMAN_DEMO3_FC0
150.234.187.34  VMAN_DEMO4_fc0
150.234.187.35  GV006906_fc0
150.234.187.36  VMAN2_GV011265_FC0
150.234.187.37  VMAN_PRO6_FC0
150.234.187.38  VMAN2_DEMO5
150.234.187.42  vman2_xre1650_fc0
150.234.187.43  vman_NE6_fc0
150.234.187.34  VMAN2_DEMO4_fc0
150.234.187.110 PDR200_2_fc0
10.16.56.174    nbclient
```

To set up a hosts file, do the following:

1. Open the following file using Notepad, or some other text editor:

   C:\WINNT\System 32\Drivers\etc\hosts

2. Enter text in a single line for each Aurora Edit workstation and K2 server on your network, as follows:

   Type the IP address, then use the TAB key or Space bar to insert a few spaces. Then type the device name, such as AuroraEdit1 followed by the characters _FC0 for Fibre Channel or _HE0 for Gigabit Ethernet.

3. Save the file and close the text editor.

4. Copy the new hosts file onto all other Aurora Edit workstations.

Chapter 4

Managing Software

This section contains the following topics:

- *Create record of software installed on devices*
- *Adding a software role to a device*
- *Removing a software role from a device*
- *Configuring deployment groups*
- *Distribute devices into deployment groups*
- *Install prerequisite files on the control point PC*
- *Prepare for installation*
- *Prepare SiteConfig for software deployment*
- *Upgrade K2 systems*
- *Set up K2 Aurora FTP*
- *Distribute devices into deployment groups*
- *Manually install software*
- *Check all currently installed software*
- *Add software package to deployment group*
- *Setting deployment options*
- *Install and configure software on a NewsShare System*
- *Install software on other Aurora Edit devices*

Create record of software installed on devices

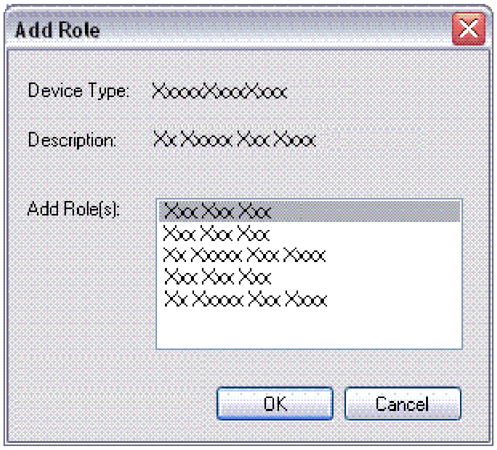
If you have not already done so, create a document to keep track of the software that you plan to install on each of your system devices, according to your system design. This is especially helpful for Aurora product devices. The following table is an example of this type of document. Then, as you proceed with subsequent tasks and remove/add software roles to devices in SiteConfig, you can refer to your table and make sure you are assigning software roles correctly.

Software	SVR-1	HD-1, 2, 3	CONF-1	EDIT-1	DSM-1	ING-1	FSM-1	HDK2-1	FTP-1
MF Server	X								
+ K2 MDI	X								
+ News MDI			X						
+ NTFS	X								
+ FlashNET MDI	X								
+ Proxy MDI	X								
+ FTP MDI	X								
Aurora Browse	X								
Proxy Encoder		X							
News Share					X				
Conform			X						
Aurora Suite						X			
+ Edit				X					
+ Edit LD				X					
+ FTP		X							X
+ SmartBins			X						
+ RMI core									
Aurora Ingest						X			
Aurora Playout						X			
K2 - Gen iSCSI		X	X	X	X				X
K2 - GVG MLib	X	X	X	X	X				X
K2 - Server							X		
K2 - Client								X	
Control Point						X			
StorNext		X	X	X	X		X	X	X

Adding a software role to a device

1. In the **Software Deployment | Devices** tree view, right-click the device and select **Add Role**.

   The Add Role dialog box opens.

   Add Role

   Device Type: XxxxxXxxxXxxx

   Description: Xx Xxxxx Xxx Xxxx

   Add Role(s):
   Xxx Xxx Xxx
   Xxx Xxx Xxx
   Xx Xxxxx Xxx Xxxx
   Xxx Xxx Xxx
   Xx Xxxxx Xxx Xxxx

   The Add Role dialog box displays only those roles that SiteConfig allows for the selected device type.

2. Select the role or roles that you want to add to the device. Use Ctrl + Click or Shift + Click to add multiple roles.
3. Click **OK** to save settings and close.

   The new role or roles appear under the device in the tree view.

Removing a software role from a device

1. In the **Software Deployment | Devices** tree view, expand a device's node to expose the roles currently assigned to the device.
2. Right-click the role you want to remove and select **Remove**.

   The role is removed from the device in the tree view.

Configuring deployment groups

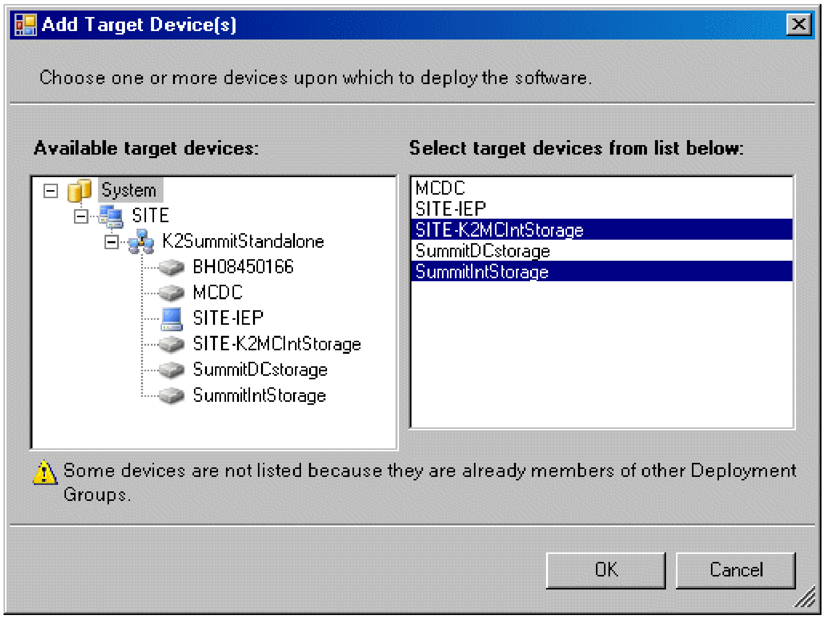
Prerequisites for this procedure are as follows:

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

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

   A deployment group appears in the tree view.
2. Right-click the deployment group, select **Rename**, and enter a name for the deployment group.
3. Right-click the deployment group and select **Add Target Device**.

   The Add Target Device(s) wizard opens.



Add Target Device(s)

Choose one or more devices upon which to deploy the software.

Available target devices:

- System
  - SITE
    - K2SummitStandalone
      - BH08450166
      - MCDC
      - SITE-IEP
      - SITE-K2MCIntStorage
      - SummitDCstorage
      - SummitIntStorage

Select target devices from list below:

- MCDC
- SITE-IEP
- SITE-K2MCIntStorage
- SummitDCstorage
- SummitIntStorage

⚠ Some devices are not listed because they are already members of other Deployment Groups.

4. In the Available Target Devices tree view, select the node that displays the devices that you are combining as a deployment group.
5. In the right-hand pane, select the devices that you are combining as a deployment group.

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

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

Distribute devices into deployment groups

You can gather devices of different types into a SiteConfig deployment group. This allows you to deploy software to all the devices in the deployment group at the same time, as part of the same deployment session. Based on the roles you have assigned to the devices, SiteConfig deploys the proper software to each device. This increases the efficiency of your software deployment with SiteConfig.

If you have not already done so, configure your deployment groups. The recommended deployment group distribution is as follows. Depending on your system design, your system might not have all the device types listed.

- In a deployment group named "Aurora_Edit_Ingest_Playout", place the following devices:
  - Aurora Edit workstation of any storage options: Shared storage, NAS storage, and stand-alone.
  - Aurora Edit LD computer
  - DSM
  - Conform Server
  - SmartBin Server
  - FTP Server
  - Aurora Ingest Platform
  - IEP
  - Aurora Playout Platform
- In a deployment group named "Aurora_Browse_MediaFrame", place the following devices:
  - MediaFrame server
  - MDI server
  - Aurora Proxy Encoder
  - K2 Basecamp Express
- If you have a K2 Nearline SAN (NAS), in a deployment group named for the SAN system, place the following devices:
  - The Nearline SAN's K2 Media Servers.

Install prerequisite files on the control point PC

Some software components, such as those for Aurora products, share common prerequisite software. You must install a prerequisite software package on the control point PC to make the prerequisite software available for software deployment to devices.

1. Check release notes for the required version of prerequisite files, if any.
2. On the SiteConfig control point PC, open Windows Add/Remove programs and look for **Grass Valley Prerequisite Files**, then proceed as follows:

    - If the required version of prerequisite files is installed, do not proceed with this task.
    - If prerequisite files are not installed or are not at the required version, proceed with this task.

3. Procure the required prerequisite software installation file. The file name is *Prerequisite Files.msi*.
4. On the SiteConfig control point PC, run the installation file. The installation program copies prerequisite files to *C:\Program Files\Grass Valley\Prerequisite Files*.

Prepare for installation

Before installing software, do the following:

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

Prepare SiteConfig for software deployment

1. Make the following files accessible to the SiteConfig control point PC:

    - AuroraSuite software installation (**.cab*) file
    - AuroraEditLD software installation (**.cab*) file
    - NewsShare software installation (**.cab*) file
    - ConformServer software installation (**.cab*) file
    - Generic iSCSI software installation (**.cab*) files
    - GVGMLib software installation (**.cab*) file
    - PCmonitoring software installation (**.cab*) file

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

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

    b) Install the new version of SiteConfig on the control point PC.

Upgrade K2 systems

Prerequisites for this task are as follows:

- If upgrading a K2 SAN, all SAN clients must be offline (all media access stopped) or shut down. Depending on your system design, this could include devices such as K2 clients, K2 appliances, Aurora Proxy (Advanced) Encoders, MDI server, Aurora Edit clients, Aurora Ingest clients, Aurora Playout clients, and generic clients.

  Upgrade your K2 systems to the compatible version of K2 system software. This includes K2 SAN systems and stand-alone K2 Media Client and K2 Summit Production Client systems. Refer to *K2 Release Notes* for procedures.

Set up K2 Aurora FTP

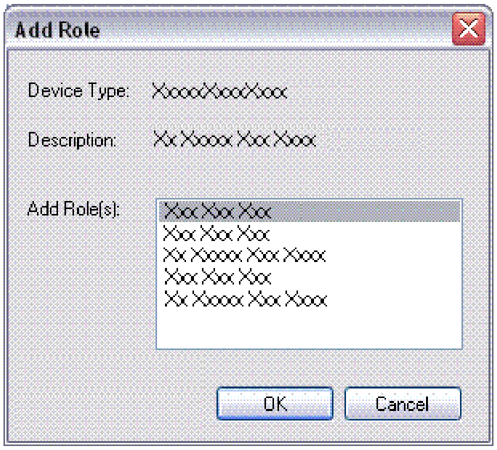
Do the following tasks if you use K2-Aurora FTP.

Adding K2-Aurora FTP software role to K2 Media Server

Use the following SiteConfig procedure to add the **K2-Aurora FTP** role to the K2 Media Server that you use as your K2-Aurora FTP server, if you have not already done so. The K2 Media Server that you use as your K2-Aurora FTP server must also have the role of K2 FTP Server.

1. In the **Software Deployment | Devices** tree view, right-click the device and select **Add Role**.

   The Add Role dialog box opens.



Add Role

Device Type: XxxxXxxxXxxx

Description: Xx Xxxxx Xxx Xxxx

Add Role(s):
Xxx Xxx Xxx
Xxx Xxx Xxx
Xx Xxxxx Xxx Xxxx
Xxx Xxx Xxx
Xx Xxxxx Xxx Xxxx

The Add Role dialog box displays only those roles that SiteConfig allows for the selected device type.

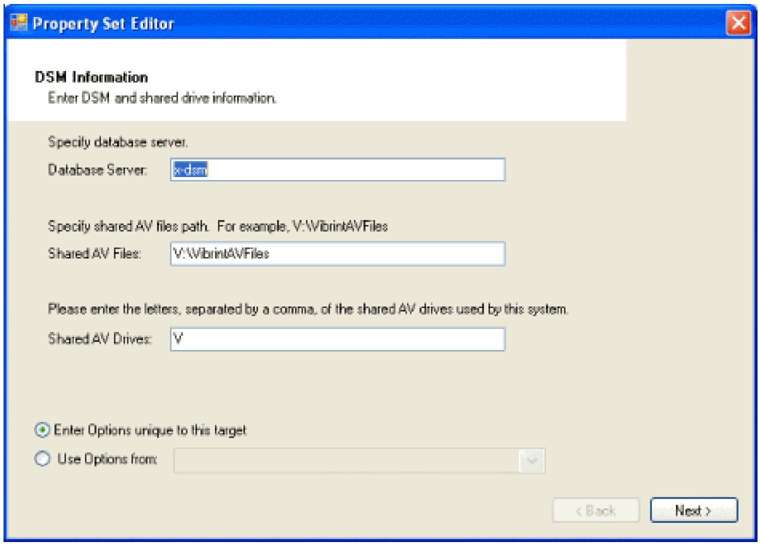
2. Select the role or roles that you want to add to the device. Use Ctrl + Click or Shift + Click to add multiple roles.
3. Click **OK** to save settings and close.

   The new role or roles appear under the device in the tree view.

Install and configure K2-Aurora FTP

1. In SiteConfig, check software on the the deployment group that contains your K2 Media Servers.
2. In SiteConfig, add the *K2AuroraFTP_x.x.x.xxx.cab* file to the deployment group that contains your K2 Media Servers.
3. Proceed with next steps to set deployment options for K2-Aurora FTP software.
4. Do one of the following to set deployment options:
   - Double-click the task.
   - Select the task and click the **Options** button.

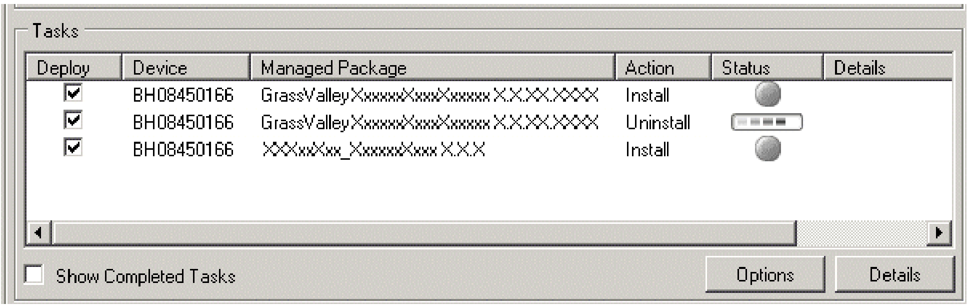
   A wizard opens.
5. Work through the wizard and set deployment options as follows:

Software	Deployment options
K2-Aurora FTP	 Property Set Editor **DSM Information** Enter DSM and shared drive information. Specify database server. Database Server: x-dsm Specify shared AV files path. For example, V:\VibrintAVFiles Shared AV Files: V:\VibrintAVFiles Please enter the letters, separated by a comma, of the shared AV drives used by this system. Shared AV Drives: V ● Enter Options unique to this target ○ Use Options from: < Back Next > Enter Database server(DSM), Shared AV Files, Shared AV Drives.

6. Deploy the following tasks:

Deploy	Managed Package	Action
✓	K2-Aurora FTP x.x.x.xxx	Uninstall (if upgrading K2-Aurora FTP)
✓	K2-Aurora FTP x.x.x.xxx	Install

7. Click the **Start Deployment** button.



Tasks

Deploy	Device	Managed Package	Action	Status	Details
☑	BH08450166	GrassValleyXxxxxXxxxXxxxxx X.X.XX.XXXX	Install	●	
☑	BH08450166	GrassValleyXxxxxXxxxXxxxxx X.X.XX.XXXX	Uninstall	▭	
☑	BH08450166	XXXxxXxx_XxxxxXxxx X.X.X	Install	●	

8. When the Status or Details columns indicate next steps, identify the software in the row, then proceed as follows:
   - For K2 software, when Details displays a **Restart required** link, click the link and when prompted "...are you sure...", click **Yes**.
   - If the Details column does not prompt you, restart the K2 Media Server manually.

   The K2 Media Server restarts. This restart is required.
9. On the K2 Media Server, to enable port range limits for passive transfers, create the following two DWORDs in the registry at HKEY_LOCAL_MACHINE/SOFTWARE/Grass Valley Group/Streaming/:
   - FtpPasvStart (starting port number, inclusive : DWORD)
   - FtpPasvEnd (ending port number, inclusive : DWORD)
10. Open MediaFrame Configuration and for the News MDI, configure the transfer server to the K2 Media Server that is your K2-Aurora FTP server.

Distribute devices into deployment groups

You can gather devices of different types into a SiteConfig deployment group. This allows you to deploy software to all the devices in the deployment group at the same time, as part of the same deployment session. Based on the roles you have assigned to the devices, SiteConfig deploys the proper software to each device. This increases the efficiency of your software deployment with SiteConfig.

If you have not already done so, configure your deployment groups. The recommended deployment group distribution is as follows. Depending on your system design, your system might not have all the device types listed.

- In a deployment group named "Aurora_Edit_Ingest_Playout", place the following devices:
  - Aurora Edit workstation of any storage options: Shared storage, NAS storage, and stand-alone.
  - Aurora Edit LD computer
  - DSM
  - Conform Server
  - SmartBin Server
  - FTP Server
  - Aurora Ingest Platform
  - IEP
  - Aurora Playout Platform
- In a deployment group named "Aurora_Browse_MediaFrame", place the following devices:
  - MediaFrame server
  - MDI server
  - Aurora Proxy Encoder
  - K2 Basecamp Express
- If you have a K2 Nearline SAN (NAS), in a deployment group named for the SAN system, place the following devices:
  - The Nearline SAN's K2 Media Servers.

Manually install software

Some tasks that might be required are not supported for SiteConfig management and/or software deployment. For these tasks you must manually install and/or configure before using SiteConfig to install software. Refer to the tasks in this section as appropriate for your system.

Install Microsoft SQL Server 2005 Standard Edition

Microsoft SQL Server 2005 Standard Edition is installed on devices as follows:

- Aurora DSM – SQL Server 2005 Standard Edition is required.

Use the following steps to manage Microsoft SQL Server 2005 Standard Edition.

Determine if you have Microsoft SQL Server 2005 Standard Edition installed and then do one of the following:

- If installed, check version compatibility information in release notes and if an upgrade is required, go to the local device and upgrade Microsoft SQL Server 2005 Standard Edition.
- If not installed, install Microsoft SQL Server 2005 Standard Edition as directed by the Microsoft product documentation.

Configuring SQL Server

SQL server software must be installed on the DSM (Data System Manager) using the procedure given below.

1. Select **Start | Programs | Microsoft SQL Server | Enterprise Manager**.
2. Expand the Tree view to reveal the DSM machine by clicking the "+" next to "Microsoft SQL Servers" and also next to "SQL Server Group."
3. Right click on the DSM icon and select **Properties**. (Except as noted in the following steps, do not change default values.)
4. Click the Security tab. Under Authentication, make sure that **SQL Server and Windows** is selected.
5. Click the Memory tab and verify that **Dynamically configure SQL Server memory** is selected. Set the memory limit to 256 MB less than the server's memory size.
6. Click **OK** to save settings and close the SQL Server Properties dialog box.

Check all currently installed software

Prerequisites for this task are as follow:

- The device is assigned in the SiteConfig system description and network connectivity is present.
- SiteConfig is able to log in to the device using the username/password credentials assigned to the device.
- The SiteConfig control point PC does not have a network drive mapped to an administrative share (such as C$) on a device on which you are checking software.
- If the SiteConfig Network Configuration Kit and/or Discovery Agent at version lower than 1.1.0.185 is currently installed, it must be manually uninstalled and updated. For more information refer to *SiteConfig Migration Instructions*.
- If Aurora product software at a version lower than 6.5.2 is currently installed, it must be manually uninstalled. For more information refer to *SiteConfig Migration Instructions*.

Do the following steps on the devices on which you are installing software.

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

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

   The Check Software dialog box appears. SiteConfig searches for software on the selected device or devices and gathers information. Progress is reported.
2. When the check is complete for the selected device or devices, close the Check Software dialog box.

An updated list of all currently installed software is displayed in the **Software Deployment | Devices | Installed Software** list view. If software is a SiteConfig managed software package, information is displayed in the Managed Package and Deployment Group columns.

Add software package to deployment group

Prerequisites for this task are as follows:

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

Use the following procedure to add one or more software package installation files to the deployment group that contains the devices in the following list. Depending on your system design, you might not have all of the device-types listed:

- Aurora Edit Workstation
- Aurora Edit LD computer
- DSM
- Conform Server
- SmartBin Server
- FTP Server

Identify and add software package installation files as follows:

Software	**File name**
Aurora Suite	*AuroraSuite_*x.x.xxx*.cab*
Aurora Edit LD	*AuroraEditLD_*x.x.xxx*.cab*
NewShare	*NewsShare_*x.x.xxx*.cab*
Conform server	*ConformServer_*x.x.xxx*.cab*
Grass Valley Windows Monitoring SNMP agent	*PCMonitoring_*x.x.xxx*.cab*

Depending on the K2 software version of your K2 SAN, also add software package installation files as follows:

NOTE: Add files for either 3.x OR 7.x. Do not add files for both 3.x AND 7.x.

- If your devices access storage on a K2 software version 3.x K2 SAN, add software package installation files as follows:

Software compatible with 3.x K2 SAN	File name
Generic iSCSI client for 32 bit systems	*GenericISCI_x86_*3.x.xxx*.cab*
GVG MLib	*GVG_MLib_*3.x.xxx*.cab*

  SNFS is bundled with the Generic iSCSI cab file.

- If your devices access storage on a K2 software version 7.x K2 SAN, add software package installation files as follows:

Software compatible with 7.x K2 SAN	File name
Generic iSCSI client for 32 bit systems	*GenericISCI_x86_*7.x.xxx*.cab*
GVG MLib	*GVG_MLib_*7.x.xxx*.cab*

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

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

   SiteConfig adds the package to the deployment group.

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

Setting deployment options

Pre-requisites for this procedure are as follows:

- A software package has been assigned to the deployment group and applicable deployment tasks are now displayed in the Tasks area.

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

2. In the Tasks list view, view tasks and determine if you must set deployment options.

   Tasks that need to have deployment options set display in the Details column a message stating "Deployment options required."

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

3. Proceed with next steps to set deployment options for the following:

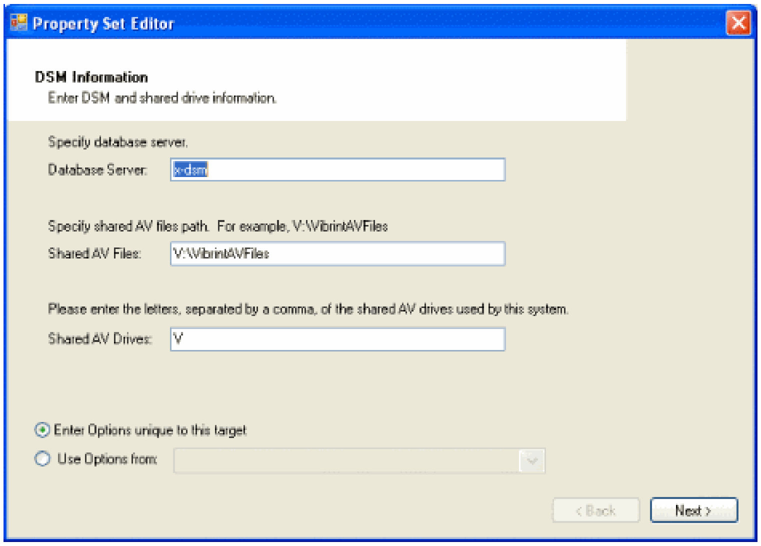
   - GVG_MLib
   - Conform Server
   - Aurora Edit LD

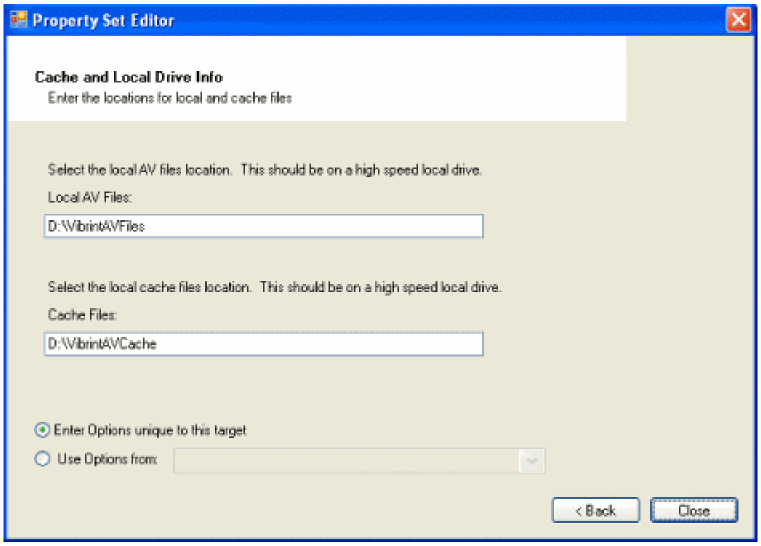
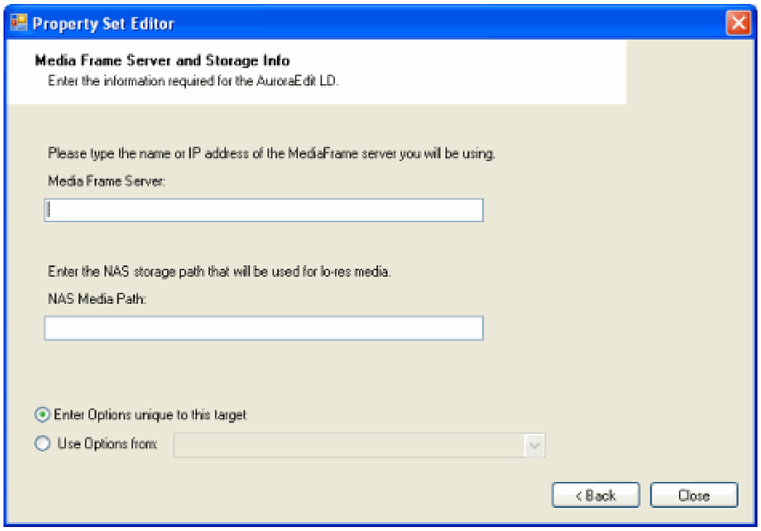
4. Do one of the following to set deployment options:

   - Double-click the task.
   - Select the task and click the **Options** button.

   A wizard opens.

5. Work through wizards and set deployment options as follows:

Software	Deployment options
GVG_MLib	Enter the name(s) of the K2 Media Server(s) with role of file system server (FSMs)
Conform Server	Database server, Shared AV Files (e.g. V:\xreAVFiles), Shared AV Drives, and the Media Frame Server
Aurora Suite	 Property Set Editor **DSM Information** Enter DSM and shared drive information. Specify database server. Database Server: x-dsm Specify shared AV files path. For example, V:\VibrintAVFiles Shared AV Files: V:\VibrintAVFiles Please enter the letters, separated by a comma, of the shared AV drives used by this system. Shared AV Drives: V ● Enter Options unique to this target ○ Use Options from: < Back Next > Enter Database server(DSM), Shared AV Files, Shared AV Drives.

Software	Deployment options
	 Property Set Editor **Cache and Local Drive Info** Enter the locations for local and cache files Select the local AV files location. This should be on a high speed local drive. Local AV Files: D:\VibrintAVFiles Select the local cache files location. This should be on a high speed local drive. Cache Files: D:\VibrintAVCache ● Enter Options unique to this target ○ Use Options from: Enter Local AV Files, Cache Files.
Aurora Edit LD	 Property Set Editor **Media Frame Server and Storage Info** Enter the information required for the AuroraEdit LD. Please type the name or IP address of the MediaFrame server you will be using. Media Frame Server: Enter the NAS storage path that will be used for lo-res media. NAS Media Path: ● Enter Options unique to this target ○ Use Options from: Enter MediaFrame Server and NAS Media Path.

6. If you have multiple devices of the same type, you can enter deployment options for one of them using the wizard. Then, when you bring up the same wizard on every device, you can choose the **Use options from** radio button and select the first device for which you set options.

SiteConfig copies the options you set for the first device and fills in the blanks on the wizard.

Install and configure software on a NewsShare System

Do not do these tasks if:

- You do not have any shared storage (NewsShare) Aurora Edit systems. Skip to the later task to install software on other Aurora Edit devices.

Do these tasks if:

- You have shared storage (NewsShare) Aurora Edit Workstations.
- You have one or more Conform Servers.
- You have SmartBins that require access to the shared storage and the SmartBin server that is not one of the above device.

You must install and configure software as instructed by the following tasks for these Aurora Edit device types.

Prerequisites for these tasks are as follows:

- The devices to which you are deploying software are in a deployment group.
- Prerequisite files are installed on the control point PC.
- You have recently done the SiteConfig "Check Software" operation on the devices to which you are deploying software.

For shared storage Aurora Edit devices, you must use a specific sequence of installation and configuration tasks. The installation sequence is summarized as follows:

1. Install the software necessary for connection to shared storage on Aurora Edit devices.
2. Map the storage volume one of the following ways:
   - If NAS storage, mount the NAS volume on Aurora Edit devices.
   - If K2 SAN storage, add all SAN connected devices to the SAN using K2 Config.
3. Install Aurora Suite software.

Use the following tasks to accomplish this sequence.

Install storage software on shared storage devices

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

   The corresponding software deployment tasks are displayed in the Tasks list view.
2. For the software you are installing, select the **Deploy** check box in the row for the install task.

Install software as follows:

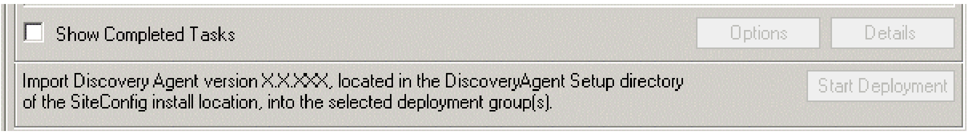
Deploy	Managed Package	Action
✓	GenericISCI x86 xxxx.xxxx (version must be compatible with K2 SAN)	Install
✓	GVGMLib xxxx.xxxx (version must be compatible with K2 SAN)	Install
✓	PCmonitoring xxxx.xxxx	Install

Also, you must install SNFS, so deploy the following tasks at the same time. Make sure you install the version of SNFS that is compatible with your K2 systems.

Deploy	Managed Package	Action
✓	SNFS nonK2 x86 x.x.x.xxx	Install

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

3. Check the area next to the Start Deployment button for a message.



□ Show Completed Tasks

Import Discovery Agent version X.X.XXX, located in the DiscoveryAgent Setup directory of the SiteConfig install location, into the selected deployment group(s).

If a message instructs you to upgrade the Discovery Agent, on the control point PC go to the directory to which SiteConfig is installed, find the `DiscoveryAgent_x.x.x.x.cab` file, add it to the deployment group, and deploy the Discovery Agent software as well.

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

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

5. When the Status or Details columns indicate next steps, identify the software in the row, then proceed as follows:

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

The device restarts.

Next follow the task as appropriate to mount your shared storage, either NAS or K2 SAN storage.

Configuring devices for NAS

For each client machine and the Conform Server running the SmartBin Service, if applicable, you need to mount the NAS volume before installing the Aurora Suite software. In addition, if the client machines are used by more than one user login, you need to log in under each user account and mount the NAS volume.

Prerequisites for this task are as follows:

- GVMLib software is installed on the Aurora Edit devices.

1. On the machine you want to map the drive to, open **My Computer** and select **Tools | Map Network Drive**.
2. Select the NAS drive.
3. Type in the name of the NAS folder where the shared database resides.
4. Check the **Reconnect at login** checkbox.
5. Click **Finish**.

Configuring devices for K2 SAN storage

This section describes configuring devices to interface to K2 SAN storage.

Prerequisites for this task are as follows:

- Generic iSCSI, GVMLib, and SNFS software is installed on SAN connected devices.

1. Following the instructions in the *K2 SAN Installation and Configuration Manual*, do the following, if not set up already:
   a) Set up the Control Point PC.
   b) Run the K2 Config application to set up the K2 Server and Gigabit Ethernet switch.
   c) Connect all SAN clients to the K2 Server via the Gigabit Ethernet switch.
2. Use K2 Config to configure each device as a generic iSCSI client.

   Given the bandwidth that a client workstation is expected to use, the K2 network can load balance workstations’ iSCSI connections to the K2 storage system. You can estimate the required bandwidth using the following formula: **(Video Bit Rate in Mbps x Number of Streams) / 8**.

   a) Determine the highest bit rate you use on the Aurora Edit device.

      DV rates for NTSC and PAL are 28.8 Mbps for DV25, 57.6 Mbps for DV50, and 115.2 Mbps for DV100. MPEG bit rates are variable; use the configured bit rate.

b) Multiply the highest bit rate by the number of streams that are licensed on the workstation.

c) Divide that number by 8 to and round to the nearest integer to convert Mbps to MB.

d) Use the final MB number in the K2 Configuration wizard's iSCSI Client Bandwidth Input screen.

See the K2 documentation for complete instructions.

Install Aurora software on shared storage devices

Prerequisites for this task are as follows:

- Generic iSCSI, GVMLib, and SNFS software is installed on the devices.
- The shared storage is mounted on the devices.
- On a Conform Server, if you are using a Fibre Channel card, verify that the IP MTU uses the same setting as other Aurora Edit clients.

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

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

2. For the software you are installing, select the **Deploy** check box in the row for the install task.

   Install Aurora software as follows:

Deploy	Managed Package	Action
✓	AuroraSuite x.x.x.xxx	Install
✓	ConformServer x.x.x.xxx	Install
✓	NewsShare x.x.x.xxx	Install

3. Click the **Start Deployment** button.

   Deployment tasks run and software is uninstalled. Progress is reported and next steps are indicated in both the Status and Details columns. If an error appears regarding prerequisite software, install the prerequisite files on the control point PC and then repeat this step.

4. When the Status or Details columns indicate next steps, identify the software in the row, then proceed as follows:

   - If Details displays a **visible dialog pending** link, continue with this procedure.

5. Remote in to the machine and enter the appropriate information, as instructed in the next task. Once the dialog is dismissed SiteConfig continues with the install.

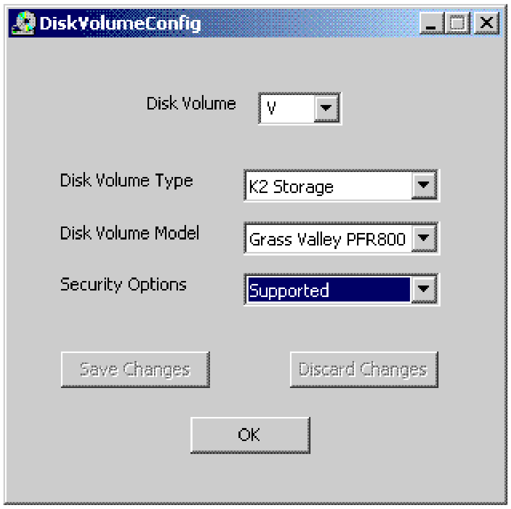
Configuring the Disk Volume

When you install Aurora Edit software for the first time, you must configure a shared volume for your type of network and equipment wherever the AuroraSuite installer is run. The Disk Volume Configuration only needs to be done once on each shared volume, on the first Aurora Edit system on which the software is installed.

Prerequisites for this task are as follows:

- Generic iSCSI, GVMLib, and SNFS software is installed on the Aurora Edit workstations.
- The shared storage is mounted on the Aurora Edit workstations.
- The installation process for Aurora Suite software is underway.

To configure the disk volume refer to the illustration and table below:



DiskVolumeConfig

Disk Volume: V

Disk Volume Type: K2 Storage

Disk Volume Model: Grass Valley PFR800

Security Options: Supported

1. Select the disk volume drive letter in the pulldown and configure the volume as follows:

Setting	Options	Description
Disk Volume Type	**Unknown** **LocalDisk** **NAS** **K2 Storage** **Open SAN**	Select your type of shared storage.

Setting	Options	Description
Disk Volume Model	**Unknown**	NAS:
	Grass Valley PFR500, PFR600, PFR700, PFR800	Choose **Ciprico 1700, 2400, 3600, or IBM NAS**.
	Ciprico 1700, 2400, 3600	K2 Storage:
	IBM NAS	Choose **Grass Valley PFR700**.
Security Options	**Supported** **Not Supported**	Select **Supported** if your system uses Domain Security; otherwise, select **Not Supported**.

2. Click **OK** to save changes and return to the software installer.

   When installing Aurora Suite using SiteConfig, continue with the following steps.

3. When the Status or Details columns indicate next steps, identify the software in the row, then proceed as follows:

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

   The device restarts.

Install software on other Aurora Edit devices

Do not do this task if:

- You are install software on shared storage (NewsShare) Aurora Edit workstations. Use the previous task instead.

Do this task if:

- You are installing software on the following types of the devices:
  - Stand-alone Aurora Edit workstation
  - Aurora Edit LD computer
  - DSM
  - SmartBin Server
  - FTP Server

Prerequisites for this task are as follows:

- The devices to which you are deploying software are in a deployment group.
- Prerequisite files are installed on the control point PC.

- You have recently done the SiteConfig "Check Software" operation on the devices to which you are deploying software.

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

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

2. For the software you are deploying, select the **Deploy** check box in the row for the uninstall task.

   NOTE: If you manually uninstalled or installed software, the uninstall task might not appear or it might appear with a different package name.

3. For the software you are installing, select the **Deploy** check box in the row for the install task.

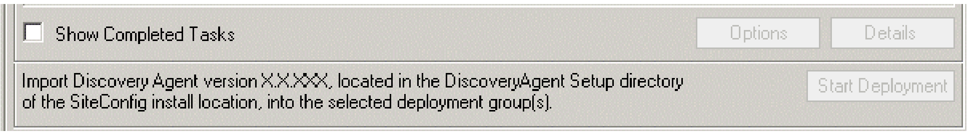
   For installing software on Aurora Edit devices, deploy the following tasks:

Deploy	Managed Package	Action
✓	AuroraSuite x.x.x.xxx	Install
✓	AuroraEditLD x.x.x.xxx	Install
✓	NewsShare x.x.x.xxx	Install
✓	GVGMLib xxxx.xxxx (version must be compatible with K2 SAN)	Install
✓	PCmonitoring x.x.x.xxx	Install

Deploy	Managed Package	Action
✓	SNFS nonK2 x86 xxxx.xxxx (version must be compatible with K2 SAN)	Install

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

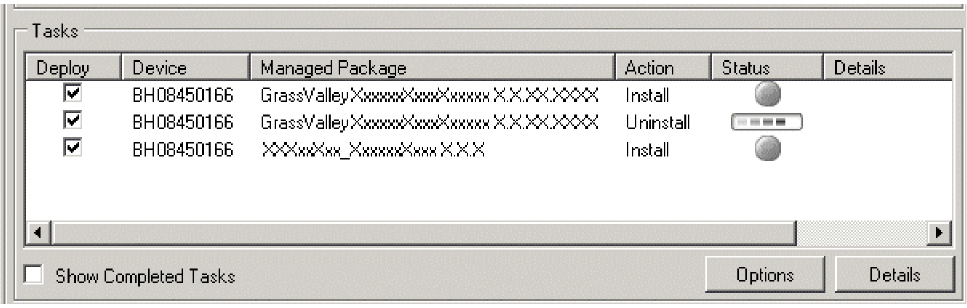
4. Check the area next to the Start Deployment button for a message.



Import Discovery Agent version X.X.XXX, located in the DiscoveryAgent Setup directory of the SiteConfig install location, into the selected deployment group(s).

If a message instructs you to upgrade the Discovery Agent, on the control point PC go to the directory to which SiteConfig is installed, find the `DiscoveryAgent_x.x.x.x.cab` file, add it to the deployment group, and deploy the Discovery Agent software as well.

5. Click the **Start Deployment** button.



Deploy	Device	Managed Package	Action	Status	Details
☑	BH08450166	GrassValleyXxxxxXxxxXxxxxx X.X.XX.XXXX	Install	●	
☑	BH08450166	GrassValleyXxxxxXxxxXxxxxx X.X.XX.XXXX	Uninstall	▭	
☑	BH08450166	XXXxxXxx_XxxxxXxxx X.X.X	Install	●	

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

6. When the Status or Details columns indicate next steps, identify the software in the row, then proceed as follows:
   - For K2 software, when Details displays a **Restart required** link, click the link and when prompted "...are you sure...", click **Yes**.

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

Chapter 5

Manually Installing Aurora Edit and LD Software

This section contains the following topics:

- *Manually Installing Aurora Edit/Aurora Edit LD Software*
- *Third Party Software Installation*

Manually Installing Aurora Edit/Aurora Edit LD Software

If you are not using SiteConfig to install software, this section describes the steps to install the Aurora Edit and Aurora Edit LD applications manually.

The Aurora Edit software is available on the CD included with the application.

1. Uninstall any previous version of Aurora Edit software using the Windows **Add or Remove Programs** program in Start/Settings/Control Panel.
2. Find the AuroraSetup directory on the CD provided and double-click on Setup.exe.

   Wait for the Aurora Suite Installation Wizard to appear.
3. When the Welcome screen appears, select **Next>**.
4. Review the License agreement and click **I accept the license agreement** and **Next>**.
5. Click the **X** next to Aurora Edit or Aurora Edit LD and select **Entire feature will be installed on local hard drive**.

   Click **Next>**.
6. If you are installing a local Aurora Edit workstation, select **Local** and click **Next>**.

   For a **Local** install, skip to step 13.
7. If you are installing a shared Aurora Edit or Aurora Edit LD, select **Shared** and click **Next>**.

   In the **Select Shared Server** field, enter the name of the database server that you are using for the **Shared** database and select **Next>**.
8. In the **Select Shared AV Files Directory**, select the directory where the Aurora Suite Video and Audio files are to be saved. This should be a directory located on a high speed AV disk drive.

   Click **Next>** to accept the default directory, **V:\VibrintAVFiles** or select the main shared AV files location you plan on using.
9. In the **Select Local AV Files Directory**, select the directory where the local Aurora video and audio files are to be saved. This should be a directory located on a high speed AV disk drive, on your local system.

   Click **Next>** to accept the default **D:\VibrintAVFiles**.
10. In the **Select AV Cache Files Directory**, select the directory where the Aurora AV Cache file are to be saved. This should be a directory located on a high speed AV disk drive, on your local system.

    Click **Next>** to accept the default **D:\VibrintCache**.
11. In the **Select Shared Drives** window, enter the letter drives, separated by a comma, of the shared AV drives used by the system.

    Select **Next>**.

12. For Aurora LD only, a **MediaFrame Server Settings** window will come up and ask for the name or IP address of the MediaFrame server you will be using. You must also enter the **NAS Media Path** for the NAS storage that will be used for media.

    Select **Next>**.

13. Click **Next>** to install the application.

    Wait for the install to completely finish. It will take a few minutes to complete.

Third Party Software Installation

Aurora Edit and Aurora Edit LD application interface with many third party products that are manufactured by other vendors (ENPS for example). Many of these products require installing plug-in or driver software. Refer to the *Aurora Edit and Aurora Edit LD Installation Manual* for instructions on installing software for any third party products. Many of these products may also include installation instructions. Be sure to use these instructions for proper installation. Please note it is very important to check the Compatible third party products software table in these release notes so you use the validated software or driver version required for this release.

Chapter 6

Aurora Edit Application Configuration

This section contains the following topics:

- *Setting Up Media Files for Sharing*
- *About Aurora Edit video sources*
- *Option Configurations*
- *Understanding the System Self-Test*

Setting Up Media Files for Sharing

Before you can transfer media files to another Aurora Edit workstation, you need to set up your workstation for sharing.

To share files:

1. In Windows Explorer, navigate to the drive where media files are stored (usually D:\).
2. Right click on the VibrintAVFiles folder and choose Sharing.
3. Select the Shared As option and leave the default share name VibrintAVFiles.

   Click **OK**.

The folder you shared appears with the standard Windows sharing icon.

About Aurora Edit video sources

Before using footage from a particular source, you need to add the source to the Aurora Edit source list. Aurora Edit pre-installs two sources for you — a video source and a clip source:

Video source	Allows you to record footage directly into the Timeline or Bin; usually a tape deck.
Clip source	Allows you to edit a clip as a Timeline source directly in the Bin, which is useful for large clips so you don't have to go back and forth from a tape deck. You only need one clip source; you don't have to create a new clip source for each clip you want to use

Add Source—General settings

Setting	Options	Description
Source Name		Enter a name for the source, such as Tape Deck.
Description		Enter a description for the source.
Source Type	Video Source	Select Video Source for all incoming sources, including audio sources.
	Clip Source	Select Clip Source to use an existing clip in the bin as a source.
	Microphone	Select Microphone for any microphone sources.
	1394 Source	Select 1394 Source when connecting to a specific 1394 source if multiple IEEE devices are present.

Add Source—Connections settings

The options available depend upon your Source Type setting on the General tab.

Setting	Options	Description	Source Type
Video Input	Composite Component SDI S-Video (Y/C)	Select the Video Input option that corresponds to the source's connection to Aurora Edit.Composite is the default video input.	Video Source Clip Source
1394 Input	Any <Device Name>	Select the 1394 device you are using.	1394 Source
Audio Input	Balanced Analog AES/EBU (BNC) AES/EBU (XLR) SDI/Embedded	Select the Audio Input option that corresponds to the source's connection to Aurora Edit. Balanced Analog is the default audio input.	Video Source Clip Source
	Mic Preamp	Default setting for a Microphone Source.	Microphone
Deck Protocol	No remote deck controls Sony 422 Protocol Sony DNW-A100 DV 1394	Select the Deck Protocol that corresponds to the type of tape deck control you are using with Aurora Edit. If you are adding a clip source, video router, or a non-video source, select No remote deck controls, which is the default setting.	Video Source Clip Source Microphone 1394 Source
Comm Port	None COM1 - COM10	Select the Comm Port you are using to connect the source to Aurora Edit.	Video Source Clip Source Microphone 1394 Source
Input Latency		Enter a duration to add an input latency when using a 1394 converter.	Video Source Clip Source Microphone 1394 Source
Number Loop Tones		Enter a duration to set how many seconds exist between loop record takes; each second, a tone plays through the system speakers.	Microphone

Add Source—Record Channels settings

Setting	Options	Description
Video		Check **Video** if you want to record video with this source.
Channel 1 Audio	A1 to A8	Check each audio channel that should record audio from this source and select the default audio track (A1–A8) on the Timeline to which you want the channel routed.
Channel 2 Audio	A1 to A8	
Channel 3 Audio	A1 to A8	
Channel 4 Audio	A1 to A8	

Setting up a microphone source that does not record video (audio-only record) greatly reduces the required disk space.

Add Source—Record Handles settings

Setting	Description
In Handles Out Handles	Enter the number of seconds for the In and Out Handle length. Handles provide the extra frames necessary to trim or add transition effects at the head or tail of a clip. When you Mark In and Mark Out, Aurora Edit begins recording the specified number of seconds before your Mark In and after your Mark Out. Only the material between your marks is edited to the Timeline

Add Source—Preroll settings

Setting	Description
Get Preroll From Deck	Check **Get Preroll From Deck** to use the preroll settings from your tape deck instead those configured in Aurora Edit.
Preroll	Enter the number of seconds of preroll to use when recording from this source. This setting overrides the source’s Preroll setting unless you check **Get Preroll From Deck**.
Aux Preroll	Enter the number of seconds of auxiliary preroll you want to use when using an auxiliary input or a non-remote source.

Option Configurations

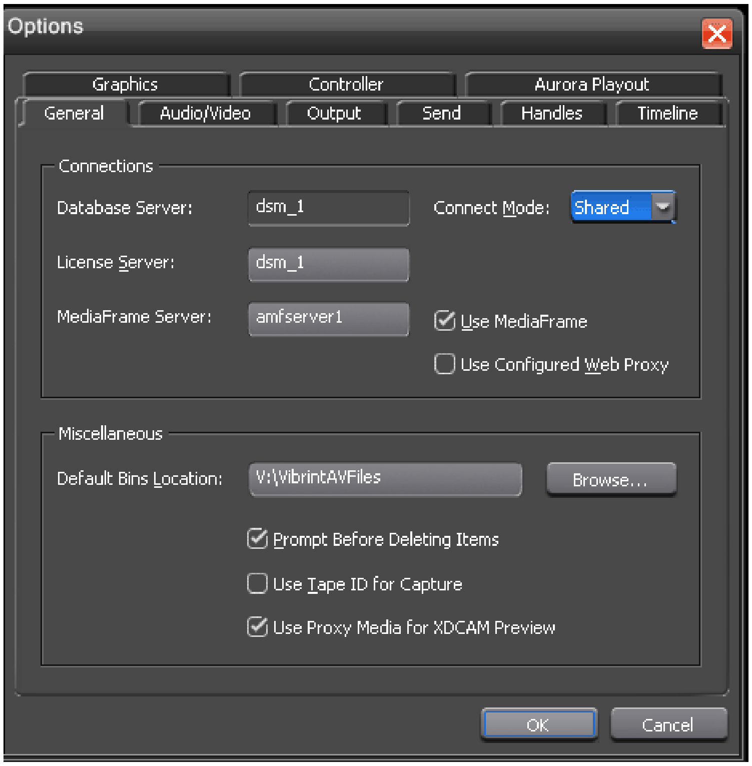
In the **Tools** main menu, use the **Options** pulldown to configure Aurora Edit options for your optional and external hardware and workflow:

The tabs included under the **Options** pulldown are summarized below:

- **General** tab: Set server connections and miscellaneous settings.
- **Audio/Video** tab: Set video standard, format, NTSC timecode, compression type, bit rate, chroma format, and audio format.
- **Output** tab: When the Breakout Box (BOB) option is present, define analog audio connectors and aspect ratio of SDI BNC out.
- **Send** tab: Set Send locations for completed sequences.
- **Handles** tab: Set handle durations for various file functions.
- **Timeline** tab: Set timeline choices for input/output channels, digital reference level, default mix routing and other timeline functions.
- **Graphics** tab: Enable or disable the Orad graphics functionality.
- **Controller** tab: Set COM port for external controllers (if used).
- **Aurora Playout** tab: Set Primary/Backup and XMOS servers for Aurora Playout.

Options—General (Aurora Edit)

The first Options tab for Aurora Edit provides general Connections and Miscellaneous settings. The various items to be configured are shown in the screen illustration and described in the table below.



Connections

Database Server: dsm_1

Connect Mode: Shared

License Server: dsm_1

MediaFrame Server: amfserver1

☑ Use MediaFrame

☐ Use Configured Web Proxy

Miscellaneous

Default Bins Location: V:\VibrintAVFiles

☑ Prompt Before Deleting Items

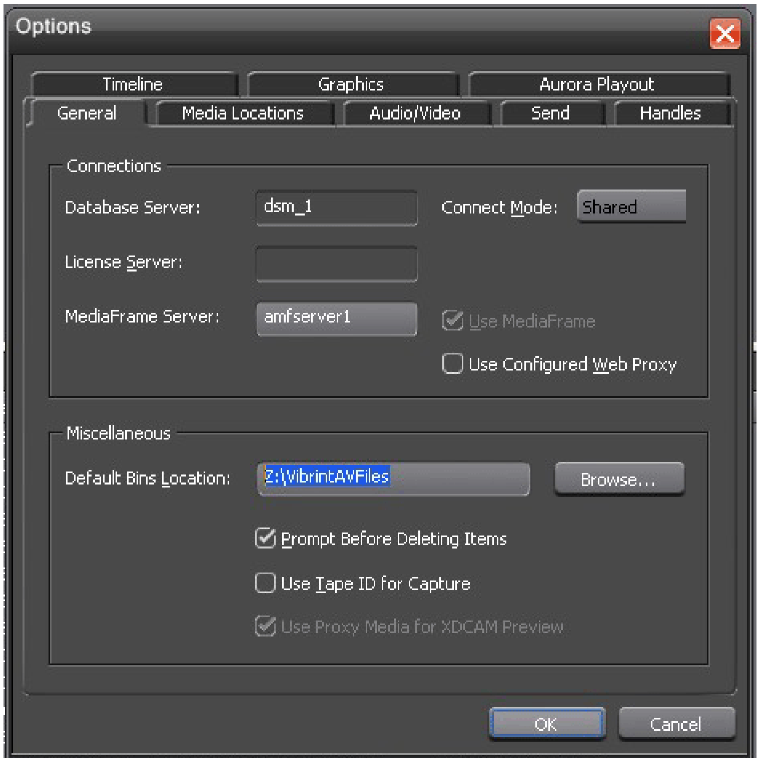
☐ Use Tape ID for Capture

☑ Use Proxy Media for XDCAM Preview

Setting	Options	Description
Database Server		Displays the name of the database server when the application is set up in shared mode.
Connect Mode	**Local** **Shared**	In the **Connect Mode** pulldown, select **Local** if you are using local disk storage and a local Aurora Edit database. You have access to files on your local machine only. Select **Shared** if you are using shared disk storage and a shared database. You share the Bin with all Aurora Edit workstations that are part of the network, according to security settings.
License Server		Enter the name of the server where the Aurora Sys and Aurora-GFX SabreTooth license resides.
MediaFrame Server		Enter the name of the MediaFrame Server.
Use Media Frame		Select this checkbox to enable MediaFrame (you can uncheck it to disable MediaFrame without losing the server name. ***NOTE: Aurora Edit LD must be connected in Shared mode and use a MediaFrame server.***
Use Configured Web Proxy		This checkbox will become active when MediaFrame is turned on in the step above. When this checkbox is selected, the application will continue to go through the configured Web Proxy settings in order to communicate with MediaFrame services. When unselected, web calls through MediaFrame services will bypass the configured settings.
Default Bin Location		Enter the default path to your media files. You may use the **Browse** button to locate the server. ***NOTE: V:\VibrintAVFiles is the default location.***
Prompt Before Deleting Items		Select this checkbox to receive a confirmation prompt before deleting files. The setting is on by default.
Use Tape ID for Capture		Select this checkbox to identify which source tape a particular clip came from; used in the Source Tool. This setting is off by default.
Use Proxy Media for XDCAM Preview		Select this checkbox to view the low-resolution proxy for media when previewing XDCAM files; doesn’t affect HD media, which always uses proxy media for previewing. This setting is on by default.

Options—General (Aurora Edit LD)

The first Options tab for Aurora Edit LD provides general Connections and Miscellaneous settings. The various items to be configured are shown in the screen illustration and described in the table below.



Database Server: dsm_1

Connect Mode: Shared

License Server:

MediaFrame Server: amfserver1

☑ Use MediaFrame

□ Use Configured Web Proxy

Default Bins Location: Z:\VibrintAVFiles

☑ Prompt Before Deleting Items

□ Use Tape ID for Capture

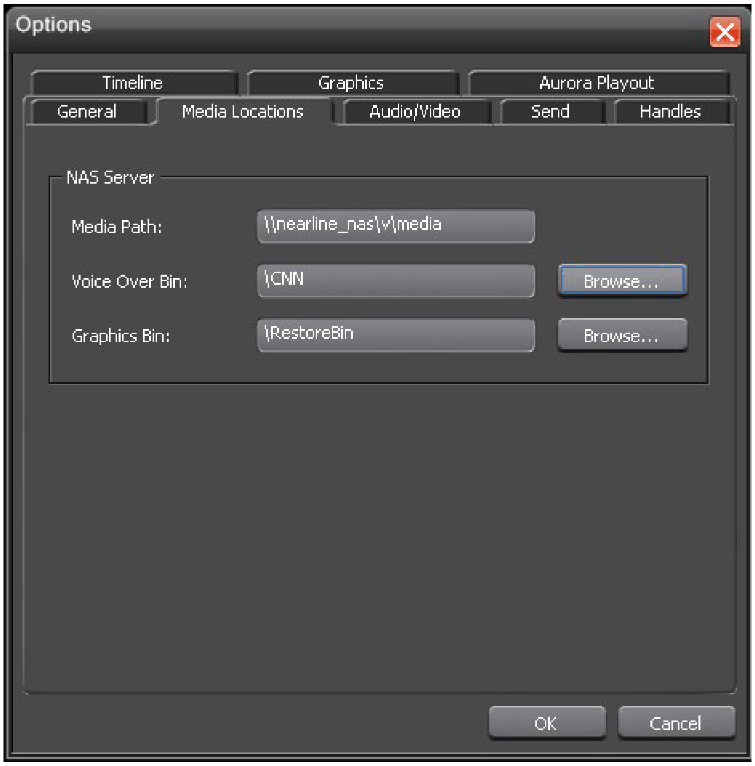
☑ Use Proxy Media for XDCAM Preview

Setting	Description
Database Server	Displays the name of the database server when the application is set up in shared mode.
Connect Mode	Aurora Edit LD is always in the **Shared** mode.
License Server	Enter the name of the server where the Aurora Sys and Aurora-GFX SabreTooth license resides.
MediaFrame Server	Enter the name of the MediaFrame Server.
Use Media Frame	Select this checkbox to enable MediaFrame (you can uncheck it to disable MediaFrame without losing the server name. ***NOTE: Aurora Edit LD must be connected in Shared mode and use a MediaFrame server.***
Use Configured Web Proxy	This checkbox will become active when MediaFrame is turned on in the step above. When this checkbox is selected, the application will continue to go through the configured Web Proxy settings in order to communicate with MediaFrame

Setting	Description
	services. When unselected, web calls through MediaFrame services will bypass the configured settings.
Default Bin Location	Enter the default path to your low resolution media files. You may use the **Browse** button to locate the server. Do not use the same directory as Aurora Edit (V:\VibrintAVFiles is this is default high resolution location for Aurora Edit). The Z:\ drive is used in this example.
Prompt Before Deleting Items	Select this checkbox to receive a confirmation prompt before deleting files. The setting is on by default.
Use Tape ID for Capture	Select this checkbox to identify which source tape a particular clip came from; used in the Source Tool. This setting is off by default.
Use Proxy Media for XDCAM Preview	Select this checkbox to view the low-resolution proxy for media when previewing XDCAM files; doesn't affect HD media, which always uses proxy media for previewing. This setting is on by default.

Options—Media Locations (Aurora Edit LD)

Use this tab to set the media locations required for the NAS server for Aurora Edit LD.



NAS Server

Media Path: \\nearline_nas\v\media

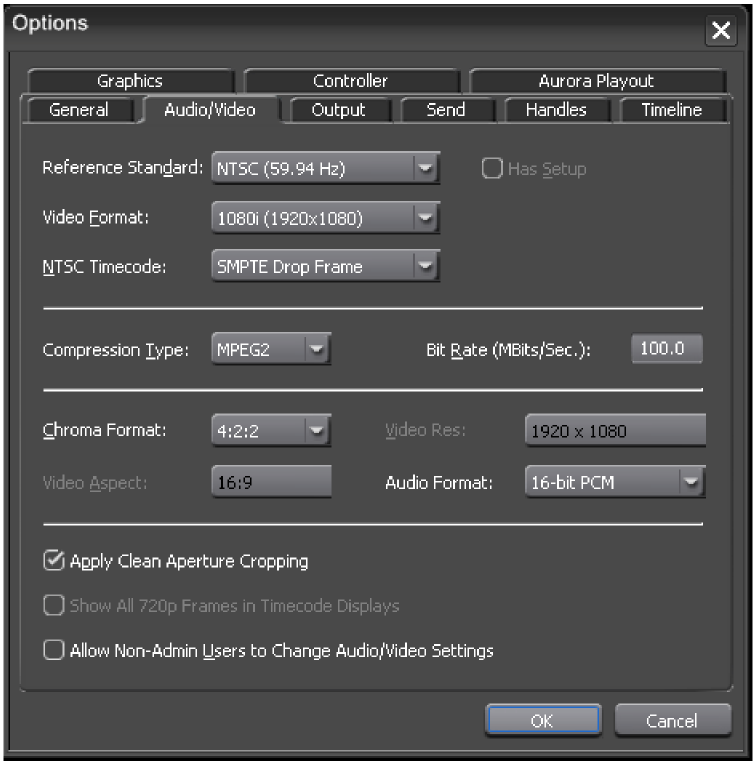
Voice Over Bin: \CNN

Graphics Bin: \RestoreBin

Setting	Description
Media Path	Enter the path to the NAS server
Voice Over Bin	Enter the directory on the NAS server for the Voice Over bin.
Graphics Bin	Enter the directory on the NAS server for the Graphics bin.

Options—Audio/Video Settings

Use this tab to set overall audio and video configuration for the system.



Reference Standard: NTSC (59.94 Hz)

□ Has Setup

Video Format: 1080i (1920x1080)

NTSC Timecode: SMPTE Drop Frame

Compression Type: MPEG2

Bit Rate (MBits/Sec.): 100.0

Chroma Format: 4:2:2

Video Res: 1920 x 1080

Video Aspect: 16:9

Audio Format: 16-bit PCM

☑ Apply Clean Aperture Cropping

□ Show All 720p Frames in Timecode Displays

□ Allow Non-Admin Users to Change Audio/Video Settings

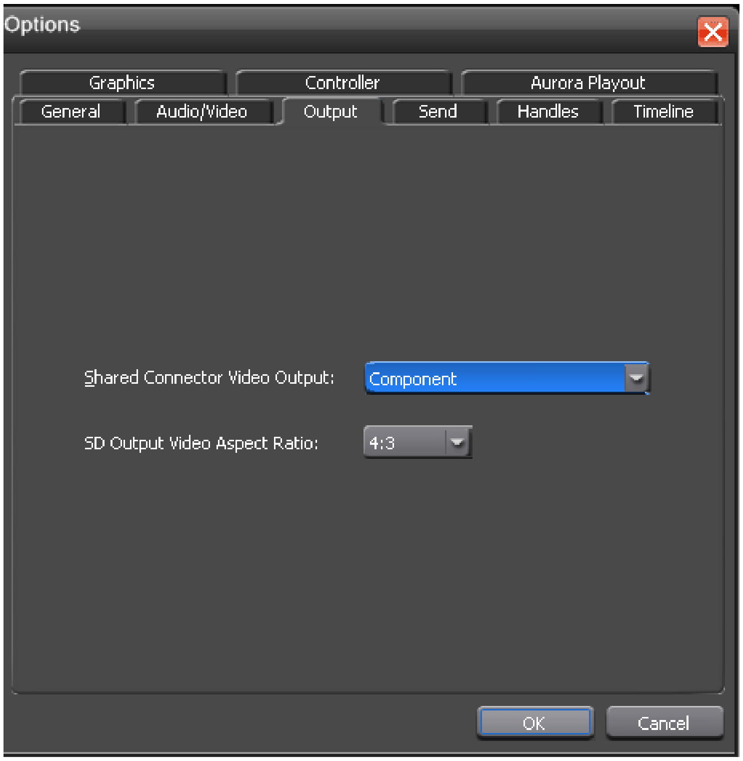
Setting	Options	Description
Reference Standard	NTSC (59.94 Hz) or PAL (50.00 Hz)	Select the Reference Standard you are using NTSC (default setting) has a frame rate of 29.97 frames/second and is used primarily in the Americas and Japan. PAL has a frame rate of 25 frames/second and is used in Europe, most of Asia, and Australia.
Has Setup		Select the **Has Setup** check box if the analog composite signal carries setup information.
Video Format	480i (SD) or 576i (SD) then	Select 480i Video Format for an interlaced (i) standard definition (SD) television format (default setting) for NTSC; select 576i for PAL. Select 720p for a progressive (p), high

Setting	Options	Description
	720p (1280x720) or 1080i (1920x1080)	definition (HD) television format. Select 1080i for an interlaced, high definition television format.
NTSC Timecode	SMPTE - Drop Frame	Recommended setting to avoid the time slipping problems associated with non-drop frame; default setting.
	SMPTE - Non-drop Frame	Standard format used to represent timecode.
Compression Type	MPEG2	MPEG2 is the default compression type available in all formats.
	IMX30	Available in NTSC 480i (SD) and PAL 576i (SD) video formats.
	IMX40	
	IMX50	
	DV25	
	DV50	
	DV100	
	AVCI-50	
	AVCI-100	
Bit Rate MBits/Sec	4-50 MBits/Sec	Enter the Bit Rate specified by your system administrator. 50 mbits is the default setting. More than 25 mbits is optional.
Chroma Format	4:1:1	The 4:1:1 Chroma Format is selected if you use DV25 compression.
	4:2:0	Select the 4:2:0 or 4:2:2 Chroma Format if you use MPEG2 compression.
	4:2:2	Select the 4:2:2 Chroma Format if you use DV50 or MPEG2 compression—4:2:2 offers more color resolution than 4:2:0 with MPEG2; this is the default setting.
Video Aspect	4:3	Select 4:3 Video Aspect for a standard definition (SD) television format; default setting.
	16:9	Select 16:9 Video Aspect for a high definition (HD) television format.
Video Resolution	720 x 512	Select for NTSC systems using MPEG2 compression.
	720 x 480	Select for NTSC systems using DV25, DV50, or MPEG2 compression; default setting.
	720 x 576	Select for PAL systems using DV25, DV50, or MPEG2 compression.

Setting	Options	Description
	720 x 608	Select for PAL systems using MPEG2 compression.
Audio Format	16-Bit PCM	The Aurora Edit application bit depth may be set for 16- or 24-bit . Both 16- and 24-bit audio can be mixed and matched in the same Timeline. Records will take on the bit depth of the configured setting, but media imports will preserve the current depth of the source media. Sending will flatten audio to the bit depth of the sequence.
	24-Bit PCM	
Apply Clean Aperture Cropping		By default, Aurora Edit automatically trims a small amount of video around the edges of a frame to ensure a clean image. This setting is on by default. Leave this option selected for SD video; setting is optional for HD video.
Show All 720p Frames in Timecode Displays		When using the 720p video format, select this checkbox to display all timecode in Aurora Edit as 60/50 frames per second. When unselected, timecode displays in the standard 30/25 frames per second format. This setting is off by default.
Allow Non-Admin Users to Change Audio/Video Settings		Select this checkbox to allow all users to change audio or video settings. This option is off by default.

Options—Output

The tab includes configuration for optional analog video connections from the optional Breakout Box (BOB) and system aspect ratio setting.



Shared Connector Video Output: Component

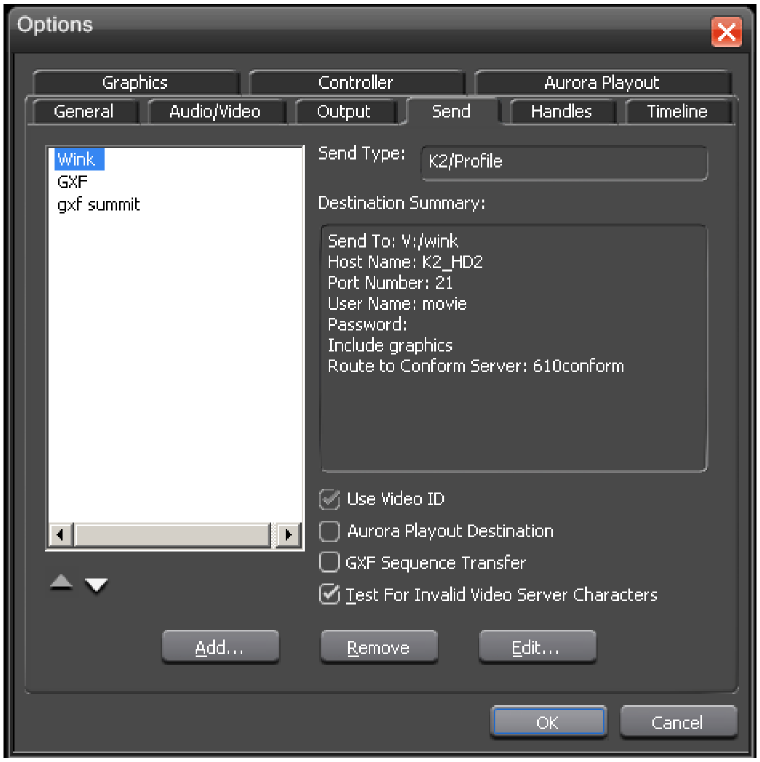
SD Output Video Aspect Ratio: 4:3

Setting	Options	Description
Shared Connector Video Output	Component Composite and Y/C	Select the Video Connection option that corresponds to the video source's connection to Aurora Edit through the optional Breakout box (BOB). Component is the default setting.
SD Output Video Aspect Ratio	4:3 16:9	Select the video aspect ratio for output. 4:3 is the default aspect ratio.

Options—Send

After completing a sequence you can send it to a playout machine or to a network video server. To send completed sequences or individual clips, you first need to configure Aurora Edit with each of your send locations.

A send location can be another Aurora Edit workstation, a Media Server, or a Bin you specify. If you want to store completed sequences on your computer, you can also add a send location for your PC.



1. Click **Add**.

   The **Add Named Destination to Send List** window appears.
2. Enter the name of the send location.
3. Select the type of location from the drop-down list:

Send Type	Description
Vibrint	Select **Vibrint** when the send location is another Aurora Edit, FeedClip, or an Aurora Playout system.
K2	Select **K2** when the send location is a K2 Server or an M-Series iVDR.
Publish	Select when you want to transfer sequences.
GXF ftp	Select **GXF ftp** to send the completed sequence as a GXF stream which can be used for a generic FTP site.
GXF file	Select **GXF file** to send the completed sequence as a GXF file.
DV Video ES	Select **DV Video ES** to send the completed sequence as a DV video elementary stream; used for Publison NewsMix.

4. Configure the send location based on the location type:

Send Type	Option	Description
Vibrint	Use Video ID	Check Use Video ID if you will be linking to stories on a Newsroom Computer System (NRCS) that contain Video IDs. When you send an Aurora Edit sequence to this location, the system uses the Video ID for the name of the file that gets sent.
	Include Graphics	Check Include Graphics if you want all graphics to remain with the sequence.
	Send to	Click Browse and select the file destination path.
K2	Use Video ID	Check Use Video ID if you will be linking to stories on a Newsroom Computer System (NRCS) that contain Video IDs. When you send an Aurora Edit sequence to this location, the system uses the Video ID for the name of the file that gets sent.
	Include Graphics	Check Include Graphics if you want all graphics to remain with the sequence.
	Send to	Type in drive letter and destination folder; e.g., V: \ default.
	Host Name	Type in the host name of the destination server; e.g., K2-1.
	User Name	Automatically fills in as movie; leave as is.
	Password	Leave this field blank.
	Aurora Playout Destination	Check Aurora Playout Destination if this send location is an Aurora Playout server.
	Send as LGOP	Check Send as LGOP to send the Aurora Edit sequence as a GXF stream with MPEG2 LGOP compression. To adjust the MPEG options, click the Settings button.
Publish	Use Video ID	Check Use Video ID if you will be linking to stories on a Newsroom Computer System (NRCS) that contain Video IDs. When you send an Aurora Edit sequence to this location, the system uses the Video ID for the name of the file that gets sent.
	Send to	Click Browse and select the file destination path.
	Render All Effects	Check Render All Effects if you want all transitions and effects rendered before sending.
	Aurora Playout Destination	Check Aurora Playout Destination if this send location is an Aurora Playout server.
GXF FTP	Use Video ID	Check Use Video ID if you will be linking to stories on a Newsroom Computer System (NRCS) that contain Video IDs. When you send an Aurora Edit sequence

Send Type	Option	Description
		to this location, the system uses the Video ID for the name of the file that gets sent.
	Include Graphics	Check Include Graphics if you want all graphics to remain with the sequence.
	Send to	Click Browse and select the file destination path.
	Host Name	Enter the name of the server computer.
	User Name	Enter your user name.
	Password	Enter the password for the send location, if you have one.
	Send as LGOP	Check Send as LGOP to send the Aurora Edit sequence as a GXF stream with MPEG2 LGOP compression. To adjust the MPEG options, click the Settings button.
GXF File	Use Video ID	Check Use Video ID if you will be linking to stories on a Newsroom Computer System (NRCS) that contain Video IDs. When you send an Aurora Edit sequence to this location, the system uses the Video ID for the name of the file that gets sent.
	Include Graphics	Check Include Graphics if you want all graphics to remain with the sequence.
	Send to	Click Browse and select the file destination path.
	Send as LGOP	Check Send as LGOP to send the Aurora Edit sequence as a GXF stream with MPEG2 LGOP compression. To adjust the MPEG options, click the Settings button.
DV Video ES	Use Video ID	Check Use Video ID if you will be linking to stories on a Newsroom Computer System (NRCS) that contain Video IDs. When you send an Aurora Edit sequence to this location, the system uses the Video ID for the name of the file that gets sent.
	Include EDL For Sequence	Check Include EDL for Sequence if you want an EDL of the sequence sent to the same destination folder as the DV video elementary stream.
	Send to	Click Browse and select the file destination path.
	Aurora Playout Destination	Check Aurora Playout Destination if this send location is an Aurora Playout server.

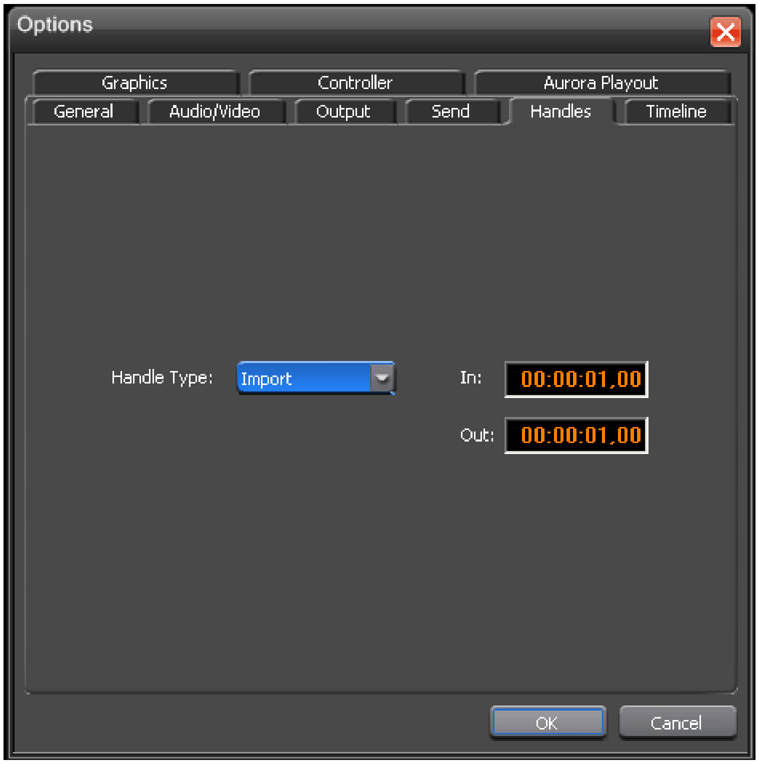
5. Click **OK**.
6. On the Send tab, configure these options:

Setting	Description
GXF Sequence Transfer	Check this option if you want to send sequences via GXF. If unselected, Aurora Edit can send sequences to a K2 in a shared storage system without using a fiber channel IP connection.
Test for Invalid Video Server Characters	Check this option to have Aurora Edit check for invalid characters when creating files, including creating a new clip, creating a new sequence, renaming a Bin object, sending a sequence with a video ID, importing a removable media clip, and editing the name of the sequence when sending to another destination. Invalid characters are: * \ | / < > : “ ? [ ] % & ‘

7. Click **OK**.

Options—Handles

Use this tab to set the handle type and in and out handle duration.



Handle Type: Import

In: 00:00:01,00

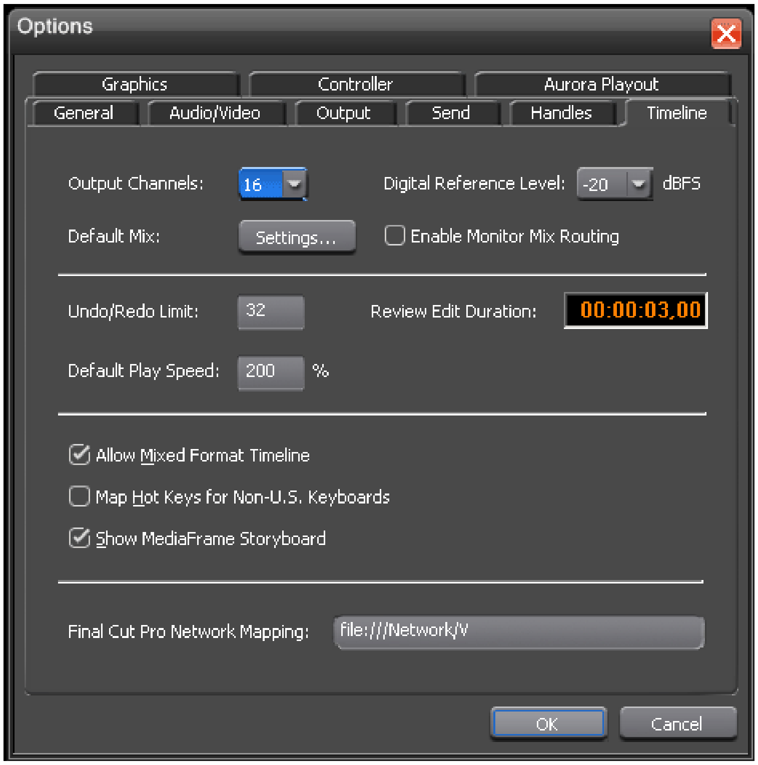
Out: 00:00:01,00

To change the handle durations, select the handle type from the drop-down menu and enter the new duration in the In or Out fields.

Setting		**Description**
Handle Type	Import	Sets handle duration that will be used when you are importing a file from another workstation to your own; 1 second is the default duration.
	Export	Sets handle duration that will be used when you are exporting files from your workstation to another workstation or server; 1 second is the default duration.
	Trimmer	Sets handle duration that will be used when you are trimming a clip with the Trim Tool and trim the set duration from either side of your clip; 10 seconds is the default duration.
	Consolidation	Sets handle duration that will be used when you are consolidating a clip or sequence, which reduces the file size by removing unused footage; 10 seconds is the default duration.
	Render	Sets handle duration that will be used when you are using media with effects and transitions; provides handles to effects that are mixed down; 1 second is the default duration.

Options—Timeline

Use this tab to set overall Timeline configuration.



Output Channels: 16

Digital Reference Level: -20 dBFS

Default Mix: Settings...

□ Enable Monitor Mix Routing

Undo/Redo Limit: 32

Review Edit Duration: 00:00:03,00

Default Play Speed: 200 %

☑ Allow Mixed Format Timeline

□ Map Hot Keys for Non-U.S. Keyboards

☑ Show MediaFrame Storyboard

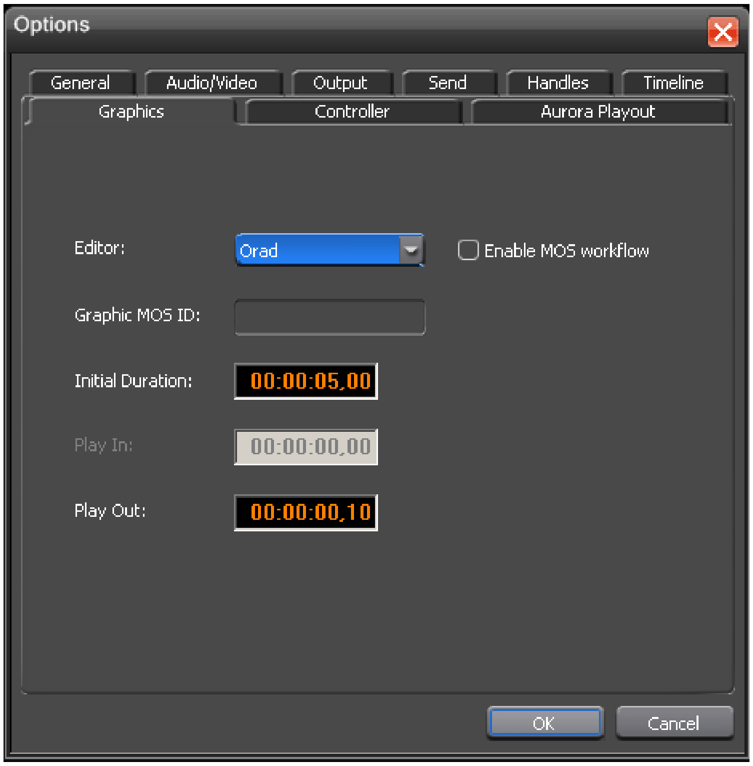
Final Cut Pro Network Mapping: file:///Network/V

Setting	Options	Description
Output Channels	1-16	Select the number of output channels to use in your sequence; configure panning and routing from via **Default Mix** settings.
Digital Reference Level	-20, -18, -12	Select the preferred dBFS level, which is indicated on audio meters with a blue tick mark. This setting does not alter recorded audio in any way; it moves the reference level so editors in different regions can ride audio at their preferred level of headroom.
Default Mix		Configures pan control and channel routing for each track of the Timeline. 1. Click **Settings**. 2. Select **Monitor Mix** or **Output Mix**. **Monitor Mix** controls panning and channel output for speakers in the edit bay, and does not affect sends to the server, play to tape, or live playout. **Output Mix** controls the panning and channel output for the actual sequence output for playout. 3. Set the pan control by dragging the pan slider for an audio channel to the right or left position; alt-click on a pan slider to set the pan direction to center. By default, odd-numbered channels pan to the left and even-numbers channels pan to the right. Changing the pan direction affects the entire track in a sequence. 4. Route audio channels by selecting specific channels (**1+2, 3+4, etc**.) or **All**. Default routing for two-channel systems is as follows: • Left >> Channel 1 • Right >> Channel 2 • Center >> All channels If you have more than eight audio tracks, click the Bank Select arrow to access the additional tracks on Bank 2.
Undo/Redo Limit		Enter the amount of preroll to play on a clip prior to playing the edit you're reviewing.The default Edit Duration is 3 seconds.
Output Channels	1-1024	Enter the number of undo levels to track; 32 is the default. ***NOTE: Increasing the number of undo levels increases Aurora Edit's system memory usage.***

Setting	Options	Description
Default Play Speed		Enter the speed at which to play clips when reviewing them in the Timeline; 200% is the default.
Review Edit Duration		Enter the amount of preroll to play on a clip prior to playing an edit; 3 seconds is the default.
Output Channels	1-8	Select the number of output channels to use; 4 is the default.
Allow Mixed Format Timeline		Allows different video formats to be mixed in real-time within the same Timeline. This setting can only be modified by administrators — it allows or disallows users from selecting a preference when creating a new Timeline. Although Aurora Edit allows for real-time mixing and matching of various formats within the Timeline, all clips that differ from the video format of the Timeline must be transcoded when the sequence is sent to a media or playout server. Therefore, some editors choose to disallow mixed formats for individual timelines based on their needs, which can be controlled in either the New Sequence or Sequence Properties windows. When disabled, all clips that don't match the Timeline settings are transcoded when they are added to the Timeline. When enabled, all clips that do not match the Timeline format will have a blue bar at the top of the clip to indicate that transcoding will take place when the sequence is sent.
Map Hot Keys For Non-QWERTY Keyboards		Check this option to keep the color-coded hot key functions in place regardless of the keyboard input language. If unchecked, the hot key functions follow the letter placement on non-QWERTY keyboards; this setting is off by default.
Show MediaFrame Storyboard		Allows the MediaFrame Storyboard to be toggled on and off from the Timeline.
Final Cut Pro Network Mapping		Enter a path for the EDL to map to on the Macintosh computer, using this format: MacOS 10.4x (Tiger): file://localhost/Volumes/K2_server_name MacOS 10.5x (Leopard): file://Network/V

Options—Graphics

You must configure some basic settings for an optional graphics system with this tab.



Editor: Orad

□ Enable MOS workflow

Graphic MOS ID:

Initial Duration: 00:00:05,00

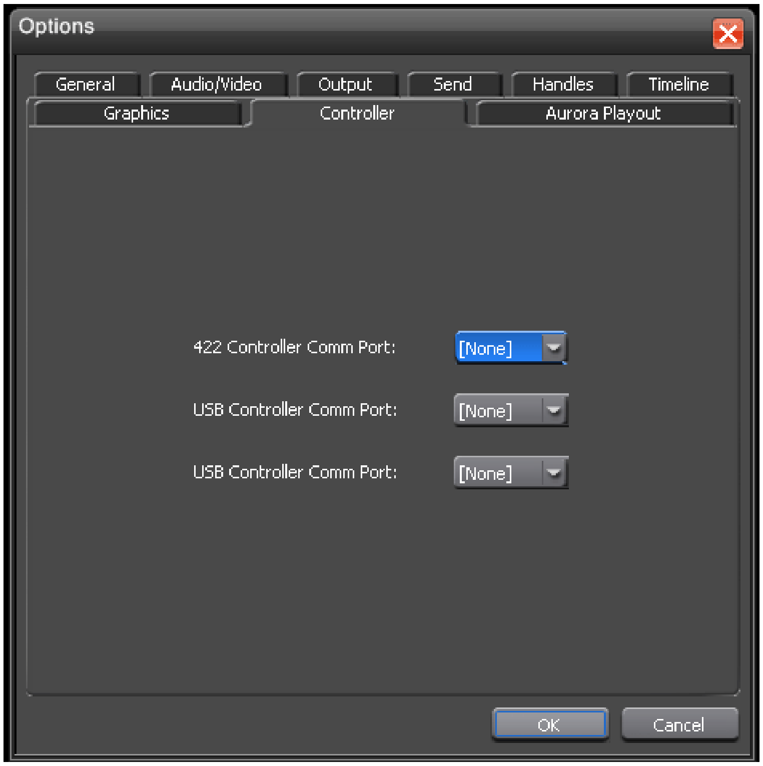
Play In: 00:00:00,00

Play Out: 00:00:00,10

Setting	Description
Editor	Select the graphics system you have installed, either Orad or VizRT.
Enable MOS workflow	Check this box enable Aurora Edit to link to a story and copy graphics from a script onto the Timeline.
Graphic MOS ID	This field will fill in with the MOS ID from the graphics system when connecting to the application.
Initial Duration	Enter the duration of the graphic if there is not Mark in or out specified on the Timeline.
Play In	What does this do?
Play out	The command within the graphics system that tells the typical duration for an animation to playout.

Options—Controller

This tab is used to configure the external communication ports on the Aurora Edit workstation.



422 Controller Comm Port: [None]

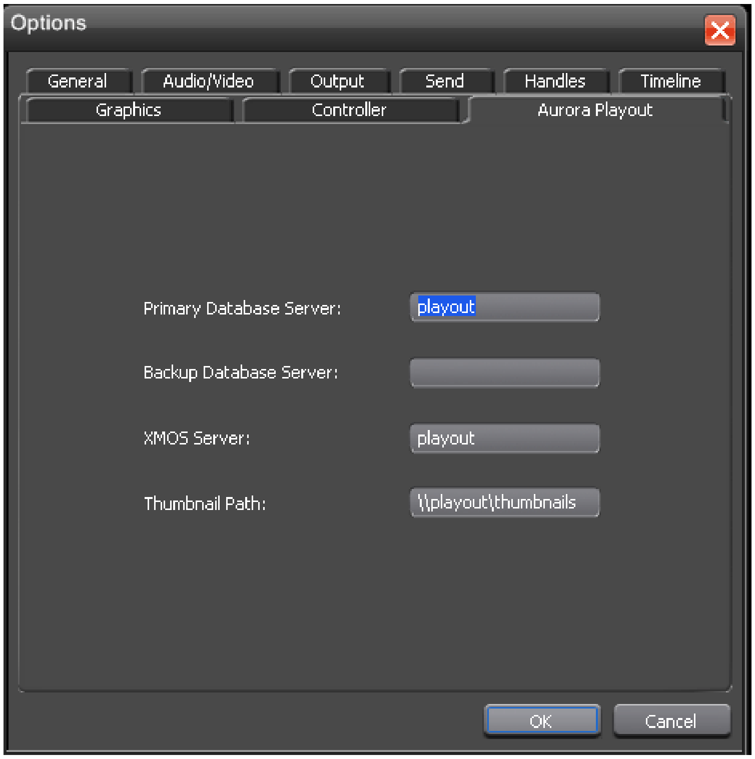
USB Controller Comm Port: [None]

USB Controller Comm Port: [None]

Setting	Options	Description
422 Controller Comm Port	None	If you are using an external 422 controller with Aurora Edit, select the COM port to which it is connected. Otherwise, select None.
USB Controller Comm Port	COM1 through COM10	Set the ports for USB devices you are using.
USB Controller Comm Port		

Options—Aurora Playout

Set the configuration for the Aurora Playout servers in this tab.



Primary Database Server: playout

Backup Database Server:

XMOS Server: playout

Thumbnail Path: \\playout\thumbnails

Setting	Description
Primary Database Server	Enter the server name where the primary Aurora Playout database resides.
Backup Database Server	Enter the server name where the secondary Aurora Playout database resides.
XMOS Server	Enter the name of the computer hosting the XMOS Server.
Thumbnail Path	Enter the path to the thumbnail directory.

Understanding the System Self-Test

The Aurora Edit workstation runs a self-test automatically each time it starts up. The System Self Test looks at three areas as described in this section.

- **Software Installation**—Checks for the correct version of K2 software, Direct X driver, operating system, video drivers, and export and cache service
- **System Configuration**—Checks for the correct version of the video board, Breakout Box firmware, audio renderer, and the VMR.
- **AV Disk Performance**—Tests the media drive’s input and output performance (local storage only).

As the System Self-Test runs, you see the results in the System Self-Test window. Each area displays one of three results as given in the table below.

This symbol...	Means...	Do this...
?	The test is currently running.	Wait for the test to complete.
✓	The test passed.	Use your Aurora Edit workstation as usual.
✗	The test failed.	Refer to the Troubleshooting System Self-Test section.

Troubleshooting the System Self-Test

On occasion, you may have a need to troubleshoot an error message from the system self-test. If any of the three tests fail, use this table to determine the cause and fix the problem.

If you see this message...	It means...
Video card driver ___ is not supported. CVFS client file system ___ is not supported. DirectX driver version ___ is not supported. AJA driver ___ is not approved. Emulex LAN driver ___ is not approved. Emulex SCSI driver ___ is not approved. QLogic LAN driver ___ is not approved. QLogic SCSI driver ___ is not approved.	You need to reinstall a driver on your system. 1. Insert the Aurora Edit CD and navigate to the Drivers directory. 2. Install the latest driver. 3. Contact your Customer Service Representative for further details.
The XX database server is not compatible.	The shared database is not compatible with your version of Aurora Edit software. On your DSM, run the SetupAuroraShareServer utility, which can be found on the Aurora Edit CD-ROM.

If you see this message...	It means...
Windows animation or fade effect is enabled.	The processing overhead of Windows' animation and fade effects may cause dropped frames. To turn these effects off: 1. Open the Display control panel and click the **Appearance** tab. 2. Click **Effects**. 3. Clear the first checkbox and click **OK**.
Hewlett-Packard HP xw8600 Workstation System BIOS ____ is older than approved version.	Update the system BIOS.
Terminal Services and Remote Desktop are not supported.	Aurora Edit must be run from the local desktop.
Recommended video driver is ___.	Install the correct video driver.
This version of Aurora Edit requires Windows XP SP3.	Install Windows XP SP3.
Stream Count not set.	Run AuroraStreamSetup.exe to configure the stream count.
The system drive is not an NTFS volume. The cache drive is not an NTFS volume	Convert the drive to NTFS using the convert command.
Aurora Edit requires at least 1 GB of RAM for Aurora Edit LD, 2 GB of RAM for Aurora Edit SD, and 3 GB of RAM for Aurora Edit HD.	Install additional RAM as necessary.

Chapter 7

SmartBins

This section contains the following topics:

- *Understanding SmartBins*
- *Running the SmartBins Setup Tool*
- *Verifying the DCOM Configuration*

Understanding SmartBins

SmartBins provide a way to automatically synchronize media access between Aurora Edit and media server bins. A SmartBin monitors a folder on a media server and automatically updates the SmartBin contents when new or updated media appears. The SmartBins Service software requires a license from Grass Valley.

A SmartBin is an Aurora Edit bin that monitors a folder on a media server and automatically updates the SmartBin contents when new or updated media appears. SmartBins work differently depending on the type of shared storage network you are using.

The Aurora Edit system offers two types of SmartBins:

- **Transfer SmartBin**—Automatically transfers clips from a Media Server to an Aurora Edit Bin.
- **Shared SmartBin**—Maps folders between a Media Server and a bin in Aurora Edit.

The two types work differently depending upon the type of shared storage network.

Transfer SmartBins

Transfer SmartBins automatically transfer clips from an M-Series iVDR or K2 media server to an Aurora Edit bin or MediaFrame database.

Transfer SmartBins use a static directory mapping so all files in a particular media server bin are monitored and automatically transferred via GXF to an Aurora Edit bin or MediaFrame database as they arrive, and are then (optionally) deleted from the media server.

Transfer SmartBins effectively create a buffered recording so that material is protected and redundantly saved (both on the media server and on the NAS or K2 storage) while still making the file available for shared editing or immediate playout. There is a 30-second delay before the recorded material is available to Aurora Edit or MediaFrame.

Transfer SmartBins on a NAS or a K2 system require a DSM or external Conform Server to provide the folder monitoring and transfer services to the NAS system. A DSM can support up to four 25-Mbit record streams (2 M-Series iVDR chassis). Additional streams can be handled by dedicated Conform Servers, which support six streams each. You also need to mount the NAS or iSCSI volume on the workstation running the SmartBins Service.

Shared SmartBin

Shared SmartBins map clips — a process known as “winking” — from a K2 media server to an Aurora Edit bin or MediaFrame database. As with drag and drop via Media Manager, this automatic synchronization never moves actual media files, but instead provides a different view into the shared media file system.

Shared SmartBins support simple (flattened) movies, but not sequences, sub-folders, or sub-clips that the K2 cannot use directly. SmartBins do not support sub-bins. The workstation running the SmartBins SAN service must have a Fibre Channel-SCSI connection to the Open SAN and a CVFS or SNFS license.

When you first create a bin in Aurora Edit, you can map that bin to a K2 bin; after an Aurora Edit bin is created, it cannot be mapped. Once an association is created, the Aurora Edit and K2 bins are kept synchronized.

When the SmartBins Service starts, it determines which Aurora Edit bins are associated with media server bins and then queries the media server database for the movies in each associated bin. Any movies in media server bins that are not in the associated Aurora Edit bin are registered to the Aurora Edit database. The SmartBins service does not verify that Aurora Edit clips are in the media server database, so the synchronization is one way only—media server to Aurora Edit.

Database Monitoring and Updating

A SmartBins Service constantly monitors the Aurora Edit, MediaFrame, and media server databases. Examples of updates to the database are listed below.

Action	System	Media Server Database	Aurora Edit Database
Rename clip	media server	Clip is renamed.	SmartBins service renames the clip; if it cannot be renamed, the databases become out-of-sync.
	Aurora Edit or MediaFrame	Clip is renamed unless there is a conflict, in which case renaming fails	Clip renamed unless there is a conflict on the media server, in which case renaming fails.
Delete clip	media server	Clip is deleted.	SmartBins service deletes the clip; if the clip is in use, the databases become out-of-sync.
	Aurora Edit or MediaFrame	Clip deleted unless there is a conflict, in which case deletion fails.	Clip deleted unless there is a conflict on the media server, in which case deletion fails
Add a movie	media server	Movie added.	SmartBins service registers clip unless it is a complex movie, in which case the clip is not registered and the databases become out-of-sync.

Action	System	Media Server Database	Aurora Edit Database
Create master clip	Aurora Edit or MediaFrame	SmartBins service registers master clip when recording is complete.	Master clip created while recording

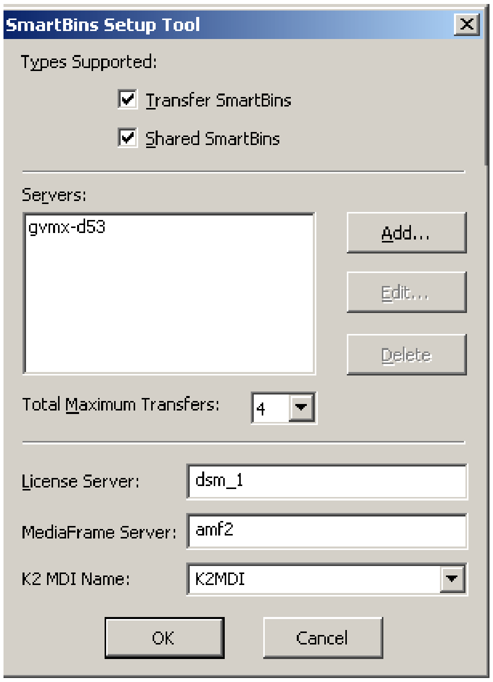
Running the SmartBins Setup Tool

If you are using SmartBins on a NAS or K2 system, you also need to configure your M-Series iVDR or K2 Media Server to use SmartBins.

To configure the SmartBins Service:

1. Go to Start | Programs | Grass Valley | Aurora | SmartBins Setup Tool.

   The SmartBins Setup Tool opens.



Types Supported:
☑ Transfer SmartBins
☑ Shared SmartBins

Servers: gvmx-d53

Total Maximum Transfers: 4

License Server: dsm_1

MediaFrame Server: amf2

K2 MDI Name: K2MDI

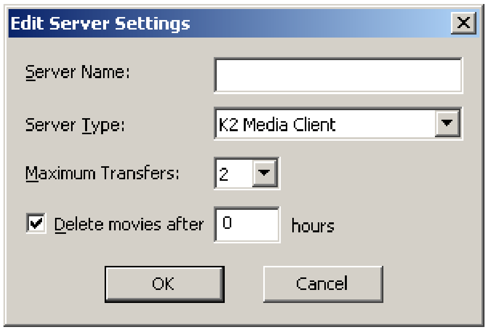
2. Select the types of SmartBins you are using with Aurora Edit

   For Shared SmartBins, no other configuration is needed. Click **OK** to close the tool.

3. For Transfer SmartBins:

   a) Click Add.

      The Edit Server Settings window appears:


Edit Server Settings

Server Name:

Server Type: K2 Media Client

Maximum Transfers: 2

☑ Delete movies after 0 hours

b) Enter the name of the M-Series iVDR or K2 Media Client you are using.

c) Select the Server Type from the drop-down list.

d) Select the number of Maximum Transfers per server from the drop-down list. If you are installing this software on a DSM, the maximum is 4.Select the number of Maximum Transfers per server from the drop-down list. If you are installing this software on a DSM, the maximum is 4.

e) Check **Delete movies after __ hours**, and enter the number of hours after a transfer is complete for media to remain in the database before being automatically removed from the video server (not the Aurora Edit workstation).

4. Click **OK** to close Server Settings.
5. Select the Total Maximum Transfers from the drop-down list.

   The Total Maximum Transfers is the total number of streams for this particular instance of the SmartBins Service. Select 4 if the SmartBins Service is installed on a DSM, or select 6 if the SmartBins Service is installed on a standalone PC.

   NOTE: Increasing the number of Total Maximum Transfers affects the bandwidth on the NAS system.

6. Enter the name of the License Server; this is the same as the License Server in Aurora Edit.
7. Enter the name of the MediaFrame Server.
8. Enter the K2 MDI Name.
9. Click **OK** to close the setup tool.

   The SmartBins Service restarts.

Verifying the DCOM Configuration

Transfer SmartBins require that DCOM permissions are configured correctly on the media server.

To verify the DCOM configuration:

1. Click **Start** on the Windows taskbar and choose **Run**.
2. Enter **Dcomcnfg.exe** and click **OK**.

3. Expand the **Component Services** branch, and the **Computers** branch beneath it.
4. Right-click on **My Computer** and choose **Properties**.
5. Click the **COM Security** tab.
6. In the Access Permissions section, click **Edit Limits**.
7. Select **ANONYMOUS LOGON** and verify that the **Remote Access** box is allowed (checked).
8. Select **Everyone** and verify that the **Remote Access** box is allowed (checked).
9. Click **OK** and then **OK** again to close the Properties window.

If you made any changes, you must reboot your system; if no changes were required you can exit Component Services.

Chapter 8

Conform Server

This section contains the following topics:

- *The Conform Server*
- *Hardware Requirements*
- *Software Requirements*
- *Conform Server Configuration*
- *Testing the Conform Server Installation*

The Conform Server

A Conform Server conforms an Aurora Edit EDL to high resolution media on the K2 Media Clients.

Hardware Requirements

See the Release Notes on the installation CD for current system requirements.

Software Requirements

The following software components are required to run the Conform Server. Be sure to check the Aurora Edit release notes for updated software versions.

- Microsoft Windows 2003 Server
- Microsoft IIS 6.0 (IIS must be installed before .NET)
- Microsoft .NET Framework 3.5 SPI

Conform Server Configuration

After installing the Conform Server software, there are additional tasks you must perform on the server itself.

The tasks required are listed below are described in this chapter:

- Disabling IE Enhanced Security Configuration
- Disabling Power Management
- Configuring IIS
- Configuring DEP

Disabling IE Enhanced Security Configuration

You must remove Internet Explorer Enhanced Security Configuration software from the conform server.

1. Open the **Add/Remove Programs** control panel.
2. Click**Add/Remove Windows Components**.
3. Uncheck **Internet Explorer Enhanced Security Configuration**.
4. Click **Apply**.

Disabling Power Management

You must disable any screen savers or power-saving features on the conform server.

1. Open the **Display Properties** control panel.
2. On the **Screen Saver** tab, select **None** as the screen saver and click **OK**.
3. Open the **Power Options** control panel.
4. On the **Power Schemes** tab, select the **Always On** power scheme.
5. Select **Never** for all monitor, hard disk, and system standby settings.
6. Click **Apply**.
7. Click the **Hibernate** tab and verify that the **Enable Hibernation** option is not checked.
8. Click **OK**.

Configuring IIS

Configure the IIS Manager as follows:

1. Open the IIS Manager.
2. Expand the **Application Pools** folder, right-click on **Default App Pool**, and select **Properties**.

   If you do not see the **Application Pools** folder, do the following:

   a) Right-click on the **Web Sites** folder and select **Properties**.
   b) Click the Service tab and verify that **Run WWW service in IIS 5.0 isolation mode** is unchecked.
   c) Click **OK**.
   d) Stop and restart IIS.
3. On the **Recycling** tab, uncheck **Recycle worker processes**.
4. On the **Identity** tab, specify **Predefined** as the security account and then select **Local System**.
5. Click **OK**.
6. Expand the tree view and select the Default Web Site. Right-click and then **Properties**. Go to the **ASP.NET** tab. Select the **2.0.x.x.x** version from the drop-down and hit **Apply**.
7. Select the **Web Service Extensions** folder.
8. Verify that **ASP.NET** extensions are **Allowed** and that all other extensions are **Prohibited**.

Configuring DEP

Configure the Data Execution Prevention (DEP) as follows:

1. Open the System control panel and click the **Advanced** tab.
2. In the Performance section, click **Settings** to display the **Performance Options** window.

3. Click the **Data Execution Prevention** (DEP) tab.
4. Select the first option (**run only for essential Windows programs and services**).
5. Click **OK**.

Testing the Conform Server Installation

Two quick tests must be done to determine if IIS and the conform service ae running properly.

Testing IIS installation

To test IIS, do the following on the conform server:

Using Internet Explorer, go to **http://<Conform_Server_name>**

If the page displayed does not indicate that the web service is running, recheck the IIS installation procedure.

Testing Conform Service Installation

To test the installation of the Conform Server, do the following:

1. Using Internet Explorer, go to **http://<Conform_Server_name>/xre/Services.asmx**.

   The Conform Server Web Services page appears.
2. Click **QueryBoxInfo**.
3. In the Test section, click **Invoke**.

   An XML page displays information such as the software version, job queue information, and service uptime.
4. From an Aurora Edit client, open the Conform Manager tool.

   The Conform Server and job queue should be visible.
5. Submit a conform Job via the **Send** command and verify that it completes.

   If errors occur, use the Thomson Event Viewer to inspect the conform server log.
6. From the Windows task bar, select **Start | Programs | Thomson | Thomson Event Viewer**.
7. Verify that, under the **View** menu, that **Aurora Application** and **Conform Service** are both checked; these are the two services you should monitor

Web.Config

The Conform Server contains an XML configuration file called Web.config that resides in the \InetPub\wwwroot\xre folder. Most of the settings in this file are used by IIS.

You can use this file to confirm settings while troubleshooting a problem with the Conform Server.

The adds several parameters in the appSettings section as in the following example:

```
<appSettings>
 <add key="resolverURL"
value="http://10.16.57.161/AMUI/AM_ResolverService.asmx" />
 <add key="resolverUserId" value="nbadmin"/>
 <add key="resolverPwd" value="newsat10"/>
 <add key="resolverDomain" value="MyDomain"/>
 <add key="xBoxAVFiles" value="V:\XreAVFiles" />
 </appSettings>
```

The appSettings section contains the following items:

- **resolverURL**. The URL of the Resolver service, used by the Conform Server to locate the High Resolution media described in the EDL.
- **resolverUserId**. The user account under which the Conform Server service runs.
- **resolverPwd**. The password for the ResolverUserId account.
- **resolverDomain**. The domain name of the resolver service.
- **xBoxAVFiles**. The fully qualified path to the temporary working directory.

Chapter 9

Aurora Edit Security

This section contains the following topics:

- *Aurora Edit Security Overview*
- *Designing a security schema*
- *Configuring the Domain Controller*
- *Configuring SNFS for SAN Security*
- *Setting Security Permissions*
- *Testing*

Aurora Edit Security Overview

Using SAN security, you can control the visibility and access for users and groups within Aurora Edit bins by associating the bins and assets with file system permission.

SAN security uses the overlapping modes of inheritance, exclusivity, and group membership, as implemented by Windows, to establish file system security.

These principals apply:

- Selective access—You create groups of users, such as Editors or Producers, and set permissions for each group.
- Partial control—You control access to branches of the Bin tree for users and groups.
- Administrative control—The Administrator has exclusive access to a tool in the top-level bin that allows the setting of permissions in the top-level bins.

When you are joining computers to the domain or setting permissions, the NewsShare system must be off line, during a maintenance window.

Designing a security schema

In order to set up security in your SAN system you need create a schema for permissions. The schema determines which groups you create, and which permissions you give each group.

Grass Valley has created a typical schema for use in illustrating security principles in this document. You may use this schema if it is appropriate for your newsroom, or create your own. For the examples in this manual, we'll assume that the newsroom has five groups: Editors, Producers, Archivists, Ingestors, and Viewers.

The SAN security principles are agnostic to these groups, though the use of groups greatly simplifies the establishment of the security schema. We picked these names as exemplary; you do not need to use them in your operation. You can have as many or as few groups as you like, named however you wish. If your domain has a tree hierarchy, you may assign permissions to global groups as well.

Sample security schema

The following table lists the groups and permissions being used as an example in this document:

News Group	Bin	Permissions
Domain Administrator	All	Full Control
Editors	Monday-Sunday	Read/Write/Delete in top level bins, but cannot delete material from newscast bins.

News Group	Bin	Permissions
	Feeds	Read only
	HFR (Hold For Release)	Read/Write
	Archive	Read/write
Producers	Monday-Sunday	Read/Write
	Feeds	Read only
	HFR (Hold For Release)	Full control
	Archive	Read/Write
Archivists	Monday-Sunday	Read only
	Feeds	ReadWrite
	HFR (Hold For Release)	Read only
	Archive	Full control
Ingestors	Monday-Sunday	Read only
	Feeds	Full control
	HFR (Hold For Release)	None (permission denied)
	Archive	Read/Write
Viewers	Monday-Sunday	Read only
	Feeds	Read only
	HFR (Hold For Release)	Read only
	Archive	Read only

NewsShare system users and groups

At a minimum, you need to create two user-group sets for use by certain components of the NewsShare system.

Group	User Members	Password
Profile Services	profile	profile
Vibrint Services	VibrintService	triton

Configuring the Domain Controller

A Domain Controller is a separate machine running Windows 2003 Server software and configured with Active Directory. If purchased from Grass Valley, a Conform Server is used. If the sole responsibility of the machine is to act as a domain controller, SMG- or customer-furnished equipment may be used, provided that it meets the specifications necessary to host Windows 2003 Server.

Guidelines

In general, you need to follow these guidelines for the Domain Controller:

- The Domain Controller cannot be an FSM.
- A separate Domain Controller and related domain node should be allocated to the technical LAN subnet. This Domain Controller should also have sufficient access to all related LANs to establish trusts and provide authentication services.
- A Conform Server can be used to host another Aurora Edit product, SmartBins.
- The domain controller may be remote to the SAN, but needs high availability and direct configurability by your newsroom engineering department.
- Consistent with the Windows domain model, the domain controller may also use a backup within the SAN subnet.
- You can either create a Domain Controller as a new domain tree or as a child domain to an existing Domain Controller on your network.
- For normal newsroom operation, if the domain controller is a member of a forest or tree, the Domain Controller can be subordinate: trusting but not trusted.

Each news organization has different infrastructure and policies regarding the configuration of domains. What NewsShare SAN security requires is an Active Directory zone with at least one dedicated Windows 2003 Server domain controller; there are several ways to achieve this, and the choice appropriate for your organization depends on your organization's culture, infrastructure, and IT policies.

In planning, you need to determine the relationship of the new domain to its tree; whether it will use integrated, delegated, or standalone DNS; and whether the domain controller's mode will be mixed, in order to interoperate with pre-Windows 2000 domain controllers, or native, allowing advanced features, particularly greater opportunity in configuring user groups. The recommended configuration to effect the most flexible control of the technical domain is to run integrated DNS on a native-mode domain controller.

This chapter details two of the many ways to set up a domain controller with Active Directory:

- First node in a domain tree, integrated DNS, (mixed-mode) permissions compatible with pre-Windows 2003 servers.
- Child node in an existing domain tree, (integrated) DNS in the parent, (native-mode) permissions compatible with Windows 2003 servers and higher.

As an adjunct step, depending on the trust relationship between the domain controllers for NewsShare and those of the larger organization, the use of a standalone DNS with forwarding may be necessary to achieve a highly isolated domain.

Creating Groups

You create groups on your Domain Controller according to the security schema you created.

Use this table as a guideline for creating your groups:

Group Name	Group Scope	Group Type	Required?
Vibrint Services	The Group Scope is dependent on the type of Domain Controller you configuring. **Note:** if your are working in a mixed domain, your only practical Scope choice is **Global**, which is documented here. In a native mode domain, other choices are available. Consult the Windows Active Directory documentation on group scopes.	Security	Yes
Profile Services		Security	Yes
Archivists		Security	Optional
Editors		Security	
Ingestors		Security	
Producers		Security	
Viewers		Security	
Other groups as necessary for your newsroom			

Creating Users

You need to create the users who will become members of the groups you just created. Users represent each person who logs on to an Aurora Edit workstation. If you are creating a new domain tree, you need to create each user using the directions below. If you are creating a child domain, and will get your users from the parent domain, you can skip this step.

Regardless of the type of Domain Controller you are configuring, you need to create these two users:

Full Name	User Logon Name	Password
profile	profile	profile
VibrintService	VibrintService	trition

Adding Users to the New Groups

Once you've created groups and users, you can add the users to their respective groups. If you are configuring a child domain, you may select users from the parent domain.

You also need to add the profile user to the Profile Services group, and the VibrintService user to the Vibrint Services group.

This table illustrates how users fit into groups you previously defined:

Group Name	Users	Required?
Profile Services	profile	Yes
Vibrint Services	VibrintService	Yes
Editors	Administrator	Optional
	joe edit 1	
	joe edit 2	
	joe edit 3	
	joe producer	

Configuring SNFS for SAN Security

The StorNext File System (SNFS) runs on the File System Manager(s) as part of the SAN network. In order to use security on Aurora Edit workstations, you need to modify the SNFS configuration to use Windows Security and then power cycle the FSMs.

NOTE: You cannot use the SNFS Configuration Tool to add Windows Security to SNFS. Using the Configuration Tool changes other settings you don't want to modify

To add windows security to SNFS:

1. On the primary FSM, go to **C:\MediaAreaNetwork\config.**
2. Using Notepad, open the file **default.cfg.**
3. Change the **Windows Security** line's value to **YES.**

   If the line item doesn't exist, add it to the file.
4. Save the file and exit Notepad.
5. Repeat these steps 1 through 4 on the backup FSM.
6. Power cycle the FSMs as follows:
   a) Shut down the backup FSM.
   b) Reboot the primary FSM.
   c) Power on the backup FSM

Setting Security Permissions

The last step in setting up security for your DNP system is to set permissions for the Aurora Edit folders and bins. You again use your security schema to determine permissions for users and groups.

You can set all permissions from one Aurora Edit machine. You need to set permissions in three different places—in the V:\ directory, in Aurora Edit options, and in the Aurora Edit bins.

You must log in as a Domain Administrator to set security permissions.

Setting Initial Shared Volume Permissions

This task assures a uniform starting point in setting volume permissions, essentially setting the secure volume's permissions to be identical to either an SNFS volume that does not implement Windows Security, or a default NTFS volume.

To set shared volume permissions:

1. Open a cmd window, switch to the V: drive, and type the following **cacls V:\* /T /G Everyone:F**.
2. IIn Windows Explorer, right-click on the V: drive and select **Properties**.
3. Click the **Security** tab.
4. If necessary, add the user **Everyone** and allow **Full Control.**
5. Click **Advanced...** and check the box **Replace permission entries on all child objects with entries shown here that apply to child objects.**
6. Click **OK** and click **Yes** in response to the dialog **This will remove explicitly defined permissions... Do you wish to continue?**
7. Click **OK** to exit the Properties window.

Setting high-level shared volume permissions

You set the high-level shared volume permissions on the V:\ folders using Windows Explorer.

You must be a Domain Administrator to perform this function.

First you add the group(s) to the drive and then set security permissions for that group. For the folders that are inheriting permissions from the folder above it, you don't need to set them; they automatically use the permissions they inherit.

	V:\	V:\media	V:\K2	V:\Thumbnails	V:\VibrintAttic
Domain Admins	F		F	(Inherit Full Control from V:\)	(Inherit Full Control from V:\)
Everyone	F	F*			
System		F*	F		
Archivists					
Editors			F		
Ingestors			F		

Producers		
Viewers		
K2 Services	F	F*
Vibrint Services	F	F*

F = Full Control * = Inherits permissions from the folder directly above it

1. Open Windows Explorer and navigate to the V:\ drive.
2. Right-click on the desired folder and select **Properties**.

   The default V:\ Properties window appears.
3. Under the Security tab, click **Add**.

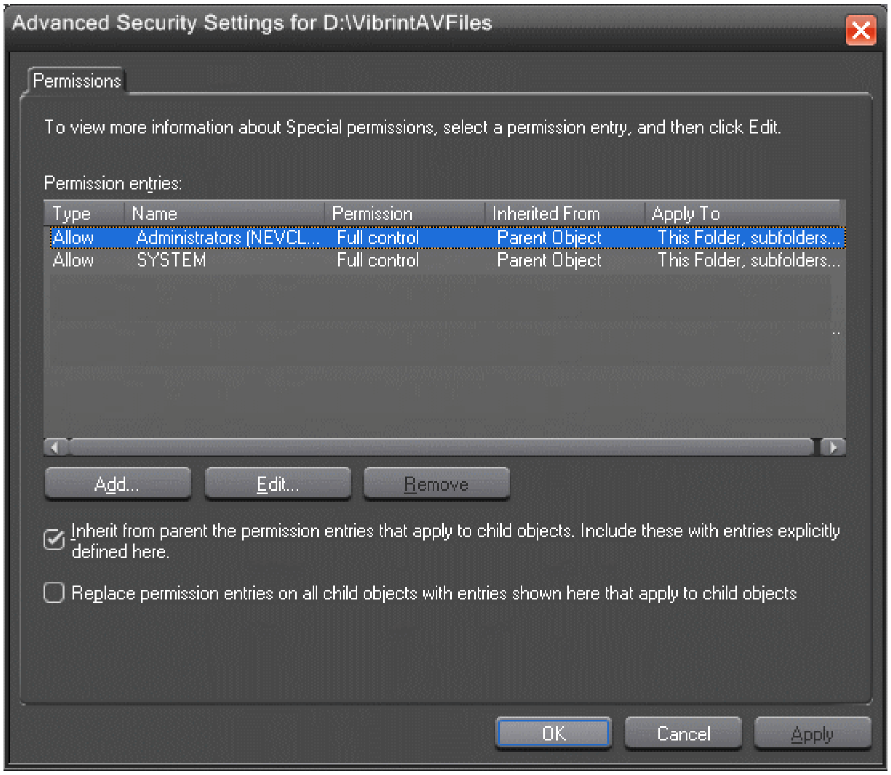
   The Select Users, Computers, or Groups window opens.
4. Select the group you want to add to the drive folder and click **Add**.

   The group adds to the bottom pane of the window.
5. Click **OK**.
6. Check the box for **Full Control** in the **Allow** column.
7. Click **OK**.
8. Give Full Control permission to the other groups—Domain Admins, Everyone, and SYSTEM.
9. Select the V:\PDR drive and do the following:
   a) Uncheck **Allow inheritable permissions from parent to propagate to this object**.
   b) Add these groups: Profile Services, Editors, and Ingestors.
   c) Set Full Control permissions for these groups.

Setting Aurora Edit Level Root Permissions

Permissions for V:\VibrintAVFiles are set in Aurora Edit options. First you add the group(s) to the drive and then set security permissions for that group.

You must log in as Domain Administrator to set root permissions in the Permissions screen.



To view more information about Special permissions, select a permission entry, and then click Edit.

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Administrators (NEVCL...	Full control	Parent Object	This Folder, subfolders...
Allow	SYSTEM	Full control	Parent Object	This Folder, subfolders...

☑ Inherit from parent the permission entries that apply to child objects. Include these with entries explicitly defined here.

□ Replace permission entries on all child objects with entries shown here that apply to child objects

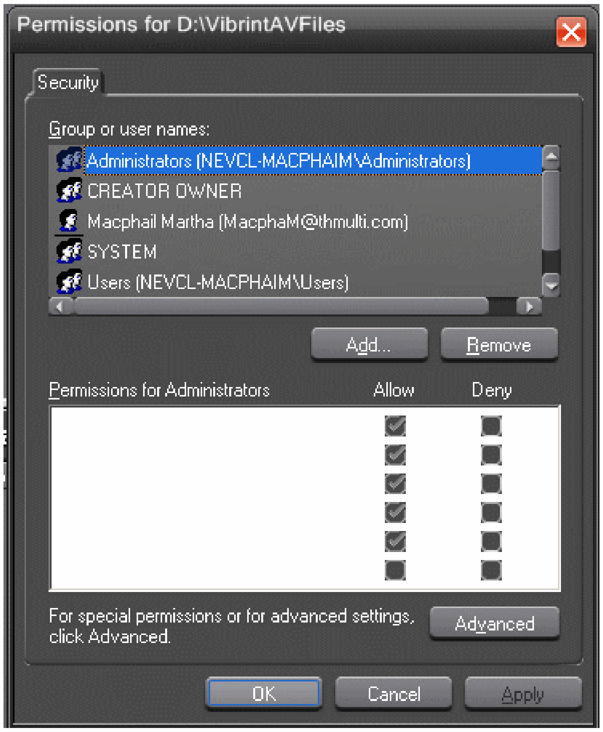
To set permissions for VibrintAVFiles:

1. Open Aurora Edit and select **Tools | Set Root Permissions**.

   The **Select a Volume** window appears.

2. Select a volume and click **OK**.

   The **Security** tab for V:\VibrintAVFiles opens.



Permissions for D:\VibrintAVFiles

Security

Group or user names:

- Administrators (NEVCL-MACPHAIM\Administrators)
- CREATOR OWNER
- Macphail Martha (MacphaM@thmulti.com)
- SYSTEM
- Users (NEVCL-MACPHAIM\Users)

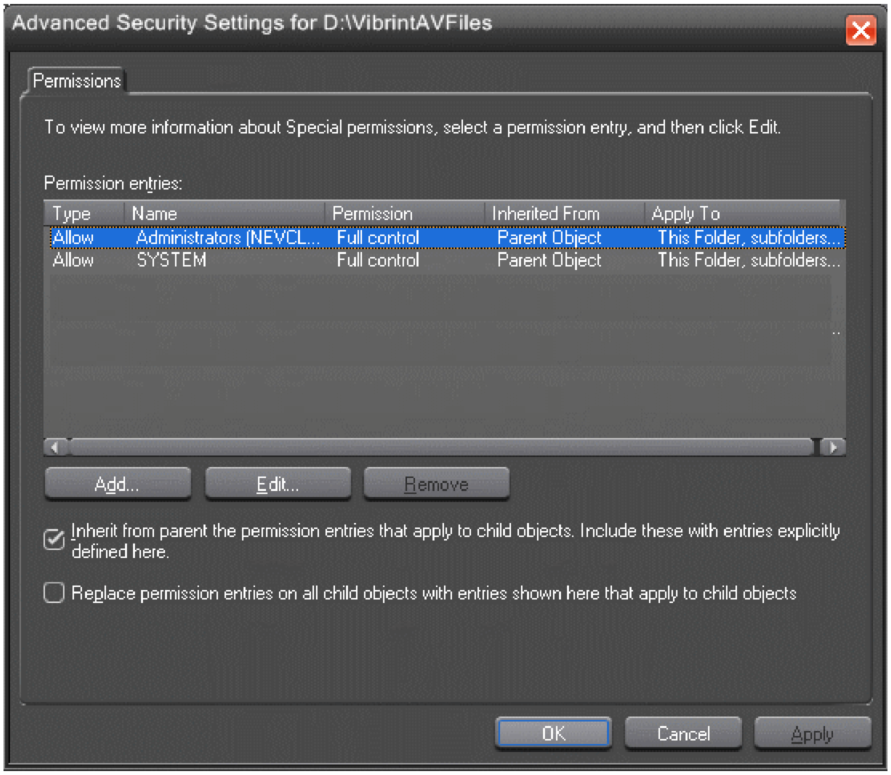
Permissions for Administrators	Allow	Deny
	☑	□
	☑	□
	☑	□
	☑	□
	☑	□
	□	□

For special permissions or for advanced settings, click Advanced.

Add and remove permissions and click **OK**.

3. For special permissions or for advanced settings, select the **Advanced** tab.

   This will bring up the **Permissions**tab.



To view more information about Special permissions, select a permission entry, and then click Edit.

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Administrators (NEVCL...	Full control	Parent Object	This Folder, subfolders...
Allow	SYSTEM	Full control	Parent Object	This Folder, subfolders...

☑ Inherit from parent the permission entries that apply to child objects. Include these with entries explicitly defined here.

☐ Replace permission entries on all child objects with entries shown here that apply to child objects

Add or edit permissions and click **OK**.

Setting Aurora Edit Bin Permissions

Aurora Edit bin permissions are set in the Properties tab for each Bin. Follow the instructions below to set permissions for each bin in your top-level Aurora Edit bin.

To set permissions for Aurora Edit bins:

1. In the Aurora Edit bin, right-click on the first bin and select **Properties**.
2. Click the **Security** tab.
3. Change permissions for each group listed based on the chart.
4. Click **OK** when you are done setting permissions.

	Monday-Sunday Bins	Feed Bin	HFR Bin	Archive Bin
Domain Admins	F*	F*	F+	F*
Everyone				
SYSTEM	F*	F*	F*	F*
Archivists	-W -D	W -D	-W -D	W D

Editors	W D	-W -D	W -D	W -D
Ingestors	-W -D	W D	-F	W -D
Producers	W -D	-W -D	W D	W -D
Viewers	L R*	L R*	L R*	L R*
K2 Services				

- **F** = Full Control
- **L** = List Folder Contents
- **R** = Read
- **W** = Write
- **D** = Delete
- - = Deny
- * = Inherits permissions from the folder directly above it
- ** = Inheritance is blocked at this level

Testing

After creating and configuring the Domain Controller and setting permissions for Aurora Edit bins, you should test the system to make sure that the security is working:

1. Aurora Edit system operation:

   Basically, check that permissions exist functionally where they should and that permissions are denied functionally where they should be denied. A Viewer user should not be able to write or delete. Significantly, where a user is denied all permissions (as might be the case for an investigative report that should be editable by only a small group) make sure that users outside the group have no access and no availability in the private group. Check that delete permissions are truly denied. Check that read only users in a particular bin cannot write.

2. Winking:

   Winking requires a complicated security relationship between several processes. Therefore, it's important to check that users who were expected to be able to wink can wink. Create a clip on the K2 media client and wink it to a non-SmartBin using Aurora Edit. Likewise, create a Aurora Edit clip and wink it to a K2 media client non-SmartBin.

3. SmartBins:

   Since SmartBins on an SAN function by winking, they have similar dependencies to user-initiated winking. Check that a clip recorded on a Profile SmartBin appears in the associated Aurora Edit SmartBin and vice-versa.

4. Conform Server:

The Conform Server has overlapping permissions needs. Publish a story out of Aurora Edit or Aurora Edit LD to make sure that it works.

Appendix **A**

Workstation Slot Map

This section contains the following topics:

- *HP z800 Workstation Board Assignment*

HP z800 Workstation Board Assignment

Slot #	Slot Type	Use
1	PCI-e Gen2 x8 (x4)	Empty (can be used as needed)
2	PCI-e Gen2 x16	NVIDIA Quadro FX1800 graphics
3	PCI-e x8 (x4)	Empty (can be used as needed)
4	PCI-e Gen 2 x16 (x8)	HDR I/O board (optional)
5	PCI-e Gen 2 x16	Empty (can be used as needed)
6	PCI	Comtrol 422 (optional) *OR* 2 nd 1394 (optional)
7	PCI-e Gen2 x16 (x8)	Empty (can be used as needed)

Appendix **B**

Database Maintenance

This section contains the following topics:

Database Maintenance

Six command-line maintenance utilities are available for the News database used by Aurora Edit, Aurora Playout, and NewsShare. These utilities are automatically installed on DNP client machines and most NewsShare servers in the C:\Program Files\Grass Valley\Aurora\DB Maintenance directory. They can also be installed from the Aurora Suite CD.

The following utilities are covered in this section:

Name	Description
newsBackUpDb	Backs up the News database
newsRestoreDb	Restores the database from a backup
newsDropDb	Removes the database (for complete uninstall)
newsInstallDb	Recreates an empty News database
newsShrinkDb	Shrinks the database
newsInitAutoBack	Schedules automatic backups of the News database

NOTE: Use these utilities with great care. The restore and drop commands, respectively, overwrite and delete existing databases such that current data will be lost.

Database Overview

This section gives an overview of using database utilities.

When used, the utilities must be run from the C:\Program Files\Grass Valley\Aurora\DB Maintenance directory of the machine whose database is being operated upon. The user must be a member of the system's Administrators group. For a local, stand-alone machine, run the utilities at that workstation. For the central News database of a shared storage system (NewsShare), run the utilities at the DSM.

To run any of the utilities, open a command window and type the command. The following sections describe each utility and its usage. Note that filenames used in the commands must be fully qualified.

Before running any of the utilities, follow these preparatory steps:

- For restore and drop operations, the News database must not be servicing clients. Close all DNP applications that would use it.
- For DSM-based News databases, observe these constraints:
  - Back up the database from the primary DSM.

- If automatic database backups are scheduled, they must be set to occur during periods of extremely low system utilization, preferably when zero NewsShare or are recording or playing clips.
- Stop all access before restoring or dropping the database.
- Take DSMs out of service before restoring or dropping the database.
- Close all SQL applications before restoring or dropping the database.
- Restore the database to the primary DSM.

newsBackUpDb

Template

newsBackUpDb <backup file name>

Example

```
C:\Program Files\Grass Valley\Aurora\DB Maintenance>
newsBackUpDb c:\backups\news.dat
Backing up this machine's News 4.1+ database to location
c:\backups\news.dat
. . .
Contents of log file vNewsBackUpDb.log:
----------------------------------------------------------
Tue 11/26/2002 4:38p
Administrator
Backing up news DB from VMAN_VBRFSM3 to file c:\backups\news.dat.

27 percent backed up.
55 percent backed up.
83 percent backed up.
99 percent backed up.
Processed 432 pages for database 'news', file 'news_dat' on
file 1.
100 percent backed up.
Processed 1 pages for database 'news', file 'news_log' on file
 1.
BACKUP DATABASE successfully processed 433 pages in 0.326 seconds
 (10.863 MB/sec).
----------------------------------------------------------
Press any key to exit . . .
C:\Program Files\Grass Valley\Aurora\DB Maintenance>
```

newsRestoreDb

WARNING: this will overwrite the current News database.

Template

newsRestoreDb <backup file name>

Example

```
C:\Program Files\Grass Valley\Aurora\DB Maintenance>
newsRestoreDb C:\backups\news.dat
```

```
Restore will overwrite any current News 4.1+ DB on this machine!

Press Cntl-C to abort, any other key to proceed . . .
Restoring this machine's News 4.1+ database from file
C:\backups\news.dat . . .
Contents of log file vNewsRestoreDb.log:
---------------------------------------------------------
Tue 11/26/2002 4:58p
Administrator
Restoring news DB on VMAN_VBRFSM3 from C:\backups\news.dat.
x percent restored.
Processed 432 pages for database 'news', file 'news_dat' on
file 1.
Processed 1 pages for database 'news', file 'news_log' on file
 1.
RESTORE DATABASE successfully processed 433 pages in 0.213
seconds (16.626 MB/sec).
'vibrint' added to role 'db_owner'.
The number of orphaned users fixed by updating users was 0.
Press any key to exit . . .
C:\Program Files\Grass Valley\Aurora\DB Maintenance>
```

newsDropDb

WARNING: this will overwrite the current News database.

If the Microsoft SQL Server is ever to be removed, this drop should be done first. Otherwise, remnant files will interfere with future installations of the News database.

Template

newsDropDb

Example

```
C:\Program Files\Grass Valley\Aurora\DB Maintenance> newsDropDb
Ensure that the Failover Service is stopped before dropping the
 news DB.
Drop will delete the News 4.1+ database on this machine!
Press Cntl-C to abort, any other key to proceed . . .
Dropping News 4.1+ database on this machine . . .
Contents of log file vNewsDropDb.log:
---------------------------------------------------------
Tue 11/26/2002 4:41p
Administrator
Deleting database file 'C:\Program Files\Microsoft SQL
Server\MSSQL\data\news.ldf'.
Deleting database file 'C:\Program Files\Microsoft SQL
Server\MSSQL\data\news.mdf'.
---------------------------------------------------------
Press any key to exit . . .
C:\Program Files\Grass Valley\Aurora\DB Maintenance>
```

newsInstallDb

First run newsDropDb, as shown above, on the host machine for the database. Then run newsInstallDb as shown here. This batch file dispatches to the dbInstall program which is placed on each client by the DNP installer. This will work for standalone editors. For DSM servers, use Add/Remove Programs to remove the TGV DNP database program entry and rerun Setup NewsShareServer. Before or after creating the empty database, you need to purge or manually reconcile the media files.

Template for local (non-shared) database

newsInstallDb -local [-noxform]

If the -noxform switch is not present and the installer finds certain markers that indicate that NewsEdit 4.0 had previously been used on the machine, the program will attempt to convert the 4.0 database to 4.1+ form for local use. If such a conversion happens, media-database skew will render the data nearly useless unless the machine has just been converted from 4.0. The noxform switch should be used except for upgrades.

Example

```
C:\Program Files\Grass Valley\Aurora\DB Maintenance>
newsInstallDb -local -noxform
Skipping MSDE installation. Ver. 8.00.194 already installed.
Installing skeletal news DB on local MSDE server.
This may take a moment...success.
Database installation complete.
Press any key to exit . . .
C:\Program Files\Grass Valley\Aurora\DB Maintenance>
```

newsShrinkDb

Since the database automatically shrinks its transaction log, this operation would be necessary only under unusual circumstances.

Template

newsShrinkDb

Example

```
C:\Program Files\Grass Valley\Aurora\DB Maintenance> newsShrinkDb

Shrinking News 4.1+ database on this machine . . .
Contents of log file vNewsShrinkDb.log:
---------------
Tue 11/26/2002 4:58p
Administrator
Cannot shrink file '2' in database 'news' to 12800 pages as it
 only contains 256 pages.
DBCC execution completed. If DBCC printed error messages, contact
 your system administrator.
---------------
Press any key to exit . . .
C:\Program Files\Grass Valley\Aurora\DB Maintenance>
```

newsInitAutoBack

WARNING: This utility should be used only by experts or as instructed by Grass Valley personnel, due to required considerations of system load, system drive space, network load, and necessary familiarity with the Windows at command and Task Scheduler.

This command schedules a system event which will automatically back up the News database every Monday at 3 am. The event in turn dispatches the vbrAutoBack batch file, which affects these files in the \Program Files\Grass Valley\Aurora\DB Maintenance\ directory:

newsAutoBack.dat	Most recent backup
newsAutoBack.old.dat	Previous backup
vNewsBackUpDb.log	Most recent backup log
vNewsBackUpDb.old.log	Previous backup log

As each successive auto-backup occurs, the previous backup is shifted onto the old images. After you have run newsInitAutoBack, use the at command or (on Windows 2000) the Task Scheduler to reschedule the event to suit your facility. Alternatively, without running newsInitAutoBack at all, you can directly schedule an event to dispatch vbrAutoBack.

Before you use this utility, consider these cautions:

- The DNP and DSM systems are highly tuned for load. The backups must occur only at times when the systems are quiescent. Disregarding this caveat may cause erratic performance or system-wide failure.
- The backup files, particularly on a DSM, can become quite large and thus deleteriously affect system performance. If your databases are large, you should plan to move the backup files off the system as part of the backup process.
- The DNP systems require very high Ethernet performance, particularly for shared storage. If your backup strategy involves network transfers of the backups, these systems must not be playing or recording any clips
- The newsInitAutoBack command does not check for overlapping backup events. Be sure to run it only once and inspect its task listing for collisions.

Template

newsInitAutoBack

Example

```
C:\Program Files\Grass Valley\Aurora\DB Maintenance>
newsInitAutoBack
Added a new job with job ID = 1
SCHEDULED TASKS:
Status ID  Day  Time  Command Line
---------------------
1 Each M  3:00 AM  "C:\Program Files\Vibrint 3.0\
  DB Maintenance\vbrAutoBack.bat"
  C:\Program Files\Grass Valley\Aurora\DB Maintenance>
```

Glossary

ASK

The central registry for all the MediaFrame components. Other software components refer to the ASK component to establish communication and exchange commands and data as well as populate fields and lists.

Asset

See Logical Asset and Physical Asset.

Asset Details

The MediaFrame view that contains detailed information about the assets, including all the associated metadata and storyboard and video proxy information.

Asset List

The MediaFrame view that lists all the assets in a search or a folder.

Asset Navigator

The MediaFrame view that is used for searching logical assets or browsing for physical assets.

Device

In Aurora Browse, a term used to designate a component that contains physical asset. Devices have MDIs that represent the device's assets in a way that is understandable by the other components of the system. This allows the MediaFrame server to coordinate the activity of the system. Different devices perform different functions in the MediaFrame system. For example, the K2 MDI device is used for transferring assets, while the News MDI is used for Aurora Edit assets and the Flashnet (SGL) MDI is used for archiving assets.

Essence

See Physical asset.

FTP

File Transfer Protocol is a common IT protocol for the bulk movement or transfer of large volumes of data. K2 servers can handle multiple FTP transfers simultaneously at faster than real-time speeds.

HD

High Definition video.

Logical Asset

A logical asset is a combination of the MediaFrame database information, physical asset or assets on the server, and proxy assets. A logical asset has a globally unique Universal resource Name (URN) that uniquely identifies it.

Material

A high-resolution clip, upon which the low-resolution proxy is based.

MDI

Managed Device Interface.

MediaFrame

A metadata storage and asset management architecture deployed in the Aurora suite. This architecture shares media asset management (MAM) components with other applications and systems such as servers, Aurora Ingest, and Aurora Edit workstations.

MediaFrame Status

A tool in Aurora Browse that tracks the status of the various components of Aurora Browse.

Metadata

Data about data. For example, metadata can include keywords, descriptions, and other terms that you would use to search for an asset in a database. Foreign metadata is imported XML metadata that is associated with a MediaFrame logical asset.

Offline

In Aurora Browse, offline refers to an asset that has been archived.An asset can be both offline and online simultaneously.

Online

In Aurora Browse, online refers to an asset that is located on the high-resolution server. An asset can be both offline and online simultaneously.

Physical Asset

A physical asset, or essence, is the raw program material, represented by pictures, sound, text video, etc. It carries the actual message or information.

Proxy

A low-resolution clip that represents high-resolution material.

SD

Standard Definition video.

Storyboard

A series of video thumbnails used to show scene changes in an asset.

Storyboard proxy

The low-resolution video clip that provides the thumbnails for the storyboard.

Subclip

A clip created by referencing a portion of media from another clip.

Thumbnail

A frame of video used for visual identification of a clip. By default, the thumbnail is generated in the K2 server from the 16th frame of video. You can select a new thumbnail using the Storyboard.

Thumbnail view

The MediaFrame view that shows the Asset List information with thumbnails instead of strictly textual information.

Transfer Monitor

A tool in Aurora Browse that monitors asset transfers.

Up Conversion

Conversion of an SD (standard definition) video format to an HD ((high definition) video format.

Index