Aurora Browse

MEDIA ASSET MANAGEMENT PLATFORM

Installation and Configuration Guide

SOFTWARE VERSION 6.5

071-8637-01
NOVEMBER 2008

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

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

Revision Status

Rev Date	Description
January 31, 2003	Release to part number 071-8217-00
July 21, 2003	Release for software version 1.5 to part number 071-8217-01
May 25, 2004	Release for software version 2.0. Part number 071-8307-00.
December 16, 2004	Release for software version 2.7. Added information about Advanced Encoder, FlashNet archive, and DIVArchive. Part number 071-8307-01.
August 2, 2005	Release for software version 3.0. New content for NewsShare NAS. Part number 071-8424-00.
April 27, 2006	Release for software version 3.1. Part number 071-8424-01.
September 22, 2006	Release for Aurora software version 6.0b. Part number 071-8518-00.
September 5, 2007	Release for Aurora software version 6.3. Part number 071-8518-01.
November 1, 2008	Release for Aurora software version 6.5. Part number 071-8637-01

Contents

Preface

This Aurora Browse Installation and Configuration Guide is part of a full set of support documentation, described as follows:

- **Aurora Browse Installation and Configuration Guide** — Provides explanations and procedures for installing and configuring the system at a customer site. Includes recovery planning and troubleshooting sections. This document is available electronic form (PDF file) on the Aurora Browse Application CD-ROM.
- **Aurora Online Help** — Provides instructions for using the Browse application. This document is available from the Browse application Help menu.
- **Aurora Browse Release Notes** — Contains the latest information about the product's hardware and the software. The information in this document includes upgrade instructions, feature changes from the previous releases, helpful system administrative information, and any known problems.
- **Aurora manuals** — Each of the Aurora products has its own documentation set. Refer to product manuals as follows:
  - Aurora Edit
  - Aurora Browse
  - Aurora Ingest
  - Aurora Playout

Grass Valley Product Support

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

Web Technical Support

To access support information on the Web, visit the product support Web page on the Grass Valley Web site. You can download software or find solutions to problems by searching our Frequently Asked Questions (FAQ) database.

World Wide Web: http://www.thomsongrassvalley.com/support/
Technical Support E-mail Address: gvgtechsupport@thomson.net.

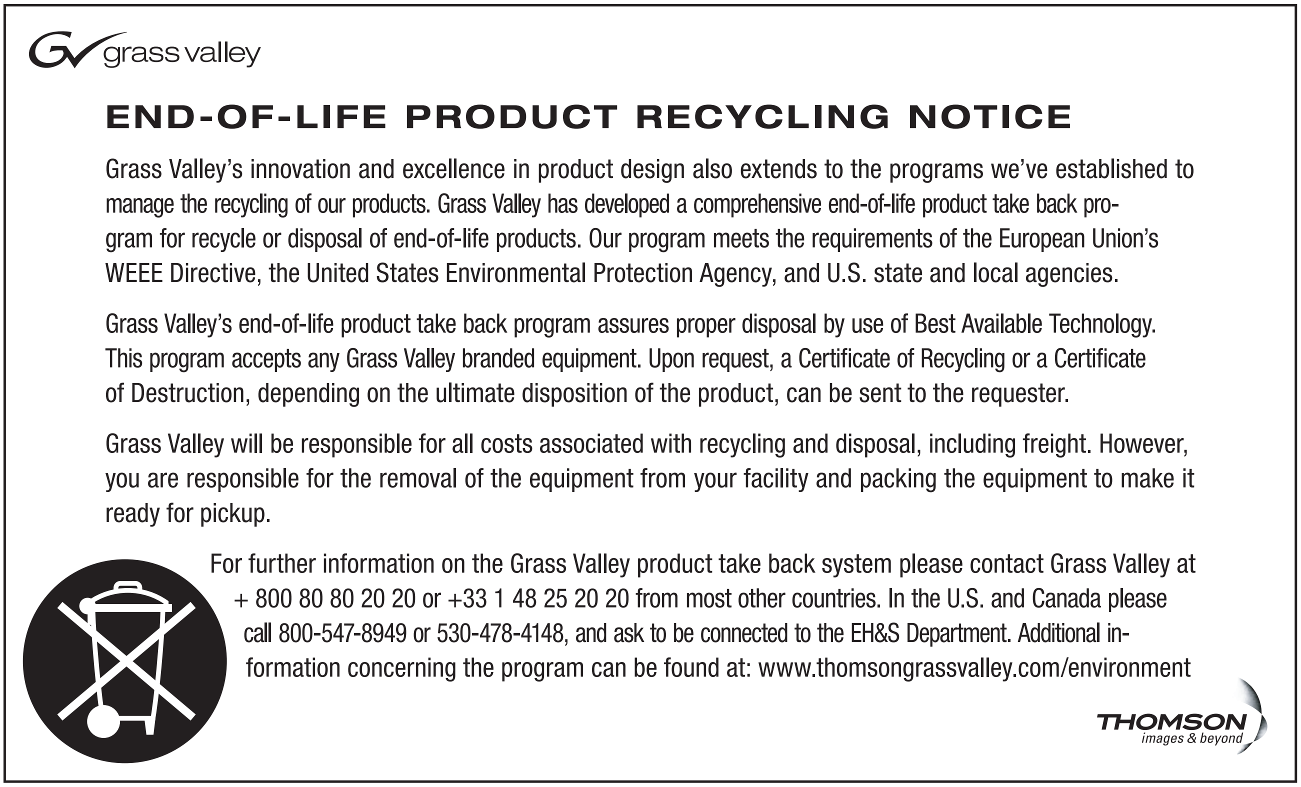
Phone Support

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

International (France)	+800 80 80 20 20 +33 1 48 25 20 20	Italy	+39 02 24 13 16 01 +39 06 87 20 35 42
International (United States, Canada)	+1 800 547 8949 +1 530 478 4148	Belarus, Russia, Tadzikistan, Ukraine, Uzbekistan	+7 095 258 09 20 +33 (0) 2 334 90 30
Hong Kong, Taiwan, Korea, Macau	+852 2531 3058	Indian Subcontinent	+91 11 515 282 502 +91 11 515 282 504
Australia, New Zealand	+61 1300 721 495	Germany, Austria, Eastern Europe	+49 6150 104 444
Central, South America	+55 11 5509 3440	Near East, Africa	+33 1 48 25 20 20
China	+861 066 0159 450	Netherlands	+31 (0) 35 62 38 421
Belgium	+32 (0) 2 334 90 30	Northern Europe	+45 45 96 88 70
Japan	+81 3 5484 6868	Singapore	+65 6379 1313
Malaysia	+603 7805 3884	Spain	+41 487 80 02
Middle East	+971 4 299 64 40	UK, Ireland, Israel	+44 118 923 0499

Authorized Support Representative

A local authorized support representative may be available in your country. To locate the support representative for your country, visit the product support Web page on the Grass Valley Web site.



grass valley

END-OF-LIFE PRODUCT RECYCLING NOTICE

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

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

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

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

THOMSON
images & beyond

Chapter 1

System Overview

Aurora Browse is a media management and editing system. Aurora Browse supports the complete broadcasting workflow — from ingest to editing to distribution to archive.

This chapter includes the following topics:

- “Functional description” on page 11
- “System diagram - K2 storage” on page 12
- “Legacy systems” on page 13

Functional description

Aurora Browse allows desktop browsing of low-resolution proxy copies of both SD and HD high-resolution video material. Aurora Browse provides a rich metadata search engine that allows you to search for clips using various criteria. You can also use the Aurora Browse application to trim assets, add keywords, create subclips, etc., using a low-resolution proxy accessible from your PC. Aurora Browse creates various low-resolution proxy formats for high-resolution material. Proxy formats include MPEG-1, video thumbnails, and storyboards. From the Aurora Browse application you can also archive and restore high-resolution material. Archived assets are still visible from the Aurora Browse application.

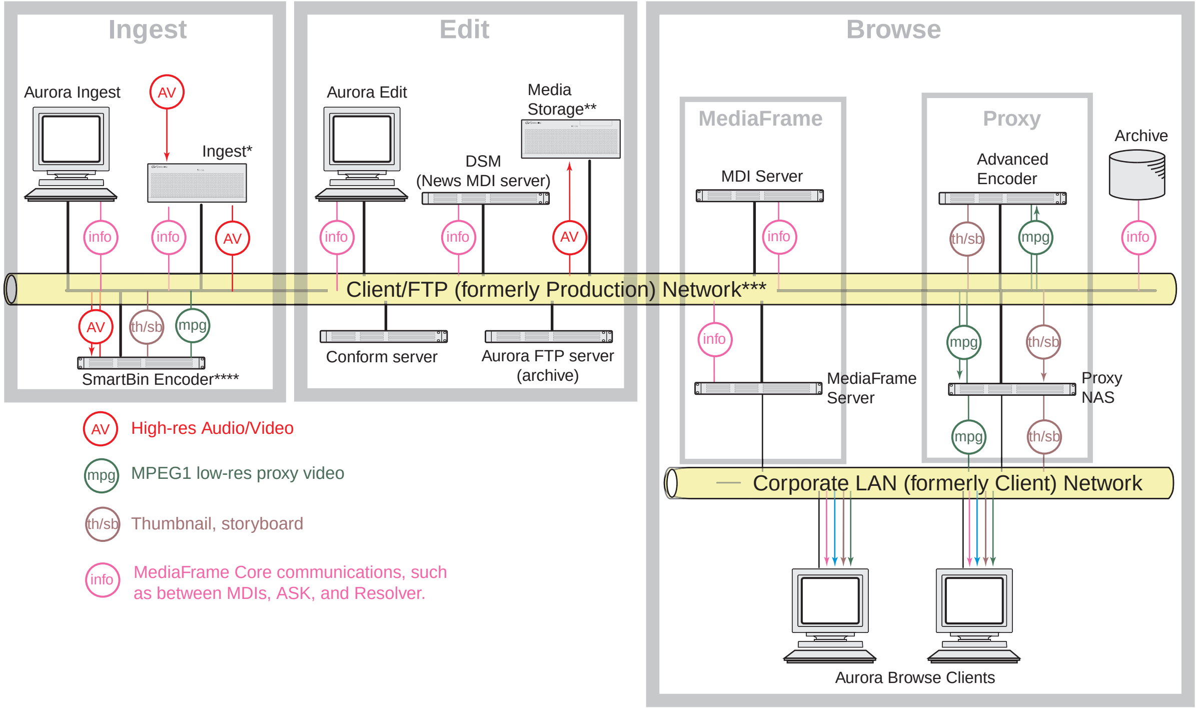
The system is compatible with the K2 storage architecture as well as M-Series iVDR and stand-alone Profile systems. Ingest is controlled by an ingest application, such as Aurora Ingest, and incorporates the K2 system as the video server. The encoder transfers an incoming feed into two formats: a proxy low-resolution (MPEG-1) format stored on the proxy NAS, and a high-resolution format stored on the storage system. Aurora Browse also monitors the storage to create proxy for new high-resolution material. In this way Aurora Edit assets are represented in the system for editing and manipulation.

For descriptions of software components, refer to Appendix A, *Component Interaction Diagrams* on page 111.

The K2 BaseCamp Express is a configuration where the MediaFrame system components are installed on one single server. For more information on the K2 BaseCamp Express, refer to Appendix B, *K2 BaseCamp Express*.

System diagram - K2 storage

This diagram illustrates an example architecture for a system that uses Aurora Ingest for ingest and that accesses high-resolution media on K2 storage.



* The Ingest system can be a K2, M-Series, or stand-alone Profile system.

** The Media Storage is a K2 system.

*** On large systems the Client (formerly called Production) Network can be separated into two networks: one for media and one for control.

**** The SmartBin Encoder also bridges between the Edit and the Browse Proxy systems.

The system illustrated here demonstrates the full range of hardware platform types. Smaller systems might not include all types of hardware platforms. Consult the system design for your specific system to determine the hardware platforms you must install.

Design considerations - Aurora Browse with Aurora Edit

Take the following into consideration when establishing the workflow for your use of Aurora Browse:

Separation of Browse Proxy and Browse metadata — In Aurora Browse 6.5, there is a clear separation of proxy and metadata. For example, someone using Aurora Edit could have a hi-res asset within the MediaFrame database without tying up encoders for the proxy. This would allow them to search, add metadata, perform other tasks.

Minimize proxy creation for short-lived material — The editing process generates multiple pieces of transitional media, but there is no need to create proxy representations of this transitional media. To do so creates an unnecessary load on the system and affects performance.

To avoid this, create at least three designated locations in which material resides to match your workflow, as follows:

- Inbox — This is the location in which newly acquired material arrives. Use a SmartBin—or configure Aurora Browse rules—to automatically create proxy for this material, so you can use Aurora Browse to evaluate and select material for further editing.
- Workspace — This is the location in which you store material undergoing the editing process. Do not configure any Aurora Browse rules to create proxy for this material. This saves encoding resources.
- Outbox — This is the location in which you place material that has been edited and is usable in its current state. You might have one outbox for on-air material and one outbox for review material. Configure Aurora Browse rules to create proxy for this material, so you can use Aurora Browse to select and use this material.

Legacy systems

This manual documents Browse systems using K2 systems for media storage. Existing systems, such as those using Profile XP/Open SAN for media storage, do not match the systems documented in this manual.

You can find some information about earlier systems in Appendix C, *Legacy systems* on page 121. If you need the entire overview and task flow for working on a legacy system, you should refer to the version of this manual that corresponds to the software version around which your system was originally built.

Chapter **2**

Installing Aurora Browse

This chapter provides instructions for installing the hardware platforms and software components that support the system. Use the instructions that are appropriate for your system.

The instructions in this chapter are as follows:

- "Rack-mount hardware components" on page 16
- "About cabling hardware components" on page 16
- "Cable hardware: MediaFrame support" on page 17
- "Cable hardware: Proxy support" on page 21
- "About Aurora Browse software" on page 23
- "Other software installation considerations" on page 29

When you are done installing the hardware and software, continue with Chapter 3, *Configuring the system* and Chapter 4, *Recovery Planning* to complete the installation of your system.

Rack-mount hardware components

Follow the instructions you received with the rack-mount hardware to install each component of the system. One rack-unit spacing is recommended between components for ventilation.

About cabling hardware components

Refer to the system design for your particular system and the appropriate system diagram in Chapter 1, *System Overview* to identify the hardware components and cabling for your system. Then turn to the appropriate cabling instructions and connect cables as required.

Be aware of the following as you cable your system:

- Zoning is not required on the Ethernet switch if five or less clients are active. If more than five clients are using the system, it is strongly recommended that you use an isolated switch or a shared, zoned switch to isolate the client-side LAN. Network traffic from the internal LAN is minimized.
- You may want to postpone cabling to external networks until after configuring respective IP addresses.

Cable hardware: MediaFrame support

The following sections provide instructions for hardware pieces that support MediaFrame components. Use the instructions that apply to your system design.

- "MediaFrame server instructions" on page 17
- "MediaFrame server instructions: HAAR platform" on page 18
- "MDI Server instructions" on page 20

MediaFrame server instructions

The central component of the system is the MediaFrame server. Depending on the design of your system, it can host the following software components:

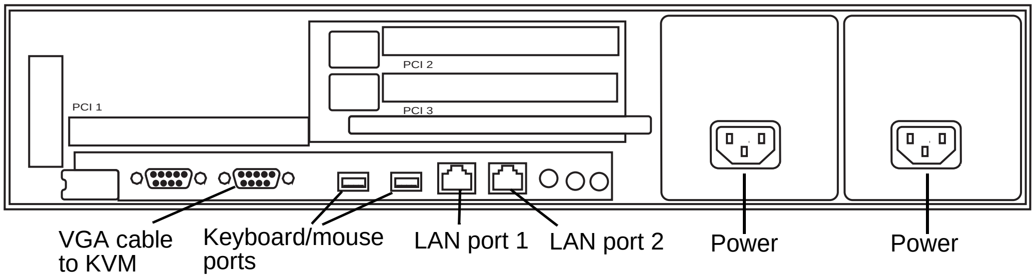
- The Aurora Browse application for user interaction
- The Rules Wizard for background processing
- Managed Device Interface services and the MediaFrame database for holding asset related information in the system

The server connects to all encoders and the Network Attached Storage via the network. Refer to the system diagrams in Chapter 1, *System Overview*. The client network is available for access to the web application.

For the MediaFrame server you have the option of the regular Dell-based platform, as explained in this section, or the HAAR platform, as explained in "MediaFrame server instructions: HAAR platform" on page 18.

The K2 BaseCamp Express also uses the Dell 2950, so the process of cabling is the same for the MediaFrame server or the K2 BaseCamp Express. For more information on the K2 BaseCamp Express, see Appendix B, *K2 BaseCamp Express*.

Regular Dell 2950 platform



Cable as illustrated and as follows:

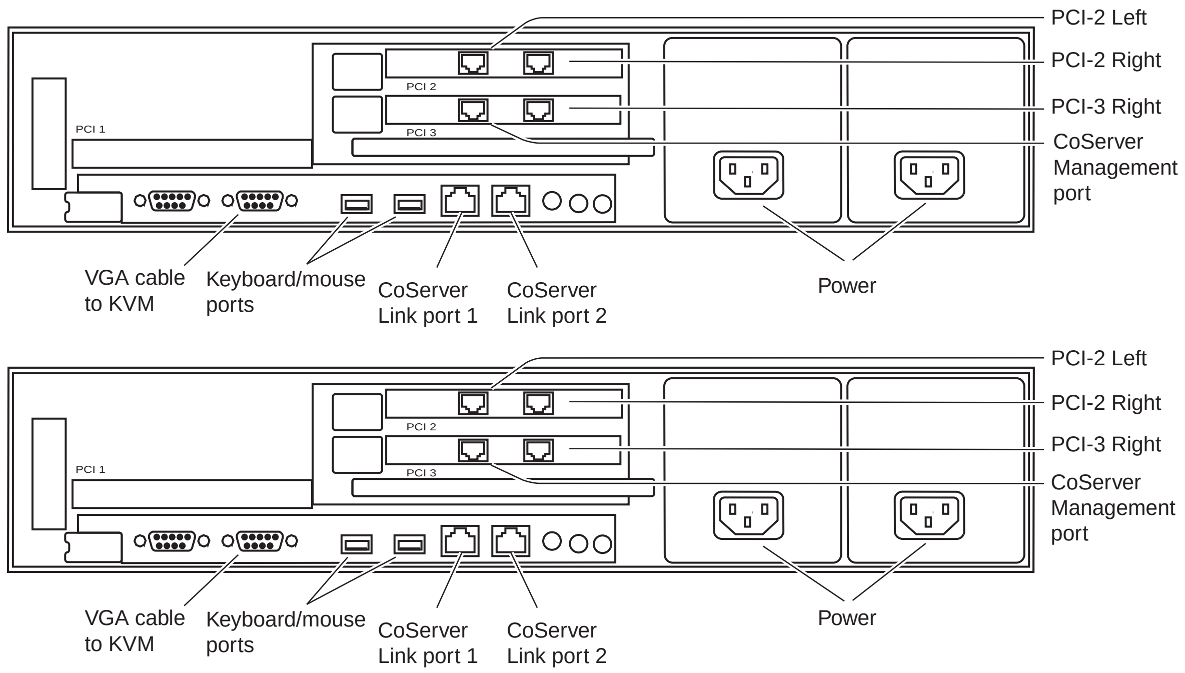
- For systems with one unified Client/FTP LAN (Production Network), connect port 1 to the Client/FTP LAN.
- For systems with a Client/FTP LAN (Production Network) consisting of a control network and an FTP network, connect port 1 to the control network. Connect port 2 to the Corporate LAN (formerly referred to as the Client Network).

MediaFrame server instructions: HAAR platform

For the MediaFrame server you have the option of the HAAR high availability HAAR platform. This platform is made up of two interconnected servers.

NOTE: It is no longer recommended to install Windows Media Player on the HAAR platform because of compatibility problems, so you can not run the Aurora Browse application locally on the HAAR platform.

HAAR platform (Dell 2950 servers)



Cable as illustrated and as follows:

- For systems with one unified Client/FTP LAN (Production Network), connect port PCI-3 Right and the CoServer Management port to the Client/FTP LAN.
- For systems with a Client/FTP LAN (Production Network) consisting of an FTP network and a control network, connect port PCI-3 Right and the CoServer Management port to the control network. Connect port PCI-2 Left to the corporate LAN (Client Network).
- Interconnect CoServer Link ports with cross-over cables.
- Connect power cables to a power supply.

Power supply units are hot-swappable.

To power up the HAAR platform, use the normal procedures for the server and log in to the Windows operating system as normal. The virtual server runs in a full screen window. To get to the physical server desktop, press **Ctrl + Shift + F12**.

To power down the HAAR platform, right-click the system tray icon and select **Manage Endurance Configuration | Shutdown**. This does an orderly shutdown of the virtual server and the physical server.

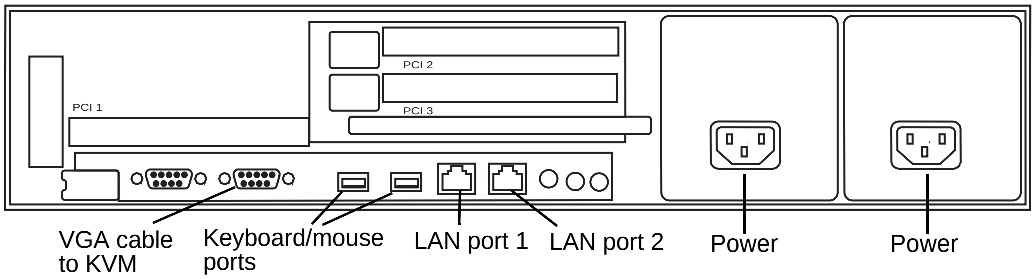
Also refer to "Configure HAAR platform" on page 38 for network configuration procedures.

MDI Server instructions

The MDI server is host for the Managed Device Interface (MDI) services, through which the system gets its visibility of the assets on the various machines in the system.

The MDI server is an optional component. It runs on the regular Dell-based platform. On systems without a MDI server, such as the K2 BaseCamp Express, the MDI services can run on the MediaFrame server (or other Aurora Browse machine).

Dell 2950 platform



Cable as illustrated and as follows:

- For systems with one unified Client/FTP LAN (Production Network), connect port 1 to the Client/FTP LAN.
- For systems with a Client/FTP LAN (Production Network) consisting of an FTP network and a control network, connect port 1 to the control network. Connect port 2 to the corporate LAN.

Cable hardware: Proxy support

The following sections provide instructions for hardware pieces that support the processing and storage of proxy media. Use the instructions that apply to your system design.

- "Encoder instructions" on page 22
- "NAS instructions - Condor" on page 22

Encoder instructions

The following components are hosted by the encoder:

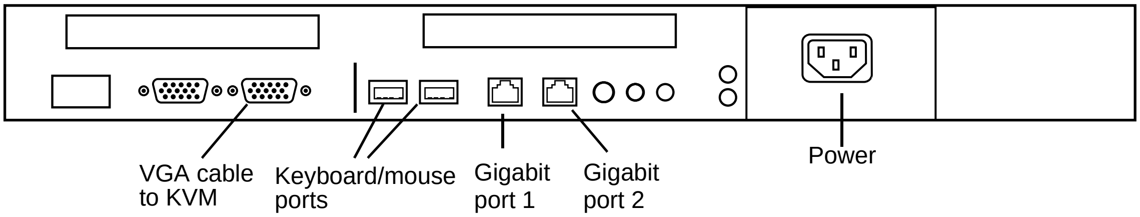
- **Aurora Proxy Encoder**
  - GV Aurora Proxy Encoder service.
  - Aurora FTP service.
- **SmartBin Encoder**
  - vbrSmartBinService
  - SmartBins Setup tool
  - Aurora FTP service.

The encoder does the following:

- Creates MPEG-1 proxy versions of high-resolution video assets that already exist or are actively being recorded on a video server
- Processes MPEG-1 proxy content
- Extracts dynamic scene detection images for storyboard/thumbnail creation

The encoder runs on a Dell 1950.

Dell 1950



Cable as illustrated and as follows:

- For systems with one unified Client/FTP LAN (Production Network), connect Gigabit port 1 to the Client/FTP LAN. Gigabit port 2 is unused.
- For systems with a Client/FTP LAN (Production Network) consisting of an FTP network and a control network, connect Gigabit port 1 to the control network and Gigabit port 2 to the corporate LAN.

NAS instructions - Condor

The Network Attached Storage (NAS) unit provides storage for MPEG-1 proxy video, storyboards, and thumbnails. For information on how to install and configure the NAS for your K2 system, see the *K2 Storage System Instruction Manual* and the *K2 Lx0 RAID Storage Instruction Manual*. For information on how to prepare the Condor NAS for Aurora Browse, refer to **"Prepare NAS - Condor" on page 46**.

About Aurora Browse software

In a new system, the hardware platforms come from the factory with software pre-installed, so you should not need to install Aurora Browse software.

If you need to install software for an upgrade, refer to the instructions listed below for general information about Aurora Browse software. For version-specific instructions, check *Aurora Browse Release Notes*. Also refer to "Other software installation considerations" on page 29.

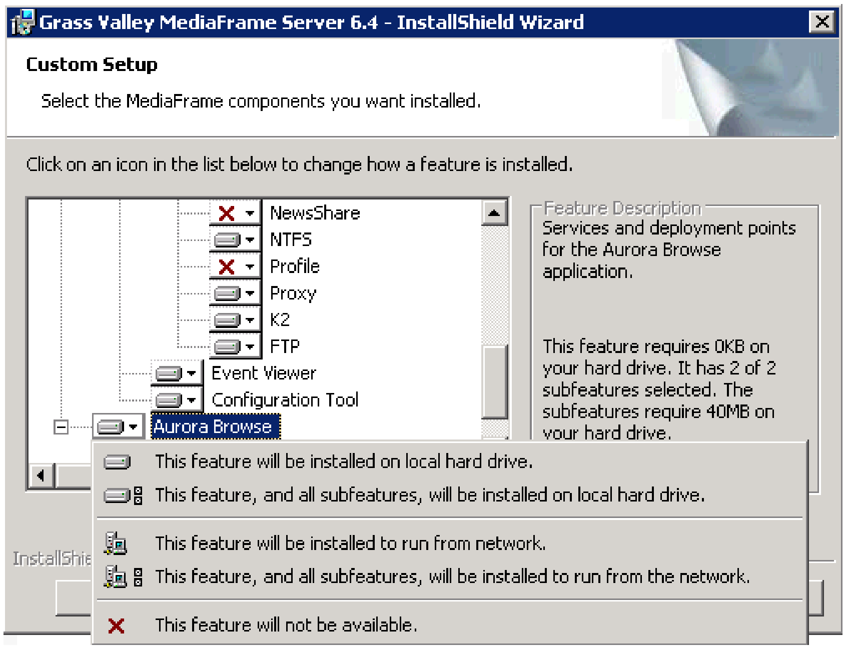
Remember to backup up the database before upgrading software, as explained in Chapter 4, *Recovery Planning*.

The following installation programs are on the Aurora Browse Application CD:

- *…\AdvancedEncoder\Setup.exe* — Use this setup file to install Aurora Browse software on an Aurora Proxy Encoder.
- *…\Server\Setup.exe* — Use this setup file to install Aurora Browse software on the MediaFrame server as well as other Aurora Browse machines. The following table indicates the machines on which the software components are typically installed. You might install components differently, depending on the design of your particular system.

Install Components	**MediaFrame server**	**MDI Server**	**DSM**	**Client PC**
Core Services	✓			
Managed Devices: FlashNet Archive		✓		
Profile		✓		
Proxy	✓			
NTFS	✓			
Avalon Network Archive		✓		
DIVA Archive		✓		
News			✓	
M-Series		✓		
K2		✓		
Generic FTP		✓		
Aurora Browse Application				✓

To install the software components listed in the preceding table, run the MediaFrame server install program and when you arrive at the Custom Setup screen, do the following:



Grass Valley MediaFrame Server 6.4 - InstallShield Wizard

Custom Setup

Select the MediaFrame components you want installed.

Click on an icon in the list below to change how a feature is installed.

Feature Description

Services and deployment points for the Aurora Browse application.

This feature requires 0KB on your hard drive. It has 2 of 2 subfeatures selected. The subfeatures require 40MB on your hard drive.

NewsShare
NTFS
Profile
Proxy
K2
FTP
Event Viewer
Configuration Tool
Aurora Browse
This feature will be installed on local hard drive.
This feature, and all subfeatures, will be installed on local hard drive.
This feature will be installed to run from network.
This feature, and all subfeatures, will be installed to run from the network.
This feature will not be available.
InstallShie

If a component that you want to install displays a red X, click the component and select **This feature will be installed on local hard drive.**

If a component that you do not want to install does not display a red X, click the component and select **This feature will not be available**.

To upgrade Aurora Browse software from a previous version, refer to *Aurora Browse Release Notes* for version-specific instructions.

NOTE: When upgrading software, read messages and respond carefully. Do not accept the default "Yes" when prompted to delete databases.

Install software for K2 support

If your system includes a K2 Storage System and Aurora Proxy Encoders, you need to install the following software, in this order:

1. StorNext File System
2. Grass Valley Generic iSCSI Client Installation
3. GVG_MLib software

After installing software, configuration is also required, as instructed in the following sections later in this manual:

- “Prepare encoders” on page 40
- “Add encoders to the K2 Storage System” on page 40.

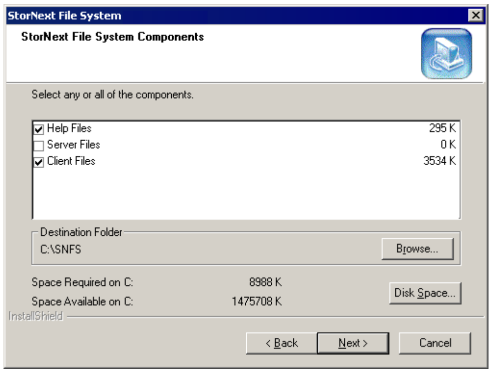
Installing the StorNext File System

The StorNext File System software is located on the Aurora Suite CD-ROM. Refer to release notes to verify the version.

NOTE: Use the standard SNFS installer, not the “simple” installer which is designed for K2 systems only.

To install the StorNext software:

1. Navigate to the directory that contains the software.
2. Double-click on the setup.exe file.
3. Install the software following these instructions:

On this screen...	Do this...
Welcome (2 screens)	Click **Next**.
License Agreement	Click **Yes**.
Choose Destination Location	Accept the default location and click **Next**.
StorNext File System Components	Select **Help Files** and **Client Files**; do not select Server Files.  StorNext File System StorNext File System Components Select any or all of the components. ☑ Help Files 295 K □ Server Files 0 K ☑ Client Files 3534 K Destination Folder C:\SNFS Space Required on C: 8988 K Space Available on C: 1475708 K Browse... Disk Space... InstallShield < Back Next > Cancel
Select Program Folder	Accept the default location and click **Next.**

On this screen...	Do this...
Start Copying Files	Click **Next**.
Choose Options to Complete the Installation	Leave the checkbox blank and click **Next**.
File System Name Service Locations	Enter the name or IP address of the K2 Media Server and click **Next**.
Confirm File System Name Services Host List	Click **Next**.
Establish StorNext File System Drive Mapping and Credentials?	Click **No**; this will be configured automatically when you run the K2 Configuration application later.
StorNext File System Setup	Click **Finish**.

4. Reboot the computer when prompted.

Installing the Generic iSCSI Client Software

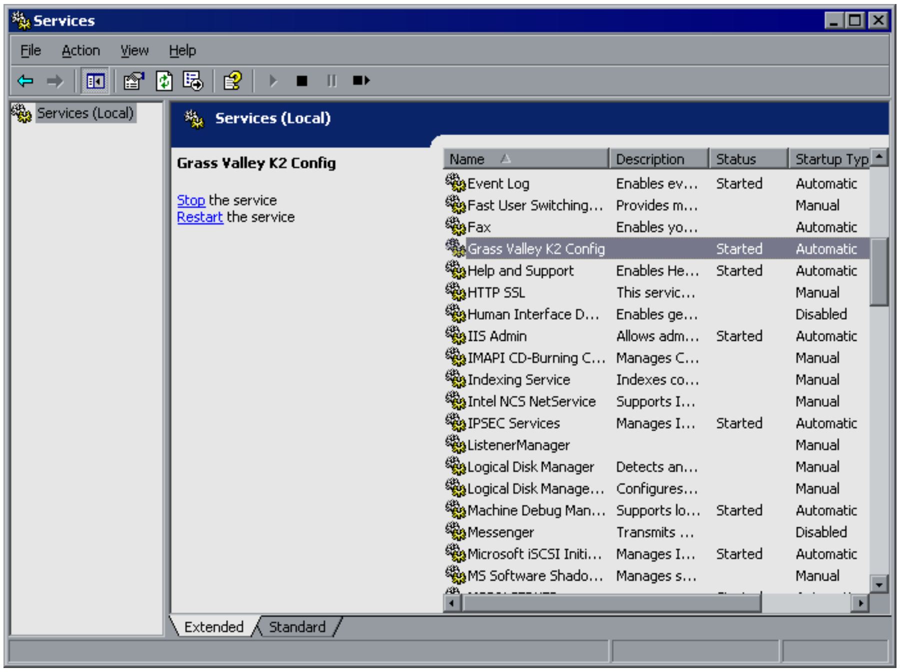
The Generic iSCSI Client software is located on the Aurora Suite CD-ROM. Refer to release notes to verify the version.

To install the software:

1. Navigate to the directory that contains the software.
2. Double-click on the setup.exe file.

   The Microsoft iSCSI Initiator software also installs. When the Microsoft iSCSI Initiator software install completes, the Generic iSCSI Client software install continues.
3. Once the Generic iSCSI software is installed, restart the machine.
4. When the machine comes back up, check the services as follows:
   - Go to **Start | Settings | Control Panel | Administrative Tools | Services**. The

Services Control Panel opens.



Grass Valley K2 Config

Stop the service
Restart the service

Name	Description	Status	Startup Typ
Event Log	Enables ev...	Started	Automatic
Fast User Switching...	Provides m...		Manual
Fax	Enables yo...		Automatic
Grass Valley K2 Config		Started	Automatic
Help and Support	Enables He...	Started	Automatic
HTTP SSL	This servic...		Manual
Human Interface D...	Enables ge...		Disabled
IIS Admin	Allows adm...	Started	Automatic
IMAPI CD-Burning C...	Manages C...		Manual
Indexing Service	Indexes co...		Manual
Intel NCS NetService	Supports I...		Manual
IPSEC Services	Manages I...	Started	Automatic
ListenerManager			Manual
Logical Disk Manager	Detects an...		Manual
Logical Disk Manage...	Configures...		Manual
Machine Debug Man...	Supports lo...	Started	Automatic
Messenger	Transmits ...		Disabled
Microsoft iSCSI Initi...	Manages I...	Started	Automatic
MS Software Shado...	Manages s...		Manual

- Make sure that the service named “Grass Valley K2 Config” is started.

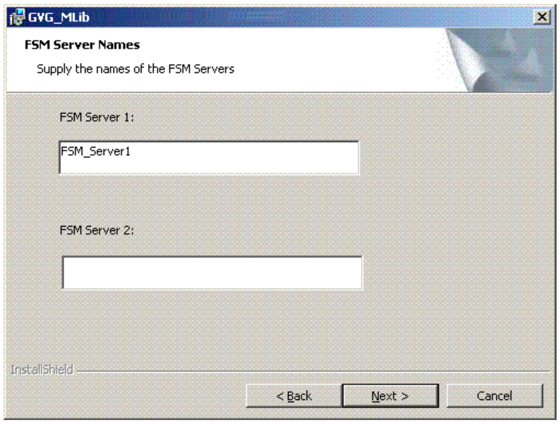
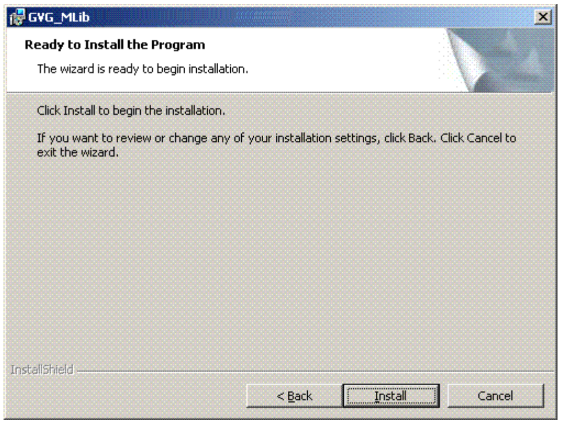
Installing the GVG_MLib Software

The GVG_MLib software is located on the Aurora Suite CD-ROM. Refer to release notes to verify the version.

To install the software:

1. Insert the Aurora Edit CD into your CD drive.
2. Navigate to **Software Installs | GV_MLib**.
3. Double-click on **Setup.exe**.

Install the software following these instructions:

On this screen...	**Do this...**
Welcome	Click **Next**.
Setup Type  GVG_MLib **FSM Server Names** Supply the names of the FSM Servers FSM Server 1: FSM_Server1 FSM Server 2: 	Enter the name of the K2 server. If you have a back-up server, enter that name as well; otherwise, leave the second entry space blank. Click **Next**.
Ready to Install l  GVG_MLib **Ready to Install the Program** The wizard is ready to begin installation. Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard. 	To review or change your settings, click **Back.** To begin the installation process, click **Install**.
Installation Complete	Click **Finish**. The workstation prompts you to reboot so the new settings take effect.

Other software installation considerations

- Make sure that Aurora FTP is installed on the Aurora Proxy Encoder.
- To support archive functionality, you must install a unique Aurora FTP on a platform somewhere in the system. Refer to "Archive stage" on page 84.
- The Aurora Browse application is no longer a web-based application. In previous versions, it was installed on the MediaFrame server and served to individual client PCs via HTTP. In Aurora Browse 6.5, like the Aurora Edit LD application, it is a Windows executable and it is installed locally on each client PC. There is no requirement to install the Aurora Edit LD application on the MediaFrame server. You can find the installation file on the Aurora Edit LD Installation CD.
- Aurora Edit and Aurora FTP are prerequisites for News MDI.
- The Aurora Browse Server and NAS need to have the clocks set to the same time, or to be connected to the network for NTP.
- If you have MediaFrame client applications on a different Windows domain from the MediaFrame server, you need to define a trust relationship (one way or two way). For example, you could have your MediaFrame system on Windows domain A with a trust in the B domain. Applications running on Windows domain B can then connect to the MediaFrame server on Windows domain A.

Chapter 3

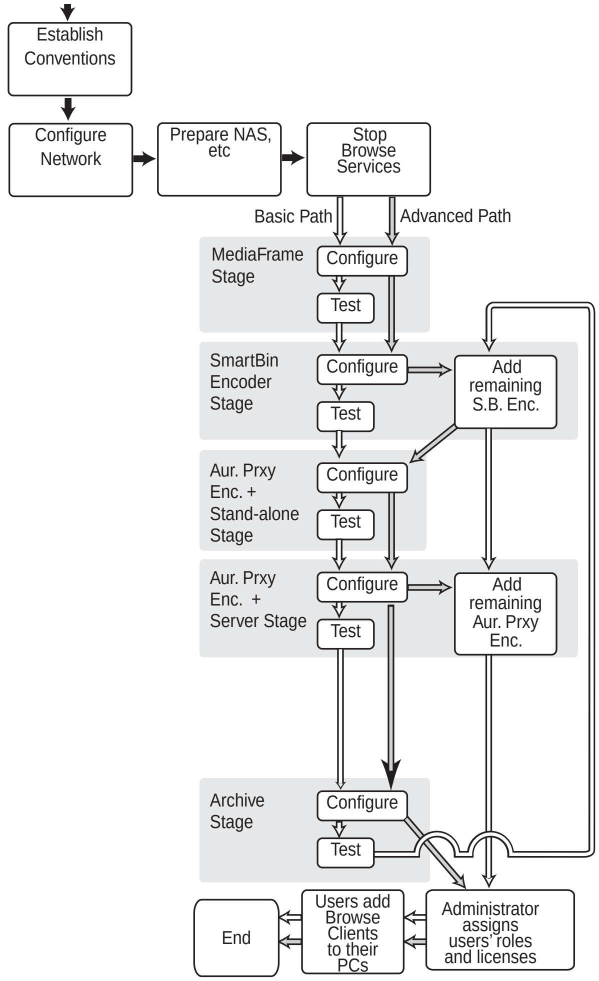
Configuring the system

You can use the topics in this chapter in the following ways:

- Initial configuration — After your system components are rack mounted, cabled, and the physical installation process is complete, continue with the configuration instructions in this chapter to create a working system. You can follow the **Basic** path or the **Advanced** path through the core configuration stages, as explained "Configuration overview - K2 storage" on page 32.
- Customizing — After the system is functioning, you can go back to the configuration pages and modify the settings to customize the system to fit any special workflow requirements.

The topics in this chapter include the following:

Configuration overview - K2 storage



This flowchart illustrates the major tasks required for configuring a system that accesses K2 storage.

Before beginning this task flow make sure that the K2 storage and iSCSI networks are set up.

Core configuration tasks are broken down into stages. You can work through the configuration stages in different ways, as follows:

> If you are new to the system, follow the **Basic** path.This path allows you to learn the system and resolve configuration problems in stages, with a minimal number of configuration variables and machines added to the system at each stage. Then, after you have gained the understanding to make each stage of the system work properly, configure the remainder of the system and add all machines.
>
> If you are experienced with the system and you want the fastest possible configuration, follow the **Advanced** path and configure the entire system in one pass, adding all machines at each stage.

You can also choose a combination of Basic and Advanced paths to suit your level of understanding and the design of the particular system you are configuring.

This task flow assumes the use of the standard Aurora Browse application for testing and verification. If you are using the Aurora Edit LD application, refer to the Aurora Edit LD Release Notes, which you can find on the Aurora Edit LD Installation CD.

Refer to the topics in the remainder of this chapter for detailed instructions on each task.

Establish conventions

The following conventions are recommended to make your system easier to work on and understand. Refer to these sections as necessary as you configure your system.

Machine naming convention

Choose a root name (based on the site, etc.) and use the following convention for naming machines. Illegal MDI names are a forward slash (/) and an asterisk (*).

Machine type	Name
MediaFrame machines	
MediaFrame server	*root*-nb-svr
Managed Device Interface (MDI) Server	*root*-nb-mdi
Proxy machines	
Aurora Proxy Encoder	*root*-nb-adv-1…n
SmartBin Encoder	*root*-nb-sbe-1…n
Network Attached Storage (NAS)[a]	*root*-nb-nas-1…n
Ingest machines	
K2 system	k2-1…n
Stand-alone Profile Media Server	pvs-1…n
M-Series iVDR	ivdr-1...n
Legacy machines	
Live monitor encoder	*root*-nb-live-1…n

[a] Some NAS devices have restricted characters for naming. For example, the Fastora NAS can't have underscores, while the Ciprico NAS can't have dashes.

If you use a UIM in your system, make sure you follow the UIM naming convention.

On Aurora Share systems, the client prefix name is used to identify the system as shared. The prefix separator can be an underscore or a hyphen. For example, WXYZ-Edit and WXYZ_Edit are valid names.

MDI and Encoder logical names convention

As you configure your system you must create and enter logical names for the various software components (services) that provide functionality. These logical names provide a mapping of the functionality of the standard Aurora Browse services to the specific machines in your particular system. For this reason you should take care to create logical names that are easy to identify and interpret as they appear in the various configuration pages.

It is especially important that you distinguish between the logical name of a software component and the hostname of the machine to which the software component relates. In the conventions suggested in this manual, machine names are lower case and logical names are upper case to make this distinction.

The software components that require logical names are as follows:

- MDIs — The system uses a Managed Device Interface (MDI) to manage a device that is not a platform for MediaFrame software. Typically these are the machines on which media resides, such as Media Servers, NAS devices, and archive devices. Each type of device has its own MDI. The MDI software component is usually hosted on the MediaFrame server or an MDI server, rather than being hosted on the same machine that it manages.
- Encoder services — The system uses services to manage the media processing that takes place on the Aurora Browse encoder machines. Typically these are a type of "transfer" service. This type of software component is hosted on the machine that it manages.

Also refer to "Ports and services mapping" on page 36.

The following table demonstrates how logical names for software components are mapped to the machines of your system and provides a suggested naming convention.

Machine type	Service that manages the machine	MDI/Encoder logical name(s)	Comments
Aurora Proxy Encoder	GV Aurora Proxy Encoder	ADV1, ADV2, ADV3…	One logical name is required for each Aurora Proxy Encoder.
Avalon Archive	GV Avalon Archive MDI	ARCHIVE1	Most systems have only one archive MDI—of the appropriate type for the archive product—that manages the entire archive system.
DIVA Archive	GV DIVA MDI		
FlashNet Archive	GV FlashNet MDI		
K2	GV K2 MDI	K2-STORAGE1	When this MDI accesses a K2 Storage System, it manages one designated K2 Media Clients on the shared storage system. The MDI should be named for the K2 Storage System.
		K2-1, K2-2, K2-3,…	When this MDI manages a stand-alone K2 Media Client, there is one MDI for each K2 Media Client. One logical name is required for each stand-alone K2 Media Client system that integrates with the system.
M-Series	GV MSeries MDI	M-SERIES1, M-SERIES2, M-SERIES3,…	One logical name is required for each M-Series iVDR that integrates with the system.
News	GV News Share MDI	NEWS1	There is only one News MDI in the system. It manages the hi-res media storage system for Aurora assets.
NTFS	GV NTFS MDI	NTFS1	There is only one NTFS MDI in the system. It manages NTFS storage on one or more machines—typically the server and the NAS machines. This MDI is used by the internal MediaFrame system only. If you need a generic Windows device for transfers, use the Generic FTP MDI.

Machine type	Service that manages the machine	MDI/Encoder logical name(s)	Comments
Profile	GV Profile MDI	PROFILE1, PROFILE2, PROFILE3,…	When this MDI manages a stand-alone Profile XP system, there is one MDI for each Profile XP. One logical name is required for each stand-alone Profile XP system that integrates with the system.
Proxy	GV Proxy MDI	PROXY1	There is only one Proxy MDI in the system. It manages the storage locations on all the NAS machines.
SmartBin Encoder	vbrSmartBinService	SBE1, SBE2, SBE3…	One logical name is required for each SmartBin Encoder.

Ports and services mapping

Aurora Browse and MediaFrame software components run as Windows services, which communicate over designated ports. Topics later in this manual provide instructions for entering port numbers on each configuration page. Do not create your own convention for port usage. Designate ports as specified in the following table:

Services	Port	Comments
MediaFrame Services		
GV Ask	9010	—
GV Asset Manager	9022 and 9023	—
GV Avalon Archive MDI	9120	—
GV DIVA MDI	9122	—
GV FlashNet MDI	9124	—
GV FTP MDI	9128	Formerly Thomson NLS MDI
GV K2 MDI	9160	The service manages a number of host processes, one for each K2 system that is being managed. These host processes require ports 9160 - 9169. Stopping/starting the service stops/starts all of the host processes.
GV License Manager	9012	—
GV Metadata	9014	Not visible on a configuration page
GV MSeries MDI	9140	The service manages one host process for each managed M-Series iVDR. These host processes require ports 9140 - 9149. Stopping/starting the service stops/starts all of the host processes.
GV News Share MDI	9150	—
GV NTFS MDI	9115	—
GV Profile MDI	9130	The service manages one host process for each managed Profile. These host processes require ports 9130-9139. Stopping/starting the service stops/starts all of the host processes.
GV Proxy MDI	9110	—
GV Resolver	9016	Not visible on a configuration page
GV Subscription Manager	9024	—
GV Transfer Manager	9020	—
Proxy Services		
GV Aurora Proxy Encoder	9230	Starting range for first control.
GV RulesWizard	9018 and 9019	Not visible on a configuration page
vbrSmartBinService	9230	Installed by the Aurora Suite, along with the SmartBins Setup tool.

These services are normally distributed on different machines in the system, not on any one machine, as explained in "Accessing services" on page 48. The system also depends upon Microsoft Internet Information Services (IIS) and SQL services.

NOTE: The K2 BaseCamp Express server supports the GV FTP MDI and the K2 MDI.

Configure network - K2 Storage

Unless otherwise indicated, all information in this chapter refers to the two tier network architecture for Aurora Browse on K2 storage. Also refer to the system diagram in Chapter 1, *System Overview*.

Set up IP addresses and name resolution

The following instructions apply for systems that do not use the classic workgroup/ host table networking.

Systems may use Microsoft DNS for name resolution. The domain controller should provide this service. If the system does not have a domain controller, another machine may be configured to provide this service. Properly configuring all client network interfaces is extremely important to make DNS name resolution work correctly.

The following applies to the control network on systems expanded to contain two networks—control and media:

- The control network should be set to use Dynamic Host Configuration Protocol (DHCP) to assign network IP addresses. All interfaces on this network should be configured to register connections with DNS automatically.

The following applies to the media network on control/media network systems and to the Production network overall on systems with a single, unified Production network:

- Network interfaces should be configured with static IP addresses. These interfaces must also be configured not to automatically register their connections with DNS; each interface on the media network should be manually added as a host entry with "_he0" appended to the host name. These entries ensure that high-priority network traffic is routed over this network.

When configuring networks, you should consider K2 Storage System networking as well. For example, the K2 Storage System "media" network is actually the iSCSI network. This is not the same as the Aurora Browse "media" network. The Aurora Browse "media" network is the equivalent of the K2 FTP/Streaming network. Also, if host tables and fixed IP addresses are required on parts of the K2 Storage System, make sure DHCP/DNS is configured to allow the fixed IP addresses.

Refer to "Host table files" on page 134 for an example of a host table.

Configure network settings on Client/FTP LAN (Production Network) machines

Use the instructions in this section to configure Client/FTP LAN (Production Network) machines, which are all those of the following types:

- Aurora Proxy Encoder
- Smartbin Encoder

From the factory, the machines are set with static IP and as members of "WORKGROUP". Change the IP addresses, using standard Windows procedures.

Configure HAAR platform

To configure the HAAR platform for the Aurora Browse networks, do the following:

1. On either CoServer 1 or CoServer 2, configure the virtual server’s network settings as follows:
   a. Configure PCI-2 A for the Production network. This is the CoServer Management port.
   b. Configure PCI-2 B for the Production network.
   c. Configure PCI-1 A for the Client network.
2. Copy these configurations onto the virtual server.

Do not modify the IP addresses of the CoServer Link ports. They are used only for communication between the servers. Refer to “MediaFrame server instructions: HAAR platform” on page 18.

Configure network settings on Client network machines

Use the instructions in this section to configure Client network machines, which include the following types:

- MediaFrame server
- Managed Device Interface (MDI) Server

NAS machines are also on the Client network. You configure NAS machines in “Prepare NAS - Condor” on page 46.

DHCP/DNS will provide IP addresses and name resolution for the Aurora Browse devices attached on the client Domain. Refer to “Set up IP addresses and name resolution” on page 37.

You will need the following information from the customer's IT department:

- Verify that the subnet mask for the Aurora Browse machines should be 255.255.255.0.
- Extra IP addresses for future growth
- The IP address for the DNS server and alternate
- The name of the Domain connected on the client side (e.g. example.com)
- The IP address for the WINS server if applicable

In addition, the customer IT department must add these computers to their Domain.

Proceed with Client network machines as follows. Use standard Windows procedures:

1. Name computer and add computer to Domain
2. Set IP address for each port, DNS servers
3. Set DNS settings

Firewall considerations

Some sites require that there be a firewall between the Production Network and the Client Network. The firewall should allow incoming HTTP (TCP port 80) connections for client and configuration connections to the MediaFrame server inside the private network. Additionally, ports should allow incoming packets so requests to the Proxy NAS can be properly processed. The port that needs to be open is port 445 for TCP and UDP for Windows and SAMBA shares

Prepare for core configuration stages

Do the following tasks in preparation for the configuration of core system functionality.

Prepare NLS device

Use the following information to prepare the Near Line Storage (NLS) device to be a part of the MediaFrame system.

You no longer need to configure an NLS MDI. Configure the Generic FTP MDI instead. (For more information, see "Configure Proxy MDI" on page 66.)

Before configuring the Generic FTP MDI to specify transfer targets, verify that the corresponding FTP communications are working without errors.

Prepare MediaFrame Server for News systems

If using the MediaFrame server with a News system, you need to add a user to the list of users and give the proper permissions.

NOTE: Users need to be added to both the administrator group and the iis_wpg group.

1. In Computer Manager, select **Local Users and Groups | Users**.
2. Add the appropriate user:
   - If on a domain, user: **Vibrint Service**
   - If not on a domain (local user), user: **VibrintLocalService**
3. Enter the password: **Vibrint01801** (the password is case sensitive).

Prepare DSM

By convention, the News MDI runs on the DSM. If this is true in your system, you must map the V: drive on the DSM. If the News MDI is not on the DSM, you must map the V: drive on whatever machine is hosting the News MDI.

Prepare encoders

- For K2 systems, make sure SNFS and iSCSI software is correctly installed. Refer to "Install software for K2 support" on page 25.
- Add encoders to the K2 Storage System, as explained in the following section. Refer to "Add encoders to the K2 Storage System".
- On your Aurora Proxy Encoders, in the Aurora FTP configuration, make sure that the drive is mapped to the K2 or AuroraShare storage. Verify that the mapped drive is V:, unless there are multiple volumes, in which case the mapped drives are V:, W:, X:, Y:.

Add encoders to the K2 Storage System

If your system includes a K2 Storage System, you must add Aurora Proxy Encoders to the K2 Storage System, as instructed in this section.

Before you add the encoders to the K2 Storage System, refer to the *K2 Storage System Instruction Manual* and other procedures in this manual as necessary to verify the following:

- Make sure you've installed the software required for K2 support on the Aurora Proxy Encoders and SmartBin encoders. Refer to "Install software for K2 support" on page 25.
- Set up the Control Point PC.

NOTE: The Control Point PC cannot be a K2 Media Client, K2 Media Server, Aurora Proxy Encoder, or SmartBin encoder, nor can it be part of a computer that is running any Profile XP software.

- Run the K2 Configuration application to set up the K2 Server and the GigE switch.
- Connect the Aurora Proxy Encoders and SmartBin encoders to the K2 Server via the GigE switch. This is the storage connection.

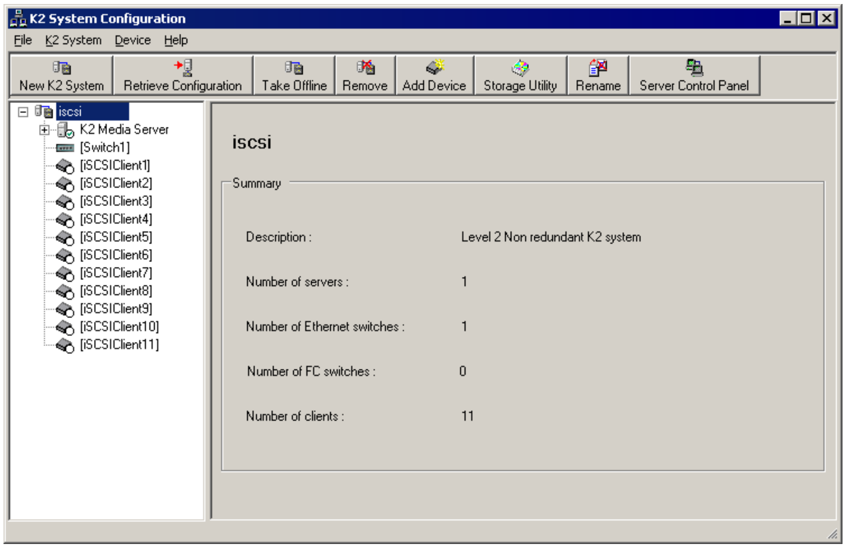
Configuring encoders with the K2 System Configuration application

You use the K2 System Configuration application wizard to configure each of the Aurora Proxy Encoders on the iSCSI network.

NOTE: You must have the same local username and password, with administrative privileges, across all the machines in your Aurora Browse system. For more information, see ***"About the administrator account" on page 47***.

1. On the Control Point PC, open the K2 System Configuration application.
2. At the login dialog box, log in with the correct administrator account.
   By default this is as follows:
   - User name: administrator
   - Password: adminK2

   The K2 System Configuration application appears, displaying a hierarchy of machines with the K2 Media Server at the top, followed by the GigE switch, and then each of the K2 Clients:



iscsi

Summary

Description : Level 2 Non redundant K2 system

Number of servers : 1

Number of Ethernet switches : 1

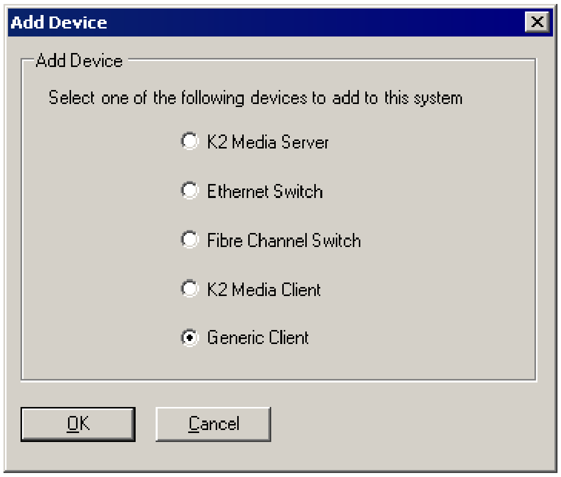
Number of FC switches : 0

Number of clients : 11

3. To add an Aurora Proxy Encoder or SmartBin encoder to the list, do the following:

   a. Select the media server and click **Add Device**.

.



Add Device

Select one of the following devices to add to this system

○ K2 Media Server

○ Ethernet Switch

○ Fibre Channel Switch

○ K2 Media Client

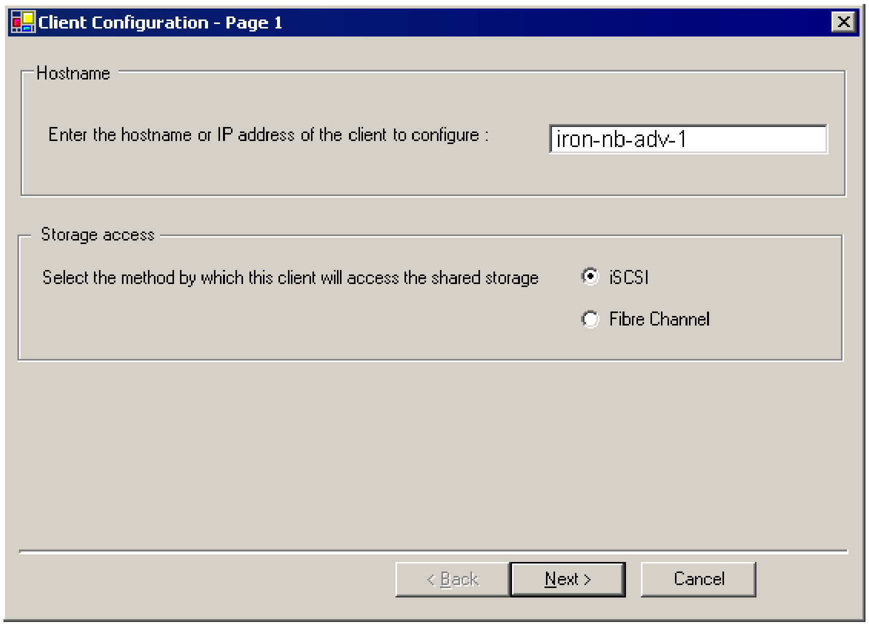
● Generic Client

   b. In the Add Device window, click **Generic Client** and click **OK**.

      A new client device gets added to the hierarchy.

4. Select the client to be configured in the hierarchy view and click **Configure**.

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



Client Configuration - Page 1

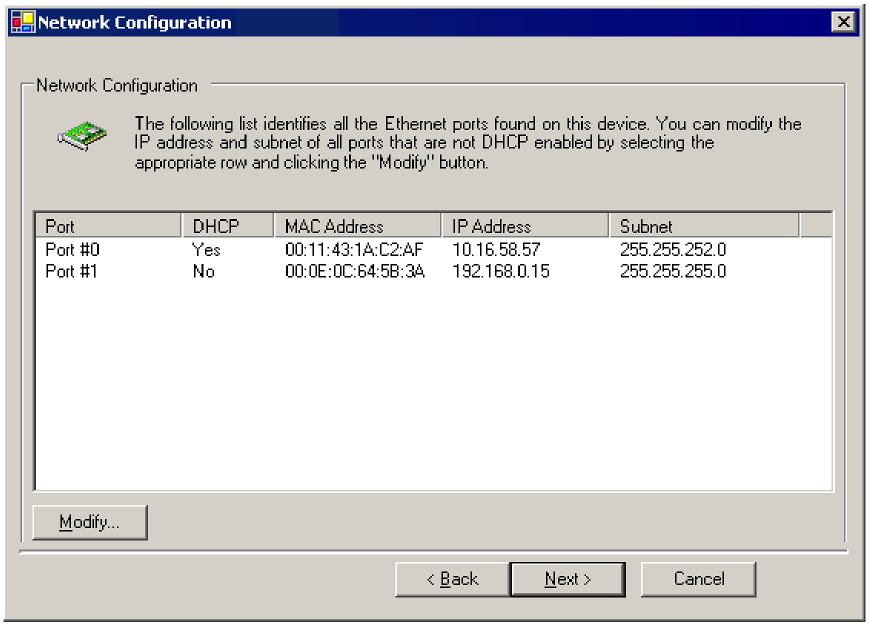
Hostname

Enter the hostname or IP address of the client to configure : iron-nb-adv-1

Storage access

Select the method by which this client will access the shared storage ● iSCSI ○ Fibre Channel

5. At the Client Configuration - Page 1 screen, do the following:
   a. Enter the machine name of the Aurora Proxy Encoder or SmartBin encoder you are configuring (such as `iron-nb-adv-1`).
   b. Select **iSCSI**.
   c. Click **Next**.



Network Configuration

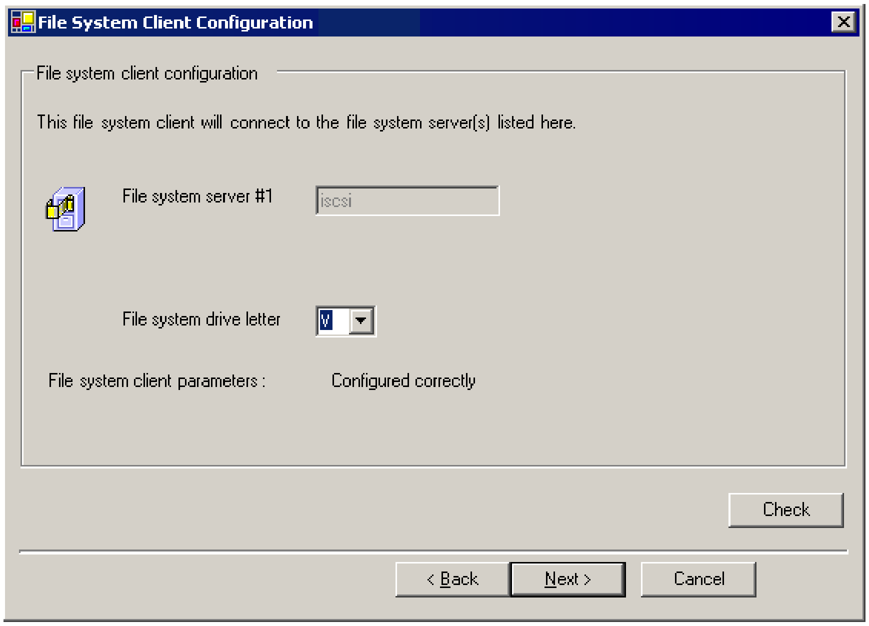
Network Configuration

The following list identifies all the Ethernet ports found on this device. You can modify the IP address and subnet of all ports that are not DHCP enabled by selecting the appropriate row and clicking the "Modify" button.

Port	DHCP	MAC Address	IP Address	Subnet
Port #0	Yes	00:11:43:1A:C2:AF	10.16.58.57	255.255.252.0
Port #1	No	00:0E:0C:64:5B:3A	192.168.0.15	255.255.255.0

6. At the Network Configuration screen, click **Modify** to change the IP address and subnet of network adapters for this machine, and then click **Next**. You cannot

configure the adapter over which the K2 System Configuration application is currently communicating.



File System Client Configuration

File system client configuration

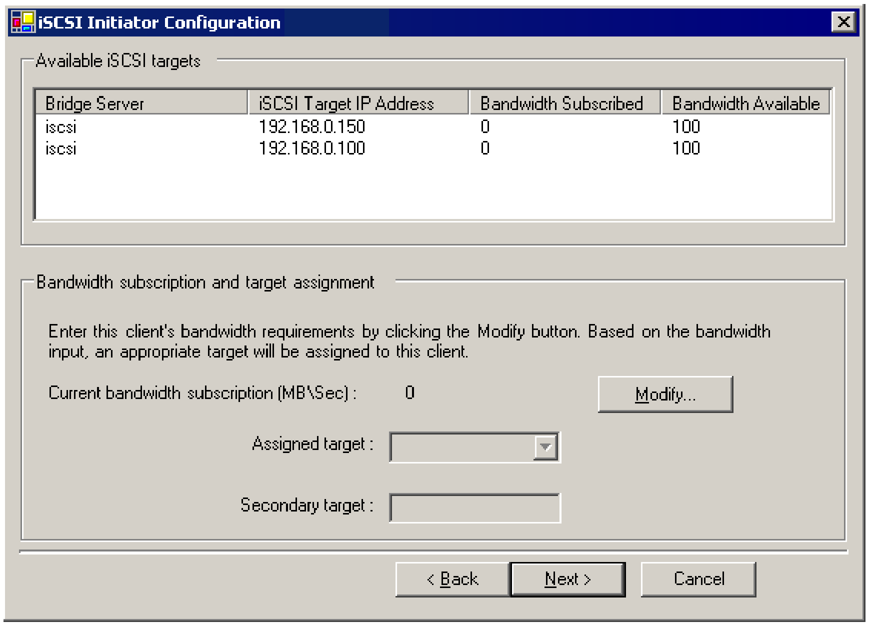
This file system client will connect to the file system server(s) listed here.

File system server #1: iscsi

File system drive letter: V

File system client parameters : Configured correctly

7. At the File System Client Configuration screen, enter the drive letter you wish to configure as the iSCSI drive on the encoder machine; click **Next**. This letter should be the same for all machines that are iSCSI clients in this K2 Storage System.



iSCSI Initiator Configuration

Available iSCSI targets

Bridge Server	iSCSI Target IP Address	Bandwidth Subscribed	Bandwidth Available
iscsi	192.168.0.150	0	100
iscsi	192.168.0.100	0	100

Bandwidth subscription and target assignment

Enter this client's bandwidth requirements by clicking the Modify button. Based on the bandwidth input, an appropriate target will be assigned to this client.

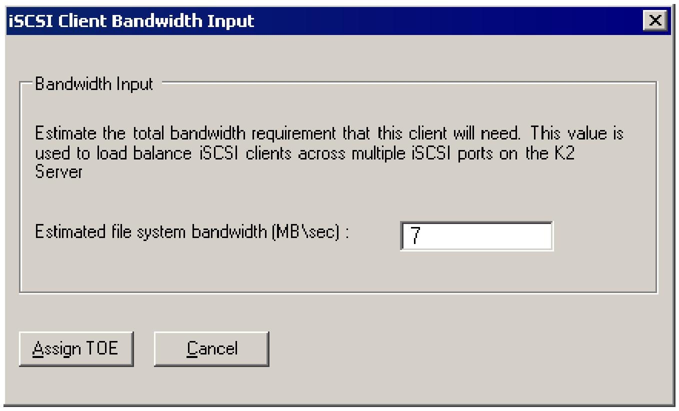
Current bandwidth subscription (MB\Sec) : 0

Assigned target :

Secondary target :

8. At the iSCSI Initiator Configuration screen, enter client bandwidth:

   a. Click **Modify**.



iSCSI Client Bandwidth Input

Bandwidth Input

Estimate the total bandwidth requirement that this client will need. This value is used to load balance iSCSI clients across multiple iSCSI ports on the K2 Server

Estimated file system bandwidth (MB\sec) : 7

b. Enter the total bandwidth requirement for this encoder machine. (For instructions see the next section, "Calculating encoder bandwidth" on page 45).

c. Click **Assign TOE**.

9. Click **Next**.

4. At the Completing the Configuration Wizard screen, click **Finish**.

   The wizard closes and the encoder reboots.

5. Repeat this procedure for each Aurora Proxy Encoder or SmartBin encoder that is an iSCSI client on the K2 Storage System.

Calculating encoder bandwidth

One feature of the K2 iSCSI network is its ability to load balance each iSCSI client's connection to the K2 storage system. In order to do this, calculate the amount of bandwidth each client machine will use, using this formula:

(Video Bit Rate in Mbps x Number of Streams) / 8 (to convert to MB)

1. Determine the highest bit rate you use on the Aurora Proxy Encoder or SmartBin encoder.

   The bit rates for the DV formats are: DV25 = 28.8 Mbps; DV50 = 57.6 Mbps; and DV100 = 115.2 Mbps for the NTSC and PAL video formats.

   MPEG bit rates are variable; enter the bit rate set in Aurora Edit.

2. Multiply the highest bit rate by the number of streams that are licensed on this machine. Only one stream should be configured on an Aurora Proxy Encoder or SmartBin encoder (Aurora FTP and SmartBin Service if there is one), so for encoders you always multiply the highest bit rate by 1, which of course does not change the value.

3. Divide that number by 8 to convert Mbps to MB.

4. Round the MB number to the nearest integer.

5. Enter this number in the iSCSI Client Bandwidth Input screen in the K2 Configuration application wizard.

6. At the conclusion of the configuration process, the K2 Configuration application restarts the encoder.

Prepare NAS - Condor

This section describes how to prepare the Condor NAS for the Aurora Browse networks. For information on how to install and configure the NAS for your K2 system, see the *K2 Storage System Instruction Manual* and the *K2 Lx0 RAID Storage Instruction Manual*.

If you are configuring the Windows Fastora NAS for the Aurora Browse network, refer to “NAS instructions - Fastora” on page 122.

Before you prepare the NAS, make sure the following requirements are met:

- The MediaFrame Server and NAS need to have the clocks set to the same time, or they need to be connected to the network for NTP.
- You must have the same local username and password, with administrative privileges, across all the machines in your Aurora Browse system. For more information, see “About the administrator account” on page 47.

To configure the Condor NAS for the Aurora Browse networks, do the following:

1. From any Production network machine, enable the network to recognize the NAS by adding an IP address within the 192.168 range.
2. Make a share. Share name: media.
3. Assign user privileges for the media folder as follows:

   Everyone — Modify

   administrators — Full Control
4. Click OK.

Verify Proxy NAS access from production network machines, which are machines of the following types:

- MediaFrame server
- Aurora Proxy Encoder

To verify access, from each production network machine do the following:

1. Open Windows Explorer and navigate to the media directory on the NAS. You can do this with the following path:

   \\root-nb-nas-1\Media
2. Verify basic read/write capabilities by creating, modifying, and deleting a simple text file.

To verify access from client network machines, choose a machine on the Client network that can represent a Aurora Browse client PC and that is convenient for testing.

3. Verify that Aurora Browse client PCs will have modify rights.

About the administrator account

You must have the same local username and password, with administrative privileges, across all the machines in your Aurora Browse system. This account is critical for most Aurora Browse proxy access, as explained in this section.

The same local administrator account is required on the following machines:

- Proxy NAS machines
- Aurora Proxy Encoder
- SmartBin encoder
- MDI server
- MediaFrame server
- Aurora DSM
- K2 systems
- M-Series iVDR
- Profile XP

All NAS machines require that an administrator account has permission to the folder on the NAS that the encoders write to, and that the MediaFrame server reads from.

The basic principle is that any service that requires write access to the Proxy NAS must run as the same administrator account. This is a local machine account (NOT a domain account). This includes all encoders, the MediaFrame server, the News MDI, the Proxy MDI (which deletes files off of the Proxy NAS) and the Profile MDI.

On K2 systems and M-Series iVDRs, security is invoked, which requires administrator privilege. This privilege comes from the administrator account, (identical username and password) on the local machine, which is identical with the administrator account on the other devices.

From a Windows networking perspective, when a user account is defined on a local computer rather than a Domain Controller, the account is a "local" account, whose complete name is <computer name>\<username>, rather than <domain>\<username>. For example, with an encoder named *Encoder1*, a MediaFrame server named *Server1*, and a NAS named *NAS1*, there are three separate local accounts: *Encoder1\admin*, *Server1\admin*, and *NAS1\admin.*

The Windows network automatically maps a local account from one computer onto the local account of another computer—as long as both the account name and the password are identical. To enable this mapping to occur, the Windows Domain Controller "synchronizes" the local accounts on computers ***at the time they join the Domain***. Therefore, if the administrator account is added to the NAS machine ***after*** the Windows NAS has joined the Windows Domain, this synchronization does not occur. If the proper sequence is not followed and the problem does occur, the workaround is to remove the NAS from the Windows Domain and then re-add it immediately thereafter.

Accessing services

Software components are distributed among the machines that make up the system. These software components run as Windows services. A machine has the services that correspond to the software components it hosts.

When you change the configuration for a particular software component through the configuration pages, you must restart that software component's service to put the changes into effect. Click **Start | Settings | Control Panel | Administrative Tools | Services** to access the services. All service names start with "GV…", so they group together in the services list.

Refer to "Ports and services mapping" on page 36 for a list of services.

Accessing system configuration settings

Once you have installed MediaFrame Config tool, you can access the configuration sections from the MediaFrame Configuration Manager. From the Start menu, navigate to Programs and **select Grass Valley | MediaFrame Config**.

The MediaFrame Configuration tool tabs allow you to configure the settings required for each component of the Aurora Browse system. You must have administrator permissions on the machine.

NOTE: You must have the same local username and password, with administrative privileges, across all the machines in your Aurora Browse system. For more information, see ***"About the administrator account" on page 47***.

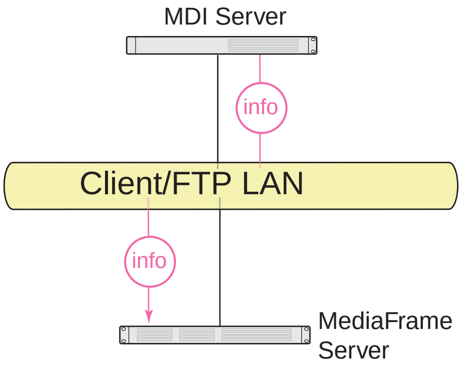
Stop services

Before beginning your initial core configuration stages, you must make sure all Thomson Grass Valley (GV) services are stopped. This prevents the creation of corrupt database records and other errors that result from a partially configured system.

Go to each machine and make sure all "GV…" services are stopped and set to manual, as described in "Accessing services" on page 48. Then, when you configure each stage, start the appropriate services to put the settings into effect. This brings the system on-line in an orderly fashion that allows you to verify system interactions and identify configuration problems.

NOTE: It is especially important that the Rules Wizard is not running during configuration stage tests that create media files. When a test media file is created, the Rules Wizard can trigger the creation of various types of proxy media. This causes problems because the partially configured system is unable to handle the proxy correctly.

MediaFrame stage



MediaFrame components make up the core platform on which Aurora Browse runs. The primary MediaFrame components that you need to configure are as follows:

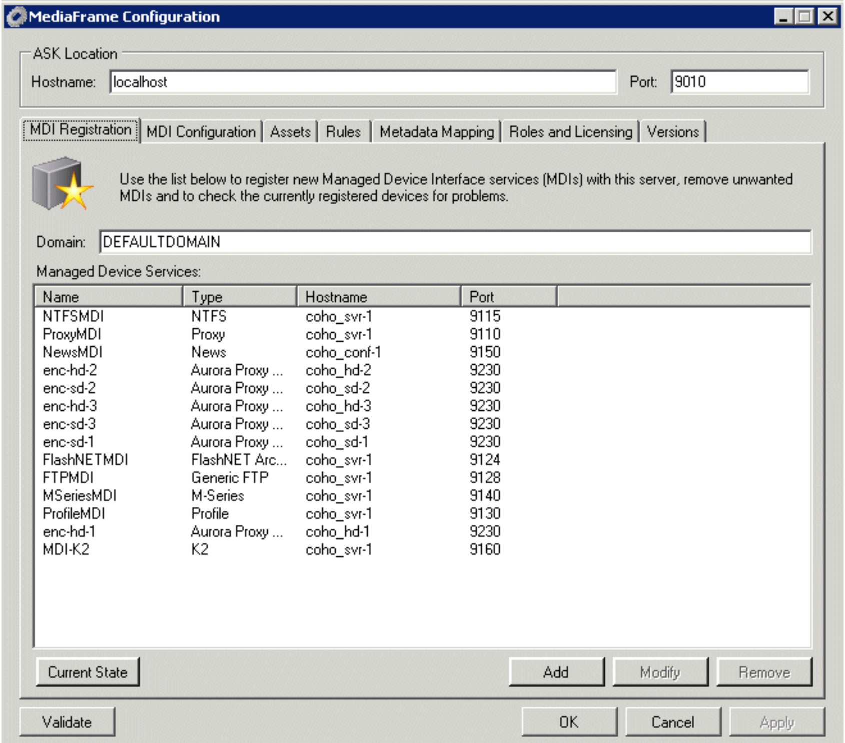
- ASK — The ASK software component runs on the MediaFrame server. It is the central registry for all the software components of the system. As software components carry out tasks in a functioning system they regularly refer to the ASK component to establish communication and exchange commands and data. The configuration pages also refer to the ASK component to populate fields and lists and to validate the values you enter as you configure the system.
- MDIs — Devices have Managed Device Interfaces (MDIs) which represents 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.

In this configuration stage you add an MDI server and then set up logical names for software components that manage devices. This brings the machines of your system on-line as managed devices. (The MediaFrame server can function as an MDI server, unless your system is very large.)

To do the basic configuration and testing of the MediaFrame software components, do the following, as appropriate for the devices in your system:

- "Configure Media Frame ASK: Register components" on page 51
- "Prepare MDI server" on page 54
- "Configuring transfer targets" on page 55
- "Configure ASK Location: MDI server" on page 56
- "Configure Generic FTP MDI" on page 57
- "Configure K2 MDI" on page 58"Configure M-Series MDI" on page 60
- "Configure News MDIs" on page 62
- "Configure Profile MDI" on page 64
- "Configure Proxy MDI" on page 66

Configure Media Frame ASK: Register components



ASK Location

Hostname: localhost Port: 9010

Use the list below to register new Managed Device Interface services (MDIs) with this server, remove unwanted MDIs and to check the currently registered devices for problems.

Domain: DEFAULTDOMAIN

Managed Device Services:

Name	Type	Hostname	Port
NTFSMDI	NTFS	coho_svr-1	9115
ProxyMDI	Proxy	coho_svr-1	9110
NewsMDI	News	coho_conf-1	9150
enc-hd-2	Aurora Proxy ...	coho_hd-2	9230
enc-sd-2	Aurora Proxy ...	coho_sd-2	9230
enc-hd-3	Aurora Proxy ...	coho_hd-3	9230
enc-sd-3	Aurora Proxy ...	coho_sd-3	9230
enc-sd-1	Aurora Proxy ...	coho_sd-1	9230
FlashNETMDI	FlashNET Arc...	coho_svr-1	9124
FTPMDI	Generic FTP	coho_svr-1	9128
MSeriesMDI	M-Series	coho_svr-1	9140
ProfileMDI	Profile	coho_svr-1	9130
enc-hd-1	Aurora Proxy ...	coho_hd-1	9230
MDI-K2	K2	coho_svr-1	9160

1. To register the MediaFrame components, select **Programs| MediaFrame Config** and select the **MDI Registration** tab.
2. Port 9010 is required. Do not modify. See "Ports and services mapping" on page 36.
3. All Domain names in the MediaFrame system must be identical.
4. To add an MDI/encoder, click **Add**.
5. When you are finished, click **OK**.
6. To put changes into effect, start or restart the ASK service.

For the conventions mentioned in the following table, refer to "MDI and Encoder logical names convention" on page 33.

When you add an MDI or Encoder logical name for this type of machine/ device…	Select "MDI/ Encoder Type"…	Enter "MDI/ Encoder Name"…	Enter "Host Name or IP"…	Enter "Port"…	Comments
A K2 Storage System (SAN)[a]	K2	As per convention.	Hostname of the machine hosting the K2 MDIs. Typically the MDI Server.	9160 - 9169	These are process ports, as explained in "Ports and services mapping" on page 36. Assign numbers in an intentional sequence, so they are easy to match in "Configure Generic FTP MDI" on page 57.
K2 Media Client - Internal storage (stand-alone)	K2				
Open SAN Profile	Profile	As per convention.	Hostname of the machine hosting the Profile MDIs. Typically the MDI server	9130 - 9139	The Open SAN Profile is not supported in 6.5, only the stand-alone. These are process ports, as explained in "Ports and services mapping" on page 36.
Stand-alone Profile	Profile				
M-Series	MSeries	As per convention.	Hostname of the machine hosting the M-Series MDIs. Typically the MDI server	9140 - 9149	These are process ports, as explained in "Ports and services mapping" on page 36.
NLS	Generic FTP	As per convention.	Hostname of the machine hosting the Generic FTP MDI. Typically the MDI server	Leave field blank. Correct port number is automatically entered on "Add MDI". Refer to "Ports and services mapping" on page 36 to verify.	—
Aurora Edit	News	As per convention.	Hostname of the machine hosting the News MDIs. This must be the DSM.		—
NTFS storage on Windows machines	NTFS	NTFS1, as per convention.	MediaFrame server hostname, as the server is the required NTFS MDI host.		—
Aurora Proxy Encoder	Aurora Proxy Encoder	As per convention	Aurora Proxy Encoder hostname		—
Proxy	Proxy	PROXY1, as per convention.	Hostname of the machine hosting the Proxy MDI. Typically the MDI server.		—
Archive device	… Archive	ARCHIVE1, as per convention.	Hostname of the machine hosting the archive MDI		—
SmartBin Encoder	SmartBin Encoder	As per convention.	SmartBin encoder hostname		

[a] For a K2 Storage System, the MDI manages one of the connected K2 Media Clients. As per convention, name the MDI for the K2 Storage System.

NOTE: The MediaFrame server must host the NTFS MDI and the Proxy MDI.

In the MediaFrame Configuration Manager, the ASK settings register the logical names for the MDIs and Encoders required by your MediaFrame system with the ASK software component, which runs on the MediaFrame server.

Note the following distinction when entering “Hostname or IP”:

- For MDIs (K2, Profile, M-Series, News, Proxy, NTFS, Archive) enter the hostname of the machine hosting the MDI software component, rather than the hostname of the machine being managed by the MDI.
- For Encoders (Aurora Proxy Encoder, SmartBin Encoder) enter the hostname of the encoder itself.

Prepare MDI server

A machine that hosts a MDI service takes the role of a MDI server. Refer to the following to identify the machines in your MediaFrame system that take the role of MDI server, and make sure that the appropriate MDI services are installed. Refer to "About Aurora Browse software" on page 23.

Dedicated MDI server — For medium to large MediaFrame systems, to ensure system performance, most MDI services are on a stand-alone MDI server machine. If your system has a dedicated MDI server, it comes from the factory with MDI services installed, so you do not need to do any further installation. The MDI server requires only network communication in preparation for its use in the MediaFrame system.

MediaFrame server as MDI server — For small MediaFrame systems, including the K2 BaseCamp Express, the MDI services can reside on the MediaFrame server. The MediaFrame server comes from the factory with MDI service installed, to support these smaller systems, so you do not need to do any further installation. The MediaFrame server also has the NTFS MDI service installed, as it is required to run on the server, regardless of the size of the system.

DSM server as MDI server — For all systems, the News MDI must be hosted on the DSM. You must install the News MDI on the DSM.

Configuring transfer targets

On many MDI configuration pages there is a section for configuring transfer targets. When you configure a transfer target, you specify the following:

- The MDI through which the MediaFrame system has access to the files sent or received.
- The IP address of the FTP interface that handles the transfer of the files.

For the different device-types that can be transfer targets, there are different relationships between the MDI that accesses the files and the device that hosts the FTP interface. The following table specifies how to configure transfer targets to maintain the correct MDI/FTP relationships.

When configuring this type of MDI as a transfer target…	And that MDI manages this type of device…	Enter this as the MDI name…	And then enter FTP IP address… (NOTE: Do not enter the FTP hostname)	And when you add the transfer target, it appears as follows, in "Existing Transfer Targets", for example…	Notes
K2	K2 Media Client (stand-alone)	The MDI that manages the K2 Media Client.	The FTP IP address of the K2 Media Client.	K2-1:192.168.101.1	—
	K2 Storage System (SAN)	The MDI that manages the one designated K2 Media Client on the SAN	The FTP IP address(es) of the K2 Media Server(s) with role of FTP server.	K2-STORAGE1:192.168.101.11,192.168.101.12	—
Profile	Profile XP (stand-alone)	The MDI that manages the Profile XP system.	The IP address of the Profile XP system.	PROFILE1 192.168.100.1	Make sure that UIM addressing requirements are correct in host tables
MSeries	M-Series iVDR	The MDI that manages the iVDR.	The IP address of the iVDR	M-SERIES1:192.168.100.51	
News	The AuroraShare storage system.	The MDI that manages the AuroraShare storage.	The IP address of the AuroraFTP (or NewsFTP) host.	NEWS1:192.168.100.71	If you use K2 FTP instead of AuroraFTP, make sure that you do not exceed K2 limits for the number of transfer sessions.

NOTE: In Aurora 6.5, you no longer need to configure transfer targets in the archives.

Configuring round robin transfers

Round robin is a method for distributing transfers requests from a K2, News, M-Series or Profile MDI server to multiple transfer servers. For example, to set up a round robin archive from a News MDI, add two transfer servers to the News MDI configuration.

First transfer request — handled by the first transfer server listed.

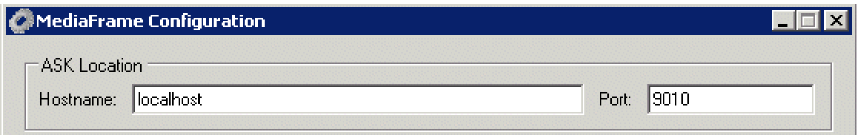
Second transfer request — handled by the second transfer server in the list.

Third transfer request — handled by the first transfer server.

Fourth transfer request — handled by the second transfer server.

Configure ASK Location: MDI server

The ASK location tells the MDI server where to look for the ASK service, which runs on the MediaFrame server. The function of the ASK is to store the location of the software components in the system, so the components can find one another.



Hostname: localhost
Port: 9010

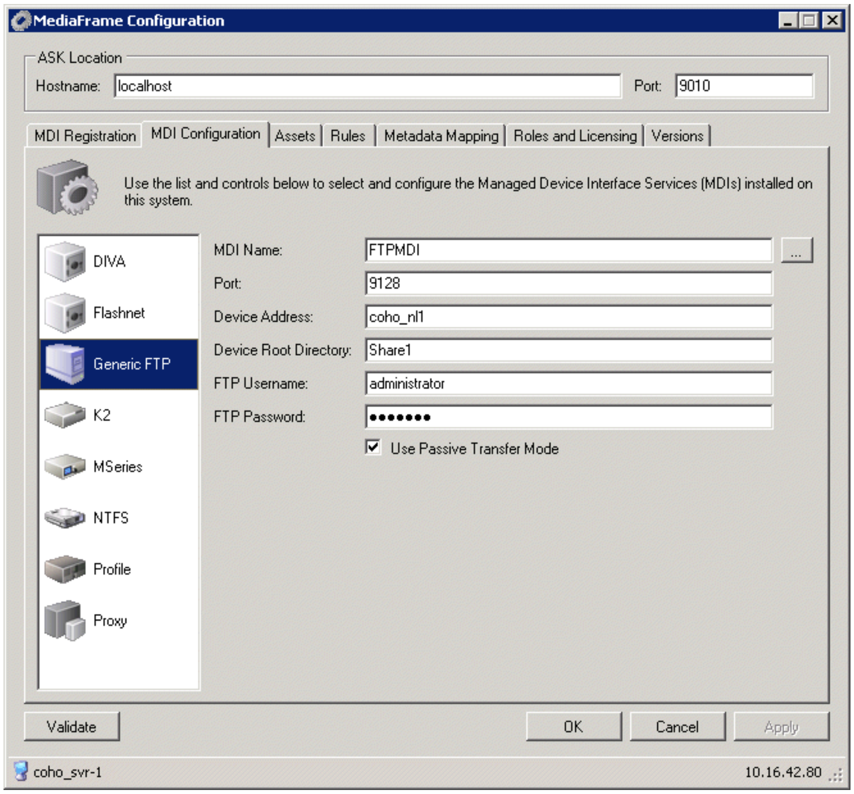
1. Select **Programs | MediaFrame Config** and select the **MDI Configuration** tab.
2. Enter the name of the MediaFrame server.
3. Port 9010 is required. Do not modify. See "Ports and services mapping" on page 36.

   It is not necessary to restart a service to put these settings into effect.

Configure Generic FTP MDI

This page configures the Generic FTP Managed Device Interface (MDI). The Generic FTP MDI replaces the NLS (Near Line System) MDI.

NOTE: You no longer need to specify transfer targets in the Generic FTP MDI. Depending on your system, specify the transfer target in the News or K2 MDI.



ASK Location

Hostname: localhost

Port: 9010

Use the list and controls below to select and configure the Managed Device Interface Services (MDIs) installed on this system.

MDI Name: FTPMDI

Port: 9128

Device Address: coho_nl1

Device Root Directory: Share1

FTP Username: administrator

FTP Password: •••••••

☑ Use Passive Transfer Mode

coho_svr-1 10.16.42.80

1. Locally on the MDI Server, select **Programs| Grass Valley | MediaFrame Config**. Select the MDI Configuration tab and the Generic FTP MDI icon.
2. Enter the MDI name to log in to the FTP interface on the NLS device. Use the **...** button to browse the list of available MDIs.
3. Port 9128 is required. See "Ports and services mapping" on page 36.
4. Enter the hostname or IP address of the device, the root directory on the FTP server to which assets will be transferred, and the FTP username and password.
5. Check Passive Transfer Mode if you want to transfer assets from one server to another without having the data go through the MDI. Enable passive transfer on the FTP server first.

To put changes into effect, click **Apply** to start or restart GV FTP MDI Service.

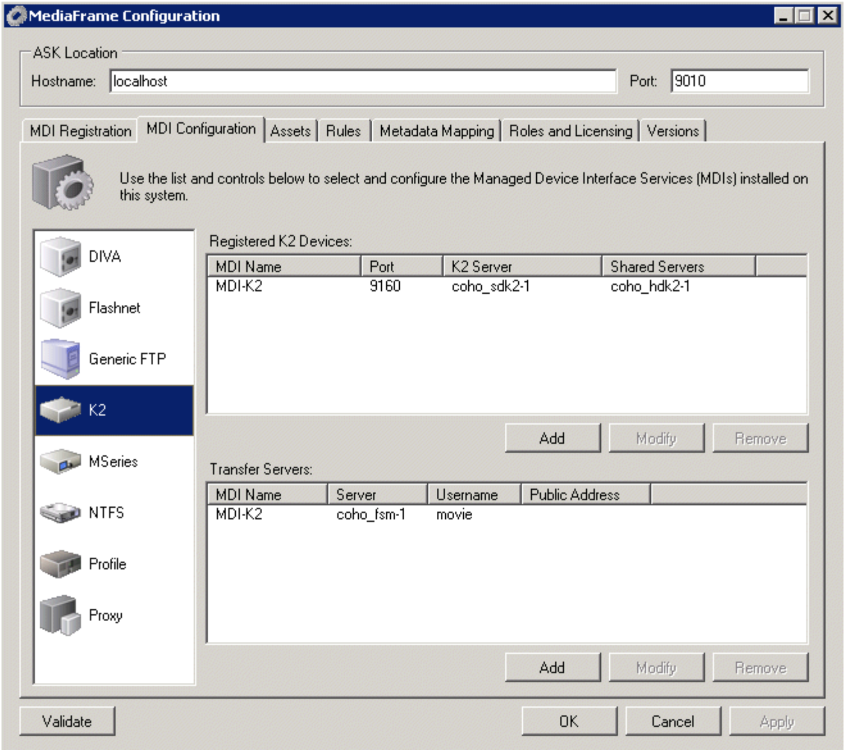
Configure K2 MDI

This page configures the Managed Device Interface (MDI) for a stand-alone K2 Media Client or a K2 Media Client on a K2 Storage System (SAN). MediaFrame depends on the K2 MDI to make K2 assets visible across the system.

As you configure the K2 MDI, make sure that you associate the K2 MDI and K2 host names correctly.

Multiple K2 MDIs run on a single machine (the MDI Server), but they each need their own process port number. For this purpose, enter incrementing numbers 9160 - 9169 in the “Port” field. The MDIs and their port numbers must match settings as in “Configure Media Frame ASK: Register components” on page 51. To make the configurations easier to read for troubleshooting purposes, add MDIs sequentially so there is a correlation between the port number and any number in the MDI name.

If you have a K2 Storage System, designate one of the K2 Media Clients on the K2 Storage System to be the managed device for the entire storage system.



Hostname: localhost

Port: 9010

Use the list and controls below to select and configure the Managed Device Interface Services (MDIs) installed on this system.

Registered K2 Devices:

MDI Name	Port	K2 Server	Shared Servers
MDI-K2	9160	coho_sdk2-1	coho_hdk2-1

Transfer Servers:

MDI Name	Server	Username	Public Address
MDI-K2	coho_fsm-1	movie	

1. On the MDI server, select **Programs| Grass Valley | MediaFrame Config**. Select the MDI Configuration tab and the K2 icon.
2. Enter the name of the MediaFrame server. Do not modify Port 9010. See “Ports and services mapping” on page 36
3. Under Registered K2 Devices, click **Add.**
4. Enter the K2 MDI. Use the ... button to choose the MDI.
5. Increment 9160-9169 so each K2 MDI has a unique process port. For each FSM, there should be one K2 MDI.

6. Enter a stand-alone K2 Media Client or the K2 Media Client on a K2 Storage System. (If shared storage, you can add the name of other servers.)

7. The default value on the Asset System Dwell Time is 120 seconds.

8. Click **Add** as a managed device.

The following settings enable transfers. You should add all available transfer targets, as specified in "Configuring transfer targets" on page 55.

9. Under Transfer Servers, click **Add**.

10.Use the drop-down list to specify the MDI name.

11.Enter the Transfer Server for the MDI selected above.

12.Username: **movie**

13.Leave the Password and Public Address fields blank.

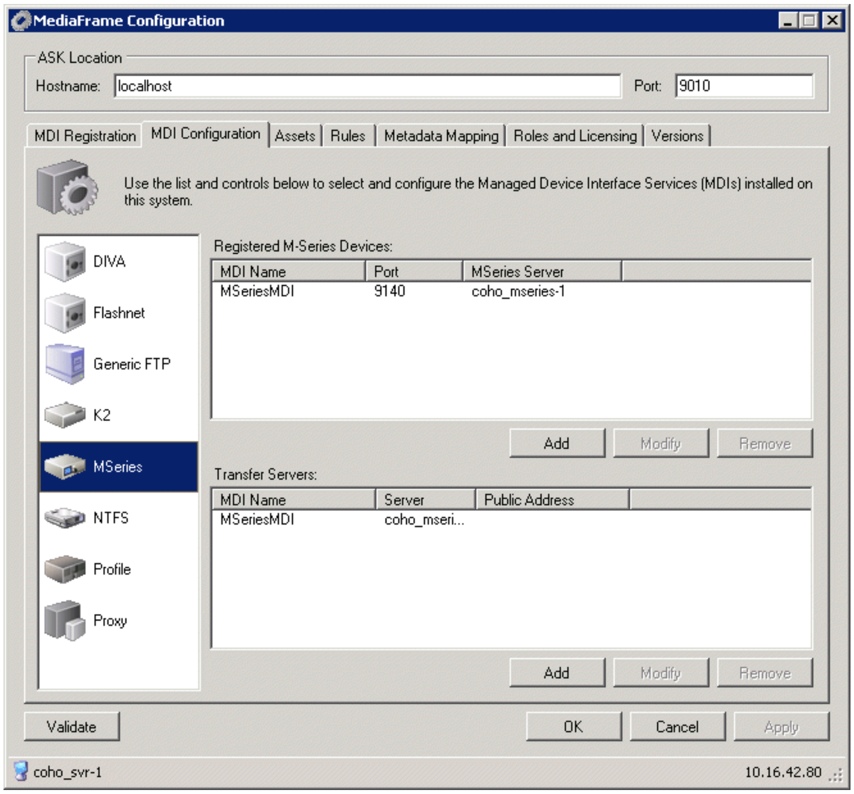
14.To put changes into effect, start or restart K2 MDI service on the MDI Server.

Configure M-Series MDI

This page configures the Managed Device Interface (MDI) for an M-Series iVDR system.

Multiple M-Series MDIs run on a single machine (the MDI Server), but they each need their own process port number. For this purpose, enter incrementing numbers in the "Port" field. The MDIs and their port numbers must match settings as in "Configure Media Frame ASK: Register components" on page 51. To make the configurations easier to read for troubleshooting purposes, add MDIs sequentially so there is a correlation between the port number and any number in the MDI name.

To make the configurations easier to read for troubleshooting purposes, add MDIs sequentially so there is a correlation between the port number and any number in the MDI name.



MediaFrame Configuration

ASK Location

Hostname: localhost

Port: 9010

Use the list and controls below to select and configure the Managed Device Interface Services (MDIs) installed on this system.

Registered M-Series Devices:

MDI Name	Port	MSeries Server
MSeriesMDI	9140	coho_mseries-1

Transfer Servers:

MDI Name	Server	Public Address
MSeriesMDI	coho_mseri...	

coho_svr-1 10.16.42.80

1. Locally on the MDI server, select **Programs| Grass Valley | MediaFrame Config**. Select the MDI Configuration tab.
2. Enter the name of the MediaFrame server. Do not modify Port 9010. See "Ports and services mapping" on page 36.
3. Select the M-Series MDI tab.
4. Under Registered M-Series Devices, click **Add.**
5. Enter the MDI name or click ... to browse for the M-Series MDI.
6. Enter the port number 9140.

7. Enter the name of the M-Series server.

8. The default value on the Asset System Dwell Time is 120 seconds.

9. Click **Add** as a managed device.

10.If adding an additional M-Series MDI, increment the port number, e.g. enter 9141.

The following settings enable transfers. You should add all available transfer targets, as specified in "Configuring transfer targets" on page 55.

11.Under Transfer Servers, click **Add**.

12.Use the drop-down list to specify the MDI name.

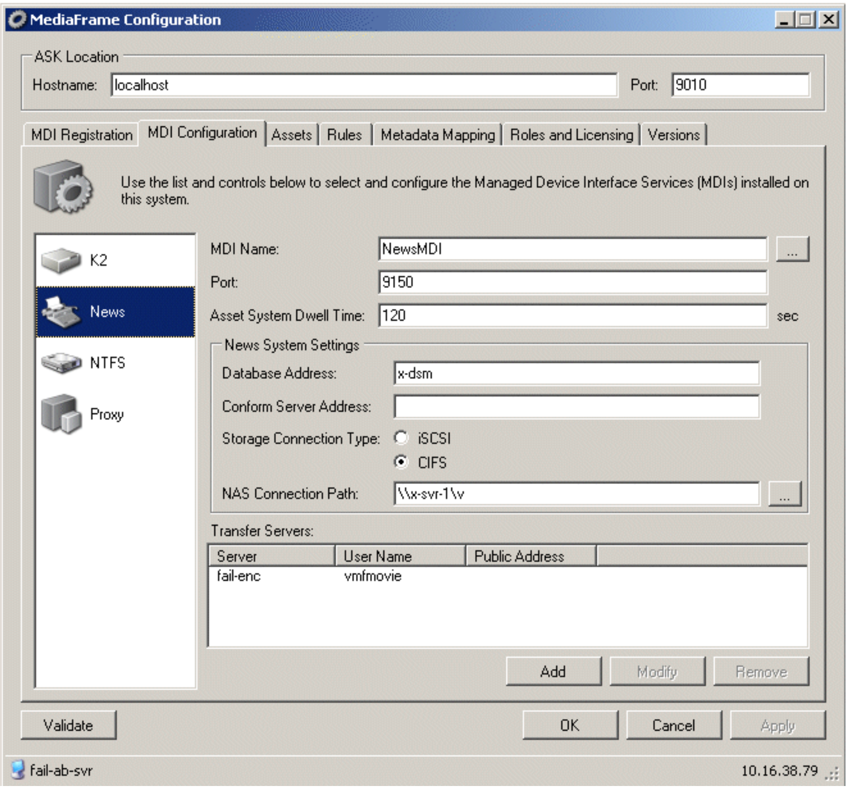
13.Enter the Transfer Server for the MDI selected above.

14.Leave the Public Address field blank.

15.To put changes into effect, start or restart M-Series MDI service on the MDI Server.

Configure News MDIs

This page configures the Managed Device Interface (MDI) for the AuroraShare system. MediaFrame depends on the News MDI to make News assets visible across the system.



ASK Location

Hostname: localhost Port: 9010

Use the list and controls below to select and configure the Managed Device Interface Services (MDIs) installed on this system.

MDI Name: NewsMDI

Port: 9150

Asset System Dwell Time: 120 sec

News System Settings

Database Address: x-dsm

Conform Server Address:

Storage Connection Type: ○ iSCSI ● CIFS

NAS Connection Path: \\x-svr-1\v

Transfer Servers:

Server	User Name	Public Address
fail-enc	vmfmovie	

fail-ab-svr 10.16.38.79

1. Locally on the DSM or MDI server, select **Programs| Grass Valley | MediaFrame Config**. Select the MDI Configuration tab.
2. Enter the name of the MediaFrame server. Do not modify Port 9010. See “Ports and services mapping” on page 36.
3. Select a News MDI.
4. Port 9150 is required. See “Ports and services mapping” on page 36
5. Asset System Dwell Time — The time that the News MDI waits before it informs the MediaFrame system that a clip has finished recording. Leave at 120 seconds.
6. Enter the machine that hosts the Aurora Edit database (the DSM).
7. Enter the machine that hosts the conform service (typically the Conform Server).If Aurora Edit has not been installed, leave blank.
8. The V: drive must be mapped on the machine that hosts the News MDI. By convention, the DSM hosts the News MDI.

The following settings enable transfers. You should add all available transfer targets, as specified in “Configuring transfer targets” on page 55.

9. Under Transfer Servers, click **Add**.

10.Enter the Transfer Server for the MDI selected above and a Username.

11.Leave the Password and Public Address fields blank.

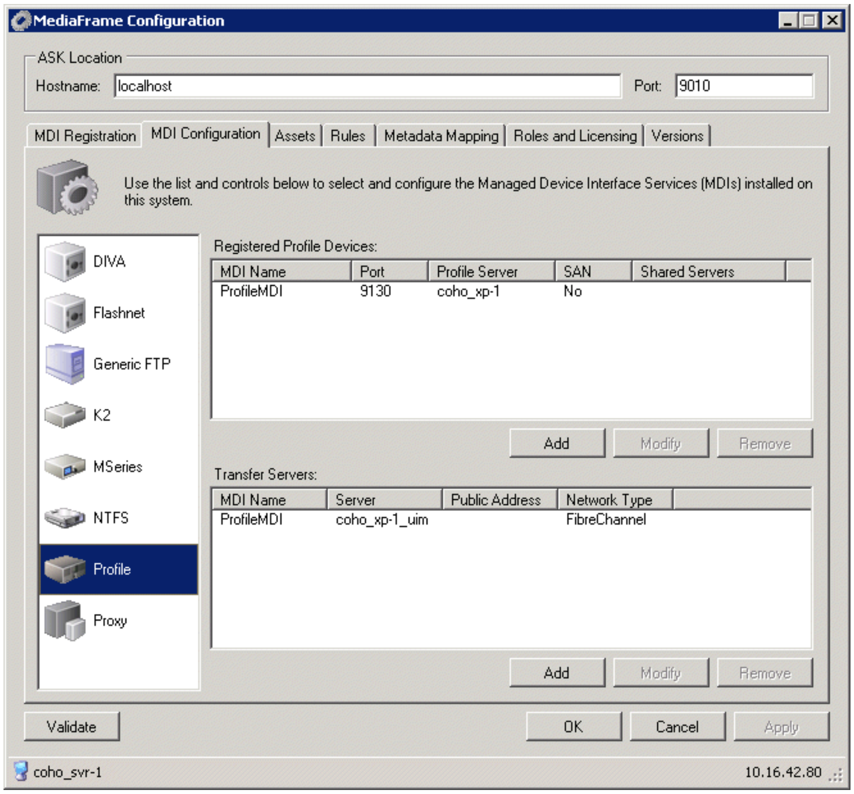
12.Click **Validate** to test the configuration settings. To put changes into effect, start or restart News MDI Service on the MDI server (DSM).

Configure Profile MDI

This page configures the Managed Device Interface (MDI) for a stand-alone Profile system.

Multiple Profile MDIs run on a single machine (the MDI Server), but they each need their own process port number. For this purpose, enter incrementing numbers in the “Port” field. The MDIs and their port numbers must match settings as in “Configure Media Frame ASK: Register components” on page 51.

To make the configurations easier to read for troubleshooting purposes, add MDIs sequentially so there is a correlation between the port number and any number in the MDI name.



Hostname: localhost

Port: 9010

Use the list and controls below to select and configure the Managed Device Interface Services (MDIs) installed on this system.

Registered Profile Devices:

MDI Name	Port	Profile Server	SAN	Shared Servers
ProfileMDI	9130	coho_xp-1	No	

Transfer Servers:

MDI Name	Server	Public Address	Network Type
ProfileMDI	coho_xp-1_uim		FibreChannel

coho_svr-1 10.16.42.80

1. Locally on the MDI server, select **Programs| Grass Valley | MediaFrame Config**. Select the MDI Configuration tab.
2. Enter the name of the MediaFrame server. Do not modify Port 9010. See “Ports and services mapping” on page 36.
3. Select the Profile MDI tab.
4. Under Registered Profile, click **Add.**
5. Enter the MDI name or click ... to browse for the Profile MDI.
6. Enter the port number 9130.
7. Enter the primary and secondary profile names.

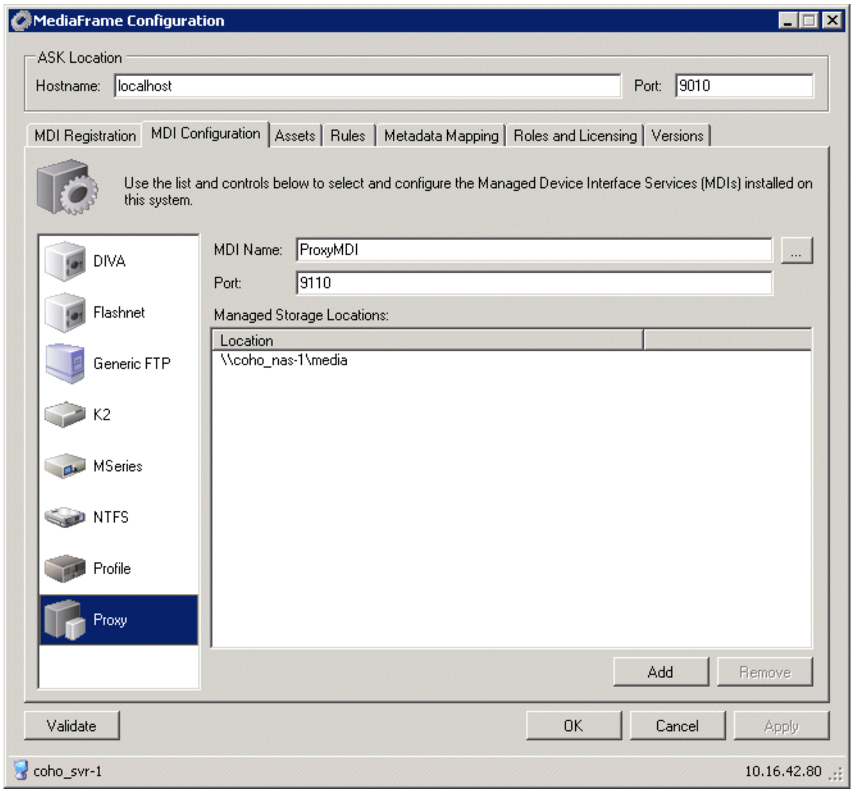
8. The default value on the Asset System Dwell Time is 120 seconds.
9. Make sure the StandAlone radio button is checked.
10. Click **Add** as a managed device.
11. If adding an additional Profile MDI, increment the port number, e.g. enter 9131.

The following settings enable transfers. You should add all available transfer targets, as specified in "Configuring transfer targets" on page 55.

12. Under Transfer Servers, click **Add**.
13. Use the drop-down list to specify the MDI name.
14. Enter the Transfer Server for the MDI selected above.
15. Use the drop-down list to specify the network type.
16. Leave the Public Address field blank.
17. To put changes into effect, start or restart the Profile MDI service on the MDI Server.

Configure Proxy MDI

This page configures the Managed Device Interface (MDI) for the NAS machines that store the low-res proxy. The system depends on the Proxy MDI to make proxy visible across the system. For the Proxy MDI, there is but one managed device. This managed device can have multiple locations. The Media directory on each NAS machine is entered as a location. Other directories can be entered as locations as well. In this way the Proxy MDI knows where to look for the low-res proxy.



Hostname: localhost

Port: 9010

Use the list and controls below to select and configure the Managed Device Interface Services (MDIs) installed on this system.

MDI Name: ProxyMDI

Port: 9110

Managed Storage Locations:

Location	
\\coho_nas-1\media	

coho_svr-1 10.16.42.80

1. Select **Programs| MediaFrame Config.** Select the MDI Configuration tab and the Proxy icon.
2. In the Ask Location hostname field, enter the name of the MediaFrame server. Do not modify Port 9010. See “Ports and services mapping” on page 36
3. Set the MDI name.
4. Port 9110 is required. See “Ports and services mapping” on page 36.
5. To add a storage location, click **Add**.
6. For each Proxy NAS machine, enter the UNC path to the “Media” folder. This is the location to which the system writes the proxy media.[1] Click **Add**.
7. Click **Apply** or **OK** after you’ve finished making changes.
8. To put changes into effect, start or restart the Proxy MDI Service on the MediaFrame server.

[1] You can define multiple locations on a single NAS machine, but for each location you must enter the complete path.

Test: MediaFrame stage

The following test exercises system functionality exclusive to the MediaFrame core platform. A successful test verifies that the basic configurations are correct.

After configuring the MediaFrame settings, click the **Validate** button on each tab. The MediaFrame system checks MDI mappings and devices for inconsistencies. This can take several minutes. A report displays.

Make sure there are no errors displayed. To troubleshoot errors, check the following:

- Make sure services are running
- Make sure you have configured the correct host name for the MDI service.
- Ping machines to verify network communication.

Checklist: MediaFrame stage

Use the following check list to verify that the basic configuration and testing of the MediaFrame stage is complete.

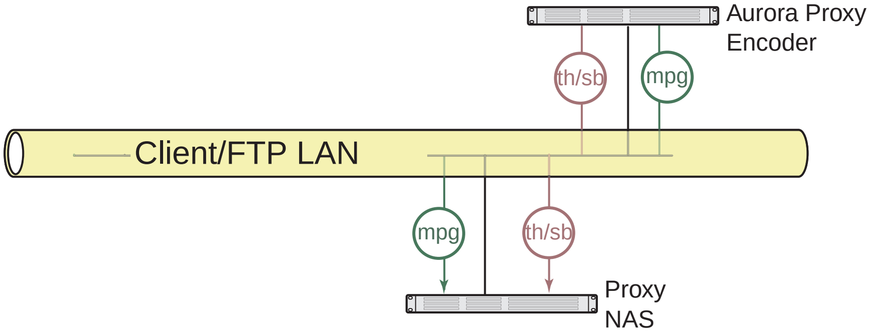
☐ All logical MDI names and Encoder service names are registered with ASK.

☐ All machines taking the role of MDI server have the appropriate MDI services installed and running.

Encoder stand-alone stage

For this configuration stage you configure and test one encoder and one proxy NAS to work together. The encoder creates storyboard and MPEG proxy. There are two types of encoder: SmartBin and Aurora Proxy. Configuration pages and procedures are the same for HD and SD encoders.

The portion of the system configured and tested in this stage is illustrated by the following diagram.



Refer to "System diagram - K2 storage" on page 12 for a view of the entire system.

To do the basic configuration and testing of a stand-alone encoder, do the following:

1. Configure the encoder:
   - "Configure SmartBin Encoder" on page 69

     or
   - "Configure Aurora Proxy Encoder" on page 73
2. "Checklist: Encoder stand-alone stage" on page 75

Configure SmartBin Encoder

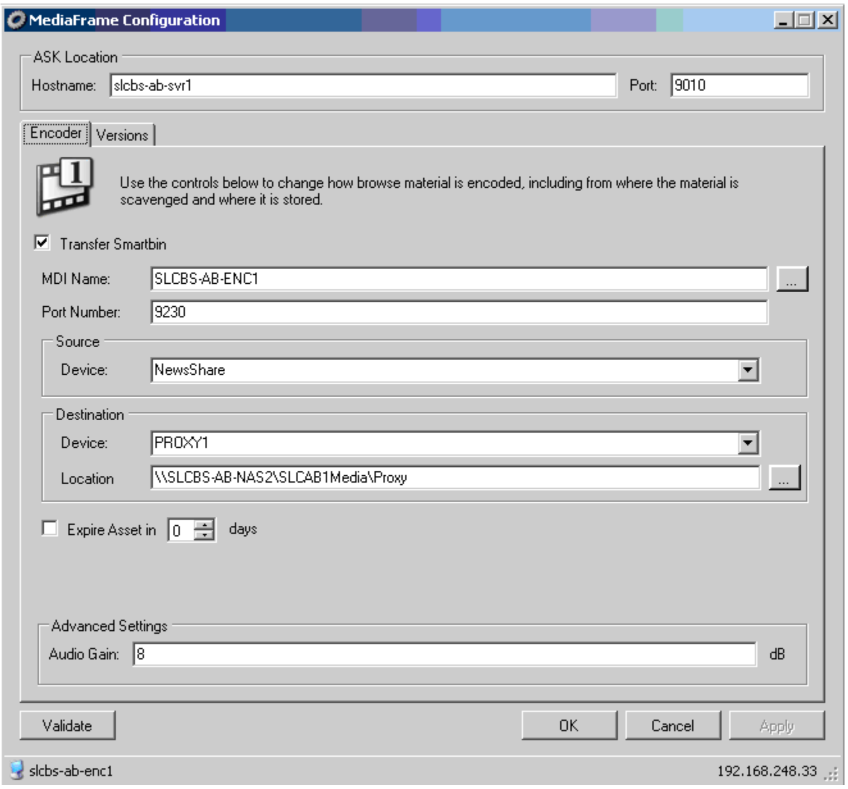
This section describes configuring the SmartBin Encoder. To configure an Aurora Proxy encoder, see **"Configure Aurora Proxy Encoder" on page 73**.

The primary workflow of the SmartBin Encoder is to integrate into a system with Aurora Ingest ingesting material to a transfer SmartBin folder. The Transfer SmartBin service transfers the material into News Share while feeding the encoder the raw data stream. In this workflow, the MediaFrame asset is associated with a media server clip, News Share master clip, and lo-resolution proxy.

If your system does not have Aurora ingest feeding the SmartBin folder, the MediaFrame asset contains the News Share master clip and has the lo-resolution proxy associated with it.

NOTE: If upgrading the encoder, be sure to review the latest upgrade instructions in the Aurora Browse Release Notes.

When the Transfer SmartBin box is checked, the SmartBin Encoder configuration page is displayed.



ASK Location

Hostname: slcbs-ab-svr1 Port: 9010

Use the controls below to change how browse material is encoded, including from where the material is scavenged and where it is stored.

☑ Transfer Smartbin

MDI Name: SLCBS-AB-ENC1

Port Number: 9230

Source

Device: NewsShare

Destination

Device: PROXY1

Location \\SLCBS-AB-NAS2\SLCAB1Media\Proxy

☐ Expire Asset in 0 days

Advanced Settings

Audio Gain: 8 dB

slcbs-ab-enc1 192.168.248.33

On the SmartBin Encoder config page, the Versions tab of the MediaFrame Config tool lets you see at a glance all the versions of the MediaFrame components that have been installed.

The Encoder tab tells the SmartBin Encoder where to look for the ASK service, which runs on the MediaFrame server. The function of the ASK is to store the location of MediaFrame components. This tab configures the connections between the SmartBin Encoder and the server from which it gets its media stream.

The Encoder tab also provides settings that allow you to set up the SmartBin Encoder to generate proxy for high-priority ingest or edited material. This dedicated SmartBin Encoder then only runs scavenge operations when new material appears in a specific location. That way you can be assured that your high-priority ingest or edited material is immediately processed, even if there are multiple other lower priority scavenge jobs that need to be done at the same time. Your other un-dedicated encoders can do the low priority jobs without interfering with the availability of the dedicated SmartBin Encoders.

It is recommended that you dedicate at least one SmartBin Encoder to scavenge newly edited material that you place in an “Outbox” folder. Refer to “Design considerations - Aurora Browse with Aurora Edit” on page 12.

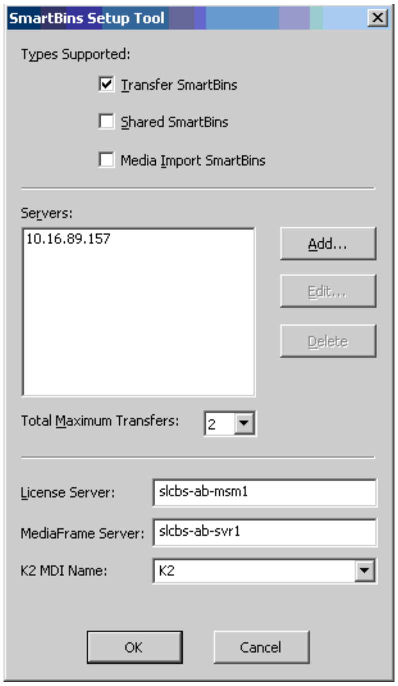
You can dedicate the SmartBin Encoder to a particular Proxy NAS location.

As part of the SmartBin Encoder configuration, configure the Transfer SmartBins. service on the same host. Transfer SmartBins set up automatic clip transfers from a media server to an Aurora Edit bin. For more information, see the ***Aurora Edit Installation and Configuration Guide***.

NOTE: Before configuring the SmartBin Encoder, you need to configure a News MDI and a media server (K2, M-Series or Profile MDI).

To configure the SmartBin Encoder, do the following.

1. On the SmartBin Encoder machine, select **Programs | Grass Valley Aurora | SmartBins Setup Tool.** The SmartBins Setup Tool opens.



SmartBins Setup Tool

Types Supported:

☑ Transfer SmartBins

□ Shared SmartBins

□ Media Import SmartBins

Servers: 10.16.89.157

Total Maximum Transfers: 2

License Server: slcbs-ab-msm1

MediaFrame Server: slcbs-ab-svr1

K2 MDI Name: K2

2. Under Types Supported, check the Transfer SmartBins box. Do not check the other boxes.

3. Click the **Add** button. The Edit Server Settings dialog box appears.

4. Enter the name of the Profile, M-Series, or K2 Media Client that you are using.

5. Select the Server Type from the drop-down list and click **OK**.

6. Specify the license server. This is the server where the MOV generation license is located.

7. Specify the MediaFrame server, and K2 MDI and click **OK**. The SmartBins Setup Tool closes, and the SmartBin service restarts.

   Now that the SmartBins service has been setup, you can configure the SmartBin Encoder.

8. Select **Programs | Grass Valley | MediaFrame Config** and select the Encoder tab.

9. Enter the host name of the machine that hosts the ASK location. If this service is on the same machine as the SmartBin Encoder, enter *localhost.* Port 9010 is required. See "Ports and services mapping" on page 36.

10. Use the **...** button to select the MDI. For the first encoder, port 9230 is required. See "Ports and services mapping" on page 36. For any additional encoders, the port number is automatically incremented, e.g. 9231.

11. In the Source section, use the drop-down list to select a source Device. For MDI Name, select the News Share MDI name.

12. In the Destination section, use the drop-down list to select a destination Device.

    - To configure the Aurora Proxy Encoder to process proxy media on one location, select that location as the Proxy Storage Location. Use the **...** button to browse to the folder (\Media) on the NAS (or other storage location) that receives the MPEG this encoder creates.[1]

    - You can only select one low-resolution destination; you cannot specify multiple locations.

13. Optionally, you can check the Expire Asset box. If unchecked, the MediaFrame asset is not set to expire. If checked, the encoder sets the MediaFrame asset to expire in the specified number of days.

NOTE: The encoder does not change the expiration date if the MediaFrame asset already has the asset expiration date set. (For example, if the expiration date was set in Aurora Ingest when the asset was created.)

14. In the Advanced Settings section, you can adjust the Audio Gain Level to calibrate Aurora Edit LD audio, or to improve the quality of the desktop audio (e.g. if the source is 'too hot').

15. In the MediaFrame Config tool, click **Apply**.

16. Press the **Validate** button to test the status of the current configurations. If the configurations are valid, click **OK** to exit the MediaFrame Config tool.

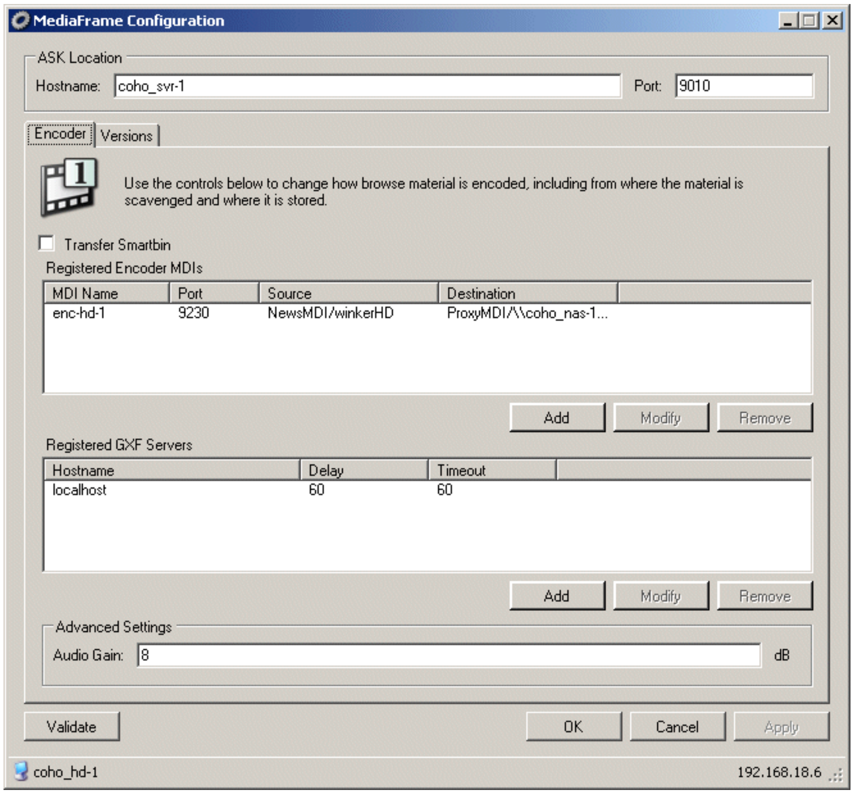
[1] This location is used when in Rules, Proxy Storage Location is blank (*).

Configure Aurora Proxy Encoder

This section describes configuring the Aurora Proxy Encoder. To configure a SmartBin encoder, see **"Configure SmartBin Encoder" on page 69**.

NOTE: If upgrading the encoder, be sure to review the latest upgrade instructions in the Aurora Browse Release Notes.

If the Transfer SmartBin box is *not* checked, the Aurora Proxy Encoder configuration page is displayed.



ASK Location

Hostname: coho_svr-1 Port: 9010

Use the controls below to change how browse material is encoded, including from where the material is scavenged and where it is stored.

□ Transfer Smartbin

Registered Encoder MDIs

MDI Name	Port	Source	Destination
enc-hd-1	9230	NewsMDI/winkerHD	ProxyMDI/\\coho_nas-1...

Registered GXF Servers

Hostname	Delay	Timeout
localhost	60	60

Advanced Settings

Audio Gain: 8 dB

coho_hd-1 192.168.18.6

On the Aurora Proxy Encoder, the Versions tab of the MediaFrame Config tool lets you see at a glance all the versions of the MediaFrame components that have been installed.

The Encoder tab tells the Aurora Proxy Encoder where to look for the ASK service, which runs on the MediaFrame server. The function of the ASK is to store the location of MediaFrame components. This tab configures the connections between the Aurora Proxy Encoder and the server from which it gets its media stream.

The Encoder tab also provides settings that allow you to set up the Aurora Proxy Encoder to generate proxy for high-priority ingest or edited material. This dedicated Aurora Proxy Encoder then only runs scavenge operations when new material appears in a specific location. That way you can be assured that your high-priority ingest or edited material is immediately processed, even if there are multiple other lower priority scavenge jobs that need to be done at the same time. Your other un-dedicated Aurora Proxy Encoders can do the low priority jobs without interfering with the availability of the dedicated Aurora Proxy Encoders.

It is recommended that you dedicate at least one Aurora Proxy Encoder to scavenge newly edited material that you place in an “Outbox” folder. Refer to “Design considerations - Aurora Browse with Aurora Edit” on page 12.

You can dedicate the Aurora Proxy Encoder to a particular Proxy NAS location. This assumes that for a single Proxy MDI there are multiple NAS locations.

To configure the Aurora Proxy Encoder, do the following.

1. On the Aurora Proxy Encoder machine, select **Programs | Grass Valley | MediaFrame Config** and select the Encoder tab.
2. For the ASK location, enter the name of the MediaFrame server. Port 9010 is required. See “Ports and services mapping” on page 36.
3. On the Encoder tab under Registered Encoder MDIs, click **Add**.
4. Use the **...** button to select the MDI. For the first encoder, port 9230 is required. See “Ports and services mapping” on page 36. For any additional encoders, the port number is automatically incremented, e.g. 9231.
5. In the Source section, use the drop-down list to select a source Device:
    - For MDI Name, select a valid MDI Name.
    - To scavenge material in an “Outbox” folder on a K2 Storage System, select the K2 MDI.
6. In the Source section, use the **...** button to select a source location:
    - For Storage Location, select a valid Storage Location.
    - To scavenge material in an “Outbox” folder on a K2 Storage System, select the specific folder.
7. In the Destination section, use the drop-down list to select a destination Device.
    - To configure the Aurora Proxy Encoder to process proxy media on one location, select that location as the Proxy Storage Location. Use the **...** button to browse to the folder (\Media) on the NAS (or other storage location) that receives the MPEG this encoder creates.[1]
8. To configure the GXF Server and MPEG encoder options, click **Add** in the Registered GXF Servers section. The Add GXF Server dialog box displays.
    a. Enter the GXF Server Host Name.
    b. Max Startup Delay — Enter the maximum time the encoder waits for recording to begin after a clip is created in the database. 60 seconds is the recommended setting.[2]
    c. Stream Timeout — Enter the maximum time the encoder waits for a break in the media stream to be restored. 60 seconds is the recommended setting.[3]

[1] This location is used when in Rules, Proxy Storage Location is blank (*).

[2] When you create a new clip name in the media database on the K2 system, the encoder is notified and waits for the media file to appear. Set this value to be the maximum time allowed in your workflow between the creation of a clip name and the commencement of recording the clip.

d. Click **OK** to exit the Add GXF Server dialog box.

9. In the Advanced Settings section, you can adjust the Audio Gain Level to calibrate Aurora Edit LD audio, or to improve the quality of the desktop audio (e.g. if the source is 'too hot').

10. In the MediaFrame Config tool, click **Apply**.

11. Press the **Validate** button to test the status of the current configurations. If the configurations are valid, click **OK** to exit the MediaFrame Config tool.

Checklist: Encoder stand-alone stage

Use the following check list to verify that the basic configuration and testing of the stand-alone encoder is complete.

☐ Encoder is connected to NAS

☐ Encoder writes to NAS

☐ MPEG created

☐ MPEG playback with audio

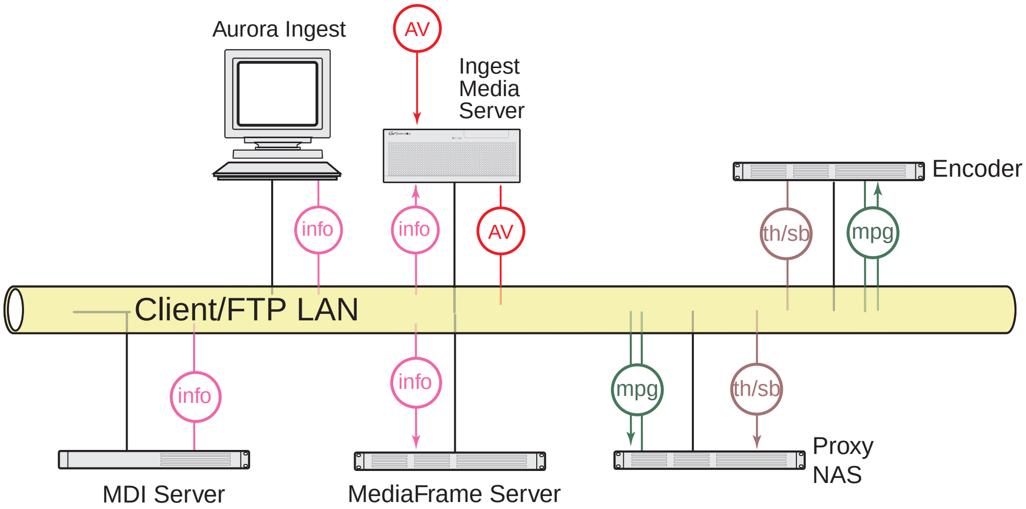
☐ Storyboard files are created.

[3] If the high-res stream for which the encoder is creating proxy material is interrupted, the encoder waits this long for the stream to continue.

Encoder + Server stage

For this configuration stage you configure the MediaFrame server to work together with the Encoder and NAS from the Encoder stand-alone stage. MDI services are also required, as configured in the MediaFrame stage.

The portion of the system configured and tested in this stage is illustrated by the following diagram.



Refer to “System diagram - K2 storage” on page 12 for a view of the entire system.

To do the basic configuration and testing of the encoder plus server, do the following:

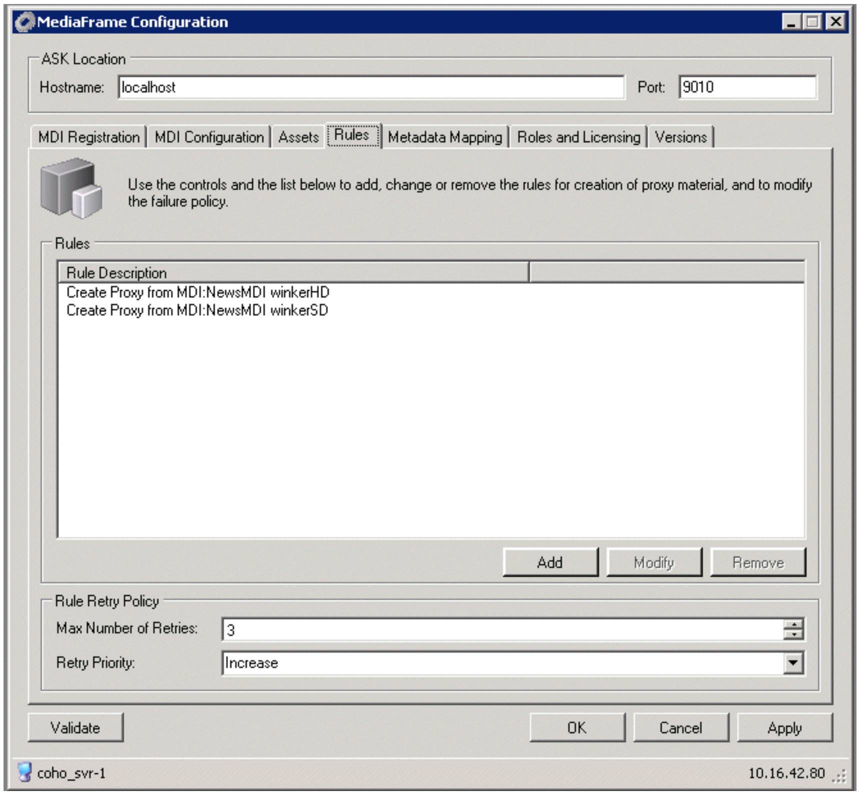
1. “Configure Media Frame Core ASK: Encoder” on page 76
2. “Configure Rules Automation: Encoder” on page 77
3. “Test: Encoder + Server stage - high-res source” on page 81

Configure Media Frame Core ASK: Encoder

Make sure the encoder’s proxy transfer service is registered with the ASK software component with a logical name, as explained in “Configure Media Frame ASK: Register components” on page 51. If ASK is down, you need to manually enter the names, and they must match exactly. Therefore, where possible, use the drop-down list to ensure the exact name.

Configure Rules Automation: Encoder

The Rules tab of the MediaFrame Config tool defines the rules for an encoder creating proxy.


MediaFrame Configuration
MDI Registration | MDI Configuration | Assets | Rules | Metadata Mapping | Roles and Licensing | Versions
Add
Modify
Remove
Validate
OK
Cancel
Apply

ASK Location

Hostname: localhost

Port: 9010

Use the controls and the list below to add, change or remove the rules for creation of proxy material, and to modify the failure policy.

Rules

Rule Description	
Create Proxy from MDI:NewsMDI winkerHD	
Create Proxy from MDI:NewsMDI winkerSD	

Rule Retry Policy

Max Number of Retries: 3

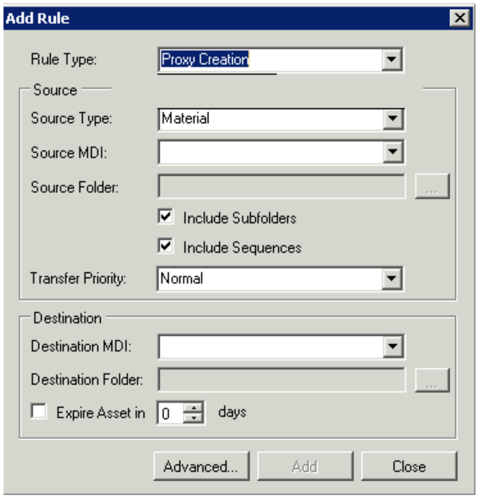
Retry Priority: Increase

coho_svr-1 10.16.42.80

To scavenge newly edited material in an “Outbox” folder on a K2 Storage System, for MDI Name, select the K2 MDI and location as in “Configure Aurora Proxy Encoder” on page 73.

To configure a rule defining the creation of proxy assets, do the following:

1. Click **Add**. The Add Rule dialog box displays.



Rule Type: Proxy Creation

Source

Source Type: Material

Source MDI:

Source Folder:

☑ Include Subfolders

☑ Include Sequences

Transfer Priority: Normal

Destination

Destination MDI:

Destination Folder:

☐ Expire Asset in 0 days

2. Using the Rule Type drop-down list, select the Rule Type:

   - **Proxy creation** — this rule creates a MediaFrame asset and associates the source material to it, if it does not already exist. If the asset does not have proxy already associated, this rule causes proxy to be created.
   - **Asset creation** — this rule only creates a MediaFrame asset and associates the source material to it, if it does not already exist. It does not create proxy. This rule is useful for systems that don't have proxy encoders, or systems that don't want to create proxy for everything (such as systems that only want to create proxy for archived material).

3. Using the Source Type drop-down list, select the Source MDI.

4. Use the ... button to select or type in the source folder on the machine that the system monitors for new material. ***Note: You must use forward slashes for this path.***

5. Check the Include Subfolders box to also monitor for material in folders nested in "MDI Storage Location".

6. Check the Include Sequences box to include Aurora Edit sequences.

7. In the Destination section, use the drop-down list to select a destination MDI.

8. Use the ... button to select or type in the destination folder.

9. Expired assets are purged from the system after this many days. Leave blank to never expire. Refer to "About expired assets" on page 80.

10. To modify the Proxy Types and Creation Options, click the **Advanced...** button.

    By default, the following are selected:

    - Create while recording
    - Recreate proxy if content modified

    For further information about these options, refer to "About configuring rules" on page 79. Click **OK** when done to exit the Advanced dialog box.

11. **Add** adds the above settings as a new Proxy Creation rule.

12. The **Update Rule** button only appears if an existing rule is selected in the Existing Rules box below, in which case the button puts into effect any changes you have made to the existing rule.

13. In the MediaFrame Config tool, all currently added rules are displayed. When a rule is selected, the options above are automatically loaded with the settings for the selected rule. You can then modify the rule and update it, or modify the rule and add it as a new rule, or remove the currently selected rule

14. The Rule Retry Policy section specifies how many times the system retries a failed rule. Keep this setting at 3 or below for most rules to prevent degradation of system performance. If all the rules have the same setting, jobs are handled in the order they were put in the database.

15. When a failed rule is retried, its priority can be changed in relation to other rules currently being processed. Set to **Increase** to promote timely processing.

16. Always click **OK** after making changes

17. You must start or restart the GV Rules Wizard service on the MediaFrame server to put changes into effect, but if you are doing the initial configuration of the Aurora Proxy Encoder + Server stage, don’t start the service until instructed to do so in the Aurora Proxy Encoder + Server stage test.

The following sections explain rules.

About configuring rules

The Rules tab offers the appropriate options based on the currently selected source, as follows:

Rules when the source is high-res material

These rules create MPEG and storyboard proxy from high-res material. This is also known as a “scavenge” operation. Depending on the desired behavior of the system you may have to create multiple rules for the MPEG creation. There are two types of rules, as follows:

- **Create while Recording** — This rule causes MPEG to be created while the system is still encoding the high-res material.
- **Recreate Proxy if Content is Modified** — This rule will cause the system to delete the proxy associated with high-res material if the material has its content modified. It will then recreate the MPEG proxy for the material. This rule is normally configured for K2 storage systems.

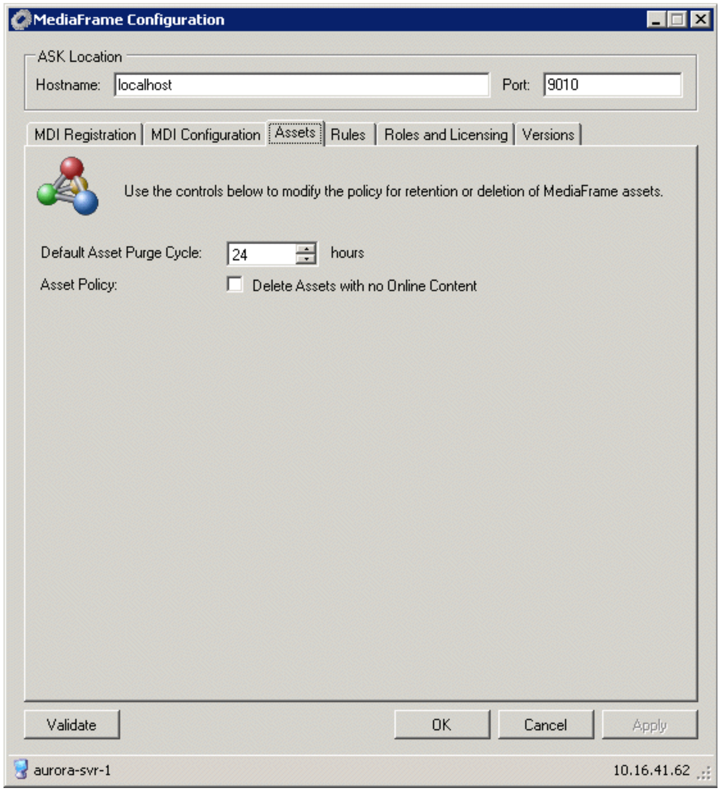
The following takes place by default with both these types of rules:

- When the Rules Wizard starts up, it traverses a high-res device MDI to see if there is any material that does not have MPEG proxy associated with it, according to the currently configured rules. The Rules Wizard will only check the system once after startup to see if it needs to create any of this proxy.
- Storyboard elements are used for thumbnails, so in effect thumbnails are generated by default.

Tips for configuring rules

- Configure one rule per folder or “location”. Multiple overlapping rules that access the same folder can produce looping behaviors and other unexpected results.

Configure Assets Tab



MediaFrame Configuration

ASK Location

Hostname: localhost Port: 9010

Use the controls below to modify the policy for retention or deletion of MediaFrame assets.

Default Asset Purge Cycle: 24 hours

Asset Policy: □ Delete Assets with no Online Content

When the GV Asset Manager service runs it looks for expired assets and orphaned assets that should be purged from the system. It also maintains the assets currently in the Resolver and if necessary initiates the creation of proxy to keep assets in synch. This tab of the MediaConfig tool configures the frequency and rules by which the Asset Manager carries out its processes.

About expired assets

When assets are created, they can be assigned a Expiration date. This is the value that you enter on the Rules tab. The Expiration date is set to the current date plus the number of “Days to Expire Asset”. If you do not set a “Days to Expire Asset” value, the asset will never be purged automatically

The Asset Manager executes a periodic purge task that runs at the frequency (in hours) that you configure on the Asset Manager tab, starting from the last time the Asset Manager service is started. This task takes the current time of day date/time stamp and compares it to the Expire date. If the date portion of the current timestamp is greater than or equal to the Expire date, the Asset Manager attempts to delete the asset. Thus, the actual purge period can occur up to a day earlier than expected.

The asset will not be deleted if the Hold checkbox has been checked in the asset in the Aurora Browse client application, or if the asset has a lock on it for some other reason. For example, if a user opens the asset in Aurora Editor, then Browse will not delete the asset.

Recommendation:

Set the “Days to Expire Asset” to one more than required to ensure that assets are not deleted sooner than required.

For example, if you want assets to reside in the system approximately (but not less than) one day, the “Days to Expire Asset” value should be set to 2. This will result in actual asset lifetimes between 24 and 72 hours in the system. If you require the maximum period to be closer to 48 hours than 72, decreasing the Purge Period from 1440 (24 hours) to a smaller value should be effective.

Test: Encoder + Server stage - high-res source

The following test exercises system functionality exclusive to the rules for creating MPEG proxy and storyboard proxy from high-res material. A successful test verifies that the basic configurations for the rules are correct.

Test description: Trigger rules by creating/modifying a high-res clip on the K2 storage while the Rules Wizard service is off, then on.

Run the test as follows:

1. Make sure that the system is not in use.
2. Make sure the GV Rules Wizard service is off on the MediaFrame server.
3. Start the GV Resolver service and the GV Metadata service on the MediaFrame server.
4. Click **Start | Programs | Grass Valley| Event Viewer** to open Event Viewer.
5. On a K2 system, copy a clip into a bin monitored by the Aurora Proxy Encoder.
6. On the MediaFrame server, start the GV Rules Wizard. Watch Event Viewer and verify that the MPEG and storyboard proxy are created for the clip.
7. On the K2 system, copy another clip into the bin. Watch Event Viewer and verify that the MPEG and storyboard proxy are created for the clip.
8. In you have a “…if content is modified” rule configured for high-res clips, on the K2 system, modify a clip (rename) in the bin. Watch Event Viewer and verify that the MPEG and storyboard proxy are created for the modified clip.
9. If you have a “Create while recording” rule configured for high-res clips, on the K2 system, record a clip into a bin monitored by the Aurora Proxy Encoder. Watch Event Viewer and verify that the MPEG and storyboard proxy are created (in real-time) as the clip is recorded.

Checklist: Encoder + Server stage

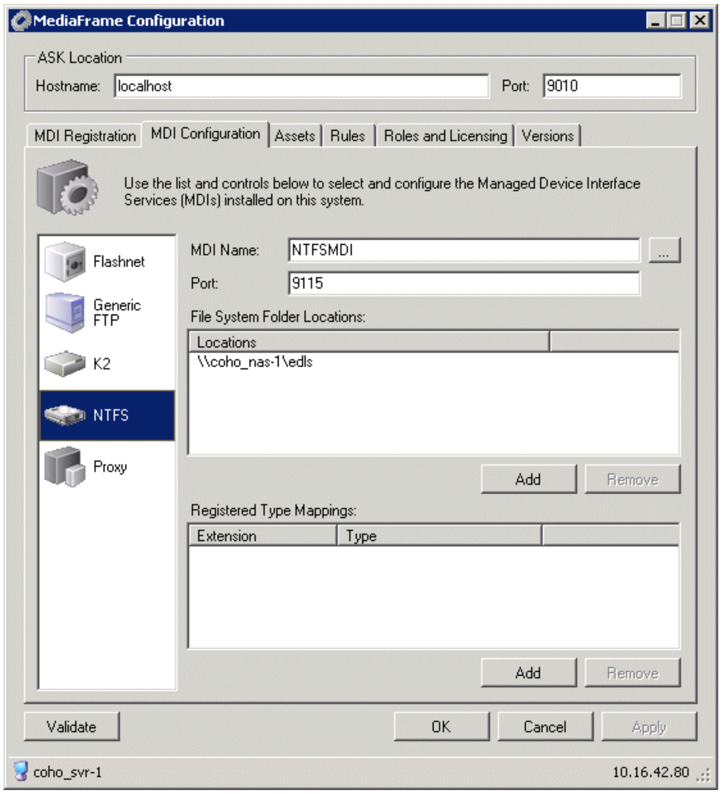
Use the following check list to verify that the basic configuration and testing of the single-channel encoder plus MediaFrame server is complete.

☐ When the Rules Wizard starts up, rules work as configured for the creation of MPEG and storyboard proxy.

☐ When a clip is ingested, rules work as configured for the creation of MPEG and storyboard proxy.

- ☐ When a high-res clip is copied into a monitored bin, rules work as configured for creation of MPEG and storyboard proxy.
- ☐ When a high-res clip is modified, rules work as configured for creation of MPEG and storyboard proxy.

Configure NTFS MDI



Hostname: localhost Port: 9010

Use the list and controls below to select and configure the Managed Device Interface Services (MDIs) installed on this system.

MDI Name: NTFSMDI

Port: 9115

\\coho_nas-1\edls

coho_svr-1 10.16.42.80

This tab of the MediaFrame Config tool specifies the machines, directories, and file types that the NTFS MDI can access. The Aurora Browse application makes these available as selections for saving and managing assets.

If you need to configure the NTFS MDI, do the following.

1. Select **Programs | Grass Valley | MediaFrame Config**. Select MDI Configuration tab and the NTFS icon.
2. Use the ... button Name of NTFS MDI, as registered with ASK. Refer to "Configure Media Frame ASK: Register components" on page 51.
3. Port **9115** is required. See "Ports and services mapping" on page 36.
4. Click the **Add** button to specify the location of the folder managed by the NTFS MDI. This must be a UNC path. The machine must have NTFS storage. (You can optionally specify the folder.)

   The Locations section lists currently added machines/folders accessible by the NTFS MDI.
5. The Registered Type Mappings section defines the types of files accessible by the

NTFS MDI.

NOTE: Do not map the edl/xml.LiteEdit type.

6. Always click **OK** or **Apply** buttons after making changes
7. Restart the GV NTFS MDI Service on the MediaFrame server.

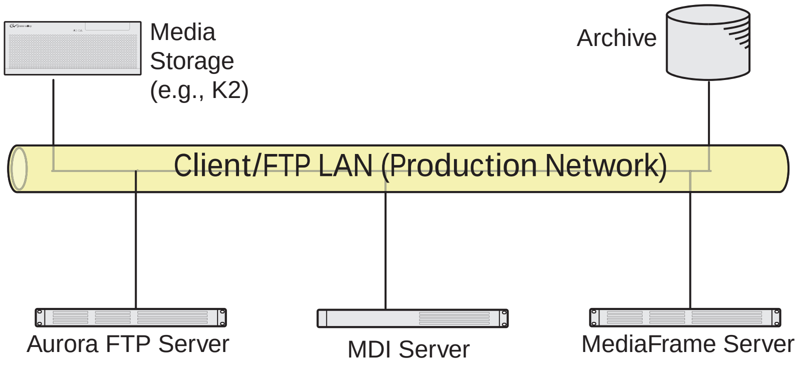
Configure NLS MDI

The NLS MDI is no longer used. Refer to "Configure Proxy MDI" on page 66.

Archive stage

For this configuration stage you configure your archive MDI, high-res storage, and the MediaFrame server to work together. This assumes that the archive devices are already installed and connected.

The portion of the system configured and tested in this stage is illustrated by the following diagram.



To support archive functionality on the News/K2 system, you must install a unique Aurora FTP on a platform somewhere in the system.

To configure and test the Archive stage, do the following:

1. "Add archive MDI" on page 85
2. "Verify archive preparations" on page 86
3. "The K2 storage or AuroraShare NAS system" on page 89
4. Configure your archive:
   a. "Configure Avalon MDI" on page 90
   b. "Configure DIVA MDI" on page 91
   c. "Configure FlashNet MDI" on page 92
   d. "Checklist: Archive stage" on page 93
5. "Checklist: Archive stage" on page 93

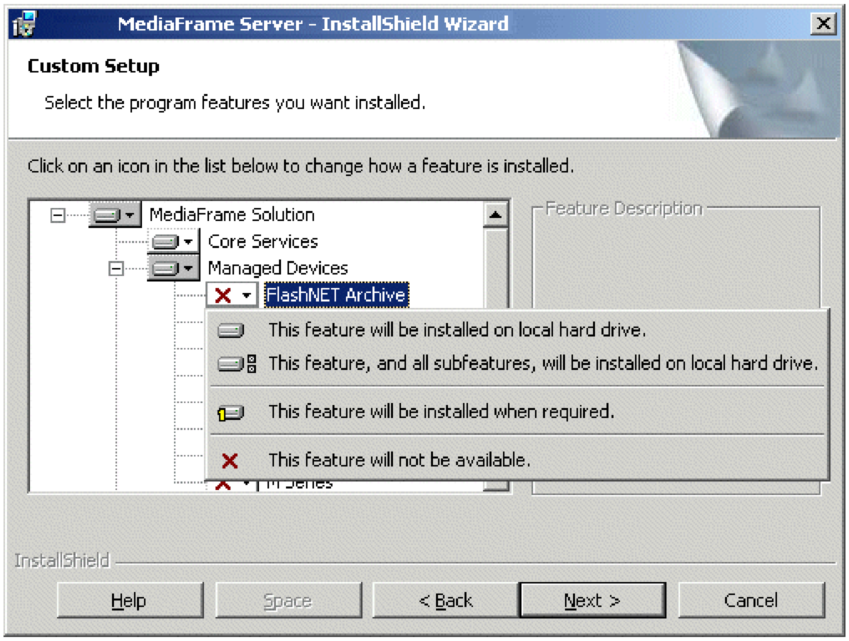
Add archive MDI

The archive MDI software component runs as a service. The archive MDIs available are as follows:

- Avalon
- DIVA
- FlashNet

The archive MDI software component must be installed on a network connected computer. Similar to the other MDIs in the MediaFrame system, the archive MDI can be installed on a MDI server or on the MediaFrame server, depending on the size and design of your system.

You can install the archive MDI software component from the MediaFrame server installation program. Select the component for your archive from the Custom setup page.



MediaFrame Server - InstallShield Wizard

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

This feature will be installed on local hard drive.

This feature, and all subfeatures, will be installed on local hard drive.

This feature will be installed when required.

This feature will not be available.

Verify archive preparations

Be aware of the following when setting up for integration with an archive system:

- Devices support a limited number of concurrent transfers, as follows:
  - A single Profile XP provides a maximum of four streams for concurrent transfers (via Fibre Channel).
  - An internal storage (stand-alone) K2 Media Client provides a maximum of four streams for concurrent transfers.
  - A K2 Media Server provides a maximum of eight streams for concurrent transfers.

  Keep this limit in mind when configuring the archive device for concurrent transfers. If the archive is configured such that it can request more than the number of supported streams simultaneously from any single system, the additional transfers will error out.

For the type of archive device you use, check the following to verify proper operation with the system.

Avalon archive preparations

Check the following on the machine that runs Avalon IDM Software (Archive):

1. Login to the machine and go to /avalon/aam/utils
2. Run aamctrl stat and verify all services running properly.
3. Make sure host tables are set correctly. Verify the machine name/IP which the IDM will talk to.
4. If archiving from a Profile XP standalone, make sure the Fibre Channel interfaces are configured so that Avalon IDM can talk to the Profiles.

Consider the following when preparing to integrate Avalon archive with Aurora Browse:

- Avalon archive has no fixed limit for concurrent transfers.

DIVA preparations

Check the following on the machine that runs DIVA software:

1. Login to the machine.
2. Verify that you can FTP from the DIVA server to the machine with the high-res online material:
   - If archiving from an M-Series or Profile XP standalone, verify that you can FTP from the DIVA server to the Profile on the Ethernet IP address and login as user `movie`.
   - If archiving from K2 storage or AuroraShare NAS, verify that you can FTP from the DIVA server to the K2 storage or AuroraShare NAS on Gigabit Ethernet and login as user `vmfmovie`.
3. Add a new Source and Destination.

4. Fill in the following information needed:
   a. Source name – any name (must correspond to the name specified in Transfer Server)
   b. IP Address – can be IP address or host name accessible from DIVA archive server (must be a reachable News, K2, M-Series or Profile server registered as the Transfer Server in the News, K2, M-Series or Profile MDI)
   c. Source Type – choose the appropriate type of server. News FTP and K2 use `FTP_STANDARD` and M-Series, and Profile use `PDR`
   d. Production System – choose the correct system
   e. Site – choose the site
   f. Connect Options – additional options for connection to source server, that is, a different login name. For example, for News FTP with a user name `vmfmovie`, put in `-login vmfmovie`; for K2 put in `-login movie`
   g. Root Path – If you’re archiving from a News server, leave this blank. If you’re archiving from a K2, M-Series, or Profile server, type in the root path, for example `/explodedFile/V:/default`
   h. Max Throughput (Mb/s) – max throughput
   i. Max Accesses – total number of access possible (default `10`)
   j. Max Read Accesses – total number of access for reading (default `10`)
   k. Max Write Accesses – total number of access for writing (default `10`)
5. Restart the DIVArchive Manager Service to enable the new settings.

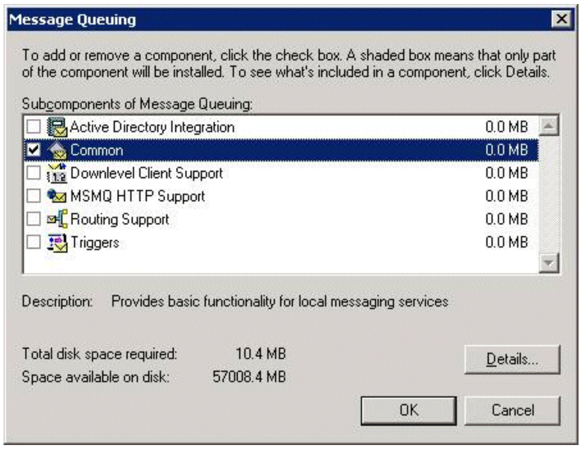
Consider the following when preparing to integrate DIVA with Aurora Browse:

- The DIVA MDI does not take any user specified name for a full restore. The clips are restored using the original name (from archive). The DIVA MDI does, however, allow a user specified name for a partial restore.
- DIVA has no fixed limit for concurrent transfers.
- If archiving from a Profile XP standalone, take the concurrent transfer limit into consideration. DIVA’s setting for concurrent transfers applies to specific source/ destination pairs. With the configuration utility/tool you can specify the concurrency limit on a server-by-server basis.
- The DIVA MDI makes an the assumption that the MDI is the only gateway to the entire DIVA file system. Any changes made outside the scope of the MDI will not be reflected in MDI immediately.
- Renaming of an asset is not supported in DIVA.
- The MDI will use whatever priority the user chooses.
- The source name must be the same as the host name specified in the Transfer Server, not the actual machine. Under that name, specify the host name or IP address of the actual machine in the IP Address field.
- If the DIVA server is rebooted, the Thomson DIVA MDI service must be restarted. Refer to “Accessing services” on page 48.

FlashNet preparations

To use Flashnet with the Aurora Browse system, make sure that you have installed the following pre-requisites on the Flashnet MDI server.

- Flashnet Client software (provided by SGL)
- MS Message Queuing, the Common subcomponent (part of the Windows Server 2003 CD)



Message Queuing

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Message Queuing:

□ Active Directory Integration	0.0 MB
☑ Common	0.0 MB
□ Downlevel Client Support	0.0 MB
□ MSMQ HTTP Support	0.0 MB
□ Routing Support	0.0 MB
□ Triggers	0.0 MB

Description: Provides basic functionality for local messaging services

Total disk space required: 10.4 MB

Space available on disk: 57008.4 MB

Check the following on the Flashnet server:

1. Login to the machine.
2. Verify that you can FTP from the FlashNet server to the high-res storage machine. If archiving from K2 storage or AuroraShare NAS, verify that you can FTP from the FlashNet server to the K2 storage or AuroraShare NAS on Control FTP and login as user *vmfmovie*.
3. Make sure the FlashNet services are up and running.

Consider the following when preparing to integrate FlashNet with Aurora Browse:

- The FlashNet MDI does allow a user-specified name for a partial restore.
- The FlashNet MDI uses a file cache to support asset functionality. As the FlashNet device does not have any support for file system updates, the FlashNet MDI assumes that the MDI is the only gateway to the entire FlashNet file system. Any changes made outside the scope of the MDI will not be reflected in MDI immediately.
- In FlashNet, renaming of an asset is not supported.
- A restore operation always defaults to highest “Time Critical” priority and archive operation defaults to “normal” priority.

Network connectivity - all archive types

To test network connectivity, ping all machines from all machines.

If archiving to/from K2 Storage or AuroraShare NAS, ping these machines on the Control FTP network:

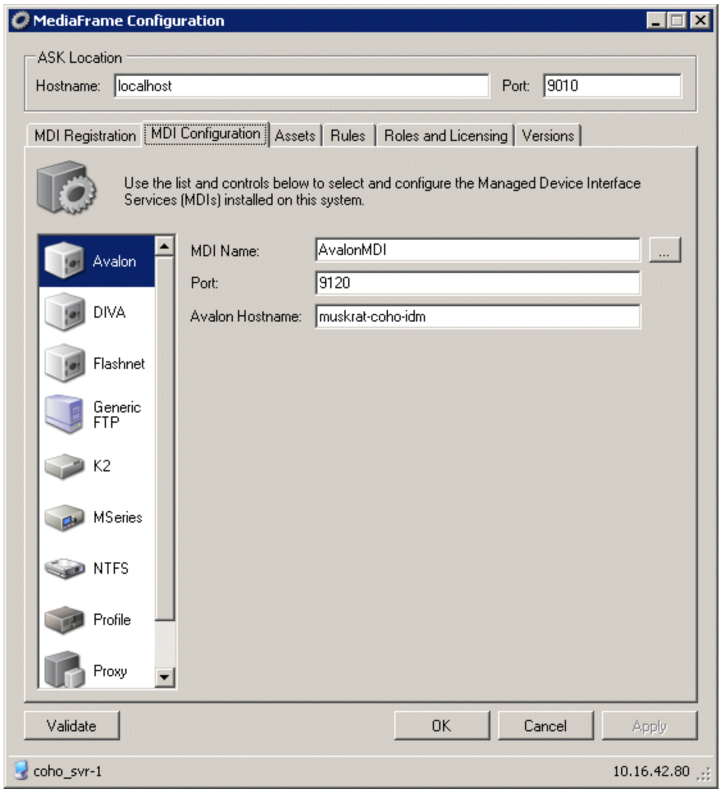
- MediaFrame server

- Archive MDI host
- News MDI host
- The machine hosting the Aurora FTP service
- Archive machine
- The K2 storage or AuroraShare NAS system

Configure Avalon MDI

Open this tab of the MediaConfig tool locally on the machine that hosts the Avalon MDI software component.

To configure the Avalon MDI, do the following.



MediaFrame Configuration

ASK Location

Hostname: localhost

Port: 9010

Use the list and controls below to select and configure the Managed Device Interface Services (MDIs) installed on this system.

MDI Name: AvalonMDI

Port: 9120

Avalon Hostname: muskrat-coho-idm

coho_svr-1 10.16.42.80

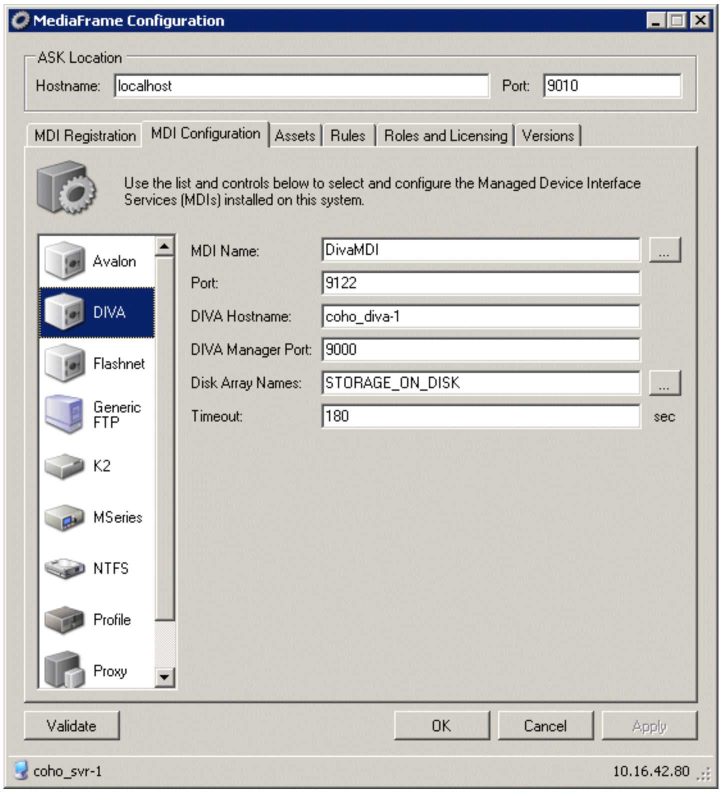
1. Select **Programs | Grass Valley | MediaFrame Config**. Select the MDI Configuration tab and the Avalon icon.
2. Enter the name of the MediaFrame server.
3. Port 9010 is required. Do not modify. See “Ports and services mapping” on page 38.
4. Use the **...** button to location the name of the Avalon MDI.
5. Port 9120 is required. See “Ports and services mapping” on page 36.
6. Enter the name or IP address of the Avalon machine.
7. Click **OK**.

NOTE: You no longer need to define FTP for archive sources/destinations.

Configure DIVA MDI

Open this tab of the MediaConfig tool locally on the machine that hosts the DIVA MDI software component.

To configure the DIVA MDI, do the following.


MediaFrame Configuration

ASK Location

Hostname: localhost

Port: 9010

Use the list and controls below to select and configure the Managed Device Interface Services (MDIs) installed on this system.

MDI Name: DivaMDI

Port: 9122

DIVA Hostname: coho_diva-1

DIVA Manager Port: 9000

Disk Array Names: STORAGE_ON_DISK

Timeout: 180 sec

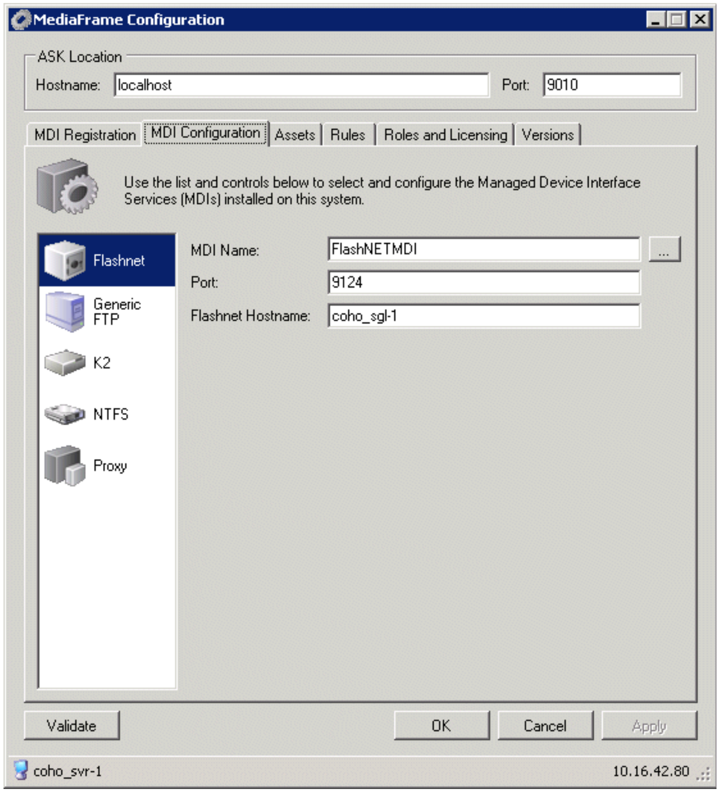
coho_svr-1 10.16.42.80

1. Select **Programs | Grass Valley | MediaFrame Config**. Select the MDI Configuration tab and the DIVA icon.
2. Use the **...** button to location the name of the DIVA MDI.
3. Port 9122 is required.
4. Enter the hostname or IP address of the DIVA machine.
5. The default value for the Diva manager port is 9000. The default timeout is 180.
6. Click **OK**.

NOTE: You no longer need to define FTP for archive sources/destinations.

Configure FlashNet MDI

Open this tab of the MediaConfig tool locally on the machine that hosts the FlashNet MDI software component. This tab tells the FlashNet MDI where to look for FTP transfer of high-res material. For K2 storage or AuroraShare NAS systems, archive transfers are handled by a single FTP server.



MediaFrame Configuration

ASK Location

Hostname: localhost

Port: 9010

Use the list and controls below to select and configure the Managed Device Interface Services (MDIs) installed on this system.

MDI Name: FlashNETMDI

Port: 9124

Flashnet Hostname: coho_sgl-1

coho_svr-1 10.16.42.80

To configure the Flashnet MDI, do the following.

1. Select **Programs | Grass Valley | MediaFrame Config**. Select the MDI Configuration tab and the Flashnet icon.
2. Enter the name of the MediaFrame server.
3. Port 9010 is required. Do not modify. See “Ports and services mapping” on page 38.
4. Use the **...** button to location the name of the FlashNet MDI.
5. Port 9124 is required. See “Ports and services mapping” on page 36.
6. Enter the name or IP address of the FlashNet machine.
7. Click **OK**.

NOTE: You no longer need to define FTP for archive sources/destinations.

Checklist: Archive stage

Use the following check list to verify that the configuration and testing of the archive stage is complete.

□ High-res material transfers (archives) to archive device.

□ High-res material transfers (restores) from archive device to restore location.

Deploy remaining machines for full system

For the basic configuration path, after you have worked through all the configuration stages and verified functionality at each stage, you deploy your remaining Aurora Browse machines.

Do the following tasks to deploy your remaining Aurora Browse machines, as appropriate for the machines included in your particular system. For instructions, refer to the applicable configuration stages early in this chapter.

- Deploy remaining Aurora Proxy Encoders. Refer to "Encoder stand-alone stage" on page 68 and "Encoder + Server stage" on page 76.

Test system level interactions

Run the following tests to verify that all machines are available and will function correctly, especially during times of heavy system activity.

Multiple scavenge test

This test verifies that scavenge operations can simultaneously control all Aurora Proxy Encoders to optimize performance during times of heavy proxy asset creation.

To test multiple scavenge operations, do the following:

1. On the machine from which high-res media is scavenged, prepare a quantity of test clips, such that you have one more test clip than the number of Aurora Proxy Encoders in your system. For example, if you have four Aurora Proxy Encoders, prepare five test clips. You must prepare the test clips without triggering the system to create any proxy assets. You can do this by recording media with a channel that is not associated with the system for ingest, or by copying existing clips to a different bin or folder. In any case, the bin or folder in which these test clips are initially placed must not be a bin that is currently monitored by the system for scavenge operations. Make the test clips at least a minute long.
2. On the MediaFrame server, open Event Viewer.
3. Prepare a bin or folder (preferably one that is currently empty) for monitoring by the system for scavenge operations. On the Aurora Proxy Encoders, define rules to create MPEG proxy for high-res material that appears in the scavenge folder.
4. On the machine from which high-res media is scavenged, simultaneously copy all the test clips into the prepared bin.
5. In Event Viewer, verify that scavenge activities occur for each channel, and that all Aurora Proxy Encoders are encoding MPEG simultaneously.
6. With Aurora Edit LD or the Aurora Browse application, validate MPEG assets.

Purge test

1. Select an asset from the results list to load details. Take note of the components associated with this asset. This can be done by looking at the Related tab in the details page. By using the mouse to hover over the entries in the related tab you can derive where the asset components exist in the system.
2. From the general tab on the details page edit the expiration date and select a date

in the past.

3. The purge process polls at configured intervals. To expedite testing go to the Windows services panel and restart the Asset Manager process. This will cause the cycle to be reset and assets meeting expiration criteria will be processed immediately.
4. Refresh the search results list by pressing the go button with no criteria specified.
5. Verify that asset components noted earlier no longer exist in the system. You will have to look at the NAS for the specific paths to proxy asset components. The asset on the high-res storage should also be removed.

Add Aurora Browse Clients

The Aurora Browse client application can be installed from the MediaFrame Server. Before giving users the path to the *setup.exe* file, an administrator needs to set up roles and licenses for the user.

Do the following tasks to enable PCs to act as a Aurora Browse clients and run the Aurora Browse application.

- "Connect server and NAS to customer LAN" on page 95
- "Configure Aurora Browse Licenses" on page 95
- "Managing Aurora Browse User sessions" on page 98

Connect server and NAS to customer LAN

The MediaFrame server and NAS machines must have network access to the external LAN of the Aurora Browse client PCs. Work with the IT personnel at the customer site to configure Domain, DNS suffix, or any other settings required by the site's LAN.

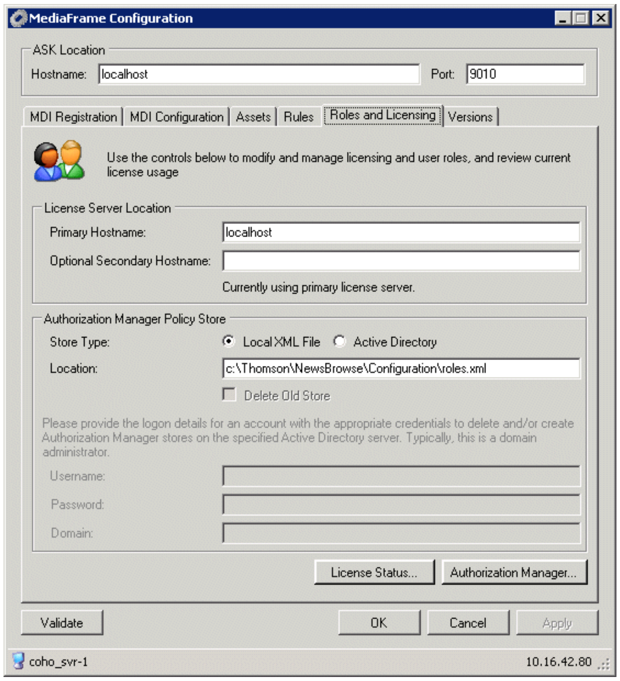
Also, make sure that permissions are correct for access to the MediaFrame server website, which serves the Aurora Browse application. The website uses Integrated Windows Authentication.

Configure Aurora Browse Licenses

You must configure the MediaFrame server, as per your Aurora Browse license, to allow user access to Aurora Browse application features. Roles and Licensing is managed centrally from the MediaFrame server. This requires that you log in as Aurora Browse administrator. A role can be leased if the user has been assigned the role by an administrator, and a license for the role exists and is available.

To configure for Aurora Browse licenses, do the following.

1. Select **Programs | Grass Valley | MediaFrame Config** and select the **Roles and Licensing** tab.



MediaFrame Configuration

ASK Location

Hostname: localhost Port: 9010

Use the controls below to modify and manage licensing and user roles, and review current license usage

License Server Location

Primary Hostname: localhost

Optional Secondary Hostname:

Currently using primary license server.

Authorization Manager Policy Store

Store Type: ● Local XML File ○ Active Directory

Location: c:\Thomson\NewsBrowse\Configuration\roles.xml

□ Delete Old Store

Please provide the logon details for an account with the appropriate credentials to delete and/or create Authorization Manager stores on the specified Active Directory server. Typically, this is a domain administrator.

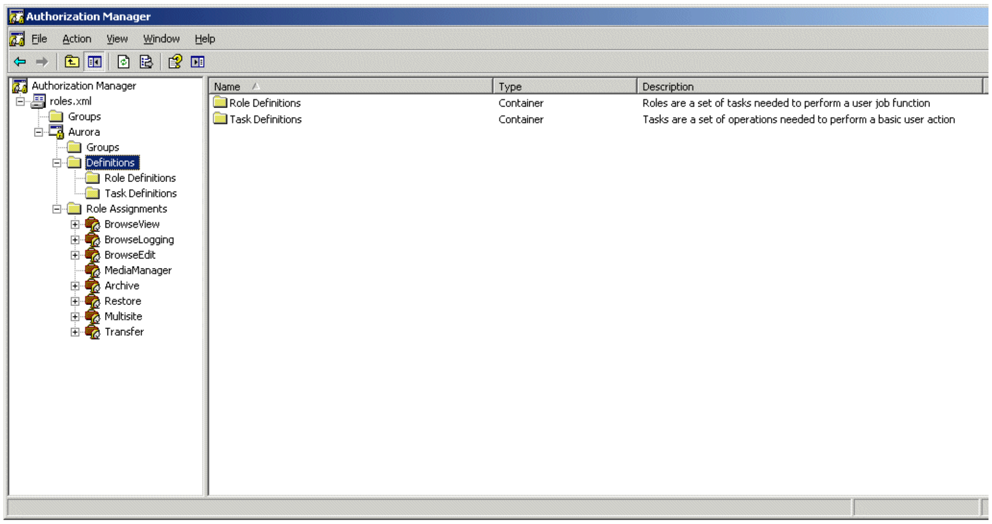
Username:

Password:

Domain:

coho_svr-1 10.16.42.80

2. To add users and assign roles, click the **Authorization Manager** button.



Authorization Manager

Authorization Manager
- roles.xml
  - Groups
  - Aurora
    - Groups
    - Definitions
      - Role Definitions
      - Task Definitions
    - Role Assignments
      - BrowseView
      - BrowseLogging
      - BrowseEdit
      - MediaManager
      - Archive
      - Restore
      - Multisite
      - Transfer

Name	Type	Description
Role Definitions	Container	Roles are a set of tasks needed to perform a user job function
Task Definitions	Container	Tasks are a set of operations needed to perform a basic user action

3. Configure according to the Microsoft Windows documentation: add a group, then add users to that group.

4. Enter the following:

- Username — This must match the account with which the Aurora Browse client accesses the Aurora Browse application.
- Roles — Select the Aurora Browse application functionality to which the user

needs access. The Roles listed are dependent upon current licensing.

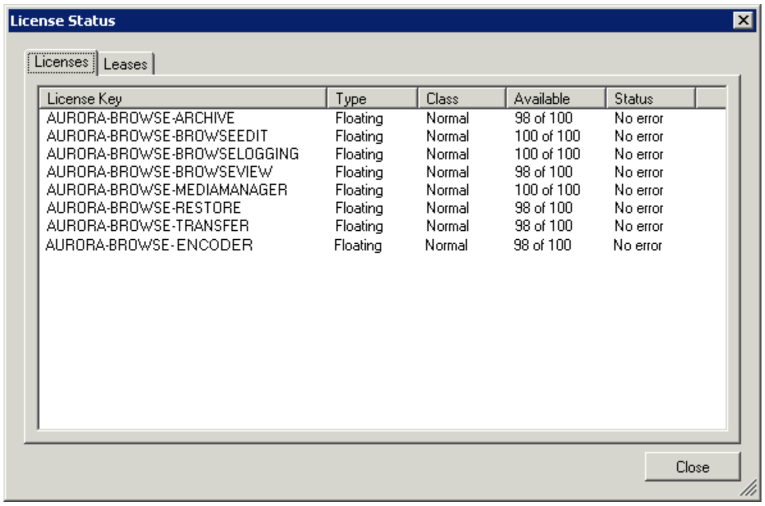
The following table defines the Roles:

Role	Description
BrowseView	Lets you search, browse, and explore assets and view them.
BrowseLogging	Lets you search, browse, edit and explore metadata.
BrowseEdit	LD editing, search, browse and explore.
MediaManager	In addition to all the other privileges in this table, MediaManager lets you search, browse, explore, delete, rename, change custom metadata schema.
Archive	Lets you transfer high-res assets from a K2 system to an archive device and optionally delete the high-res assets from the K2 system.
Restore	Lets you restore high-res assets from an archive device to a K2 system.
Multi-site	Lets you search, browse, and explore remotely as well as locally. Also allows transfer between sites. (Not available in Aurora Browse 6.5)
Transfer	Lets you transfer locally on the Aurora Browse system. You need to add this role even if the user has the MediaManager role.
Encoder	Lets you create or recreate proxy on the Aurora Browse system. You need to add this role even if the user has the MediaManager role.

If you assign a Role to more users than the session count for which it is licensed, the Role is not available to all users at times when sessions exceed the count.

Verify license status and user sessions

To check the status of the licenses or the status of the leased user sessions, click the **License Status** button on the MediaConfig tool.



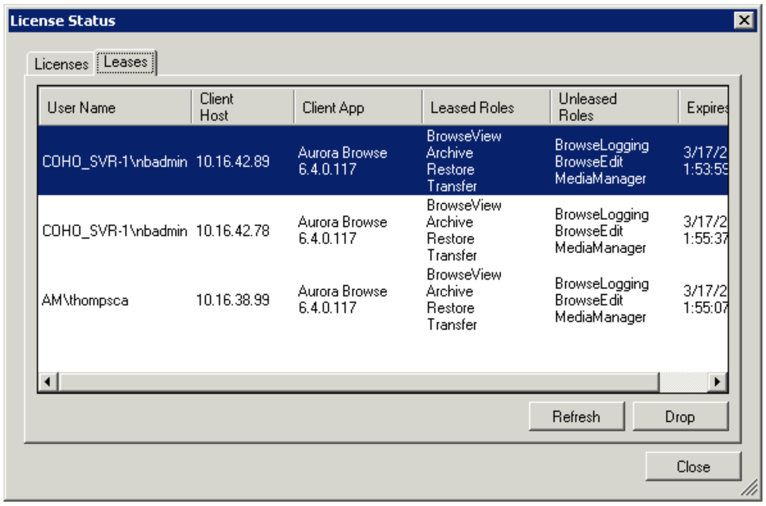
License Key	Type	Class	Available	Status
AURORA-BROWSE-ARCHIVE	Floating	Normal	98 of 100	No error
AURORA-BROWSE-BROWSEEDIT	Floating	Normal	100 of 100	No error
AURORA-BROWSE-BROWSELOGGING	Floating	Normal	100 of 100	No error
AURORA-BROWSE-BROWSEVIEW	Floating	Normal	98 of 100	No error
AURORA-BROWSE-MEDIAMANAGER	Floating	Normal	100 of 100	No error
AURORA-BROWSE-RESTORE	Floating	Normal	98 of 100	No error
AURORA-BROWSE-TRANSFER	Floating	Normal	98 of 100	No error
AURORA-BROWSE-ENCODER	Floating	Normal	98 of 100	No error

The Aurora Browse administrator sets up Aurora Browse users and can restrict their access to Aurora Browse application features and assets, as explained in the following procedures.

Managing Aurora Browse User sessions

The Aurora Browse administrator can view the current users with active sessions and force a session to be dropped, as follows:

1. Select **Programs | Grass Valley | MediaFrame Config** and select the Roles and Licensing tab.
2. Click the License Status button and select the Leases tab.



User Name	Client Host	Client App	Leased Roles	Unleased Roles	Expires
COHO_SVR-1\nbadmin	10.16.42.89	Aurora Browse 6.4.0.117	BrowseView Archive Restore Transfer	BrowseLogging BrowseEdit MediaManager	3/17/2 1:53:59
COHO_SVR-1\nbadmin	10.16.42.78	Aurora Browse 6.4.0.117	BrowseView Archive Restore Transfer	BrowseLogging BrowseEdit MediaManager	3/17/2 1:55:37
AM\thompsca	10.16.38.99	Aurora Browse 6.4.0.117	BrowseView Archive Restore Transfer	BrowseLogging BrowseEdit MediaManager	3/17/2 1:55:07

3. To drop a user's current active session, select the user name and click the **Drop** button.

Adding custom fields and metadata mapping

Custom fields enhance site-specific management of assets. The Aurora Ingest or Aurora Browse administrator defines a custom field to create an asset metadata-type that uniquely fits the site's workflow.

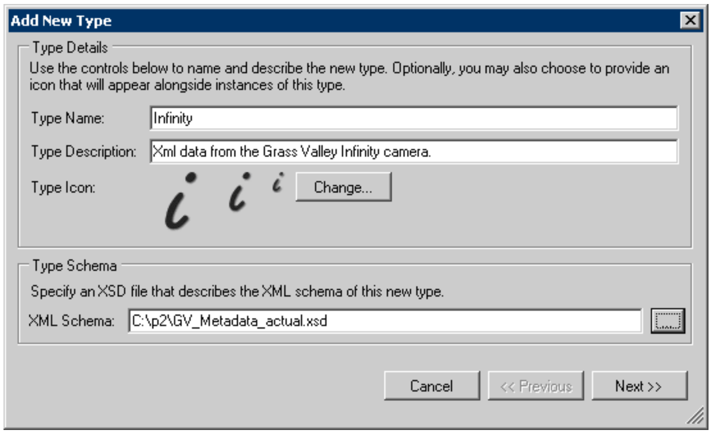
The user of the Aurora Browse application can then assign metadata to an asset by entering text or making a selection in the custom field. Adding custom fields is optional. If you have administrator-level privileges, you can add custom metadata fields in the Aurora Browse client. For more information, see the ***Aurora Browse User Guide***.

Setting up metadata mapping

Metadata mapping registers and maps any foreign metadata (such as metadata from a camera) into the MediaFrame system. Since it is in XML format, an XML schema is needed.

You need to set up metadata mapping before importing the metadata in Ingest. To set up metadata mapping, follow these steps:

1. Select **Programs | Grass Valley | MediaFrame Config**. Select the Metadata Mapping tab.
2. Click **Add**. The Add New Type —Type Details dialog box displays.



Use the controls below to name and describe the new type. Optionally, you may also choose to provide an icon that will appear alongside instances of this type.

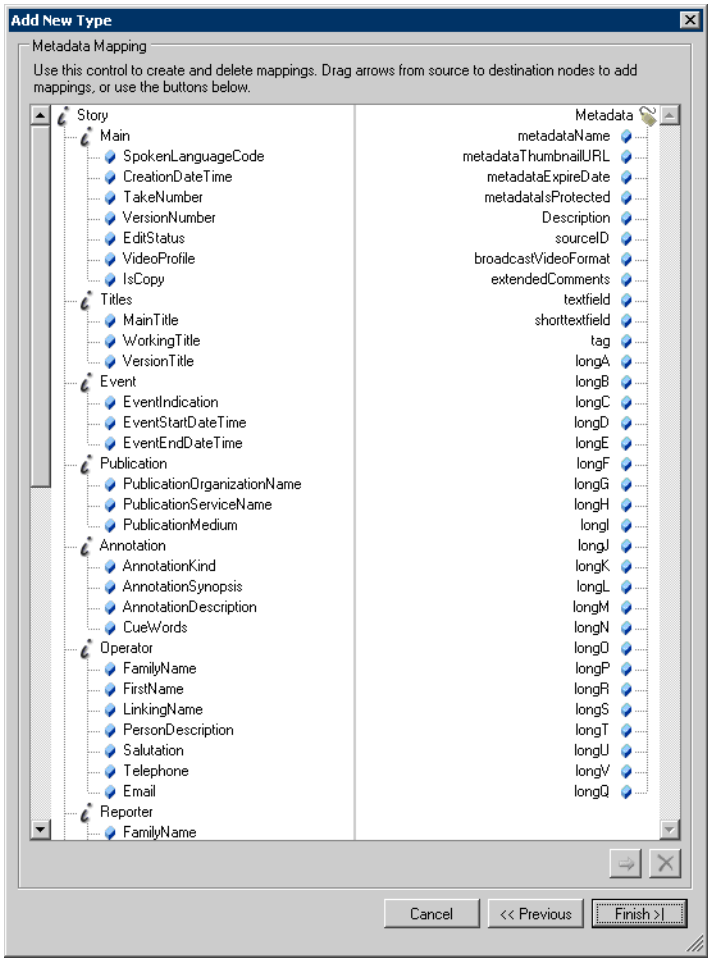
Type Name: Infinity

Type Description: Xml data from the Grass Valley Infinity camera.

Specify an XSD file that describes the XML schema of this new type.

XML Schema: C:\p2\GV_Metadata_actual.xsd

3. Enter the type name and description. If you want to change the type icon, click the **Change...** button.
4. Click the **...** button to select the XML schema for this type.
5. Click **Next**. The Add New Type — Metadata Mapping dialog box displays.

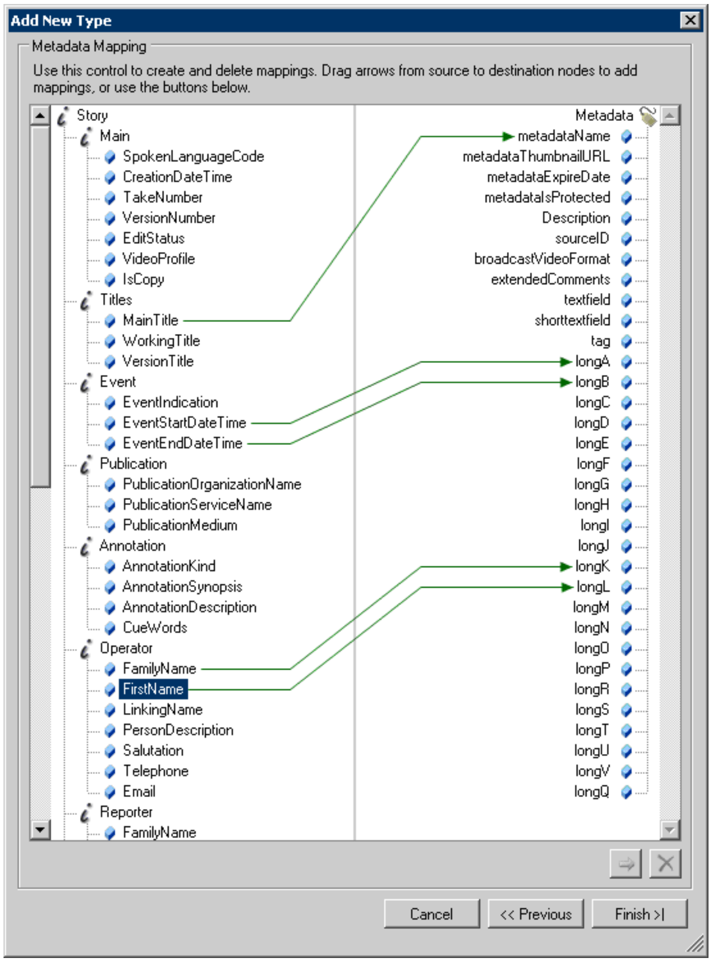


Add New Type

Metadata Mapping

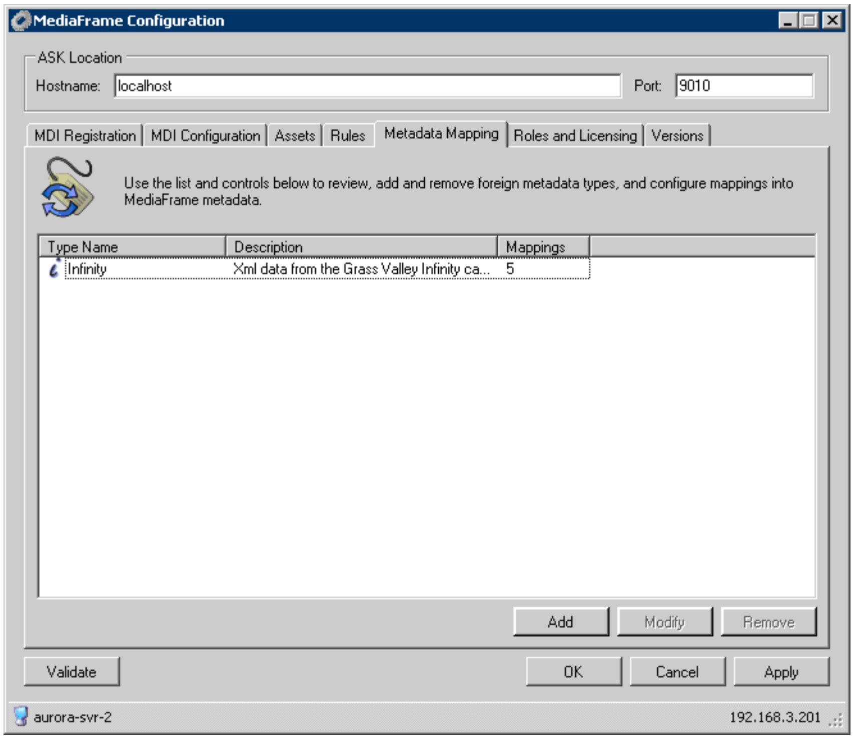
Use this control to create and delete mappings. Drag arrows from source to destination nodes to add mappings, or use the buttons below.

6. To map the metadata, select the desired field in the Story column and drag it to the appropriate item in the Metadata column.



Use this control to create and delete mappings. Drag arrows from source to destination nodes to add mappings, or use the buttons below.

7. Click **Finish**. The mapped metadata information is displayed.



Hostname: localhost

Port: 9010

Use the list and controls below to review, add and remove foreign metadata types, and configure mappings into MediaFrame metadata.

Type Name	Description	Mappings
Infinity	Xml data from the Grass Valley Infinity ca...	5

aurora-svr-2 192.168.3.201

Chapter 4

Recovery Planning

Establish a recovery plan in the event an Aurora Browse MediaFrame system fails, so that services can be re-configured rapidly to minimize impact.

Encoder failure considerations

Encoders provide redundancy through numbers. A plan should identify the critical encoders in the system and alternate encoders that can be reconfigured to substitute in the case of failure. There are no automated fail-over capabilities with Aurora Browse MediaFrame components. It is important to identify which machine(s) host Managed Device Interface services. These services can be pre-installed on secondary devices, although the server should not be configured to monitor them unless a failure of the primary service occurs. Managed Device Interface services can exist on any encoder and the server need only to be reconfigured to point to the new machine in case of failure.

Encoding jobs can be assigned to any available Aurora Proxy Encoder. N+1 redundancy is achieved by adding an extra Aurora Proxy Encoder.

MediaFrame server failure considerations

The MediaFrame server must have a database maintenance plan in place. The maintenance plan backs up the SQL database on a regular basis and stores it in a safe location. In the case of server failure the database can then be restored to minimize data loss.

MediaFrame servers shipped from the factory prior to June 2007 have Microsoft SQL Server 2000 installed. For these servers you must configure a database maintenance plan. Refer to previous version of this manual for procedures.

MediaFrame server shipping from the factory beginning in June 2007 have Microsoft SQL Server 2005 installed. For these servers there is a pre-configured SQL Server maintenance plan in place that provides the necessary backups.

If the SQLSERVERAGENT service is ever stopped, so is your maintenance plan. Make sure that the service is set to start automatically.

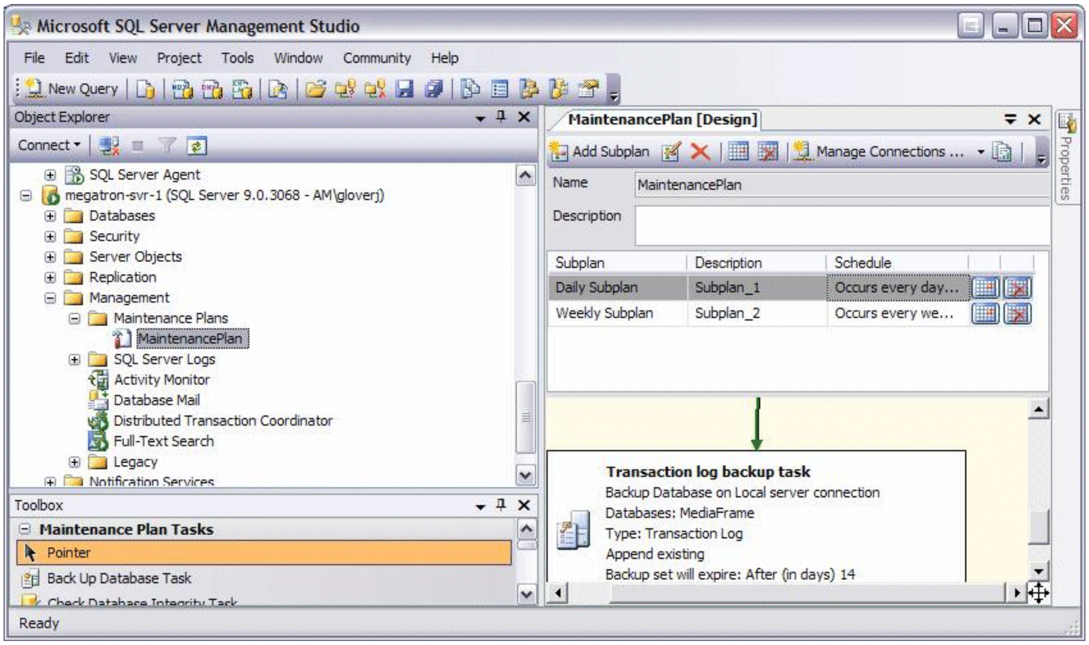
If an off-line backup server is purchased it should be pre-configured to operate in the system so in case of primary server failure, minimal time will be spent bringing up the backup system. The backed up database could be restored to this backup server on a regular basis.

Newer systems have redundant power supplies and mirrored disks to further protect the integrity of the system.

Verifying the database maintenance plan status

1. To determine the maintenance plan status, look in SQL Server Management Studio under **<*server name*> + Management + Maintenance Plans**.

2. Right-click on the plan and select **View History**.



Name: MaintenancePlan

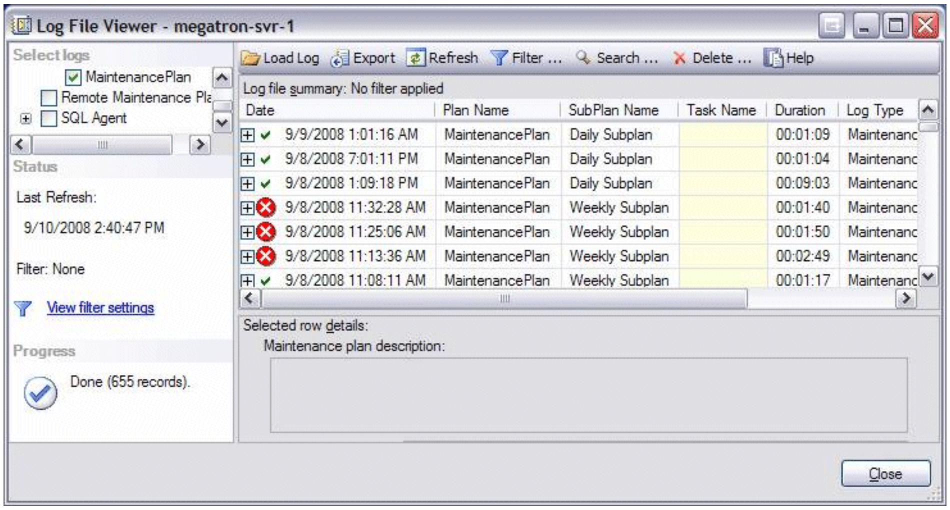
Description:

Subplan	Description	Schedule
Daily Subplan	Subplan_1	Occurs every day...
Weekly Subplan	Subplan_2	Occurs every we...

Transaction log backup task
Backup Database on Local server connection
Databases: MediaFrame
Type: Transaction Log
Append existing
Backup set will expire: After (in days) 14

3. Verify the status:

- Green check mark — everything is good
- Red X — indicates an error



☑ MaintenancePlan
□ Remote Maintenance Pla
□ SQL Agent

Last Refresh:

9/10/2008 2:40:47 PM

Filter: None

Done (655 records).

Log file summary: No filter applied

Date	Plan Name	SubPlan Name	Task Name	Duration	Log Type
✓ 9/9/2008 1:01:16 AM	MaintenancePlan	Daily Subplan		00:01:09	Maintenanc
✓ 9/8/2008 7:01:11 PM	MaintenancePlan	Daily Subplan		00:01:04	Maintenanc
✓ 9/8/2008 1:09:18 PM	MaintenancePlan	Daily Subplan		00:09:03	Maintenanc
☒ 9/8/2008 11:32:28 AM	MaintenancePlan	Weekly Subplan		00:01:40	Maintenanc
☒ 9/8/2008 11:25:06 AM	MaintenancePlan	Weekly Subplan		00:01:50	Maintenanc
☒ 9/8/2008 11:13:36 AM	MaintenancePlan	Weekly Subplan		00:02:49	Maintenanc
✓ 9/8/2008 11:08:11 AM	MaintenancePlan	Weekly Subplan		00:01:17	Maintenanc

Selected row details:

Maintenance plan description:

Modifying the database maintenance plan

The following section applies to the pre-configured database maintenance plan for SQL Server 2005.

The MediaFrame server uses the SQL full recovery model, and the maintenance plan is essential to keeping the database in working order. The maintenance plan backs up the database and the accompanying transaction log.

Database maintenance plan description

The pre-configured maintenance plan contains two sub-plans, as follows:

- The first sub-plan executes weekly every Sunday at 1:30 a.m. to check the database integrity, release any unused data storage space, update database statistics and perform a full backup of the database.
- The second sub-plan executes daily (except Sunday) at 1:30 a.m. to create a differential backup which contains any changes since the full backup.

Together, these two sub-plans perform all of the maintenance required by the MediaFrame database.

Modifying the maintenance plan backup location

The pre-configured maintenance plan places database backup files in the following location:

C:\MediaFrame\backup

If your site has a different location specified for database backup files, use the following procedure to modify the location:

1. Open the Windows operating system Services control panel and verify that the SQLSERVERAGENT service is set to start automatically and that it is currently running.
2. Open **Microsoft SQL Server Management Studio** and log in with the appropriate credentials. To create or manage maintenance plans, you must be a member of the sysadmin fixed server role.

   Server Management Studio opens.
3. In Management Studio Object Explorer, expand the node for the MediaFrame server, expand **Management**, and then expand **Maintenance Plans**.
4. Right-click **MediaFrame Maintenance Plan**, and click **Modify**.

   A Plan Design panel opens.
5. Double-click **Backup Database Task**.

   A Backup Database Task dialog box opens.
6. In the Backup Database Task dialog box, in the **Folder** field, modify the backup directory path.

NOTE: SQL can only see local drives and cannot see shared directories or disks that are not native to the machine.

7. Click **OK** on the Backup Database Task dialog box.
8. Close Server Management Studio and answer **Yes** when prompted to save changes.

Modifying the maintenance plan schedule

The backup should occur at a time that does not conflict with peak usage of the system. The pre-configured maintenance plan schedules the backup for 1:30 a.m. If this schedule conflicts with your system usage patterns, use the following procedure to modify the schedule:

1. Open the Windows operating system Services control panel and verify that the SQLSERVERAGENT service is set to start automatically and that it is currently running.
2. Open **Microsoft SQL Server Management Studio** and log in with the appropriate credentials. To create or manage maintenance plans, you must be a member of the sysadmin fixed server role.

   Server Management Studio opens.
3. In Management Studio Object Explorer, expand the node for the MediaFrame server, expand **Management**, and then expand **Maintenance Plans**.
4. Right-click **MediaFrame Maintenance Plan**, and click **Modify**.

   A Plan Design panel opens.
5. In the Plan Design panel list, select one of the following subplans:
   - weekly_maintenance
   - daily_maintenance
6. With the subplan selected, click **Subplan Schedule** in the toolbar.

   The Job Schedule Properties dialog box opens
7. In the Job Schedule Properties dialog box, enter the new schedule details.
8. Click **OK** on the Job Schedule Properties dialog box.
9. Repeat preceding steps as necessary to modify the other subplan schedule.
10. Close Server Management Studio and answer **Yes** when prompted to save changes.

Restoring the MediaFrame server database

If your MediaFrame server is correctly running the database maintenance plan, the database backup files allow you to restore the database. You should only need to restore the database if a catastrophic system failure occurs and you lose the database.

To restore the database, you must accomplish tasks such as restoring the full backup, restoring each subsequent differential backup, restoring the tail-log, and recovering the database. Only database administrators or persons with similar experience and knowledge should attempt to restore the MediaFrame server database. Based on your modifications to the database maintenance plan and the time the system failure occurred, a database administrator can refer to Microsoft SQL Server procedures as necessary and determine the proper steps. If you need help with this, contact Grass Valley Support.

Troubleshooting the transaction log

This section applies to Microsoft SQL Server 2005. For similar information that applies to Microsoft SQL Server 2000, refer to previous versions of this manual.

The transaction log is responsible for keeping track of all the edits to data until it reaches what is known as a checkpoint. Once the checkpoint is reached, the data should be permanently committed to the database. The maintenance plan does this automatically.

If the database is rendered inoperable due to the transaction log becoming too large, it is highly likely that the transaction log has never been backed up, a database maintenance plan has not been enabled on the system, or the SQL Server agent is not running to implement your maintenance plan.

In a database which is not being backed up properly, the log file will grow until there is no more space available on the hard drive. This will cause the system to eventually fail. Backing up the transaction log at this point solves the problem of continuing growth and ensures the database is a better position to be recovered should it fail, but the log file would still be much larger than necessary.

Use the procedures in this section to fix the problem.

Back up the transaction log

First, back up the database and the transaction log to keep a record of its current state.

1. Identify the location of transaction log backups. The default location is as follows:

   C:\Program Files\Microsoft SQL Server\MSSQL\MSSQL\BACKUP\<database name>

2. Open **Microsoft SQL Server Management Studio** and log in with the appropriate credentials. To create or manage maintenance plans, you must be a member of the sysadmin fixed server role.

   Server Management Studio opens.

3. Select **New Query**, and change the selected database to **MediaFrame**.
4. Run the following command:

   ```
   BACKUP LOG <database name>
     TO DISK=’<default backup
     location>\MediaFrame_tlog_<date in YYYYMMDDHHMM
     format>’

   GO
   ```

   Where <default backup location> is where the transaction log backups are kept and the date is the current date.

5. If the log file is so big that it would be inappropriate to back it up, follow steps 1-4, then use this command instead:

   ```
   backup log <database name> with truncate_only
   GO
   ```

6. Continue with the next procedure “Shrink the transaction log”.

Shrink the transaction log

After backing up the transaction log, you must flush and shrink the transaction log file to reduce its size. This must be done very soon after backing up the transaction log.

1. If it is not already open, open **Microsoft SQL Server Management Studio** and log in with the appropriate credentials. To create or manage maintenance plans, you must be a member of the sysadmin fixed server role.

   Server Management Studio opens.

2. Select **New Query**, and change the selected database to **MediaFrame**.

3. Run the following command:

   ```
   DBCC SHRINKFILE(MediaFrame_Log, 10)
   ```

Chapter 5

Troubleshooting the system

Troubleshooting tools

The following troubleshooting utilities can be found on Aurora Browse machines in the Windows menu **Start | Programs | Grass Valley**.

MediaFrame troubleshooting tool

EventViewer — This utility is available on all Aurora Browse machines and provides a log of information and errors for services running on that particular device.

Aurora Browse application troubleshooting tips

Use the following table to identify and resolve problems related to the access and operation of the Aurora Browse user interface.

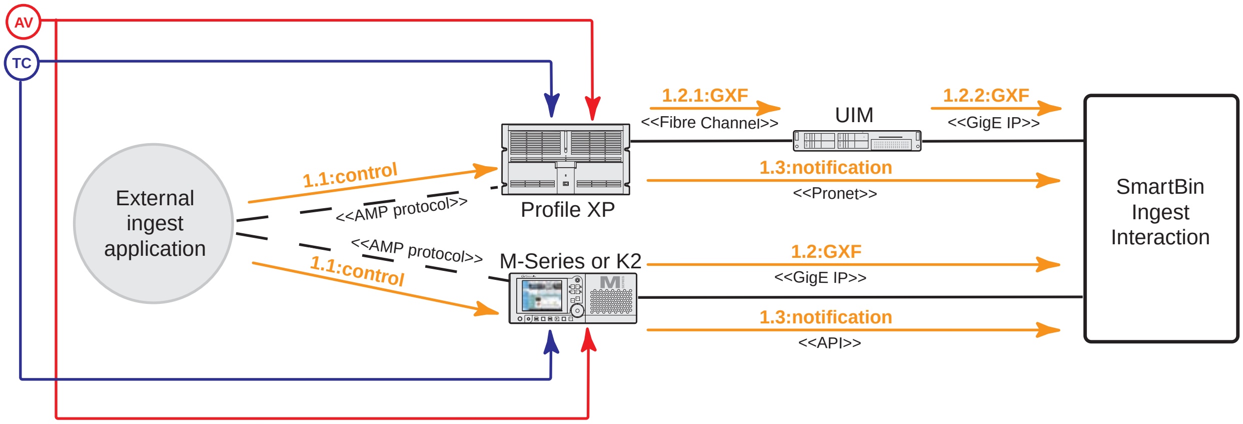
Symptom	Solution
Problem searching for specific words in the Aurora Browse search	Verify that the word or words you are searching for is not in the noise words list that SQL automatically screens out of search terms. To modify the list of noise words, edit the file that is contained at $SQL_Server_Install_Path\Microsoft SQL Server\MSSQL.1\MSSQL\FTDATA\ on your SQL Server host. Be aware that modifying this list might affect expected execution times.
Problem accessing the Aurora Browse system.	Check the Status window. Verify ASK and the other components are running. Check that the server is running. Check that the server is connected to the client network. Check that connections are secure. Check that IIS is running on the server.
Problem searching for or opening proxy	Check to make sure the low-res NAS location is a mapped drive.
MediaFrame server is accessible using IP address but not server name	Host tables or DNS entries must be set to map name to IP address. This should be coordinated with facility IT personnel.
Problem Accessing the Aurora Browse application - permission denied	Check that the account used to log into the client workstation is licensed on the server. See “Configure Aurora Browse Licenses” on page 95.

Appendix ***A***

Component Interaction Diagrams

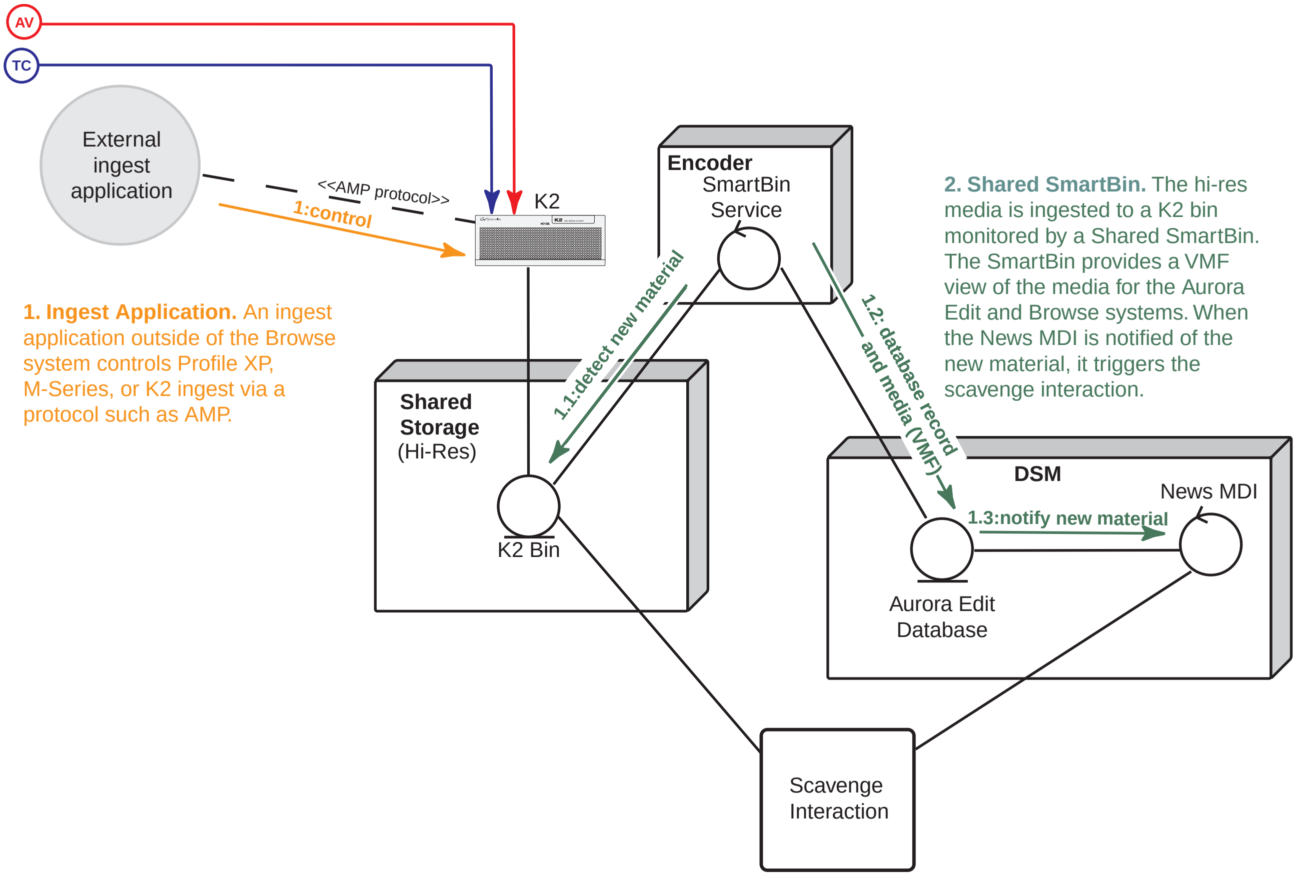
This appendix provides diagrams and explanations of how the system software components interact.

External Ingest Application to Transfer SmartBin



1. Ingest Application. An ingest application outside of the Browse system controls Profile XP, M-Series, or K2 ingest via a protocol such as AMP. When hi-res media is ingested, the Profile XP or M-Series sends the media as a GXF stream and sends a notification about the newly ingested media to the SmartBin Ingest Interaction.

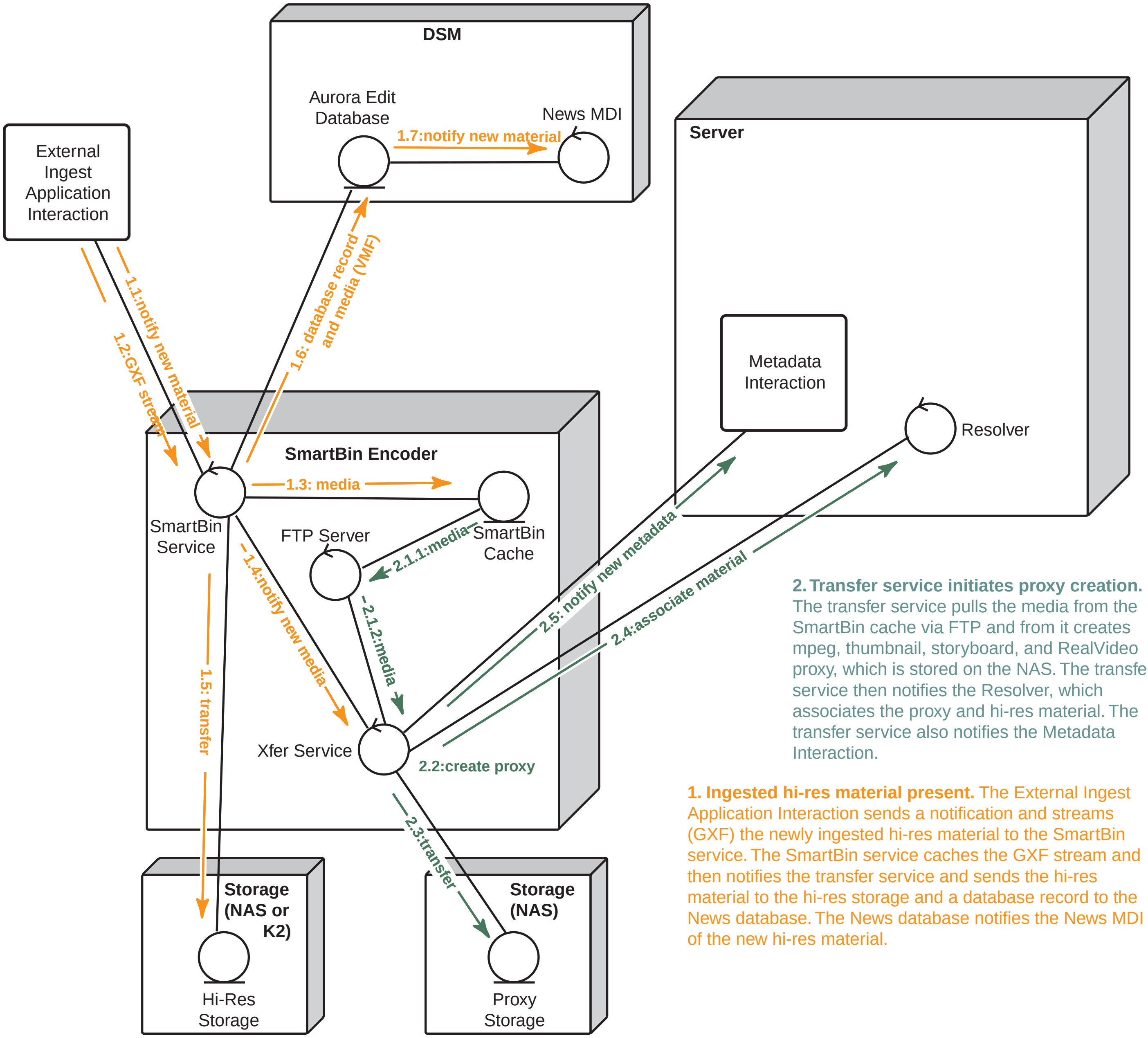
External Ingest Application to Shared SmartBin



1. Ingest Application. An ingest application outside of the Browse system controls Profile XP, M-Series, or K2 ingest via a protocol such as AMP.

2. Shared SmartBin. The hi-res media is ingested to a K2 bin monitored by a Shared SmartBin. The SmartBin provides a VMF view of the media for the Aurora Edit and Browse systems. When the News MDI is notified of the new material, it triggers the scavenge interaction.

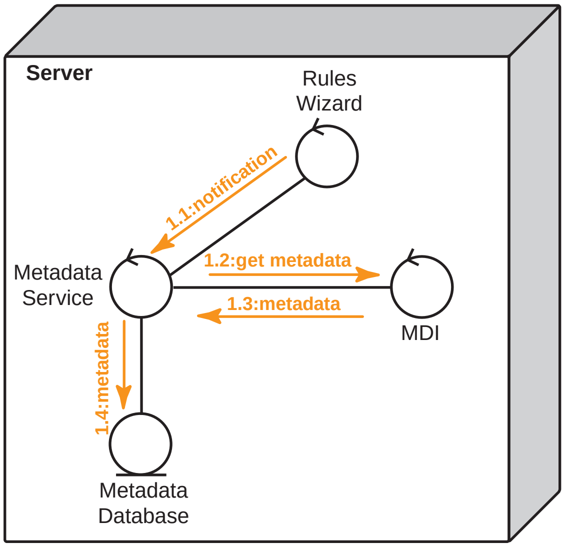
Transfer SmartBin Ingest



2. Transfer service initiates proxy creation. The transfer service pulls the media from the SmartBin cache via FTP and from it creates mpeg, thumbnail, storyboard, and RealVideo proxy, which is stored on the NAS. The transfer service then notifies the Resolver, which associates the proxy and hi-res material. The transfer service also notifies the Metadata Interaction.

1. Ingested hi-res material present. The External Ingest Application Interaction sends a notification and streams (GXF) the newly ingested hi-res material to the SmartBin service. The SmartBin service caches the GXF stream and then notifies the transfer service and sends the hi-res material to the hi-res storage and a database record to the News database. The News database notifies the News MDI of the new hi-res material.

Metadata

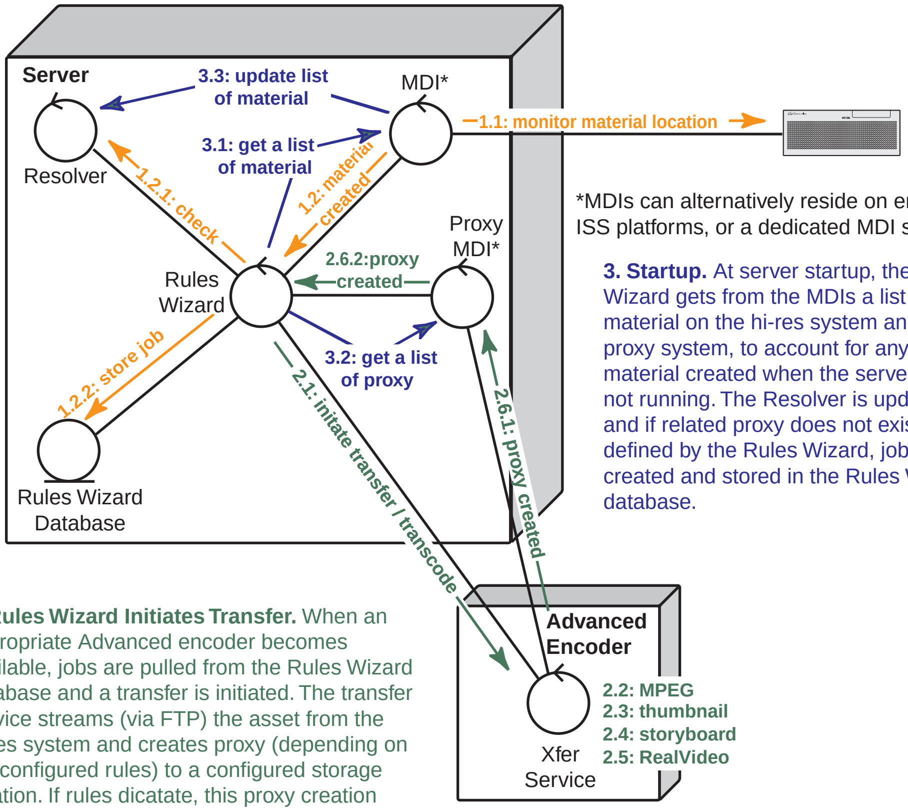


1. Metadata. When the Rules Wizard or transfer service initiates the creation or modification of proxy, it notifies the Metadata Service. The Metadata Service gets the new or modified metadata from the MDI that has knowledge of the associated hi-res material and puts it in the metadata database.

Scavenge

1. Material Created. The MDI monitors the high-res system (K2 system or News DSM). When hi-res material creation is detected the MDI notifies the Rules Wizard. If rules apply to the high-res material location, the Rules Wizard checks to see if the material already has proxy associated with it. If not, a job is created and stored in the database.

The Proxy MDI can also trigger this interaction by notifying the Rules Wizard of proxy MPEG creation.

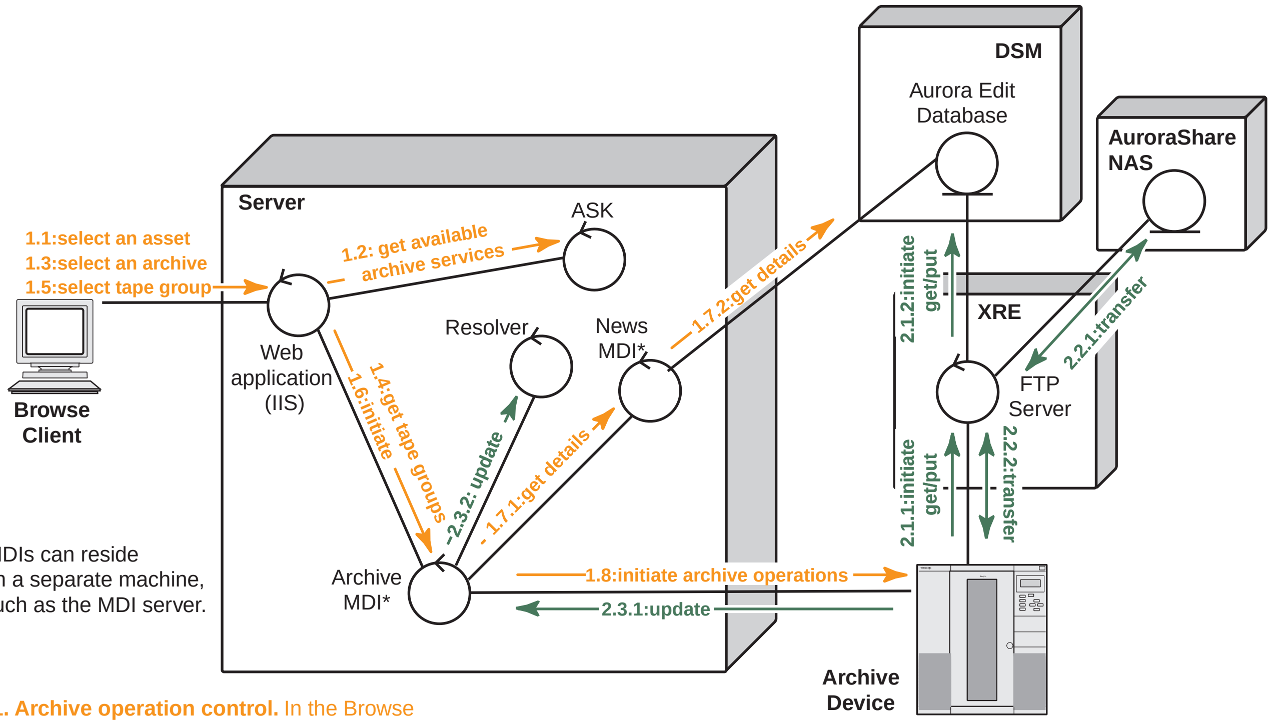


*MDIs can alternatively reside on encoders, ISS platforms, or a dedicated MDI server.

3. Startup. At server startup, the Rules Wizard gets from the MDIs a list of the material on the hi-res system and on the proxy system, to account for any material created when the server was not running. The Resolver is updated and if related proxy does not exist as defined by the Rules Wizard, jobs are created and stored in the Rules Wizard database.

2. Rules Wizard Initiates Transfer. When an appropriate Advanced encoder becomes available, jobs are pulled from the Rules Wizard database and a transfer is initiated. The transfer service streams (via FTP) the asset from the hi-res system and creates proxy (depending on the configured rules) to a configured storage location. If rules dicatate, this proxy creation occurs while the high-res material is still recording. Then the transfer service communicates to the Resolver to associate the proxy and hi-res material. Once the proxy is created the transfer service notifies the Proxy MDI.

Archive operations on Aurora system



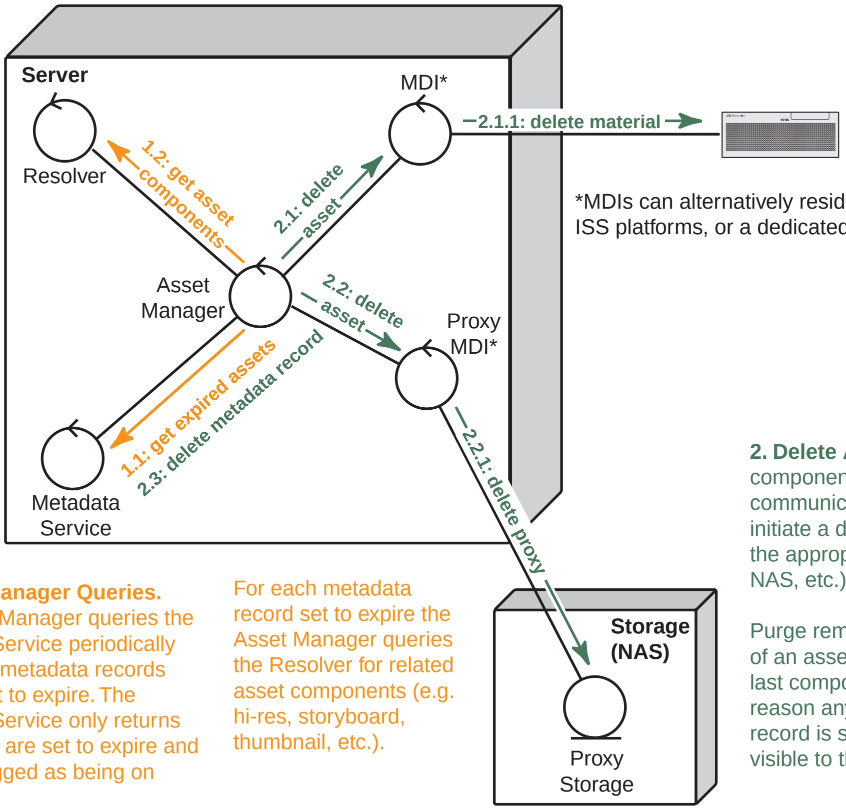
*MDIs can reside on a separate machine, such as the MDI server.

1. Archive operation control. In the Browse application, the user selects an asset, navigates to the management tab, and selects the archive option. The system queries the ASK for available archive devices. (Also filters out for hi-res material that already exists in archive by querying the Resolver). The user then chooses an available archive. The system queries the archive MDI to obtain a list of available tape groups. The user then selects the target tape group and initiates the archive operation. IIS accepts the request and submits a transfer job to the Archive MDI. The Archive MDI gets details about the affected material from the News MDI. The Archive MDI intiates the archive operation on the archive device.

2. Transfer material. The archive device initiates the transfer of material to/from the News system. Once the transfer is complete, the Archive MDI updates the Resolver to link the newly transfered hi-res material to the existing metadata record in the system. The MDI optionally initiates the removal of the online hi-res material from the Aurora system if the option to do so was initially selected.

During the archiving process the system displays the archive status which is retrieved from the Archive MDI.

Purge



*MDIs can alternatively reside on encoders, ISS platforms, or a dedicated MDI server.

1. Asset Manager Queries. The Asset Manager queries the Metadata Service periodically for a list of metadata records that are set to expire. The Metadata Service only returns assets that are set to expire and are not flagged as being on hold.

For each metadata record set to expire the Asset Manager queries the Resolver for related asset components (e.g. hi-res, storyboard, thumbnail, etc.).

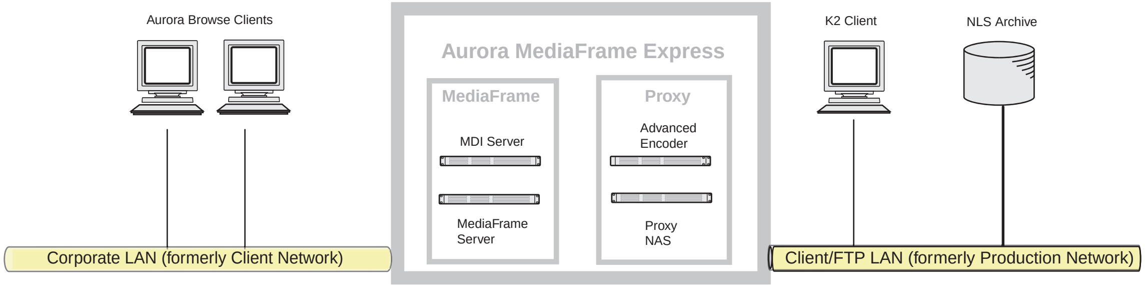
2. Delete Asset. For each asset component the Asset Manager communicates the appropriate MDI to initiate a delete. The MDI communicates to the appropriate hi-res system (K2, Media NAS, etc.) to complete the delete.

Purge removes all associated components of an asset. The metadata record is the last component deleted, so that if for any reason any component fails to delete, its record is still intact and the component is visible to the Browse application.

Appendix **B**

K2 BaseCamp Express

The K2 BaseCamp Express is a single dual-quad core Dell 2950 server with MediaFrame system components including a low-res NAS storage, an internal RAID, the MediaFrame database, and MDIs such as Generic FTP and K2.


Aurora Browse Clients
Aurora MediaFrame Express
MediaFrame
MDI Server
MediaFrame Server
Proxy
Advanced Encoder
Proxy NAS
K2 Client
NLS Archive
Corporate LAN (formerly Client Network)
Client/FTP LAN (formerly Production Network)

The BaseCamp Express does not scavenge assets; proxy is created on demand. It can utilize multiple encode streams. The speed of the encoder will be “throttleable,” that is, it can be slowed to less than real time. However, the encoder maintains one real-time encode of 100mb/s 1080i MPEG.

NOTE: Multiple encoder streams may affect encoder performance.

Configuring K2 BaseCamp Express

The K2 BaseCamp Express comes from the factory with the Aurora system components already installed. You need to configure the network settings as described in “Set up IP addresses and name resolution” on page 37.

Upgrading the K2 BaseCamp Express

You can add additional encoders to the BaseCamp Express. For more information, see your Grass Valley support representative.

Using K2 BaseCamp Express

You can access the BaseCamp Express using the Aurora Browse application on client PCs exactly as you would access the MediaFrame server, to search for or archive assets. Up to 25 users can access a BaseCamp Express server at one time. For more information, see the *Aurora Browse User Guide*.

Appendix **C**

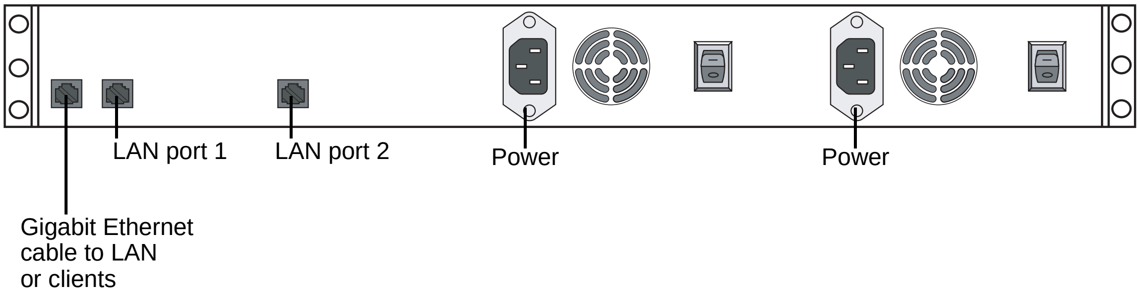
Legacy systems

This appendix documents system architectures, hardware platforms, and software components that are no longer recommended for new systems, but that are retained in existing systems and supported by current software releases.

NAS instructions - Fastora

The Network Attached Storage (NAS) unit provides storage for MPEG-1 proxy video, storyboards, and thumbnails. It may also be configured to store Edit Decision Lists (EDL) that are saved to the system. Encoders are configured to write to specific locations on the NAS via 100Tx connections over the network. Client access is provided via Gigabit Ethernet uplink to the Client Network.

Aurora Browse Proxy NAS (Fastora 104)



Cable as illustrated and as follows:

- For systems with one unified Production network, connect LAN port 1 to the Production network.
- For systems with a Production network consisting of a media network and a control network, connect LAN port 1 to the media network and LAN port 2 to the control network.
- Connect Gigabit port 1 to the Client network.
- Connect both power cables from the back of the NAS to a power supply.

Power supply units are hot-swappable. Once power is applied using switches on the rear panel, use the power switch on the front panel to power down. Failure to use the front switch will cause the disk array to rebuild on the next power up.

Prepare NAS - Windows Fastora

For the Linux version, refer to "Prepare NAS - Linux Fastora" on page 134.

NOTE: Procure IP addresses from the local network administrator prior to configuring the NAS unit.

When you configure the Windows Fastora NAS for the Aurora Browse networks, you can make network settings in the following ways:

- **Use Windows Remote Desktop Connection**, as explained in step 4 of the following procedure, and then use standard Windows procedures to make all settings. If you do this, read the subsequent steps in the procedure to identify the required settings.
- **Use the Fastora configuration pages** (Web based), as documented in the following procedure, and make settings as instructed.

NOTE: If you plan to change the name of the NAS unit and you intend to use the underscore character, such as in root_nb_nas_n, you must do so using standard Windows procedures via the remote desktop. The Fastora configuration page does not allow the underscore character.

To configure the Windows Fastora NAS for the Aurora Browse networks, do the following:

1. From any Production network machine, enable the network to recognize the NAS by adding an IP address within the subnet range of 192.168.50.0.
2. For the first NAS machine (*nb-nas-1)*, open the NAS configuration software in Internet Explorer by entering the following in the browser address bar:

   https://192.168.50.31:8098

NOTE: Notice the s in the https: address. Also, make sure your browser allows cookies and JavaScript (or JIT).

   Subsequent NAS machines (*nb-nas-2*, *nb-nas-3*) have IP addresses incremented accordingly (192.168.50.32, 192.168.50.33).

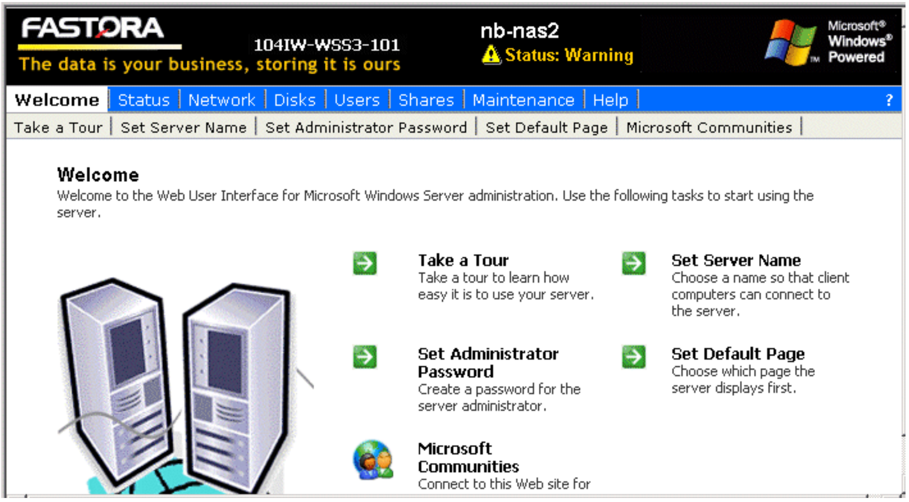
   If you received your NAS unit directly from Fastora, the default Fastora IP address is 192.168.1.11.

3. Log on as follows:

   Username: `administrator`

   Password: `triton`

   The Fastora Welcome page opens.


FASTORA
The data is your business, storing it is ours
104IW-WSS3-101
nb-nas2
Status: Warning
Microsoft® Windows® Powered
Welcome | Status | Network | Disks | Users | Shares | Maintenance | Help | ?
Take a Tour | Set Server Name | Set Administrator Password | Set Default Page | Microsoft Communities |

Welcome

Welcome to the Web User Interface for Microsoft Windows Server administration. Use the following tasks to start using the server.

Take a Tour Take a tour to learn how easy it is to use your server.

Set Server Name Choose a name so that client computers can connect to the server.

Set Administrator Password Create a password for the server administrator.

Set Default Page Choose which page the server displays first.

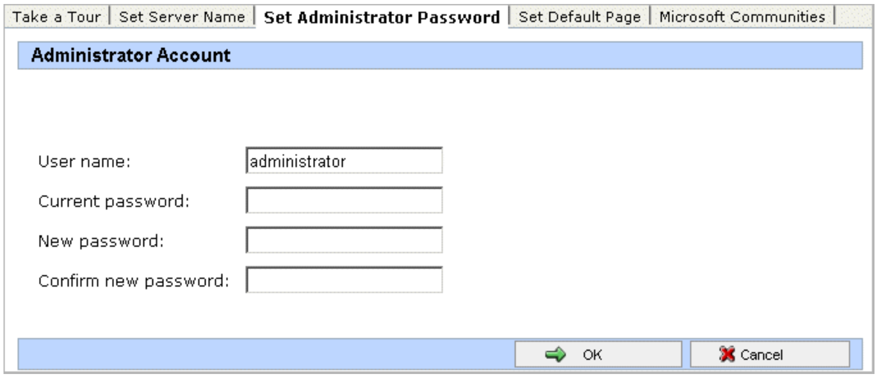
Microsoft Communities Connect to this Web site for

4. Do one of the following:
   - To use the remote Windows desktop rather than the Fastora configuration pages, click **Maintenance | Remote Desktop**. This feature prompts you to again log on to the NAS unit, and then allows you to access the Windows desktop. Make settings with standard Windows procedures.
   - To use the Fastora configuration pages, continue with this procedure.
5. Click **Set Server Name** and, if necessary, change the name, DNS suffix, and Domain/Workgroup setting. Work with IT at the customer site to add the NAS to a Domain.

   If you make a change, click **OK**.

NOTE: After making changes on a configuration page, you must click OK or else your changes are lost.

6. Click **Set Administrator Password**.


Take a Tour | Set Server Name | Set Administrator Password | Set Default Page | Microsoft Communities |
OK
Cancel

Administrator Account

User name: administrator
Current password:
New password:
Confirm new password:

Set a password according to the customer site requirements. Click **OK** to save settings.

7. Click **Network | Interfaces**. If required by the customer site network, change IP, DNS, and WINS settings. A recommended configuration is to use the Gigabit port for the Client network, use LAN Port 1 for the Production network and leave LAN Port 2 at the default static IP for system maintenance access. For systems with a Production network consisting of a media network and a control network, use LAN port 1 for the media network and LAN port 2 to for the control network.

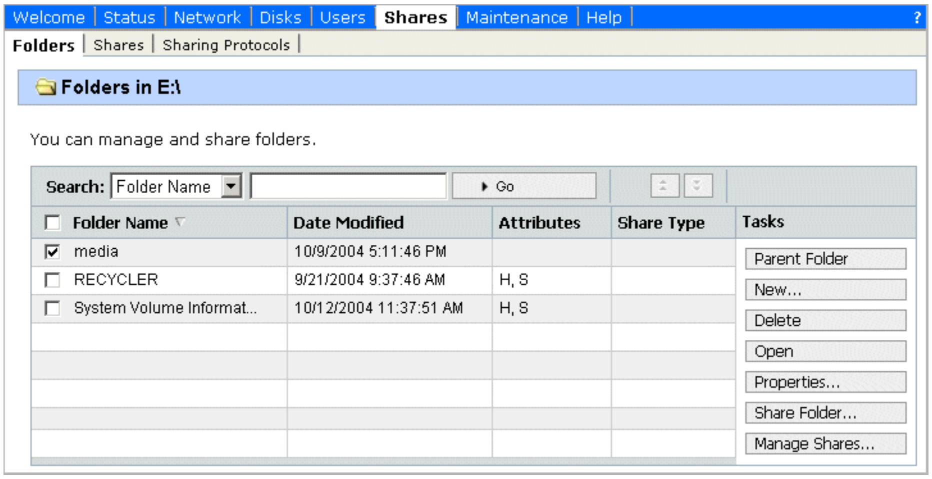
8. Click **Administration Web Site**. If required by the customer site security policies, change the IP addresses and/or ports for encrypted and non-encrypted access used to access the administration Web site. If you make a change, click **OK** and then reconnect via the new port and/or IP address.

9. Click **Shares | Folders**. Share the media directory as follows:

   a. Select **New Volume (E:)**

   b. Click **Manage Folders**.

   c. Select **media**.



You can manage and share folders.

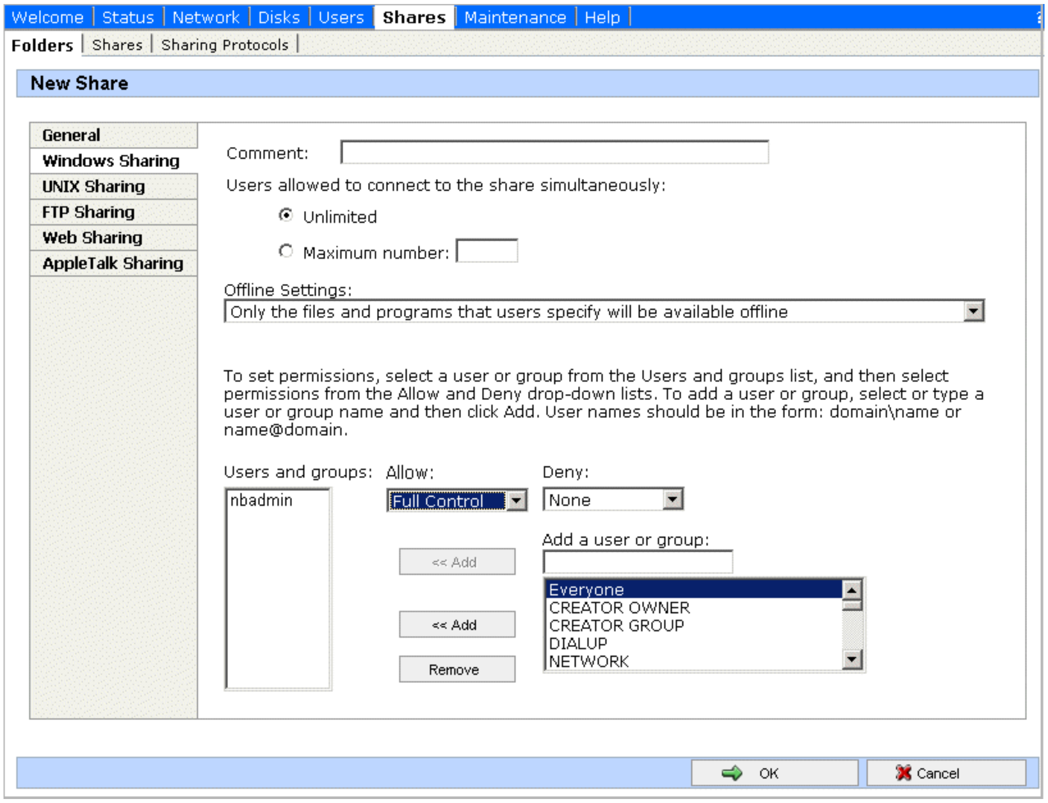
	Folder Name	Date Modified	Attributes	Share Type
☑	media	10/9/2004 5:11:46 PM		
☐	RECYCLER	9/21/2004 9:37:46 AM	H, S	
☐	System Volume Informat...	10/12/2004 11:37:51 AM	H, S	

   d. Click **Share Folder**.

   e. Enter the following:

   Share name: `media`

   f. Click **Windows Sharing**. After a pause, the Windows Sharing tab opens.


Welcome | Status | Network | Disks | Users | Shares | Maintenance | Help
Folders | Shares | Sharing Protocols
General
Windows Sharing
UNIX Sharing
FTP Sharing
Web Sharing
AppleTalk Sharing
<< Add
<< Add
Remove
OK
Cancel

New Share

Comment:

Users allowed to connect to the share simultaneously:

● Unlimited

○ Maximum number:

Offline Settings: Only the files and programs that users specify will be available offline

To set permissions, select a user or group from the Users and groups list, and then select permissions from the Allow and Deny drop-down lists. To add a user or group, select or type a user or group name and then click Add. User names should be in the form: domain\name or name@domain.

Users and groups: nbadmin

Allow: Full Control

Deny: None

Add a user or group:

Everyone
CREATOR OWNER
CREATOR GROUP
DIALUP
NETWORK

g. User privileges for the media folder should be as follows:

Everyone — Read only access

nbadmin — Full Control

h. Click **OK**.

10. Close the NAS configuration pages.

Verify NAS access

Verify Proxy NAS access from production network machines, which are machines of the following types:

- MediaFrame server
- Aurora Proxy Encoder
- SmartBin encoder

To verify access, from each production network machine do the following:

1. Open Windows Explorer and navigate to the media directory on the NAS. You can do this with the following path:

   \\root-nb-nas-1\Media

2. Verify basic read/write capabilities by creating, modifying, and deleting a simple text file.

To verify access from client network machines, choose a machine on the Client network that can represent a Aurora Browse client PC and that is convenient for testing. From this machine do the following:

1. Open Windows Explorer and navigate to the media directory on the NAS. You can do this with the following path:

   \\root-nb-nas-1\Media

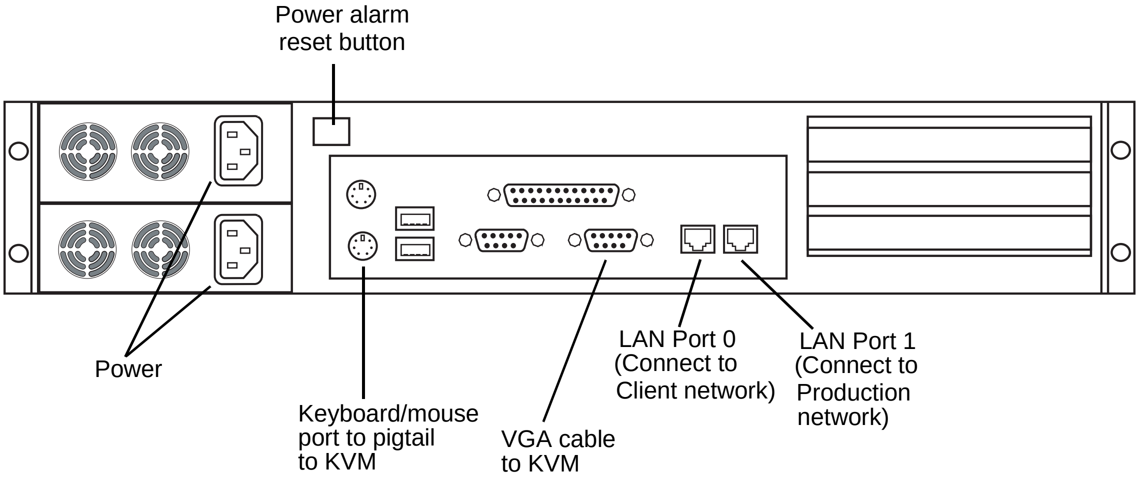
Verify that Aurora Browse client PCs will have read only rights.

NAS instructions - Serial ATA network platform

For the Network Attached Storage (NAS) unit you have the option of the Serial ATA network (a.k.a. Ciprico 1700 or DiMedia) platform.

Platform Specifications are as follows:

- Redundant Power Supplies.
- 100BT LAN (x2)
- RAID protected drives


Power alarm reset button
Power
Keyboard/mouse port to pigtail to KVM
VGA cable to KVM
LAN Port 0 (Connect to Client network)
LAN Port 1 (Connect to Production network)

Make cable connections as illustrated.

Power supply units are hot-swappable. If the power supply fails or when power is cycled, an alarm will sound. To disable the alarm, press the power alarm reset button to the In position.

Power up the appliance by pressing the small, round On/Standby switch on the front left of the machine. Once the electrical cables are connected, the system has electrical power. Turning the On/Standby switch to standby does not remove power. To remove power, hold down the On/Standby switch for at least five seconds or disconnect the electrical cables.

Prepare Profile Media Servers

On each Profile Media Server that is to interact with the system, check the following configurations and modify settings as necessary.

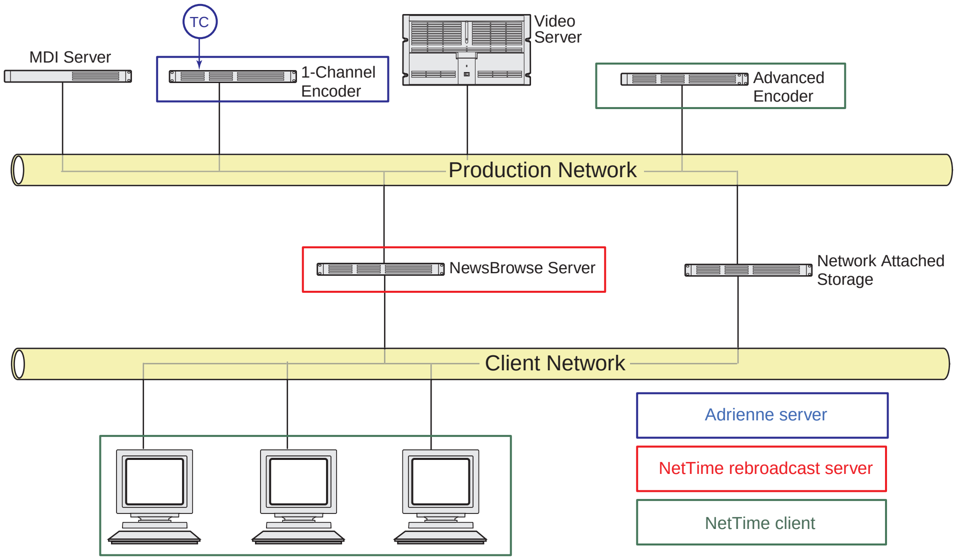
1. Set up as a NetTime client. Refer to preceding procedures.
2. Click **Start | Run**, enter *regedit* and press **Enter**. The Registry Editor opens.
3. In the Registry Editor open the following key:

   HKEY_LOCAL_MACHINE/SOFTWARE/Tektronix/Profile/ShuttleAtMode

   Set the key to **TRUE**.
4. On the Profile XP, start **PortServer**.
5. Add a shortcut to PortServer to the startup folder. This ensures that PortServer always runs on the Profile XP, as it is required for Aurora Browse operation.
6. Verify that the following account has been added to the Profile system:
   - username: nbadmin
   - password: (contact Grass Valley Support for password)

NetTime system

The following diagram illustrates the NetTime system. This system is required for the Profile XP/Open SAN environment.



For the K2 storage environment there is not an exacting requirement for clock synchronization, but you can use NetTime to keep logging entry times in sync on Production Network machines. Client machines do not need NetTime.

Prepare NetTime

This section provides instructions for NetTime on the Profile XP/Open SAN system. On the K2 storage Browse system, the requirement for clock synchronization is only to keep log entries matching on production network machines. On the K2 storage Browse system, you do not need to install NetTime on Aurora Browse clients.

NetTime keeps the system clocks on Aurora Browse machines in sync. Since the Profile Media Servers and single-channel encoders use the house timecode feeds, the other machines need to be kept in sync as well. On systems that control ingest and have single-channel encoders, the primary purpose of NetTime is to keep the Ingest Scheduler, which runs on the MediaFrame server, and the Aurora Browse client machines synchronized to house time. On systems that do not control ingest, NetTime is still useful to keep clocks synchronized so that system logs can be correlated.

The following procedure uses a single-channel encoder as the Adrienne Absolute Time Server. If your system does not control ingest and has no single-channel encoders, you can use any machine as the Adrienne Absolute Time Server.

The single-channel encoder runs the Adrienne Absolute Time Server. NetTime clients on the production network reference the Adrienne Absolute Time Server. A NetTime server runs on the MediaFrame server, which rebroadcasts the time to the client network. NetTime clients on the client network reference the NetTime server.

Set up NetTime with the following procedures:

- "Prepare NetTime servers" on page 130
- "Prepare NetTime clients" on page 130

Prepare NetTime servers

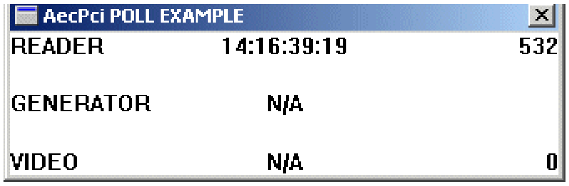
You use one single-channel encoder as the primary Adrienne Absolute Time Server, and another single-channel encoder as the secondary (redundant) Adrienne Absolute Time Server. A LTC connection to house timecode is required for single-channel encoders functioning as Adrienne Absolute Time Servers.

NOTE: Make sure that the Thomson Ingest Control service is off before starting this procedure. If the service is on and you run AecPciPoll.exe, the single-channel encoder locks up.

To prepare a single-channel encoder as a Adrienne Absolute Time Server, do the following:

1. On the single-channel encoder, run the following:

   C:\AecPciPoll.exe

   ```
   READER        14:16:39:19      532

   GENERATOR        N/A

   VIDEO            N/A             0
   ```

   This verifies that the Adrienne card is properly installed and the house timecode is valid.

2. Run *C:\Load Service.bat* and in Task Manager, verify that *NtPciClk.exe* is running.
3. Restart the encoder and verify that *NtPCiClk.exe* restarted automatically.
4. Open *C:\ATCS10.exe* and click **Yes** to install.
5. Restart the encoder and verify that the Absolute Time Server icon appears in the system tray.
6. The encoder is now functioning as the primary Adrienne Absolute Time Server. Repeat this procedure on a second single-channel encoder, to make it the secondary Adrienne Absolute Time Server.

Prepare NetTime clients

You can also optionally prepare encoders and other Aurora Browse machines as NetTime clients, in case you want to use them to run the Aurora Browse application for test purposes or to keep the PC clock in sync with the rest of the system for the log files.

Some clients need special configuration to ensure time synchronization throughout the system. Since your single-channel encoder Adrienne Absolute Time Server is on the Production Network, only NetTime clients on the Production Network have access. You must provide access for the external (Client Network) NetTime clients as well. To do this, you configure a NetTime client machine (in this case, the MediaFrame server) which has access to both Production and Client Networks to rebroadcast the time sync to external networks. NetTime clients on external networks can then look to the MediaFrame server as their NetTime server.

To prepare a NetTime client, do the following:

1. Open the following folder:

   C:\Time Sync Software\Client

2. Open *NetTime-2b6.exe* and click **Yes** to install. Choose the defaults, including **configure as service**.

3. Set Net Time options as follows:

   a. Enter the host name for the primary and secondary server according to the following table:

NetTime Client	Primary Server	Secondary Server
A Production Network Client	First Encoder	Second Encoder
MediaFrame server	First Encoder	Second Encoder
External (Client Network) Client	MediaFrame server	—

   b. Select the **RFC868(TCP)** protocol for both servers

   c. For the MediaFrame server, select **Allow other computers to sync to this computer**.

   d. Leave other fields at the defaults and click **Okay**.

4. The PC clock should automatically update to match the server. If not, check network connectivity and review install steps. All machines must be set for the same time zone to function properly.

Prepare NAS - Serial ATA network platform

To configure the Serial ATA network (a.k.a. Ciprico 1700 or DiMedia) NAS for the Aurora Browse networks, check the following configurations and modify settings as necessary.

NOTE: Procure IP addresses from the local network administrator prior to configuring the NAS unit. Access to configuration pages is dependent upon valid IP addresses.

1. From any Production network machine, enable the network to recognize the NAS by adding an IP address within the subnet range of 192.168.50.0.

2. For the first NAS machine (*nb-nas-1)*, open the NAS configuration software in Internet Explorer by entering the following in the browser address bar:

   https://192.168.50.31:9890

NOTE: Notice the s in the https: address. Also, make sure your browser allows cookies and JavaScript (or JIT).

Subsequent NAS machines (*nb-nas-2, nb-nas-3*) have IP addresses incremented accordingly (192.168.50.32, 192.168.50.33)

The NAS Administration Tool window opens at the Welcome page.

3. Enter the password. The default password is *triton*. The Status page opens.
4. In the tree view click **Network | Network Ports**. The Configure Network Ports page opens.
5. Configure network ports as follows:

   a. **Port 0 Client Network -** Set the IP address and subnet mask for the Client network as specified by the local network administrator.

NOTE: The DiMeda NAS requires a static IP address for the client port. Set this up with the local network administrator.

   b. **Port 1 Production Network -** Set the IP address for the production network as specified by the local network administrator, then set the subnet mask to 255.255.255.0.

NOTE: For detailed information about configuration options, click the Help icon (?) in the upper right corner of each window.

   c. Click **Save**, then select the **Restart** option to restart. Reboot takes 2-10 minutes. Do not power-down the enclosure during reboot.

6. After the NAS reboots, access the NAS configuration software as described earlier in step 2 and step 3, except this time, enter the following in the browser address bar:

   https://<*Client IP Address*>:9890

   The Status page appears.

7. In the Status page tree view, click **Network | Names/IPs**. The Names and IPs page opens.
8. Set the following:
   - **Domain name -** Enter the Client network Domain name.
   - **Gateway -** Enter the IP address for the Client network gateway. Consult the network administrator.
   - **Node Name -** For example: (*root*-nb-nas-*n*)
9. In the tree view click **System | System Administration | Date/Time**. The Date/Time page opens.
10. Select the correct time zone, date, and time.
11. Click **Save**, then select the **Restart** option to restart.

    Reboot takes 2-10 minutes. Do not power-down the enclosure during reboot.

12. After the NAS reboots, access the NAS configuration software again as described

in step 6. The Status page appears.

13. In the Status page tree view, click **Storage | Shares | Create** and then click the **Next** button. The CIFS Share page opens.
14. Specify CIFS options as follows:
    a. Enter *Media* as the share name.
    b. Set user privileges. Select all of the following options:
    - Writeable
    - Public
    - Browseable
    - Available

    (Do not select Case Sensitive)

    c. Click **Save**.
15. Close the NAS Administration Tool.

Prepare NAS - Linux Fastora

On Linux Fastora NAS devices, check the following configurations and modify settings as necessary.

1. Using Internet Explorer, browse to the NAS machine. For example:

   http://*root*-nb-nas-*n*

2. Login as administrator. The password is *triton*.
3. Navigate in left pane to **Server Configuration | Basic Configuration**.
4. Under the general tab set the following:
   - Server Name
   - Domain name (for client network)
   - DNS server (from customer IT dept.).
5. Under LAN Port 1 tab, do the following:
   - Select manual configuration
   - Set the IP address
   - Subnet mask is 255.255.255.0
6. Leave LAN Port 2 unchanged (disconnected)
7. Under LAN Port 3 tab, select **Get network configuration through DHCP**
8. At **Server Configuration | Date Setup**, set the date and time.
9. Click **Security Setup | Shared Folder Setup**. Select the **Windows/Apple/Novell privileges** tab. User privileges for the media folder should be as follows:
   - everyone - RO
   - nbadmin - RW
10. Click **Network Setup | Windows Network**. Check **Enable Windows Networking**.
11. Enter the following:
    - customer Domain
    - account and password (customer IT dept. will need to provide this)
    - enter the WINS server

Host table files

Find host table files at *C:\WINNT\system32\drivers\etc*

Devices share a common host table, which lists out the Production Network IP settings. For security purposes, the IP addresses should be non-routable (e.g. 192.168.xxx.xxx) and be part of the same subnets used by the Profile/Open SAN systems. The customer may request a particular subnet (routable or not) depending on the needs of the facility. The only client side IP address needed in the host table is for the client switch itself, which is useful for accessing the web management page from the Aurora Browse devices.

The following is an example of host table entries. Not shown are entries for Profile systems, UIMs, and other machines on the network. Refer to the documentation for these other machines for host table requirements.

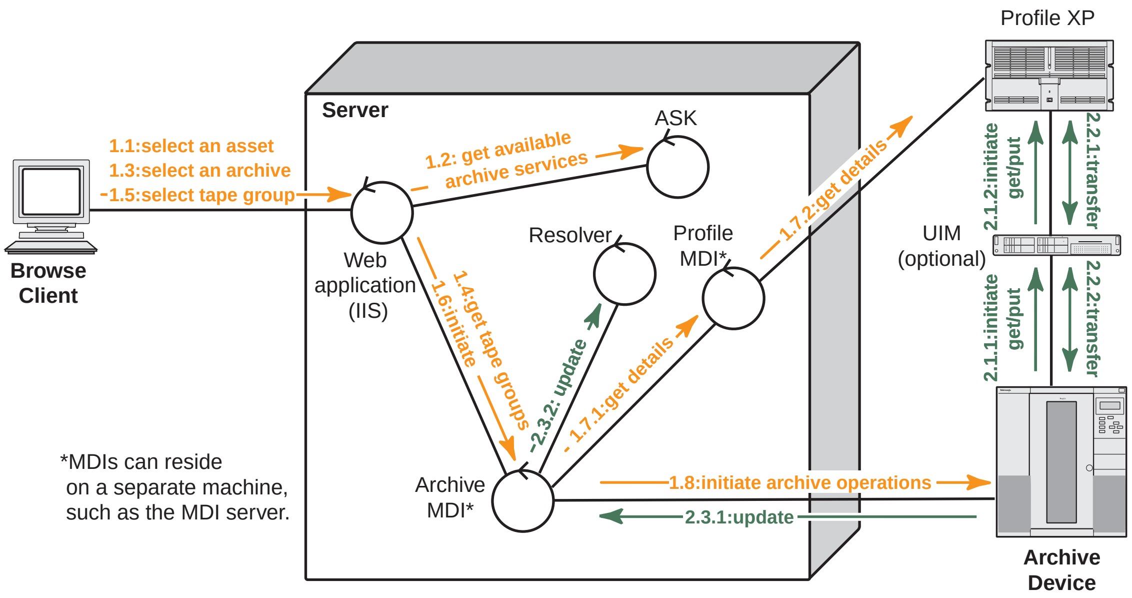
```
#--------------------------------------------------------
#General Host Table
#--------------------------------------------------------

#MediaFrame server

192.168.30.21     iron-nb-svr


#Browse MDI server

192.168.30.101    iron-nb-mdi


#Browse NAS

192.168.30.71     iron-nb-nas-1
192.168.30.72     iron-nb-nas-2


#Browse Advanced encoders

192.168.30.50     iron-nb-adv-1
192.168.30.51     iron-nb-adv-2


#Browse single-channel encoders

192.168.30.26     nb-enc-1          #Open SAN Profile mpvs-1 vtr 01
192.168.30.27     nb-enc-2          #Open SAN Profile mpvs-1 vtr 02
192.168.30.28     nb-enc-3          #Open SAN Profile mpvs-1 vtr 03
192.168.30.29     nb-enc-4          #Open SAN Profile mpvs-1 vtr 04


#NB Router Gateway

192.168.30.111    iron-nb-rtr

#The following Client LAN entries are included in this host table for
#reference only. Machines on client network use DNS lookup only.

#Browse live monitor encoder

10.16.37.91       iron-nb-live-1            #Client LAN
```

```
10.16.37.92       iron-nb-live-2            #Client LAN

#Browse Ethernet Switch

10.16.37.20       iron-nb-2950-client-1     #Client LAN
192.168.30.200    iron-nb-2950-prod-1
```

Host table tips:

- If you are exporting EDLs to Aurora Edit, the Aurora Edit workstation must be able to resolve the Profile MDI name (present in the EDL) to the IP address of the Profile XP system to which the MDI connects. The recommended solution is to map the MDI name to the Profile IP address in the Aurora Edit workstation's host table. Refer to "MDI and Encoder logical names convention" on page 33.
- The NAS and MediaFrame server IP address need to be resolved using the Client side IP address via DNS lookup, not the host table.
- If the server has a canonical name, the host table for any machine that runs MDIs that are subscribed to by the server must match case for the entire canonical name. E.g., if the server's canonical name is "NB-SERVER1.mycorp.net", then the host table entry in the MDI server(s) must match; if the entry is "NB-SERVER1.MYCORP.NET", then it will not work. Pinging will not show the problem. The problem doesn't show up until the MDIs attempt to notify the server.

Archive operations on Profile XP



*MDIs can reside
on a separate machine,
such as the MDI server.

1. Archive operation control. In the Browse application, the user selects an asset, navigates to the management tab, and selects the archive option. The system queries the ASK for available archive devices. (Also filters out for hi-res material that already exists in archive by querying the Resolver). The user then chooses an available archive. The system queries the archive MDI to obtain a list of available tape groups. The user then selects the target tape group and initiates the archive operation. IIS accepts the request and submits a transfer job to the Archive MDI. The Archive MDI gets details about the affected material from the Profile MDI. The Archive MDI intiates the archive operation on the archive device.

2. Transfer material. The archive device initiates the transfer of material to/from the Profile XP. Once the transfer is complete, the Archive MDI updates the Resolver to link the newly transfered hi-res material to the existing metadata record in the system. The MDI optionally initiates the removal of the online hi-res material from the Profile XP if the option to do so was initially selected.

During the archiving process the system displays the archive status which is retrieved from the Archive MDI.

Index