Aurora Browse

MEDIA ASSET MANAGEMENT PLATFORM

Installation and Configuration Guide

SOFTWARE VERSION 6.3

071-8518-01
SEPTEMBER 2007

THOMSON
images & beyond

Revision Status

Rev Date	Description
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.

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
    - Aurora Transfer

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. Contact Grass Valley first regarding problems with third party software on Grass Valley products, such as the Microsoft® Windows® operating system, Windows Media® player, Internet Explorer® internet browser, and SQL Server™.

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 newsroom workflow — from ingest to editing to distribution to archive.

This chapter includes the following topics:

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 edit stories using the low-resolution proxy, which is accessible from the journalist's desktop. 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.

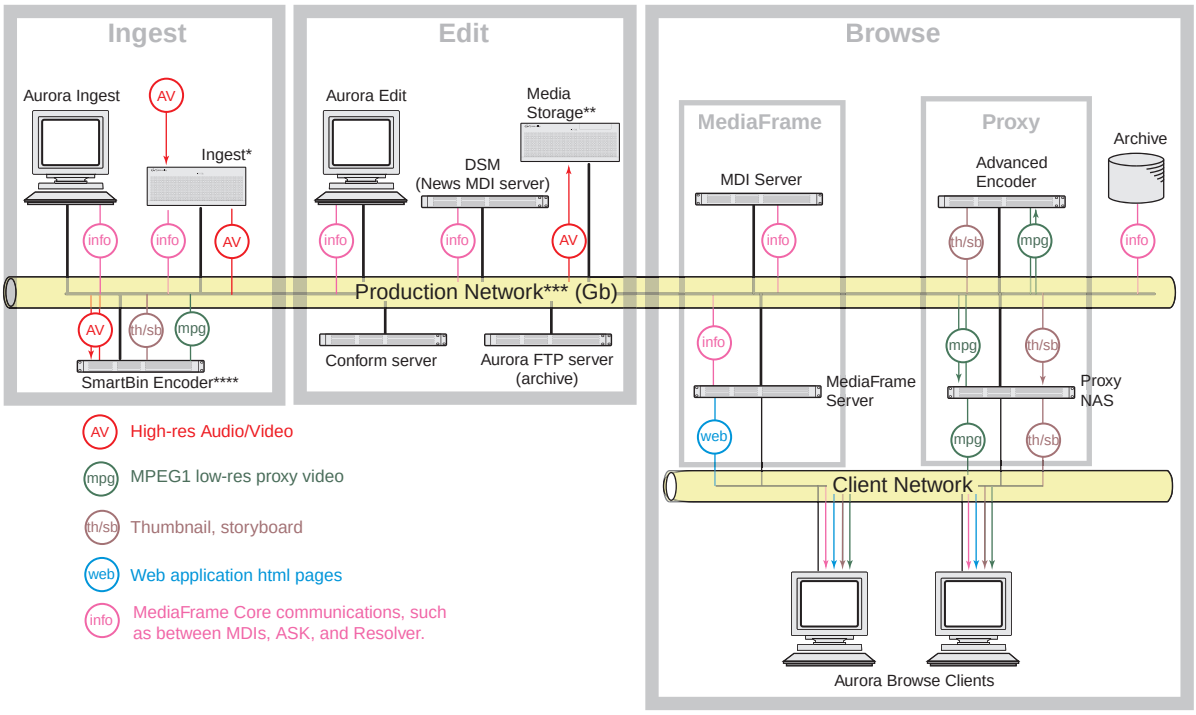
The system is compatible with the K2 storage architecture. Ingest is controlled by an ingest application, such as Aurora Ingest, and incorporates the K2 system as the video server. The SmartBin encoder transfers an incoming feed into two formats: a proxy low-resolution (MPEG-1) format stored on the proxy NAS, and a high-resolution format stored the K2 storage system. Aurora Browse also monitors the K2 storage to create proxy for new high-resolution material. In this way Aurora Edit clips are represented in the system for editing and manipulation. The EDL export feature creates a sequence directly in the Aurora Edit target bin.

For descriptions of the machines used as platforms for the system, refer to Chapter 2, *Installing Aurora Browse* on page 15.

For descriptions of software components, refer to Appendix A, *Component Interaction Diagrams* on page 127.

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 system or an M-Series system.

** The Media Storage is a K2 system.

*** On large systems the 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 considerations when establishing the workflow for your use of Aurora Browse:

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 B, *Legacy systems* on page 137. 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:

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: XRE-2 platform

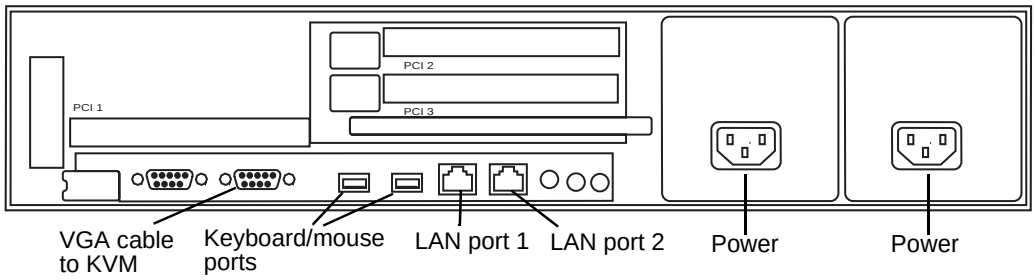
The central component of the system is the MediaFrame server. Depending on the design of your system, it can host the following software components:

- The Aurora Browse web-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 XRE-2 platform, as explained in this section, or the HAFT-2 platform, as explained in "MediaFrame server instructions: HAFT-2 platform" on page 18.

XRE-2 platform (Dell 2950)



Cable as illustrated and as follows:

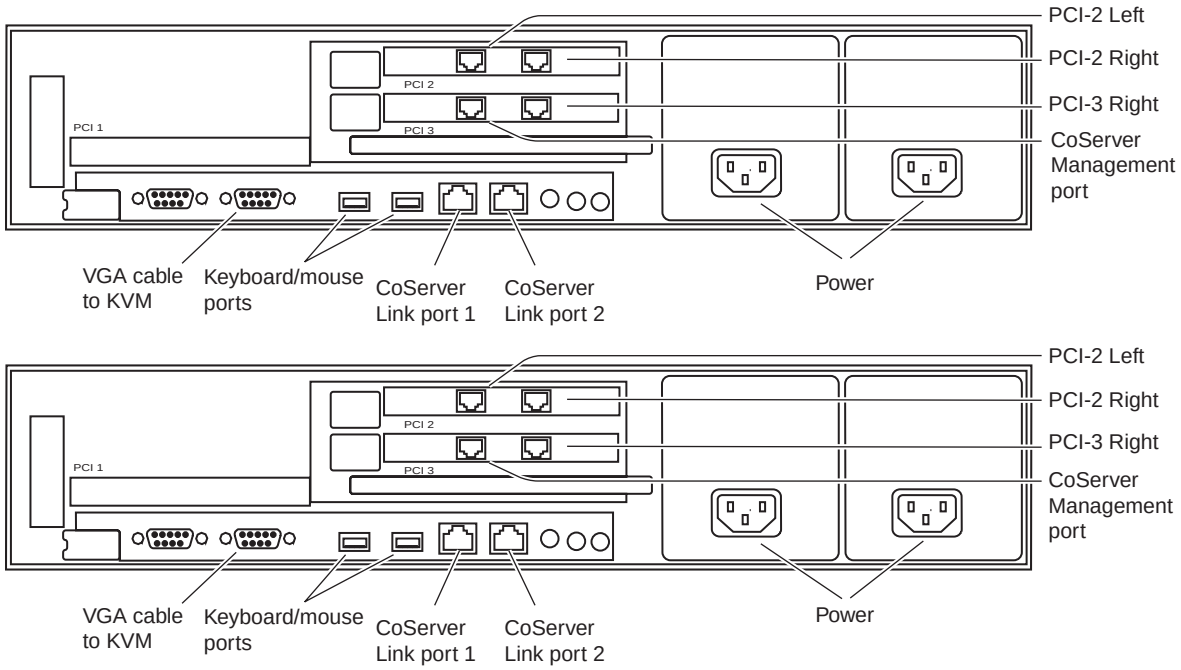
- For systems with one unified Production Network, connect port 1 to the Production Network.
- For systems with a Production Network consisting of a media network and a control network, connect port one to the control network.
- Connect port 2 to the Client Network.

MediaFrame server instructions: HAFT-2 platform

For the MediaFrame server you have the option of the High Availability, Fault Tolerant (HAFT) platform, also known as the Marathon platform. This platform is made up of two interconnected servers.

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

HAFT-2 platform (Dell 2950 servers)



Cable as illustrated and as follows:

- For systems with one unified Production Network, connect port PCI-3 Right and the CoServer Management port to the Production Network.
- For systems with a Production Network consisting of a media 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 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 HAFT 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 HAFT 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.

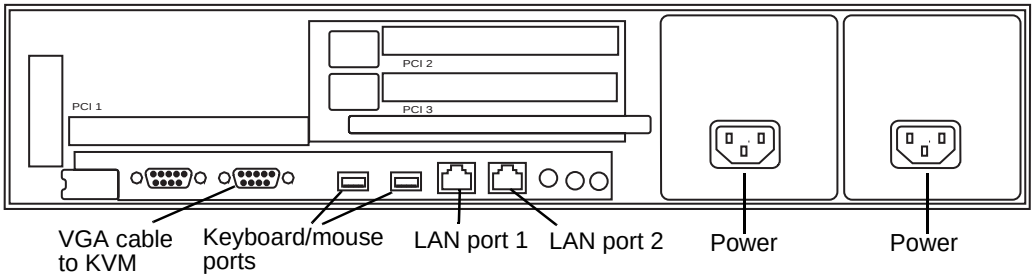
Also refer to "Configure HAFT platform" on page 40 for network configuration procedures.

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 XRE-2 platform. On systems without a MDI server, the MDI services can run on the MediaFrame server or other Aurora Browse machine.

XRE-2 platform (Dell 2950)



Cable as illustrated and as follows:

- For systems with one unified Production Network, connect port 1 to the Production Network.
- For systems with a Production Network consisting of a media network and a control network, connect port one to the control network.
- Connect port 2 to the Client Network.

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.

Advanced Encoder instructions

The following components are hosted by the Advanced encoder:

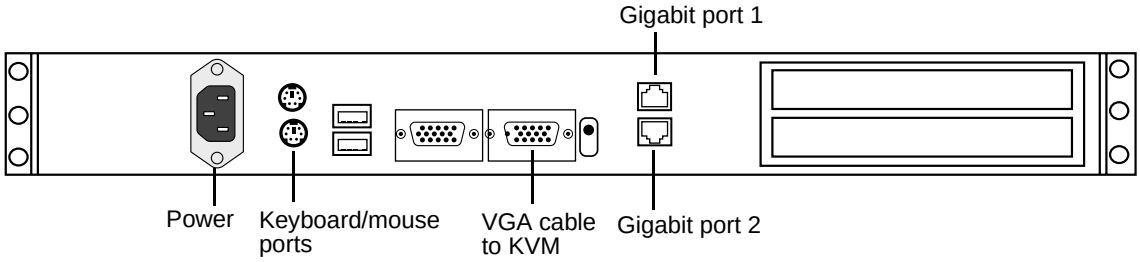
- Thomson Proxy Transfer service.
- Aurora FTP service.

The Advanced Encoder does the following:

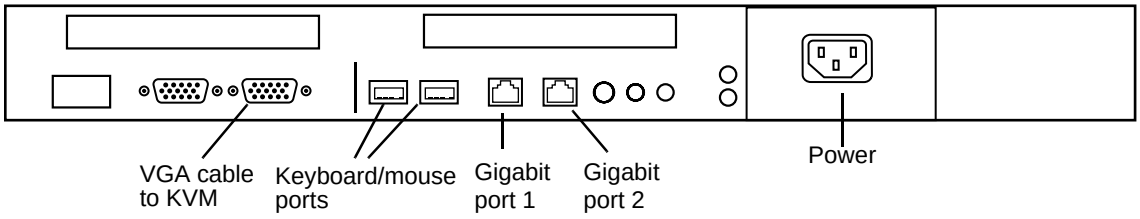
- Creates MPEG-1 proxy versions of high-resolution video assets that already exist or are actively being recorded on a video server
- Processes MPEG-1 proxy content
- Extracts dynamic scene detection images for storyboard/thumbnail creation

The Advanced Encoder processes entirely in the digital domain. The SD Advanced Encoder runs on the XRE-3 platform. The HD Advanced Encoder runs on the XRE-4 platform.

XRE-3 (Dell 860) platform



XRE-4 (Dell 1950) platform



Cable as illustrated and as follows:

- For systems with one unified Production Network, connect Gigabit port 1 to the Production network. Gigabit port 2 is unused.
- For systems with a Production Network consisting of a media network and a control network, connect Gigabit port 1 to the media network and Gigabit port 2 to the control network.

SmartBin Encoder instructions

The following components are hosted by the SmartBin encoder:

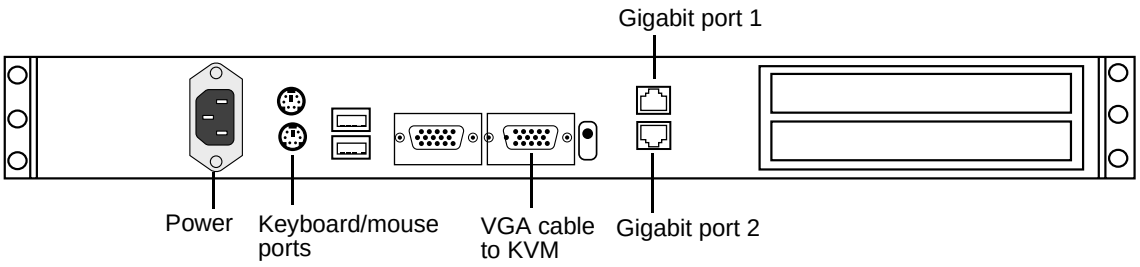
- Thomson SmartBin Proxy Transfer service. Refer to "About Aurora Browse software" on page 24.
- SmartBins Service and Aurora FTP service. Refer to "Other software installation considerations" on page 31.

The SmartBin encoder does the following:

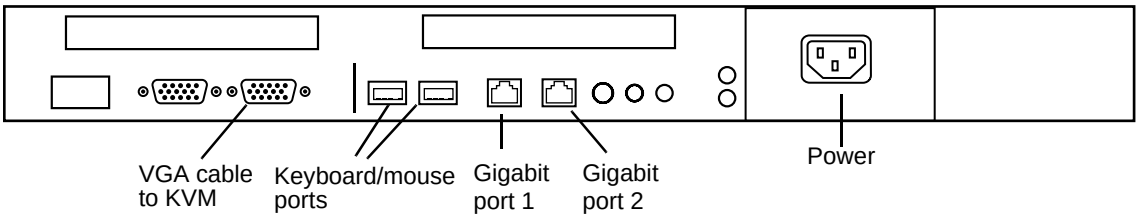
- Creates MPEG-1 proxy versions of high-resolution material
- Processes high-resolution material
- Extracts dynamic scene detection images for storyboard/thumbnail creation

The SmartBin encoder processes entirely in the digital domain. The SmartBin encoder runs on the XRE-3 platform. The HD SmartBin encoder runs on the XRE-4 platform.

XRE-3 (Dell 860) platform



XRE-4 (Dell 1950) platform



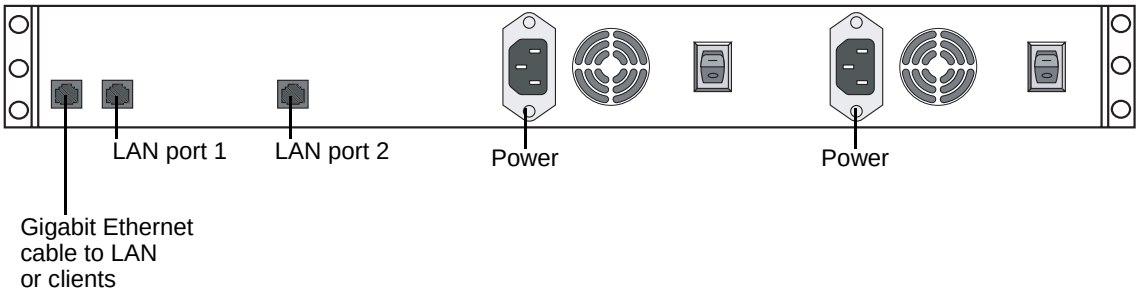
Cable as illustrated and as follows:

- For systems with one unified Production network, connect Gigabit port 1 to the Production network. Gigabit port 2 is unused.
- For systems with a Production network consisting of a media network and a control network, connect Gigabit port 1 to the media network and Gigabit port 2 to the control network.

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.

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 31.

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

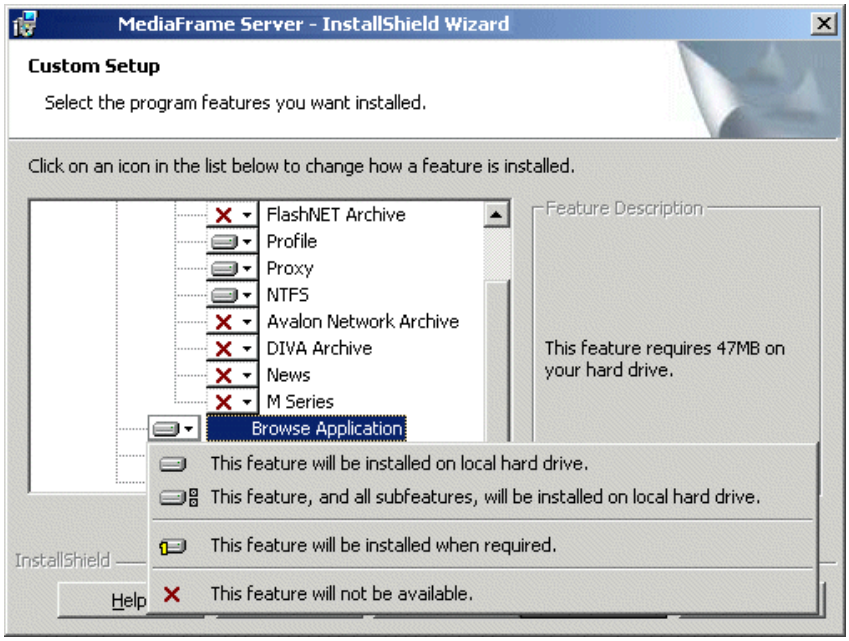
The following installation programs are on the Aurora Browse Application CD:

- *…\SingleChannelEncoder\Setup.exe* — Use this setup file to install Aurora Browse software on a single-channel encoder.
- *…\AdvancedEncoder\Setup.exe* — Use this setup file to install Aurora Browse software on an Advanced encoder.

- …*SmartBinEncoder**Setup.exe* — Use this setup file to install Aurora Browse software on a SmartBin 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	Router Gateway	DSM
Core Services	✓			
Managed Devices: FlashNet Archive		✓		
Profile		✓		
Proxy		✓		
NTFS	✓			
Avalon Network Archive		✓		
DIVArchive		✓		
News				✓
M-Series		✓		
K2		✓		
NLS		✓		
Aurora Browse Application	✓			
Ingest	✓			
Router Gateway			✓	

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:



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, on Advanced Encoders and SmartBin 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 SmartBins" on page 43
- "Prepare Advanced encoders" on page 43
- "Add encoders to the K2 Storage System" on page 43.

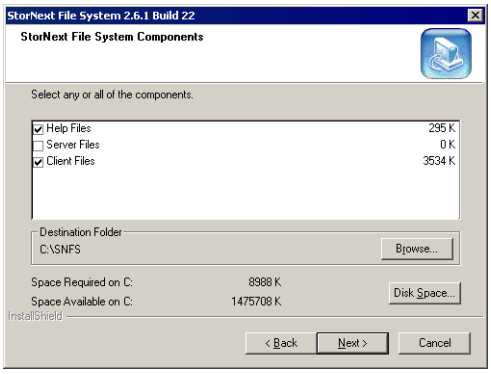
Installing the StorNext File System

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. 

On this screen...	Do this...
Select Program Folder	Accept the default location and click **Next.**
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

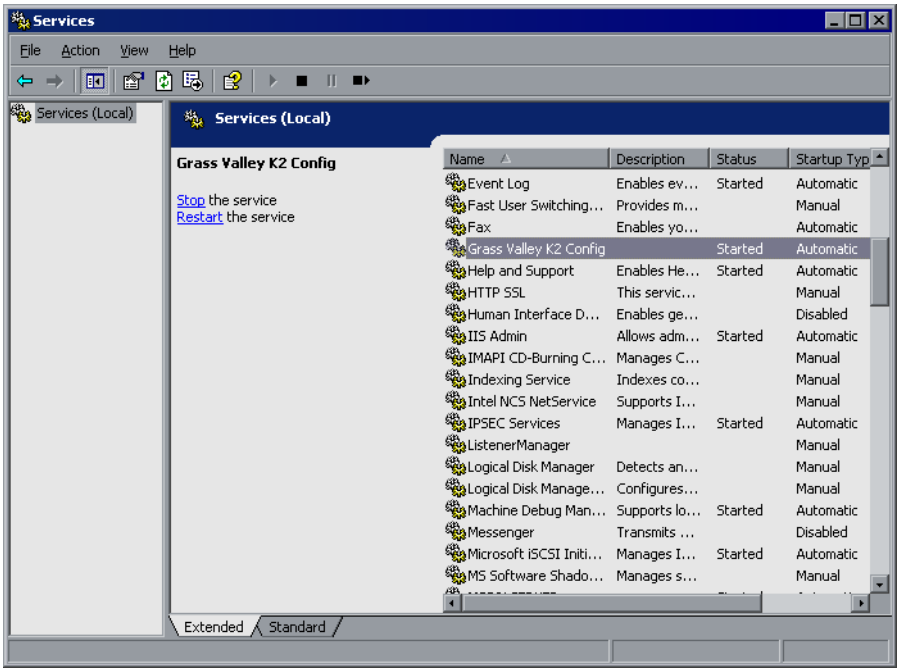
The Generic iSCSI Client software is located on the Aurora Suite CD-ROM. Refer to release notes to verify the version.

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



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

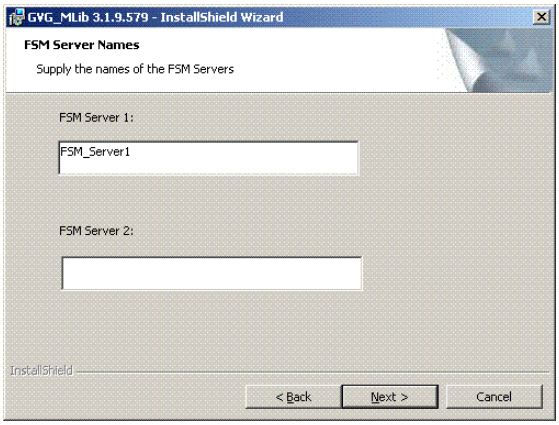
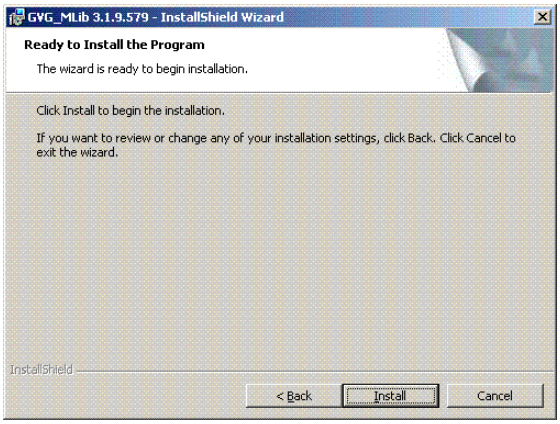
Installing the GVG_MLib Software

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 	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 	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 Advanced 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 94.
- The standard Aurora Browse application is a web-based application. As such it is installed on the MediaFrame server and served to individual client PCs via HTTP. In contrast, the Aurora Edit LD application 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.
- News Edit and News FTP are pre-requites for News MDI.

Chapter 3

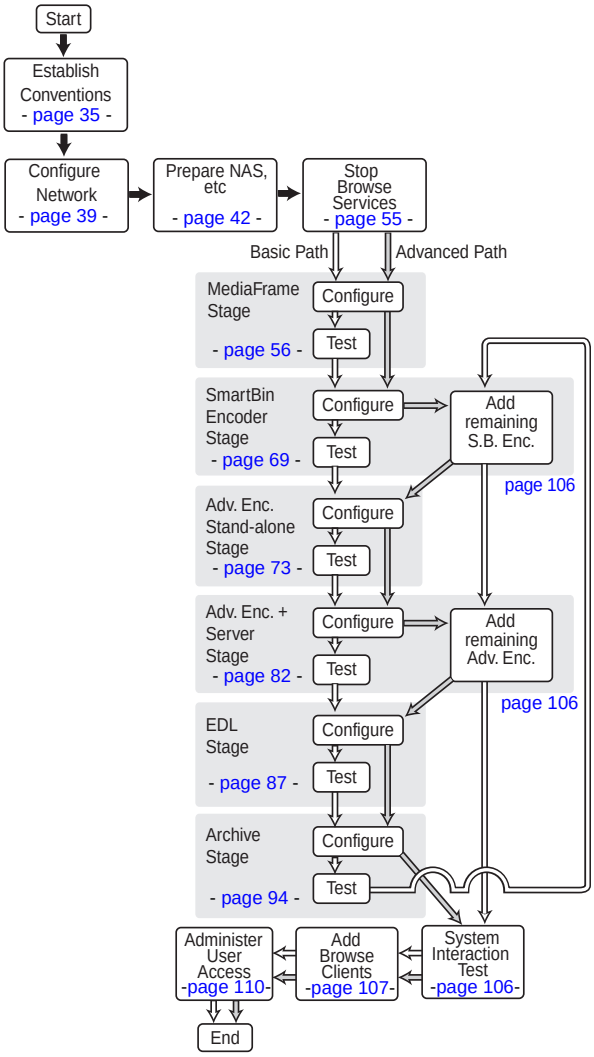
Configuring the system

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 34.
- Customizing — After the system is functioning, you can go back to the configuration pages and modify the settings documented in this manual as **Advanced** ✓ 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 Aurora Edit system is fully functioning on the K2 storage. You should have at least one SmartBin Encoder as part of the Aurora Edit/K2 system. In this role, the SmartBin Encoder is not yet being used as an Aurora Browse machine. Rather, it is just used to host the SmartBins service.

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. At each configuration page, configure only those settings documented in this manual as **Basic** ✓. 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. At each configuration page, you can configure settings documented as **Advanced** ✓ as well as those documented as **Basic** ✓.

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 Readme file, 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.

Machine type	Name
MediaFrame machines	
MediaFrame server	*root*-nb-svr
Managed Device Interface (MDI) Server	*root*-nb-mdi
Proxy machines	
Advanced 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
Open SAN Profile Media Server	mpvs-1…n
M-Series iVDR	ivdr-1…n
Legacy machines	
Live monitor encoder	*root*-nb-live-1…n
Single-channel encoder	*root*-nb-enc-1…n
Router Gateway	*root*-nb-rtr

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, such as the Thomson SmartBin Proxy Transfer service. This type of software component is hosted on the machine that it manages.

Also refer to "Ports and services mapping" on page 38.

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
Advanced Encoder	Thomson Proxy Transfer	ADV1, ADV2, ADV3…	One logical name is required for each Advanced encoder.
Avalon Archive	Thomson 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	Thomson DIVA MDI		
FlashNet Archive	Thomson FlashNet MDI		
K2	Thomson 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	Thomson MSeries MDI	M-SERIES1, M-SERIES2, M-SERIES3,…	One logical name is required for each M-Series iVDR that integrates with the system.
News	Thomson News MDI	NEWS1	There is only one News MDI in the system. It manages the hi-res media storage system for Aurora assets.

Machine type	Service that manages the machine	MDI/Encoder logical name(s)	Comments
NTFS	Thomson 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 NLS MDI.
Profile	Thomson Profile MDI	SAN1	When this MDI manages an Open SAN system, it manages one designated Profile on an Open SAN. One logical name per Open SAN system is required.
		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	Thomson Proxy MDI	PROXY1	There is only one Proxy MDI in the system. It manages the storage locations on all the NAS machines.
SmartBin Encoder	Thomson SmartBin Proxy Transfer	SBE1, SBE2, SBE3…	One logical name is required for each SmartBin Encoder.

NOTE: 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. Another option is to name the Profile MDI name the same as the Profile host name, but this is only an option for systems in their initial configuration, before any customer assets have been added.

Ports and services mapping

Aurora Browse and MediaFrame software components run as Windows services, which communicate over designated ports. As you configure the system, you must correctly designate port numbers. Topics later in this manual provide specific 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		
Thomson Ask	9010	—
Thomson Asset Manager	9022 and 9023	—
Thomson Avalon Archive MDI	9120	—
Thomson DIVA MDI	9122	—
Thomson FlashNet MDI	9124	—
Thomson Metadata	9014	Not visible on a configuration page
Thomson MSeries MDI	9140	The service manages a number of host processes, one for each M-Series iVDR that is being managed. These host processes require ports 9140 - 9149. Stopping/starting the service stops/starts all of the host processes.
Thomson 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.
Thomson News MDI	9150	—
Thomson NTFS MDI	9115	—
Thomson NLS MDI	9128	—
Thomson Profile MDI	9130	The service manages a number of host processes, one for each Profile that is being managed. These host processes require ports 9130-9139. Stopping/starting the service stops/starts all of the host processes.
Thomson Proxy MDI	9110	—
Thomson Resolver	9016	Not visible on a configuration page
Proxy Services		
Thomson Proxy Transfer	9230	Starting range for first control.
Thomson RulesWizard	9018 and 9019	Not visible on a configuration page
Thomson SmartBin Proxy Transfer	9230	—

These services are distributed on different machines in the system. They would not normally run on any one machine, as explained in “Accessing services” on page 53.

The system also depends upon Microsoft Internet Information Services (IIS) and SQL services. SmartBin encoders also need vbrCacheService and vbrSmartBinsService.

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.

NOTE: 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.

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. 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 145 for an example of a host table.

Configure network settings on Production network machines

Use the instructions in this section to configure Production network machines, which are all those of the following types:

- Advanced 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 HAFT platform

To configure the HAFT 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: HAFT-2 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 - Windows Fastora" on page 48.

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 39.

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 (i.e. *mycorp*.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 ports 80 and 280) 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.

Verify that the NLS device has the following software installed:

- Operating System - Windows 2003 Standard Server / Windows 2000 Server.
- Microsoft Internet Information Server (IIS) 6.0 with Microsoft FTP server

Configure the NLS device as follows:

1. Verify that the NLS device as a local *nbadmin* account and that the account has administrator privileges.
2. From the Windows desktop, click **Start | Run** and enter the following:

   ```
   inetmgr
   ```

   IIS opens.
3. Under IIS, right-click **Default FTP Site** from FTP Sites category.
4. Select the **Security Accounts** tab.
5. Select the checkbox for **Allow IIS to control password**.
6. Deselect the checkbox for **Allow only anonymous connections**.
7. Select the **Home Directory** tab.
8. In the FTP Site Directory, give the absolute path of the shared folder on the NLS device which is to be monitored by the NLS MDI. For example, enter the following:

   ```
   C:\Inetpub\ftproot
   ```
9. Provide **read/write/Log visits** permission for user nbadmin.
10. Open Windows Explorer and navigate to the FTP Site Directory.
11. Right-click on the **FTP Site** directory.
12. Select the **Sharing** tab.
13. Select **Share this folder**.
14. Click **Permission**.
15. Under Permission for Everyone, select all the checkboxes for **Allow**
16. Deselect all checkboxes for **Deny**.

Before configuring the NLS MDI to specify transfer targets, verify that the corresponding FTP communications is working without errors. Also make sure that the logged in user has full permissions for the following:

C:\Thomson\MediaFrame\Configuration\NLS_MDIService.exe.config

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 SmartBins

If your system has SmartBin encoders, refer to *SmartBins Instruction Guide* and do the following:

- For K2 systems, make sure SNFS and iSCSI software is correctly installed. Refer to "Install software for K2 support" on page 27.
- Configure the SmartBins service on the Aurora NAS (hi-res) system
- Verify that the mapped drive is V:, unless there are multiple volumes, in which case the mapped drives are V:, W:, X:, Y:.
- Verify configuration to transfer one stream only.
- Create SmartBins in Aurora Edit

Prepare Advanced encoders

- For K2 systems, make sure SNFS and iSCSI software is correctly installed. Refer to "Install software for K2 support" on page 27.
- On your Advanced 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 Advanced encoders and SmartBin 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 Advanced encoders and SmartBin encoders. Refer to "Install software for K2 support" on page 27.
- Set up the Control Point PC.

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

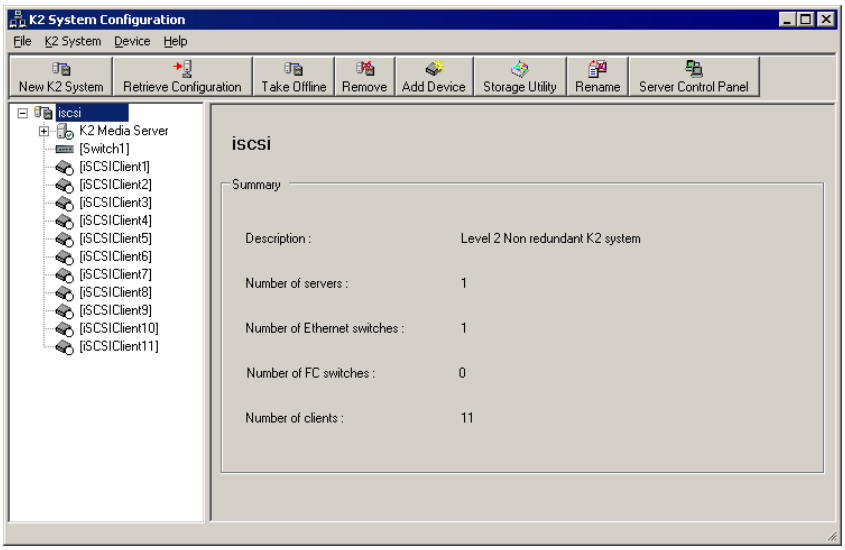
- Run the K2 Configuration application to set up the K2 Server and the GigE switch.
- Connect the Advanced encoders and SmartBin encoders to the K2 Server via the GigE switch. This is the storage connection.

Configuring encoders with the K2 System Configuration application

You use the K2 System Configuration application wizard to configure each of the Advanced encoders or SmartBin encoders on the iSCSI network, as follows:

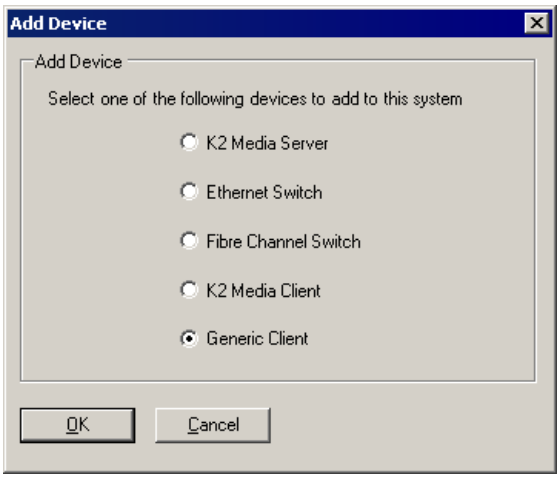
1. On the Control Point PC, open the K2 System Configuration application.
2. At the login dialog box, log in with the correct administrator account. By default this is as follows:
   - User name: administrator
   - Password: adminK2

   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:



3. To add an Advanced encoder or SmartBin encoder to the list, do the following:
   a. Select the media server and click **Add Device**.

.

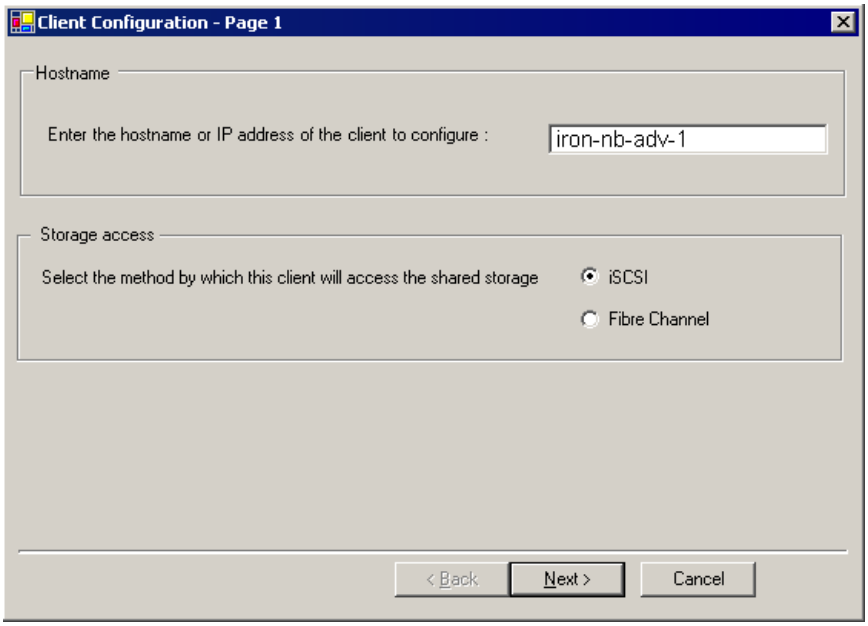


b. In the Add Device window, click **Generic Client** and click **OK**.

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.

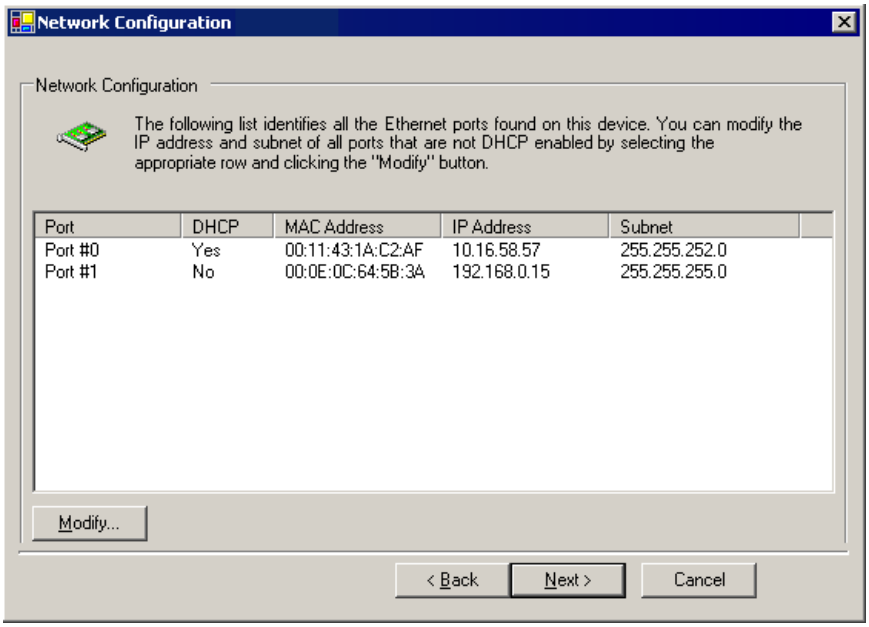


5. At the Client Configuration - Page 1 screen, do the following:

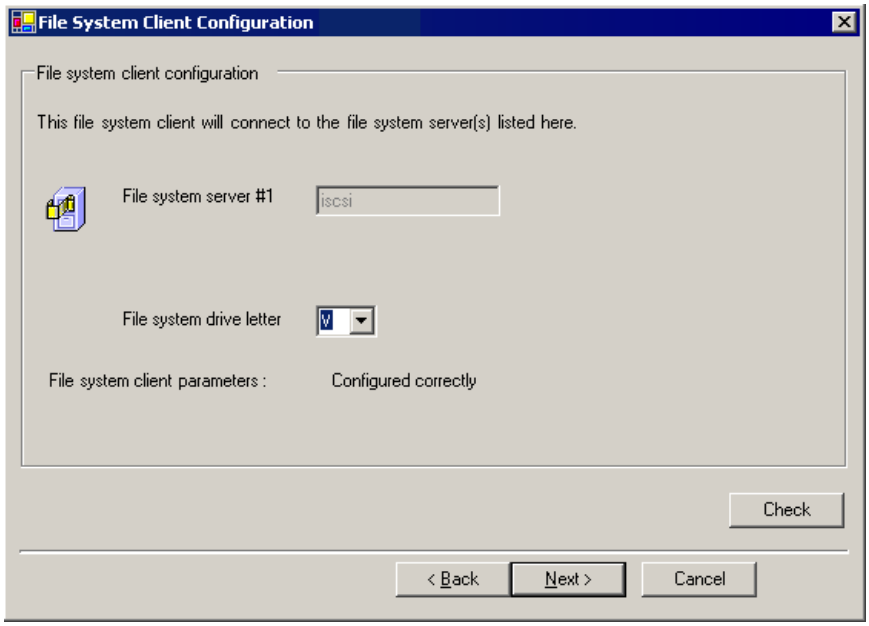
a. Enter the machine name of the Advanced encoder or SmartBin encoder you are configuring (such as `iron-nb-adv-1`).

b. Select **iSCSI**.

c. Click **Next**.

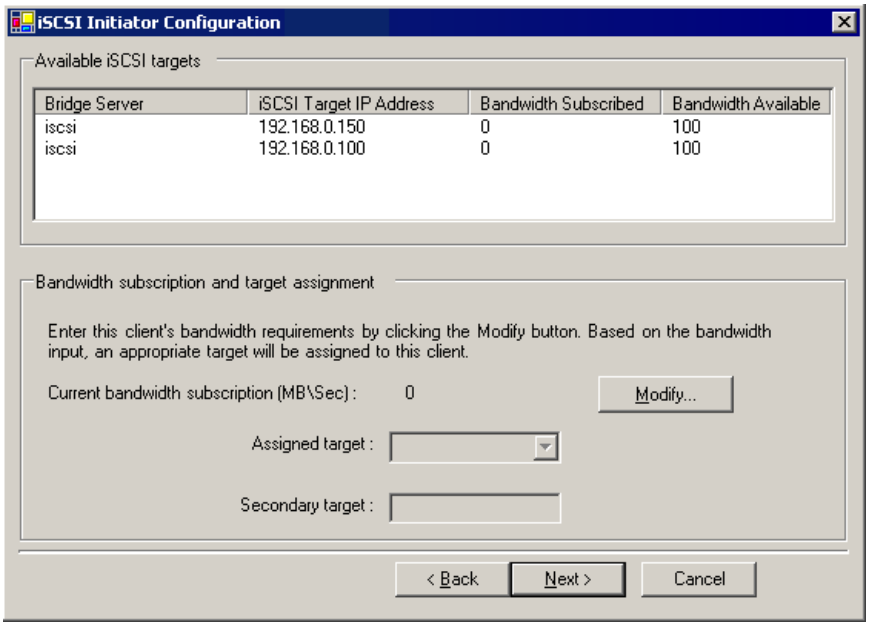


6. At the Network Configuration screen, click **Modify** to change the IP address and subnet of network adapters for this machine, and then click **Next**. You cannot configure the adapter over which the K2 System Configuration application is currently communicating.

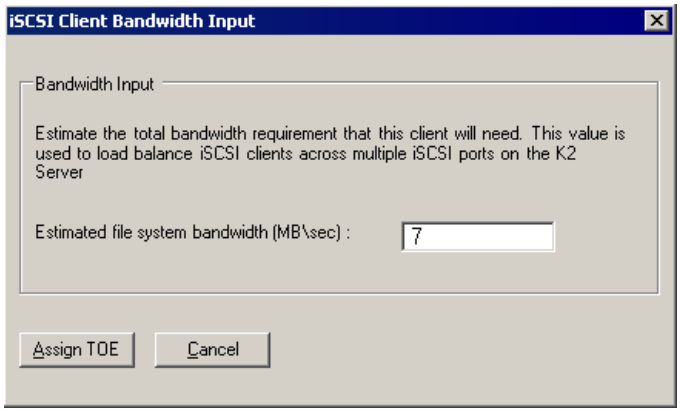


7. At the File System Client Configuration screen, enter the drive letter you wish to configure as the iSCSI drive on the encoder machine; click **Next**. This letter should

be the same for all machines that are iSCSI clients in this K2 Storage System.



8. At the iSCSI Initiator Configuration screen, enter client bandwidth:
   a. Click **Modify**.



   b. Enter the total bandwidth requirement for this encoder machine. (For instructions see the next section, "Calculating encoder bandwidth" on page 48).
   c. Click **Assign TOE**.
9. Click **Next**.
10. At the Completing the Configuration Wizard screen, click **Finish**.

    The wizard closes and the encoder reboots.
11. Repeat this procedure for each Advanced 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 Advanced 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 a Advanced 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 - Windows Fastora

For the Linux version, refer to "Prepare NAS - Linux Fastora" on page 145.

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).

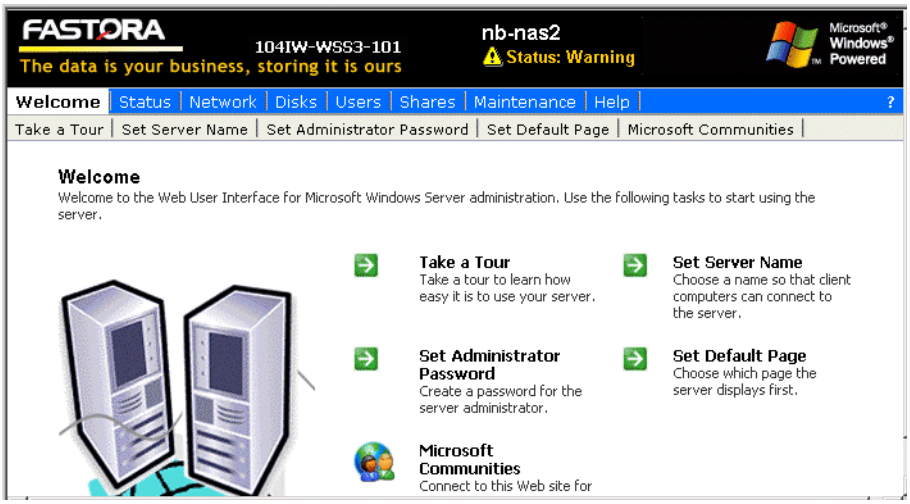
   If you received your NAS unit directly from Fastora, the default Fastora IP address is 192.168.1.11.

3. Log on as follows:

   Username: `administrator`

   Password: `triton`

   The Fastora Welcome page opens.



4. Do one of the following:

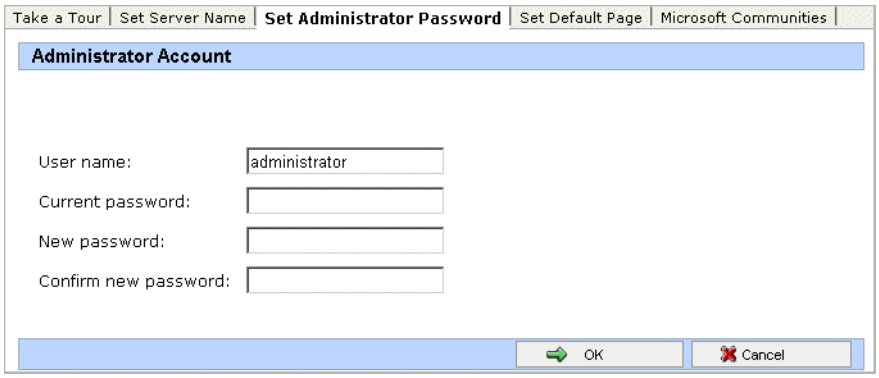
   - To use the remote Windows desktop rather than the Fastora configuration pages, click **Maintenance | Remote Desktop**. This feature prompts you to again log on to the NAS unit, and then allows you to access the Windows desktop. Make settings with standard Windows procedures.
   - To use the Fastora 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**.

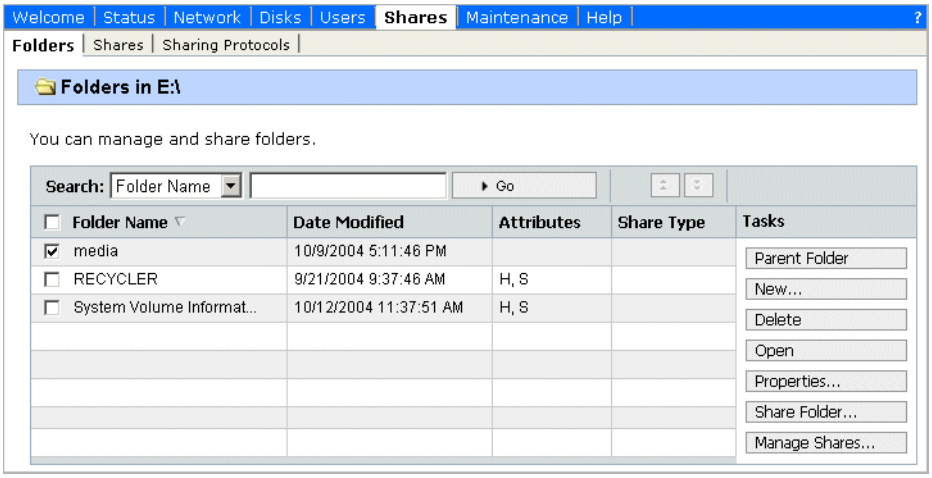
NOTE: After making changes on a configuration page, you must click OK or else your changes are lost.

6. Click **Set Administrator Password**.



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**.

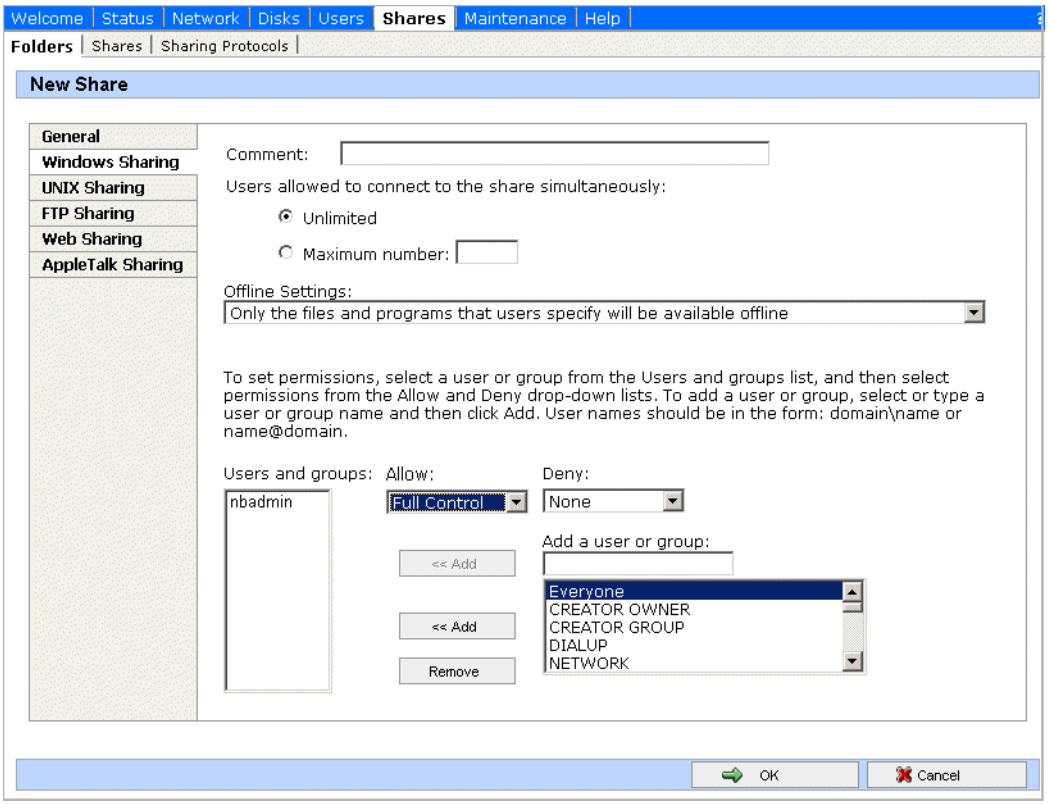


d. Click **Share Folder**.

e. Enter the following:

Share name: `media`

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



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
- Advanced 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

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

About the nbadmin account

The nbadmin account should be set up by default on Aurora Browse machines that you receive from the factory. This account is critical for most Aurora Browse proxy access, as explained in this section.

A local nbadmin account is required on the following machines:

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

All NAS machines require that an *nbadmin* account (contact Grass Valley Support for password) has permission to the folder on the NAS that the encoders write to, and that the web service running on the MediaFrame server reads from.

The basic principle is that any service that requires write access to the Proxy NAS must run as the nbadmin account. This is a local machine account (NOT a domain account). This includes all encoders, the MediaFrame server (which creates EDL files on the Proxy NAS), the News MDI (which writes/deletes a temporary EDL file off of the Proxy NAS), the Proxy MDI (which deletes files off of the Proxy NAS) and the Profile MDI (which deletes temporary EDLs off of the Proxy NAS).

On K2 systems and M-Series iVDRs, security is invoked, which requires administrator privilege. This privilege comes from the nbadmin account, which is another way the nbadmin comes into play on these 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\nbadmin*, *Server1\nbadmin*, and *NAS1\nbadmin*.

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 *nbadmin* account is added to the NAS machine ***after*** the Windows NAS has joined the Windows Domain, this synchronization does not occur. This should not be a problem on factory-prepared Aurora Browse machines, as they come with the *nbadmin* account pre-configured. However, 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 "Thomson…", so they group together in the services list.

Refer to "Ports and services mapping" on page 38 for a list of services.

Accessing system configuration pages

Use Internet Explorer to browse to port 280 of a machine to access its configuration pages. You must have administrator permissions on the machine. For example, to log on to the configuration pages on the MediaFrame server with administrator permissions, use the following:

Username: *root*-nb-svr\nbadmin

Password: (contact Grass Valley Support for password)

The settings you find on a particular computer's configuration pages depend on the software installed on the computer. For example, if the Proxy MDI component is hosted on a single-channel encoder, you find the Proxy Managed Device configuration settings at port 280 of that single-channel encoder. However, if the Proxy MDI component is hosted on a dedicated MDI server, you find the Proxy Managed Device configuration settings at port 280 of the MDI server machine.

You can access a computer's configuration pages as follows:

- From the local computer, use the following URL:

  ```
  http://localhost:280
  ```

- For configuration pages on the MediaFrame server, you can also open the Aurora

Browse launch page and then click the **Configuration** link. To open the Aurora Browse launch page, use the following URL:

```
http://localhost/nbui
```

The Aurora Browse launch page resides on the MediaFrame server only.

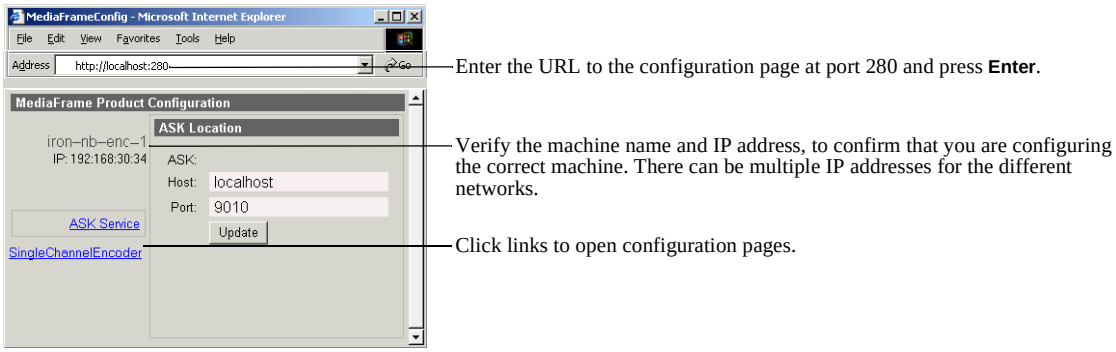
- From a network-connected computer, in the URL replace “localhost” with the network name of the computer hosting the configuration pages. For example, to access the configuration pages or the Aurora Browse launch page on a MediaFrame server named *iron-nb-svr*, use the following URLs:

```
http://iron-nb-svr:280
```

```
http://iron-nb-svr/nbui
```

You must have network access to open configuration pages. You can access all Aurora Browse devices from the MediaFrame server. However, devices on the Client Network, such as a Aurora Browse client PC, do not have access to all Aurora Browse devices. From an Aurora Browse client PC you cannot access devices that are on the Production network only.

To access configuration pages, do the following:



Some pages use Active X controls that require special browser settings, such as the following:

- In Internet Explorer, click **Tools | Internet Options**. The Internet Options dialog box opens. Click **Security | Local intranet | Custom Level**. The Security Settings dialog box opens. Under “Initialize and Script ActiveX Controls not marked as safe”, click **Enable**.

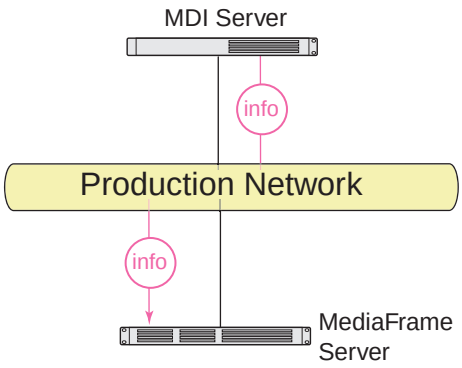
Stop services

Before beginning your initial core configuration stages, you must make sure all Thomson 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 "Thomson…" services are stopped and set to manual, as described in "Accessing services" on page 53. Then, when you configure each stage, you 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:

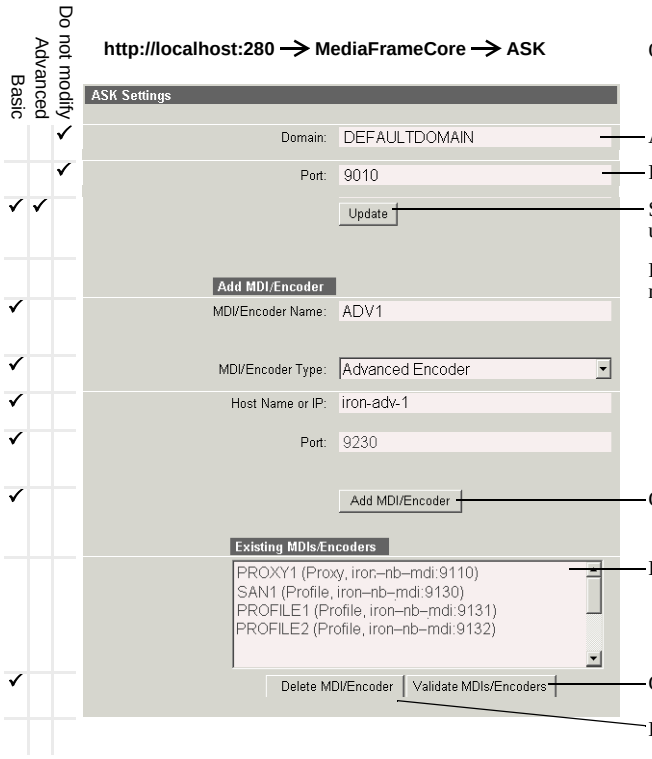
- ASK — The ASK software component runs on the MediaFrame server. It is the central registry for all the software components of the system. As software components carry out tasks in a functioning system they regularly refer to the ASK component to establish communication and exchange commands and data. 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 a 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.

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 57
- "Prepare MDI server" on page 59
- "Configuring transfer targets" on page 60
- "Configure ASK Location: MDI server" on page 61
- "Configure Proxy MDI" on page 62
- "Configure K2 MDIs" on page 63
- "Configure Profile MDIs" on page 64
- "Configure News MDIs" on page 65
- "Configure M-Series MDIs" on page 66
- "Configure NLS MDIs" on page 67
- "Test: MediaFrame stage" on page 68

Configure Media Frame ASK: Register components



Open this configuration page locally on the MediaFrame server machine.

All Domain names in the MediaFrame system must be identical.

Port 9010 is required. See "Ports and services mapping" on page 38.

Saves changes. Changes are lost if you leave the configuration page without updating.

For the following settings, use the table below. Add each MDI and/or Encoder required by your system

Click to add an MDI/Encoder.

Lists currently added MDIs and Encoders.

Checks MDIs. Refer to "Test: MediaFrame stage" on page 68

Deletes the currently selected MDI or Encoder.

Always click **Update…** buttons after making changes

To put changes into effect, start or restart the ASK service on the MediaFrame server.

For the conventions mentioned in the following table, refer to "MDI and Encoder logical names convention" on page 35

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 38. Assign numbers in an intentional sequence, so they are easy to match in "Configure K2 MDIs" on page 63.
K2 Media Client - Internal storage (stand-alone)	K2				
Open SAN Profile[b]	Profile	As per convention.	Hostname of the machine hosting the Profile MDIs. Typically the MDI server	9130 - 9139	These are process ports, as explained in "Ports and services mapping" on page 38. Assign numbers in an intentional sequence, so they are easy to match in "Configure Profile MDIs" on page 64.
Stand-alone Profile	Profile				

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
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 38. Assign numbers in an intentional sequence, so they are easy to match in "Configure M-Series MDIs" on page 66.
NLS	NLS	As per convention.	Hostname of the machine hosting the NLS MDIs. Typically the MDI server	Leave field blank. Correct port number is automatically entered on "Add MDI". Refer to "Ports and services mapping" on page 38 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.		—
Advanced encoder	Advanced Encoder	As per convention	Advanced 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.

[b.] Enter only one Profile per Open SAN. As per convention, name the MDI for the Open SAN, rather than for the Profile.

NOTE: The MediaFrame server must host the NTFS MDI.

The ASK settings page registers 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 (Advanced 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 24.

Dedicated MDI server — For medium to large MediaFrame systems, most MDI services are on a stand-alone MDI server machine, to ensure system performance. 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, 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.

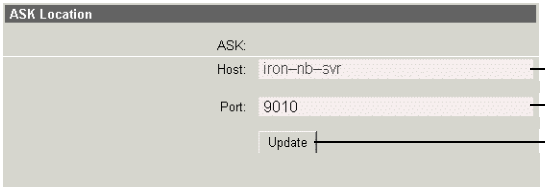
When configuring this type of MDI as a transfer target…	And that MDI manages this type of device…	Enter this as the MDI name…	And then enter FTP IP address… (NOTE: Do not enter the FTP hostname)	And when you add the transfer target, it appears as follows, in "Existing Transfer Targets", for example…	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
	Open SAN system	The MDI that manages the one designated Profile XP system on the SAN	The IP address designated Profile XP system.	SAN1 192.168.100.101	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.

Refer to Archive configuration stages for information on configuring Archive transfers.

Configure ASK Location: MDI server

Basic	Advanced	Do not modify
✓		
	✓	
✓		

http://localhost:280 → ASK Location



Access this page locally on the MDI server.

Enter the name of the MediaFrame server

Port 9010 is required. See "Ports and services mapping" on page 38.

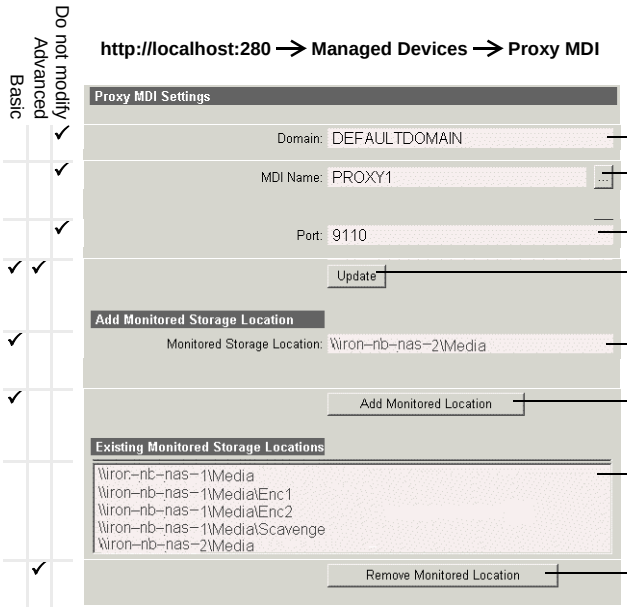
Saves changes. Changes are lost if you leave the configuration page without updating.

Always click **Update...** buttons after making changes

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

This page 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.

Configure Proxy MDI



Access this page locally on the MDI server.

All Domain names in the MediaFrame system must be identical.

Must be set to PROXY1, as per convention.

Port 9110 is required. See "Ports and services mapping" on page 38.

Saves changes. Changes are lost if you leave the configuration page without updating.

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.[a]

Click to add as a location.

Lists the currently added locations. You can add multiple locations. You should have one or more locations listed for each NAS machine.

Removes the currently selected location.

Always click **Update…** buttons after making changes

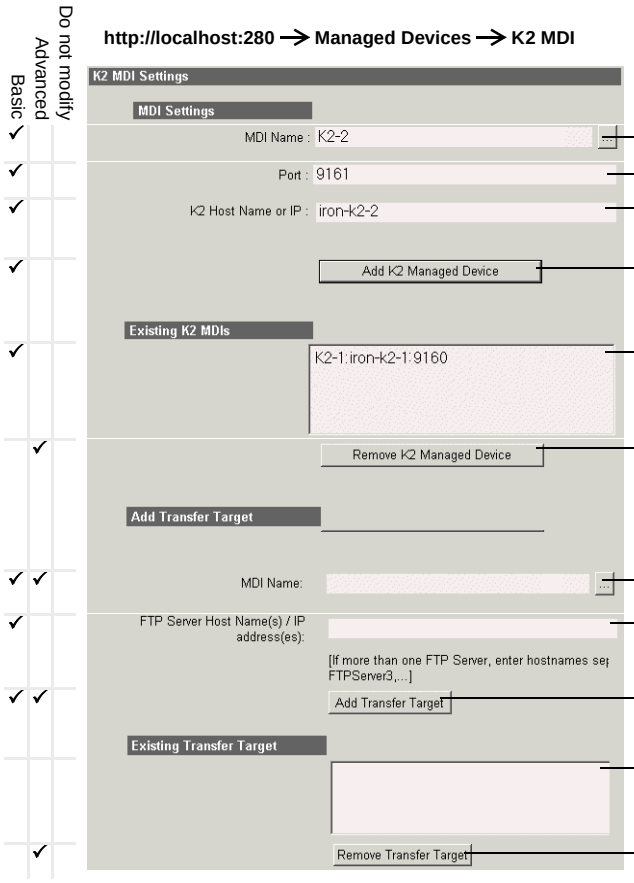
To put changes into effect, start or restart the Proxy MDI Service on the MDI server.

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

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, with the logical name PROXY1. 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.

Configure K2 MDIs



Access this page locally on the MDI Server.

Select a K2 MDI.

Increment 9160-9169 so each K2 MDI has a unique process port.

Enter a stand-alone K2 Media Client or the one K2 Media Client on a K2 Storage System.

Click to add as an existing managed device.

Verify the MDIs currently on-line.

Click to remove the selected managed device.

The following settings enable transfers. You should add all available transfer targets, as specified in "Configuring transfer targets" on page 60.

Lists all MDIs that are available transfer targets. Select and configure each one.

Enter the FTP interface for the MDI selected above.

Click to add as a transfer target.

Systems with which transfers are enabled.

Click to remove the selected transfer target.

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

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

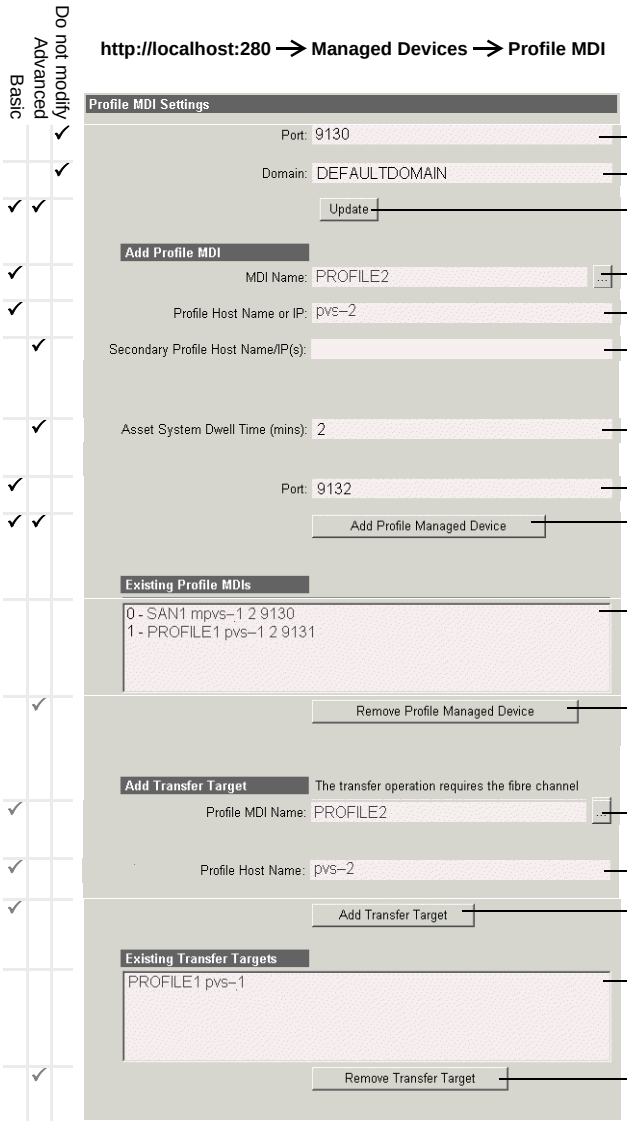
As you configure the K2 MDI make sure that you associate the K2 MDI and K2 host names correctly.

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 57. 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, do the following:

1. Designate one of the K2 Media Clients on the K2 Storage System to be the managed device for the entire storage system.
2. Under MDI Settings, enter only the designated K2 Media Client and add it as a managed device. Do not enter any other K2 Media Clients that are on the K2 Storage System.

Configure Profile MDIs



Access this page locally on the MDI server.

Port 9100 is required. See "Ports and services mapping" on page 38.

All Domain names in the MediaFrame system must be identical.

Saves changes. Changes are lost if you leave the configuration page without updating.

Select a Profile MDI.

Enter the hostname of the Profile for the MDI selected above.

For Open SAN systems, enter here the names of the other Profile XP systems on the Open SAN that are managed by this MDI. Separate hostnames with commas.

The time that the Profile MDI waits before it informs the MediaFrame system that a clip has finished recording. Leave at 2.

Automatically increments so each Profile MDI has a unique process port.

Click to add as an existing managed device. For stand-alone Profile Media Servers, add a MDI for each one. For Open SAN Profile Media Servers, add only one MDI per Open SAN.

Verify the MDIs currently on-line.

Click to update settings.

The following settings enable transfers. You should add all available transfer targets, as specified in "Configuring transfer targets" on page 60.

Lists all MDIs that are available transfer targets. Select and configure each one.

Enter the FTP interface for the MDI selected above.

Click to add as a transfer target.

Systems with which transfers are enabled.

Click to remove the selected transfer target.

Always click **Update…** buttons after making changes
To put changes into effect, start or restart Profile MDI Service on the MDI server.

This page configures the Managed Device Interfaces (MDI) for the Profile Media Servers. As you add Profile MDIs make sure that you associate Profile MDIs and Profile host names correctly.

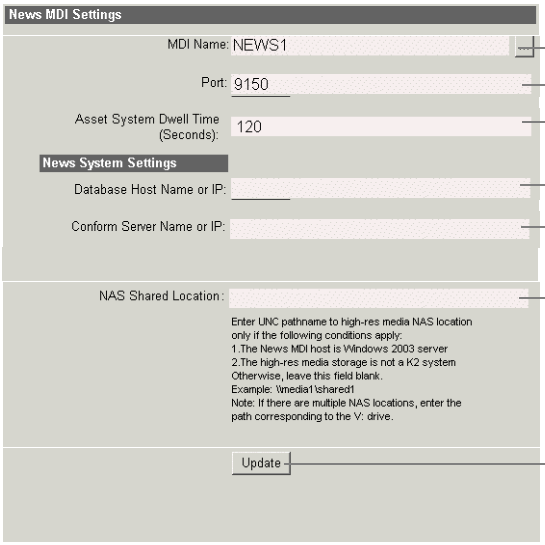
Multiple Profile MDIs run on a single machine (the MDI server), but they each need their own process port number. For this purpose the "Port" field automatically increments. To use the automatically incremented port numbers, make sure you add Profile MDIs in the correct sequence. You can also manually enter port numbers. The MDIs and their port numbers must match settings as in "Configure Media Frame ASK: Register components" on page 57.

For configuring the basic MediaFrame stage, do not yet configure transfer targets.

Configure News MDIs

Basic	Advanced	Do not modify
✓		
	✓	
✓		
✓		
✓	✓	
✓	✓	

http://localhost:280 → Managed Devices → News MDI



Access this page locally on the DSM or MDI server.

Select a News MDI.

Port 9150 is required. See "Ports and services mapping" on page 38.

The time that the News MDI waits before it informs the MediaFrame system that a clip has finished recording. Leave at 2.

Enter the machine that hosts the Aurora Edit database (the DSM).

Enter the machine that hosts the conform service. Typically the Conform Server.

Leave blank or enter UNC path to shared storage. See below.

Saves changes. Changes are lost if you leave the configuration page without updating.

Always click **Update…** buttons after making changes

To put changes into effect, start or restart News MDI Service on the MDI server. (DSM)

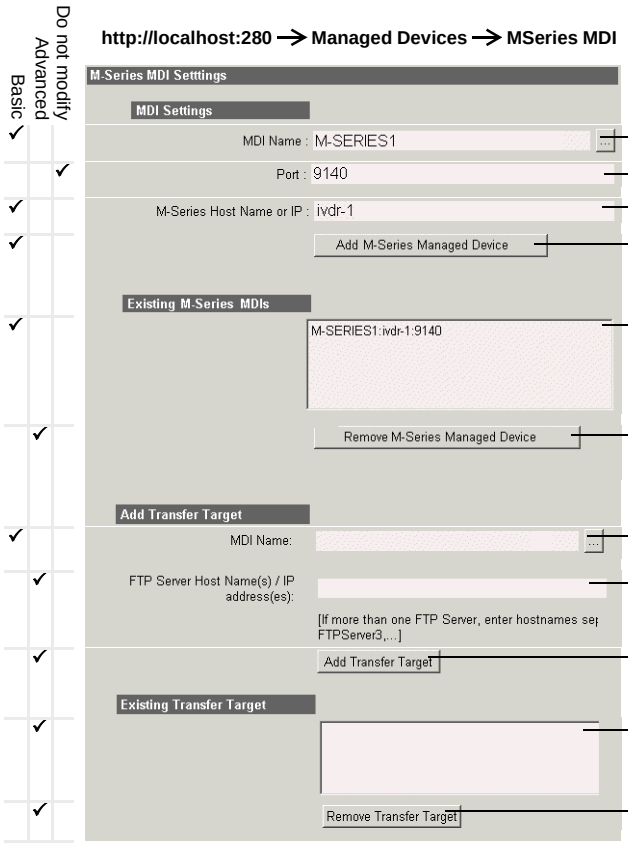
This page configures the Managed Device Interface (MDI) for the AuroraShare system. MediaFrame depends on the News MDI to make News assets visible across the system.

The V: drive must be mapped on the machine that hosts the News MDI. By convention, the DSM hosts the News MDI.

The NAS Shared Location can be left blank for most systems. An example of a system for which the path must be entered is a AuroraShare NAS system whose DSM (the News MDI host) has been upgraded to Windows 2003 Server. The path is required because of enhanced security in the Windows 2003 Server operating system.

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

Configure M-Series MDIs



Access this page locally on the MDI server.

Select a M-Series MDI.

Automatically increments so each M-Series MDI has a unique process port.

Enter the M-Series managed by the MDI.

Click to add as an existing managed device.

Verify the MDIs currently on-line.

Click to remove the selected managed device.

The following settings enable transfers. You should add all available transfer targets, as specified in "Configuring transfer targets" on page 60.

Lists all MDIs that are available transfer targets. Select and configure each one.

Enter the FTP interface for the MDI selected above.

Click to add as a transfer target.

Systems with which transfers are enabled.

Click to remove the selected transfer target.

Always click **Update...** buttons after making changes

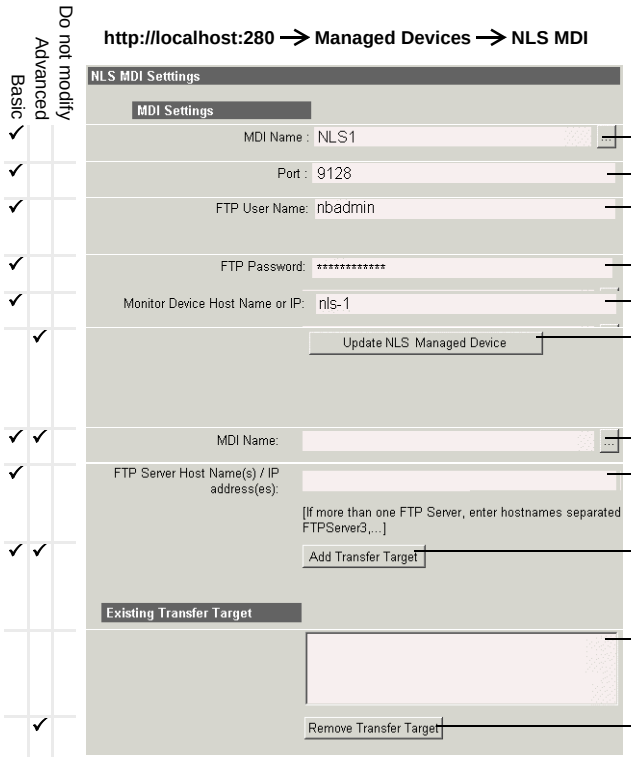
To put changes into effect, start or restart M-Series MDI Service on the MDI server.

This page configures the Managed Device Interface (MDI) for the M-Series iVDR. MediaFrame depends on the M-Series MDI to make M-Series assets visible across the system.

As you configure the M-Series MDI make sure that you associate the M-Series MDI and M-Series host names correctly.

Multiple M-Series MDIs run on a single machine (the MDI server), but they each need their own process port number. For this purpose the "Port" field automatically increments. To use the automatically incremented port numbers, make sure you add M-Series MDIs in the correct sequence. You can also manually enter port numbers. The MDIs and their port numbers must match settings as in "Configure Media Frame ASK: Register components" on page 57.

Configure NLS MDIs



Access this page locally on the MDI Server.

Select the NLS MDI.

Port 9128 is required. See "Ports and services mapping" on page 38.

Enter the username for the account that the Transfer server (the computer that hosts the NLS MDI) uses to log in to the FTP interface on the NLS device.

Enter the password for the account specified above.

Enter the hostname or IP address of the NLS device managed by the MDI.

Click to update settings.

The following settings enable transfers. You should add all available transfer targets, as specified in "Configuring transfer targets" on page 60.

Lists all MDIs that are available transfer targets. Select and configure each one.

Enter the FTP interface for the MDI selected above.

Click to add as a transfer target.

Systems with which transfers are enabled.

Click to remove the selected transfer target.

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

This page configures the Managed Device Interface (MDI) for the Near Line Storage (NLS). MediaFrame depends on the NLS MDI to make NLS assets visible across the system.

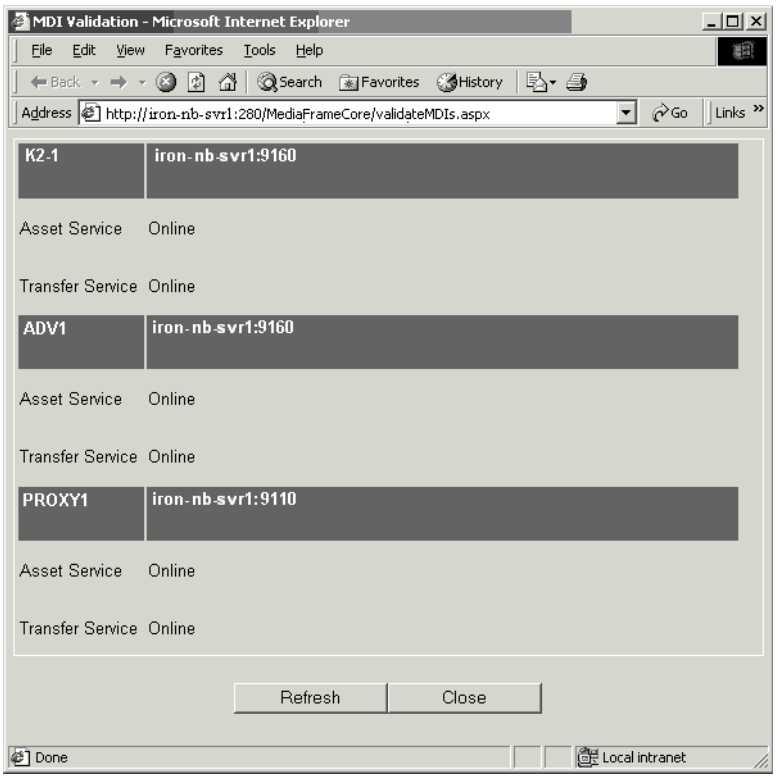
As you configure the NLS MDI make sure that you associate the NLS MDI and NLS host names correctly.

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.

Run the test as follows:

On the Ask Settings configuration page, click **Validate MDIs**. The MediaFrame core system checks MDI mappings and devices for inconsistencies. This can take several minutes. A report is displayed.



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.

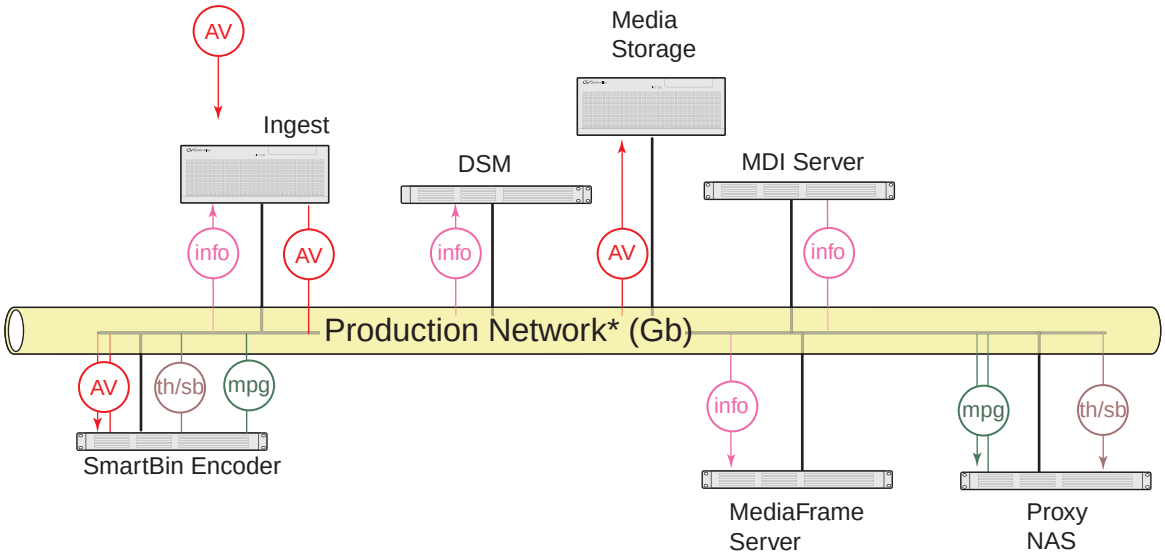
☐ All machines taking the role of MDI server have the appropriate MDI services installed and running.

SmartBin encoder stage

Before starting this configuration stage you should have a working Aurora Edit/K2 system that uses at least one SmartBin Encoder. In this role, the SmartBin Encoder is not yet being used as a Aurora Browse machine. Rather, it is just used to host the SmartBins service. Refer to *SmartBins Instruction Guide.*

For this configuration stage you configure the SmartBin encoder to work together with the ingest system, the Media storage and the Proxy NAS. MDI services are also required, as configured in the MediaFrame stage. Configuration pages and procedures are the same for HD and SD Smartbin encoders.

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

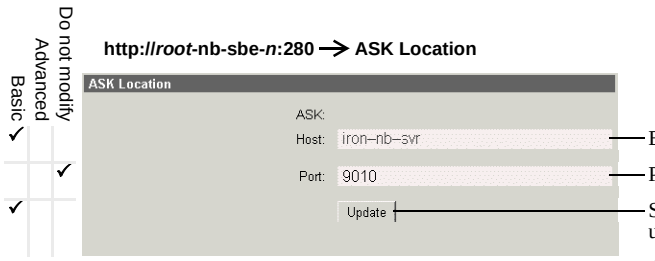


Refer to “System diagram - K2 storage” on page 12 for a view of the entire system.

To do the basic configuration and testing of the SmartBin, do the following:

1. “Configure ASK Location: SmartBin encoder” on page 70
2. “Configure Media Frame Core ASK: SmartBin encoder” on page 70
3. “Configure SmartBin Encoder Control” on page 70
4. “Configure Proxy Asset (NAS): SmartBin encoder” on page 71
5. “Configure MPEG encoder: SmartBin encoder” on page 71
6. “Test: SmartBin encoder” on page 71

Configure ASK Location: SmartBin encoder



Enter the name of the MediaFrame server

Port 9010 is required. See "Ports and services mapping" on page 38.

Saves changes. Changes are lost if you leave the configuration page without updating.

Always click **Update...** buttons after making changes

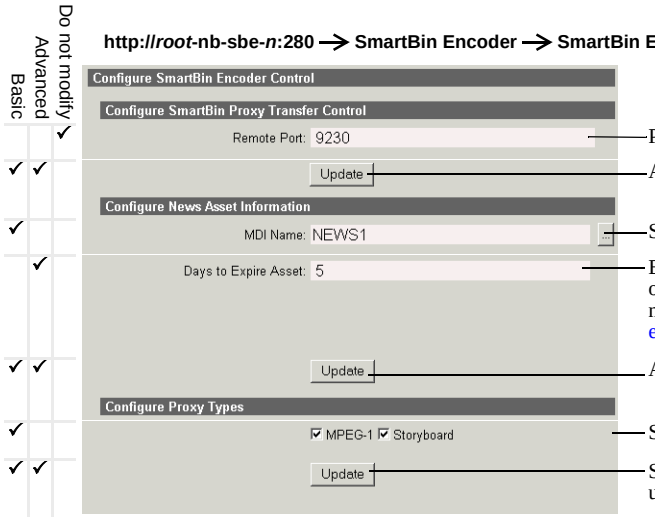
It is not necessary to restart a service to put these settings into effect.

This page 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.

Configure Media Frame Core ASK: SmartBin encoder

Make sure the SmartBin encoder is registered with the ASK software component with a logical name, as explained in "Configure Media Frame ASK: Register components" on page 57.

Configure SmartBin Encoder Control



Port 9230 is required. See "Ports and services mapping" on page 38.

Always click **Update...** buttons after making changes

Select the News MDI.

Expired assets are purged from the system after this many days. Defines the age of the MPEG asset after which it is automatically deleted from the system the next time the purge rule runs. Leave blank to never expire. Refer to "About expired assets" on page 85.

Always click **Update...** buttons after making changes

Select the proxy formats this SmartBin encoder creates.

Saves changes. Changes are lost if you leave the configuration page without updating

Always click **Update...** buttons after making changes

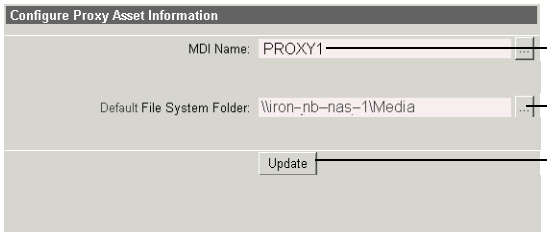
To put changes into effect, start or restart the Thomson SmartBin Proxy Transfer service on the SmartBin encoder.

This page configures the SmartBin encoder.

Configure Proxy Asset (NAS): SmartBin encoder

Do not modify / Advanced / Basic

http://*root*-nb-sbe-*n*:280 → SmartBin Encoder → Proxy Asset Information



There is but one logical Proxy Managed Device in the system, named PROXY1.[a]

Select the path to the folder (\Media) on the NAS (or other storage location) that receives the MPEG this encoder creates.[b]

Validates the current configurations with the Proxy MDI settings and saves changes. Changes are lost if you leave the configuration page without updating.

Always click **Update…** buttons after making changes

To put changes into effect, start or restart the SmartBin Proxy Transfer service on the SmartBin encoder.

a. PROXY1 can have multiple folders (on multiple machines) defined as locations for proxy files. These locations are defined on the Proxy MDI configuration page.

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

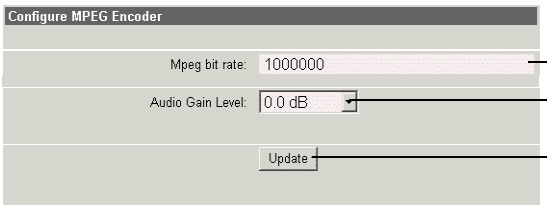
This page specifies the default location (on a NAS machine) in which the SmartBin encoder places the MPEG and storyboard proxy it creates.

When this page opens and when you click a **...** button, fields and lists are populated with valid information as currently defined on the Proxy MDI settings page.

Configure MPEG encoder: SmartBin encoder

Do not modify / Advanced / Basic

http://*root*-nb-sbe-*n*:280 → SmartBin Encoder → MPEG Encoder



Leave at default of 1000000.

The MPEG encoder audio output. Adjust to calibrate Aurora Edit LD audio, or to improve the quality of the desktop audio (i.e. if the source is 'too hot')

Saves changes. Changes are lost if you leave the configuration page without updating.

Always click **Update…** buttons after making changes

Restart the Thomson Proxy Transfer service on the Advanced encoder.

This page configures the parameters the encoder uses when it creates the MPEG proxy.

Test: SmartBin encoder

On the Aurora Browse launch page, the “Smart Bin Encoder Status” page displays the status of all Smart Bin Encoders in the system. This page displays the list of all jobs attempted by the Smart Bin Encoders. For each job, the following are provided:

- encoder name,

- the source and destination file names,

- the time the job was run,

- job status (with error information if the job was unsuccessful), and

- job completion percentage (if job is currently running)

Check the Smart Bin Encoder Status page as you run the following test.

The following test exercises system functionality exclusive creating MPEG and storyboard proxy from a high-res source clip. A successful test verifies that the basic configurations are correct.

ASK configuration, as in "MediaFrame stage" on page 56, is required for this test.

Test description: Trigger proxy creation by placing high-res material in the location monitored by the SmartBin Encoder.

Run the test as follows:

1. Make sure that the system is not in use.
2. Start the Thomson Resolver service and the Thomson Metadata service on the MediaFrame server.
3. Start the Thomson SmartBin Proxy Transfer service on the SmartBin encoder.
4. Click **Start | Programs | Thomson | Event Viewer** to open Event Viewer.
5. Use Aurora Ingest to record to a SmartBin.
6. Watch Event Viewer and verify that the MPEG and storyboard proxy are created and copied to the proxy NAS. Also verify that the high-res media goes to the K2 high-res media storage.

Checklist: SmartBin stage

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

☐ When high-res material appears in the location monitored by the SmartBin encoder, MPEG and/or storyboard proxy are created.

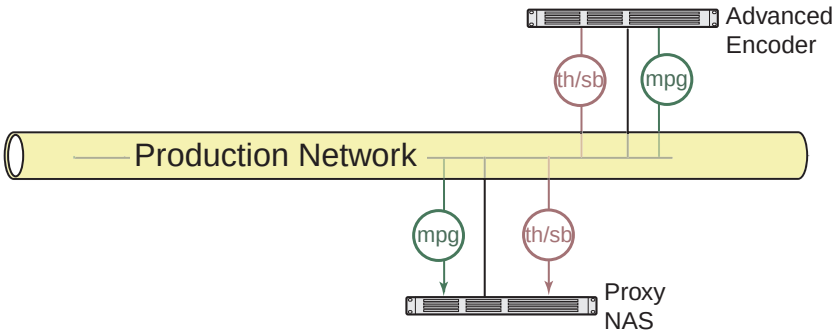
☐ SmartBins Service writes to K2 system.

☐ SmartBin encoder writes to NAS

Advanced encoder stand-alone stage

For this configuration stage you configure and test one Advanced encoder and one Proxy NAS to work together. The Advanced encoder creates storyboard and MPEG proxy. Configuration pages and procedures are the same for HD and SD Advanced encoders.

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

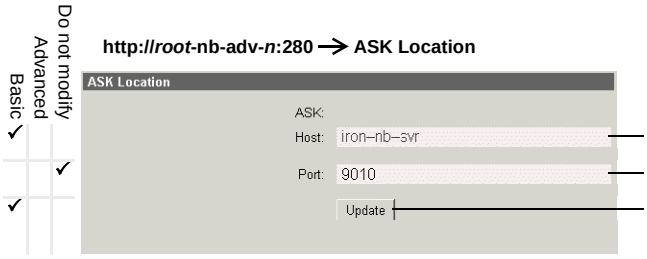


Refer to “System diagram - K2 storage” on page 12 for a view of the entire system.

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

1. “Configure ASK Location: Advanced encoder” on page 74
2. “Configure Advanced Encoding Control” on page 75
3. “Configure Proxy Asset (NAS): Advanced encoder” on page 77
4. “Configure MPEG encoder: Advanced encoder” on page 77
5. “Test: Advanced encoder stand-alone stage - high-res source” on page 77
6. “Test: Advanced encoder stand-alone stage - MPEG proxy source” on page 79

Configure ASK Location: Advanced encoder



Enter the name of the MediaFrame server

Port 9010 is required. See "Ports and services mapping" on page 38.

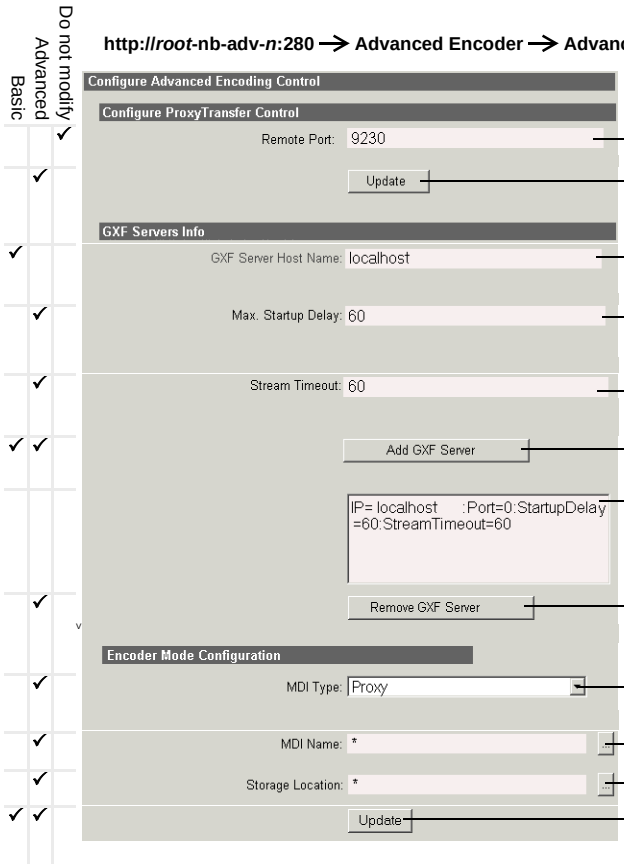
Saves changes. Changes are lost if you leave the configuration page without updating.

Always click **Update...** buttons after making changes

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

This page tells the Advanced 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.

Configure Advanced Encoding Control



Port 9230 is required. See "Ports and services mapping" on page 38.

Always click **Update...** buttons after making changes

Usually the Advanced Encoder hosts the Aurora FTP service, so enter *localhost*. Otherwise, enter the host name of the Aurora FTP service.

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.[a]

Enter the maximum time the encoder waits for a break in the media stream to be restored. 60 seconds is the recommended setting.[b]

Click to add as a GXF server for this encoder.

GXF servers currently added for this encoder.

Remove the currently selected GXF server

Refer to "Configuring Encoder Mode" on page 75 for the following settings.

Select **Material** to create proxy from a high-res source. Select **Proxy** to create additional proxy from an existing MPEG proxy source.

The MDI of the device on which the source resides.

The location of the source.

Saves changes. Changes are lost if you leave the configuration page without updating

Always click **Update...** buttons after making changes

To put changes into effect, start or restart the Thomson Proxy Transfer service on the Advanced encoder.

a. 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.

b. 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.

This page configures the connections between the Advanced encoder and the server from which it gets its media stream.

Configuring Encoder Mode

These settings allow you to set up the Advanced Encoder to generate proxy for high-priority ingest or edited material. This dedicated Advanced 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 Advanced Encoders can do the low priority jobs without interfering with the availability of the dedicated Advanced Encoders.

It is recommended that you dedicate at least one Advanced 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.

To dedicate the Advanced Encoder to a folder, do the following:

- For MDI Type, select **Material**.
- For MDI Name, select a valid MDI Name (other than “*”). To scavenge material in an “Outbox” folder on a K2 Storage System, select the News MDI.
- For Storage Location, select a valid Storage Location (other than “*”). To scavenge material in an “Outbox” folder on a K2 Storage System, select the specific folder.

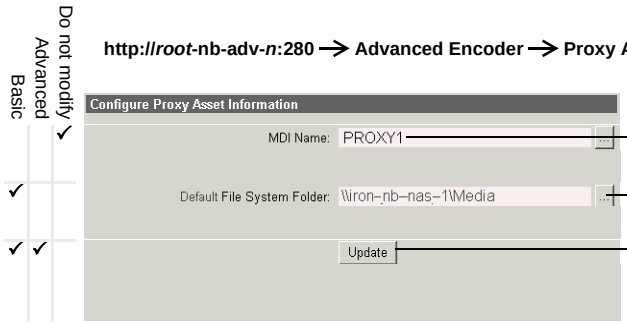
You can dedicate the Advanced encoder to a particular Proxy NAS location. This assumes that for a single Proxy MDI (PROXY1) there are multiple NAS locations.

- To configure the Advanced encoder to process proxy media on all locations, enter “*”.
- To configure the Advanced encoder to process proxy media on one location, select that location as the Proxy Storage Location.

Configuration rules:

- If the MDI name is “*”, the Storage Location must be “*”.
- If the configuration file is manually updated (not recommended) to disable both Material Source and Proxy Source, the following occurs:
  - Proxy Transfer Service will log an error message “Error: Both Scavenge Mode and ISS Mode are disabled. This Encoder will not be able to do any encoding” in the log.
  - On the Advanced Encoding Control configuration page, red text “Error: Both Scavenge Mode and ISS Mode are disabled. This Encoder will not be able to do any encoding” is displayed.

Configure Proxy Asset (NAS): Advanced encoder



There is but one logical Proxy Managed Device in the system, named PROXY1.[a]

Select the path to the folder (\Media) on the NAS (or other storage location) that receives the MPEG this encoder creates.[b]

Validates the current configurations with the Proxy MDI settings and saves changes. Changes are lost if you leave the configuration page without updating.

Always click **Update...** buttons after making changes

To put changes into effect, start or restart the Proxy Transfer service on the Advanced encoder.

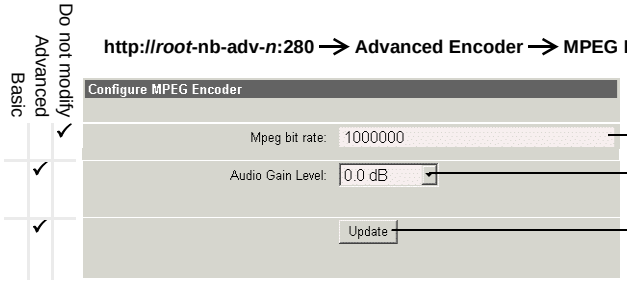
a. PROXY1 can have multiple folders (on multiple machines) defined as locations for assets. These locations are defined on the Proxy MDI configuration page.

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

This page specifies the default location (on a NAS machine) in which the Advanced encoder places the MPEG proxy and storyboard assets it creates.

When this page opens and when you click a **...** button, fields and lists are populated with valid information as currently defined on the Proxy MDI settings page.

Configure MPEG encoder: Advanced encoder



Leave at default of 1000000.

The MPEG encoder audio output. Adjust to calibrate Aurora Edit LD audio, or to improve the quality of the desktop audio (i.e. if the source is 'too hot')

Saves changes. Changes are lost if you leave the configuration page without updating.

Always click **Update...** buttons after making changes

Restart the Thomson Proxy Transfer service on the Advanced encoder.

This page configures the parameters the encoder uses when it creates the MPEG proxy assets.

Test: Advanced encoder stand-alone stage - high-res source

The following test exercises Advanced encoder functionality for creating proxy using News high-res material as the source. A successful test verifies that the basic configurations are correct.

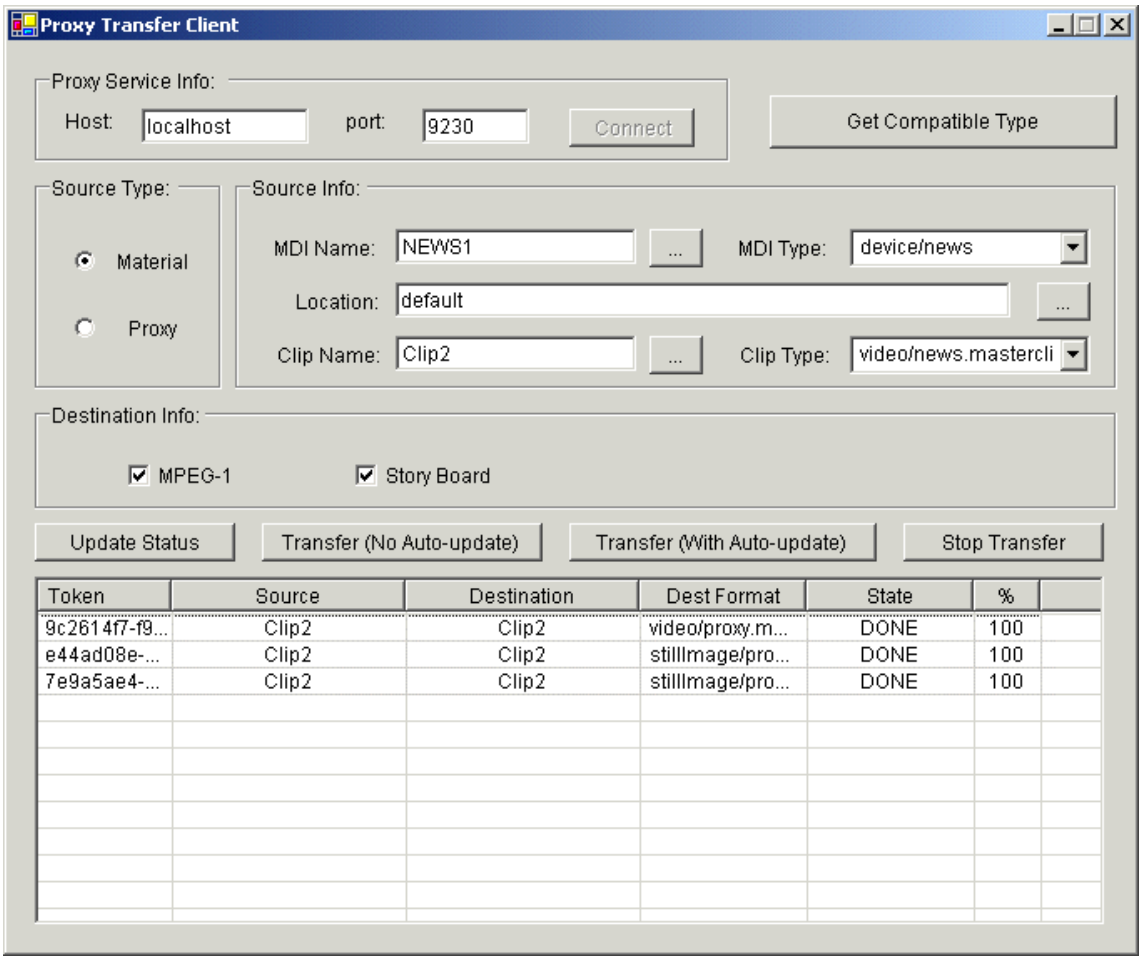
Test description: New proxy types (MPEG, storyboard) are created from high-res material and are transferred to a different location.

ASK configuration, as in "MediaFrame stage" on page 56, is required for this test.

NOTE: Run this test only in the stand-alone stage, with machines that have not yet been added as managed devices (as in the + Server stage). Once the server is connected, this test can result in corrupt database records.

Run the test as follows:

1. Make sure that the system is not in use.
2. Make sure the Rules Wizard Service, Thomson Resolver service, and the Thomson Metadata service are off on the MediaFrame server.
3. On the Advanced encoder, click **Start | Programs | Thomson | Aurora Browse | Diagnostic Tools | Proxy Transfer Client**. The Proxy Transfer Client application opens.



4. Configure as follows to check the connection:
   - Host: **localhost**
   - Port: **9230**
5. Click **Connect**. Verify that the "…Update…" and "…Transfer…" buttons become enabled, which means the connection is successful.

6. Configure as follows to define the source clip on the News hi-res storage:
   - Source Type: Select **Material**.
   - MDI Name: Select the logical name of the News MDI.
   - MDI Type: This should automatically fill in as **device/news**
   - Location: Select the bin on the News hi-res storage that holds the test material.
   - Clip Name: Select the test clip.
   - Clip Type: This should automatically fill in as **video/news.masterclip**
7. Select the following to transfer/transcode proxy:
   - MPEG-1
   - Story Board
8. Click **Transfer (With Auto update)**. Watch the report in the State column to verify that the proxy creation is successful. The proxy files are written to the location configured on the Proxy Asset configuration page as "Default File System Folder".
9. Using Windows Explorer, verify the MPEG and storyboard proxy is created. Open and play the MPEG clip. Validate video and audio.

Test: Advanced encoder stand-alone stage - MPEG proxy source

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

Test description: Storyboard proxy is created from MPEG proxy.

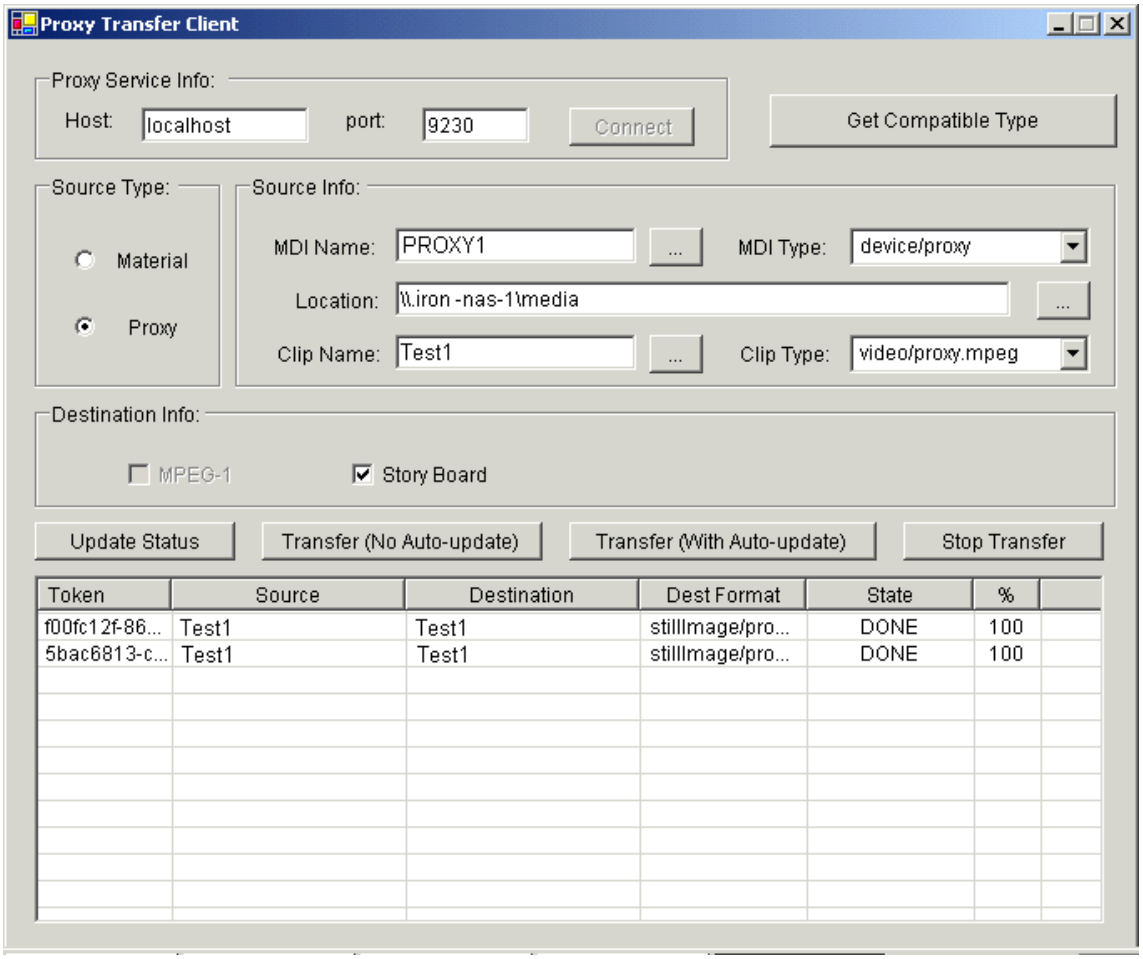
ASK configuration, as in "MediaFrame stage" on page 56, is required for this test.

NOTE: Run this test only in the stand-alone stage, with machines that have not yet been added as managed devices (as in the + Server stage). Once the server is connected, this test can result in corrupt database records.

Run the test as follows:

1. Make sure that the system is not in use.
2. Make sure the Rules Wizard Service, Thomson Resolver service, and the Thomson Metadata service are off on the MediaFrame server.

3. On the Advanced encoder, click **Start | Programs | Thomson | Aurora Browse | Diagnostic Tools | Proxy Transfer Client**. The Proxy Transfer Client application opens.



4. Configure as follows to check the connection:
   - Host: **localhost**
   - Port: **9230**
5. Click **Connect**. Verify that the "…Update…" and "…Transfer…" buttons become enabled, which means the connection is successful.
6. Configure as follows to define the MPEG source on the NAS:
   - Source Type: Select **Proxy**.
   - MDI Name: Select the logical name of the Proxy MDI.
   - MDI Type: Select **device/proxy**.
   - Location: Select the directory on the NAS that holds the test proxy MPEG.
   - Clip Name: Select the test clip.

- Clip Type: Select **video/proxy.mpeg**

7. Select the following to transfer/transcode proxy:
   - Story Board
8. Click **Transfer (With Auto update)**. Track progress in the State column until it reports DONE. The proxy files are written to the location configured on the Proxy Asset configuration page as “Default File System Folder”
9. Using Windows Explorer, verify that the storyboard test files were written to the proper directory.

Checklist: Advanced encoder stand-alone stage

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

☐ Advanced encoder is connected to NAS

☐ Encoder writes to NAS

☐ MPEG created

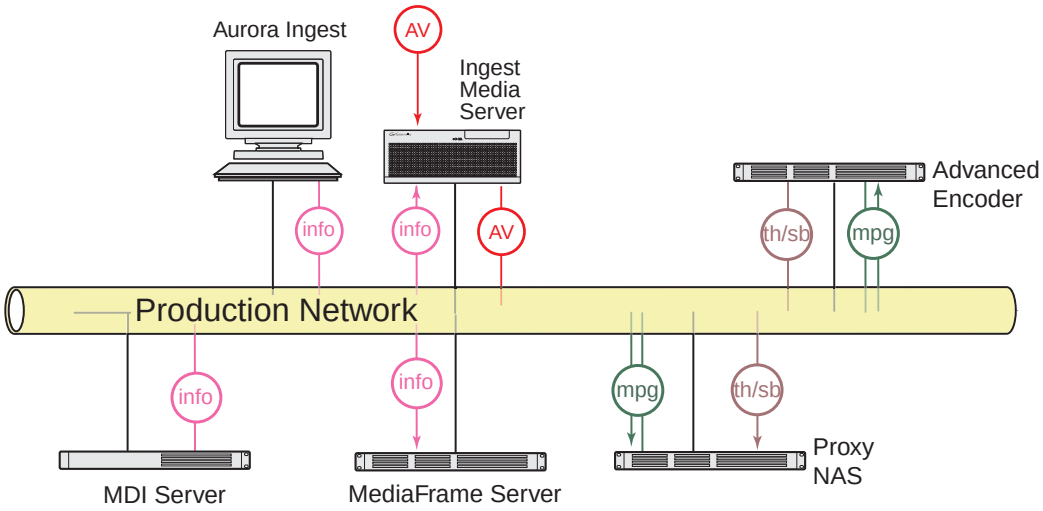
☐ MPEG playback with audio

☐ Storyboard files are created.

Advanced encoder + Server stage

For this configuration stage you configure the MediaFrame server to work together with the Advanced encoder and NAS from the Advanced encoder stand-alone stage. MDI services are also required, as configured in the MediaFrame stage. Configuration pages and procedures are the same for HD and SD Advanced 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.

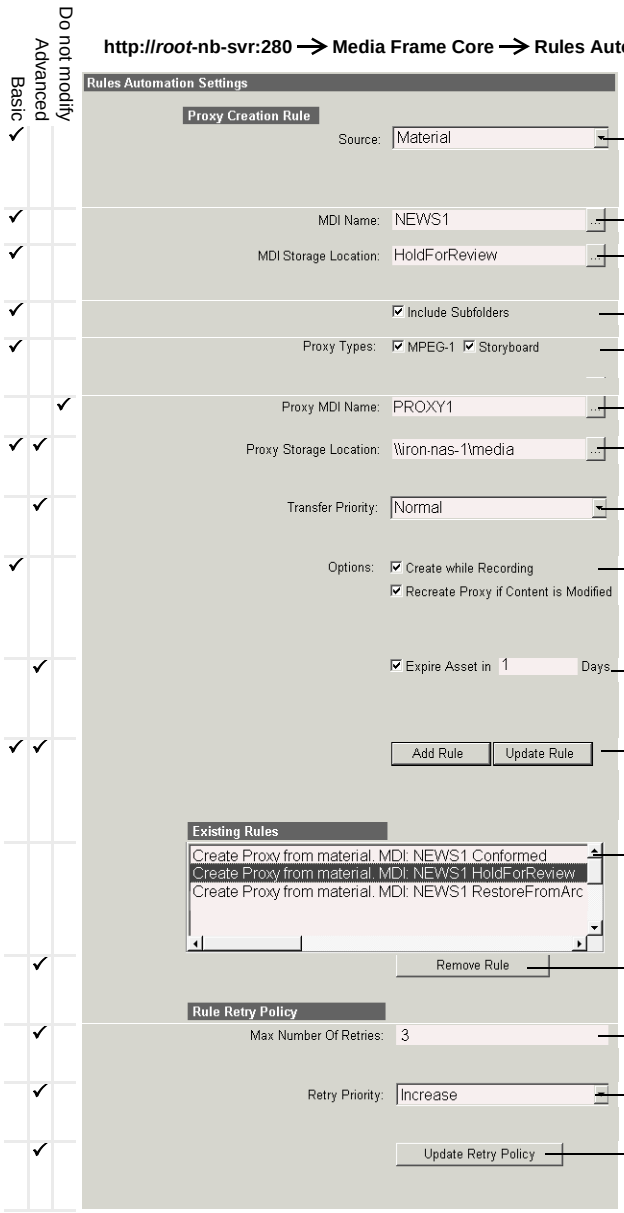
To do the basic configuration and testing of the encoder plus server, do the following:

1. "Configure Media Frame Core ASK: Advanced encoder" on page 82
2. "Configure Rules Automation: Advanced encoder" on page 83
3. "Test: Advanced encoder + Server stage - high-res source" on page 85

Configure Media Frame Core ASK: Advanced encoder

Make sure the Advanced 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 57.

Configure Rules Automation: Advanced encoder



The following settings define the creation of proxy assets.

Select **Material** if this rule creates proxy from a high-res source. Select **MPEG-1** if this rule creates additional proxy from an existing MPEG proxy source. Refer to "About configuring rules" on page 84.

Select the MDI for the machine monitored by the Advanced encoder.

Enter the location on the machine that the system monitors for new material. ***Note: You must use forward slashes for this path.***

Select to also monitor for material in folders nested in "MDI Storage Location".

Select the proxy types to be created by this rule. (MPEG-1 option appears only if Source = Material above.)

Must be PROXY1. (This option appears only if Source = Material above.)

Enter the location. Enter * so the system can use any NAS and keep proxy assets together.[a] (This option appears only if Source = Material above.)

Set all rules to Normal to ensure all are processed in the order received. Higher or lower priority settings can cause a delay for the lower priority rules.

Select one or both. Refer to "About configuring rules" on page 84. (These options appear only if Source = Material above.)

Expired assets are purged from the system after this many days. Leave blank to never expire. Refer to "About expired assets" on page 85. (This option appears only if Source = Material above.)

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

Displays all currently added rules. 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.

Removes the currently selected rule

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.

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.

Save Retry setting changes

Always click **Update...** buttons after making changes

You must start or restart the Thomson Rules Wizard service on the MediaFrame server to put changes into effect, but if you are doing the initial configuration of the Advanced encoder + Server stage, don't start the service until instructed to do so in the Advanced encoder + Server stage test.

a. When the Rule specifies "*" as the Proxy Storage Location the Default File System Folder is used, as configured in "Configure Proxy Asset (NAS): Advanced encoder" on page 77

This page defines the rules for an Advanced Encoder creating proxy.

To scavenge newly-edited material in an "Outbox" folder on a K2 Storage System, for MDI Name, select the News MDI and location as in "Configure Advanced Encoding Control" on page 75.

The following sections explain rules.

About configuring rules

The Rules Automation Settings page dynamically 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.

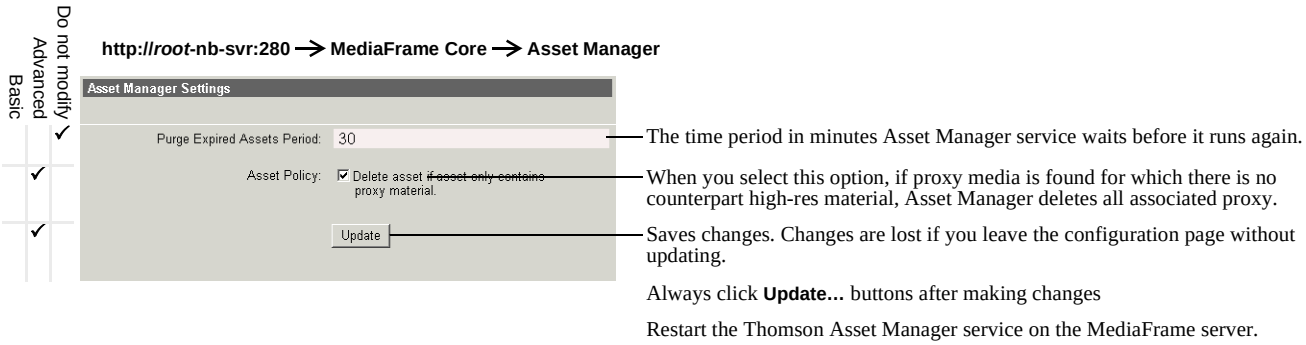
Rules when the source is MPEG proxy

These rules create storyboards from MPEG 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.
- If using SmartBin Encoders, don't use Advanced Encoder rules for ingest.

Configure Asset Manager



When the 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 page 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 “MetadataExpire” date. This is the value that you enter on the Rules Automation Setting configuration page or on the SmartBin Encoder Control configuration page. The “MetadataExpire” 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 minutes) that you configure on the Asset Manager Settings configuration page, 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 “MetadataExpire” date, and if the date portion of the current timestamp is <= the “MetadataExpire” date, the Asset Manager will attempt to delete the asset. Thus, the actual purge period can occur up to a day earlier than expected.

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: Advanced 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 Thomson Rules Wizard service is off on the MediaFrame server.
3. Start the Thomson Resolver service and the Thomson Metadata service on the MediaFrame server.
4. Click **Start | Programs | Thomson | Event Viewer** to open Event Viewer.
5. On a K2 system, copy a clip into a bin monitored by the Advanced encoder.
6. On the MediaFrame server, start the Thomson 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 Advanced Encoder. Watch Event Viewer and verify that the MPEG and storyboard proxy are created (in real-time) as the clip is recorded.

Checklist: Advanced 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.

EDL Export, Save, Conform stage

For this configuration stage you configure the settings for the following Edit Decision List (EDL) features. These features are available in the Aurora Browse application when EDLs are created:

- Export — Exports an EDL to a pre-defined location.
- Save — Saves the EDL as an asset for future use.
- Conform — Creates a high-res asset that matches the EDL on a K2 system. This functionality is available for M-Series iVDRs and Profile XP systems as well.
- Conform to Air — Creates a high-res asset that matches the EDL on one K2 system, then transfers the asset to another K2 system. This functionality is available for M-Series iVDRs and Profile XP systems as well.

Conform server requirements are as follows:

- V:\ should be mapped to the share1 on the high-res storage system.
- Host table should have an entry for the K2 system connection, as in the following example:

  192.168.18.8 iron-k2-1 iron-k2-1_he0

- If conforming to a M-Series the host table should have an entry for the M-Series High Speed Ethernet connection, as in the following example:

  192.168.20.8 iron-ivdr-1 iron-ivdr-1_he0

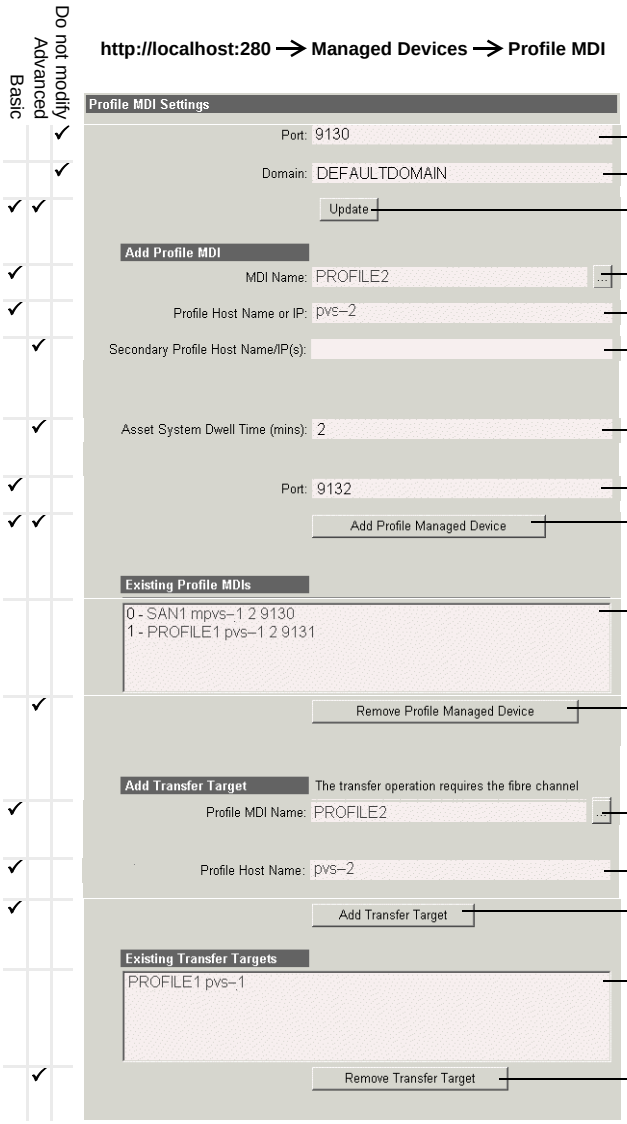
- If conforming to a Profile the host table should have an entry to the High Speed Ethernet connection on the UIM, as in the following example:

  192.168.18.61 iron-xp-uim-1 iron-xp-1-uim_he0

To do the basic configuration and testing of the EDL stage, do the following:

1. “Configure Profile MDI: Conform to air settings” on page 88
2. “Configure NTFS MDI” on page 89
3. “Configure Media Frame Core ASK: NTFS” on page 89
4. “Configure Conform Services” on page 90
5. “Configure Export Services” on page 91
6. “Configure Save EDL settings” on page 92
7. “Test: EDL stage” on page 93

Configure Profile MDI: Conform to air settings



Access this page locally on the MDI server.

Port 9100 is required. See "Ports and services mapping" on page 38.

All Domain names in the MediaFrame system must be identical.

Saves changes. Changes are lost if you leave the configuration page without updating.

Select a Profile MDI.

Enter the hostname of the Profile for the MDI selected above.

For Open SAN systems, enter here the names of the other Profile XP systems on the Open SAN that are managed by this MDI. Separate hostnames with commas.

The time that the Profile MDI waits before it informs the MediaFrame system that a clip has finished recording. Leave at 2.

Automatically increments so each Profile MDI has a unique process port.

Click to add as an existing managed device. For stand-alone Profile Media Servers, add a MDI for each one. For Open SAN Profile Media Servers, add only one MDI per Open SAN.

Verify the MDIs currently on-line.

Click to update settings.

The following settings enable transfers. You should add all available transfer targets, as specified in "Configuring transfer targets" on page 60.

Lists all MDIs that are available transfer targets. Select and configure each one.

Enter the FTP interface for the MDI selected above.

Click to add as a transfer target.

Systems with which transfers are enabled.

Click to remove the selected transfer target.

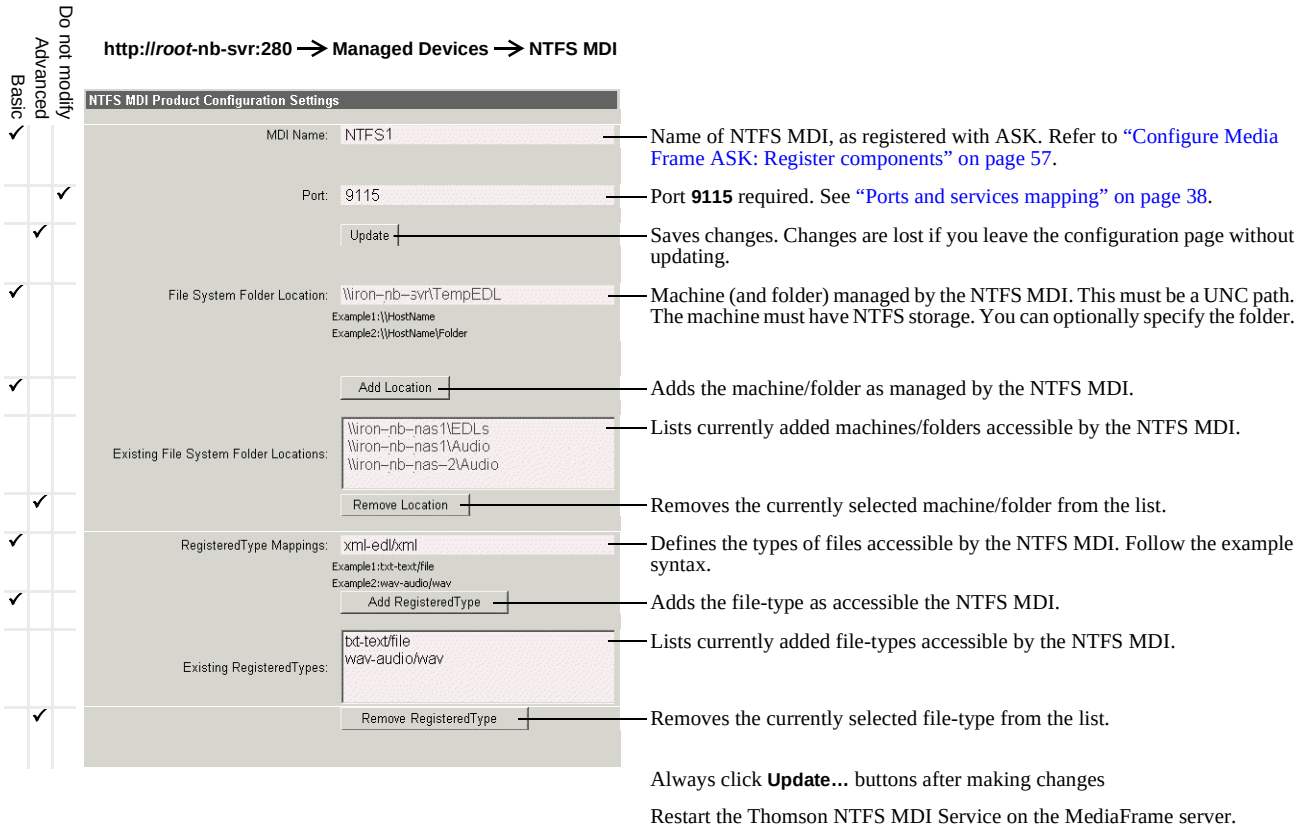
Always click **Update…** buttons after making changes
To put changes into effect, start or restart Profile MDI Service on the MDI server.

This page configures the Managed Device Interface (MDI) for the Profile Media Servers that record and store the high-res media. The MediaFrame system depends on the Profile MDI to make high-res media assets visible across the system.

For the EDL stage, configure the settings related to the EDL Conform to air feature. Specify one of more on-air Profiles as the targets to which conformed high-res clips can be transferred for playout.

For other settings, refer to "Configure Profile MDIs" on page 64.

Configure NTFS MDI



This page 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, including EDLs.

- Enter a location for saving EDLs. Typically this would be on a NAS machine, such as *root*-nas-*n*\EDLs.
- Enter a location for temporarily saving EDLs as they are being conformed. Typically this would be on the MediaFrame server, such as *root*-nb-svr\TempEDL.

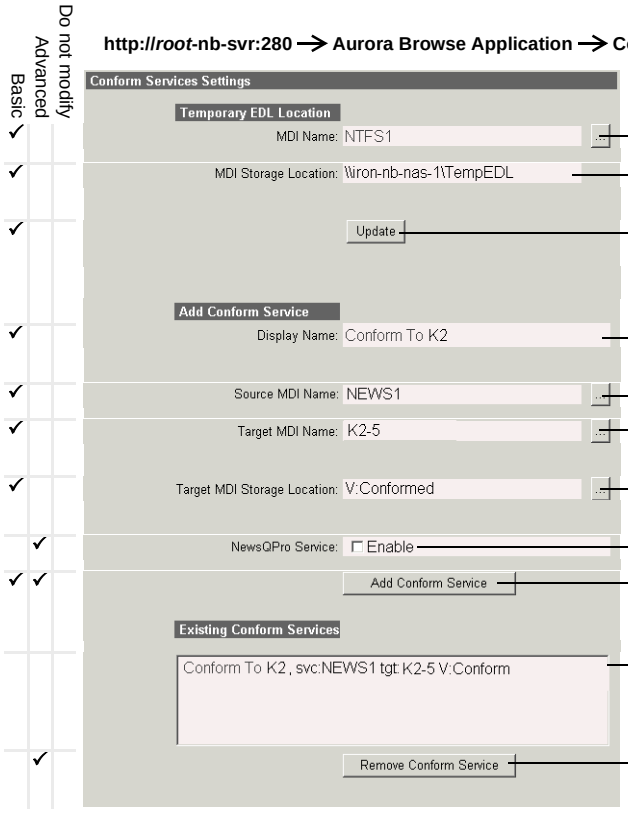
NOTE: Configure different locations for EDL operations. Do not use the same locations for saving, temporary saving, conforming, and exporting EDLs.

- Enter a location for saving audio files. Typically this would be on a NAS machine, such as *root*-nas-*n*\Audio.
- Enter *xml-edl/xml* and *wav-audio/wav* as a file-types.

Configure Media Frame Core ASK: NTFS

Make sure the NTFS MDI is registered with the ASK software component with a logical name, as explained in "Configure Media Frame ASK: Register components" on page 57.

Configure Conform Services



When an EDL is conformed it is temporarily stored in the location specified by the following settings.

Select the name for the NTFS MDI (NTFS1).

Enter a full UNC path to the directory (on a machine with NTFS storage) in which the EDLs are temporarily stored.[a]

Saves changes. Changes are lost if you leave the configuration page without updating.

The following settings specify a media server used to conform an EDL.

Enter the label for display in the Aurora Browse application that identifies the location to which the media is conformed.

Select the MDI for the machine that stores the hi-res material.

The machine managed by this MDI is typically a play-to-air media server to which Conform-to-Air high-res assets are transferred.

Location (bin) on the play-to-air machine where the Conform-to-Air high-res asset is stored.[b]

Select to make the EDL available to NewsQPro.

Add the service to conform EDLs.

Currently added services available to conform EDLs. You can add services using several machines, so that they can be selected in the Aurora Browse application when conforming an EDL.

Removes the currently selected EDL service.

Always click **Update…** buttons after making changes

Restart the Aurora Browse application to put changes into effect.

a. This directory must be shared so it can be accessed by the MediaFrame server.

b. This list is automatically populated by reading the volume and bin names from the media servers indicated by "Target MDI Name" above.

This page tells the Aurora Browse application where to store EDLs that are to be conformed and specifies location to which EDLs are conformed. You can add multiple machines, each of which is then available for selection from the Aurora Browse application.

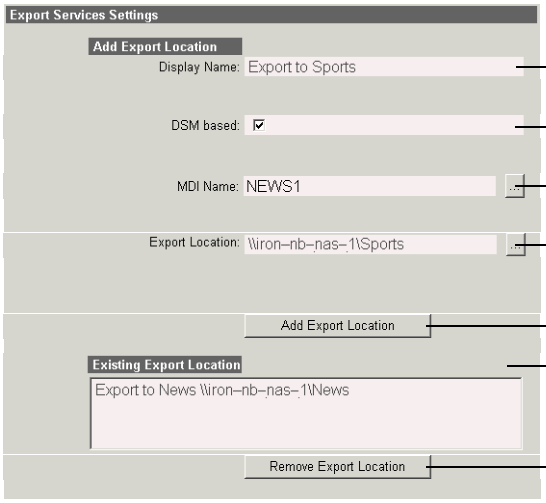
NOTE: Configure different locations for EDL operations. Do not use the same locations for saving, temporary saving, conforming, and exporting EDLs.

For a Conform-To-Air service, the resultant high-res asset is transferred to an On-Air media server (usually a stand-alone system) for playout. You must define the Aurora Browse application display name, the media servers, and the locations to make this type of Conform-to-Air service available in the Aurora Browse application.

Configure Export Services

Basic | Advanced | Do not modify

http://*root*-nb-svr:280 → Aurora Browse Application → Export Services



- Enter the label for display in the Aurora Browse application that identifies the location to which EDLs can be exported.
- Select if EDLs are to be accessed by Aurora Edit.
- Select the News MDI.
- Select[a] the directory to which the EDLs are exported.[b] This should be a working folder, not an "Inbox" or "Outbox" folder. Refer to "Design considerations - Aurora Browse with Aurora Edit" on page 12.
- Adds the location as an export location.
- Currently added location available for exporting EDLs. You can add several locations, so that they can be selected in the Aurora Browse application when exporting an EDL.
- Removes the currently selected location.

Always click **Update…** buttons after making changes

Restart the Aurora Browse application to put changes into effect.

a. If the Export Location button does not open a Browse dialog box, enable the Internet Explorer setting "Initialize and Script ActiveX Controls…". Refer to "Accessing system configuration pages" on page 53 for procedures.

b. This directory must be shared so it can be accessed by the MediaFrame server.

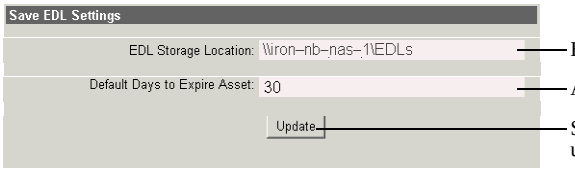
This page tells the Aurora Browse application the locations available for exporting EDLs. You can add multiple locations, each of which is then available for selection from the Aurora Browse application. Name locations and add them according to workflow needs.

NOTE: Configure different locations for EDL operations. Do not use the same locations for saving, temporary saving, conforming, and exporting EDLs.

Configure Save EDL settings

Do not modify
Advanced
Basic

http://*root*-nb-svr:280 → Aurora Browse Application → Save EDL



EDLs are saved to this location, usually a NAS machine.

After this many days, a saved EDL is deleted. Enter 0 to never delete.

Saves changes. Changes are lost if you leave the configuration page without updating.

Always click **Update…** buttons after making changes

Restart the Aurora Browse application to put changes into effect.

This page tells the Aurora Browse application where to save EDLs and how long to keep them in the system.

NOTE: Configure different locations for EDL operations. Do not use the same locations for saving, temporary saving, conforming, and exporting EDLs.

Test: EDL stage

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

Test description: Using the Aurora Browse application, create an EDL, then export, save, and conform it.

Run the test as follows:

1. Make sure that the system is not in use.
2. Load a clip in the Aurora Browse application.
3. Mark in/out region of the clip and press the Insert to Timeline button to add to the timeline. Do this a couple of times with this and other assets.
4. Select Save from the timeline control. Enter and take note of the name used for saving. The save should be successful.
5. Refresh the results list by clicking the Go button with no criteria selected. The EDL asset name should appear in the results list.
6. Select the Export button from the timeline control. Select a destination and choose export.
7. Select Conform from the timeline control. Enter and take note of the name used for conforming. Select a target (not a Conform to Air target) and choose Conform.
8. Select Conform again from the timeline control. Enter and take note of the name used for conforming. Select a Conform to Air target and choose Conform.
9. To verify export, go to the Aurora Edit system and check for the exported sequence in the expected location.

Checklist: EDL stage

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

☐ EDL is created and saved.

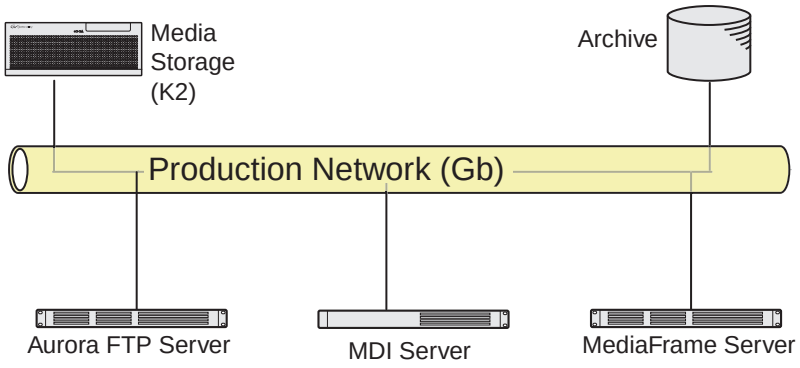
☐ Saved EDL available as asset from Aurora Browse application

☐ EDL exports to specified location

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 95
2. “Verify archive preparations” on page 96
3. “Configure ASK Location: Archive MDI host” on page 100
4. “Configure Media Frame Core ASK: Archive” on page 100
5. “Configure Avalon Archive MDI” on page 101
6. “Configure FlashNet MDI” on page 102
7. “Configure DIVA MDI” on page 103
8. “Configure NLS MDI” on page 104
9. “Configure Archive Services.” on page 104
10. “Test: Archive stage” on page 104

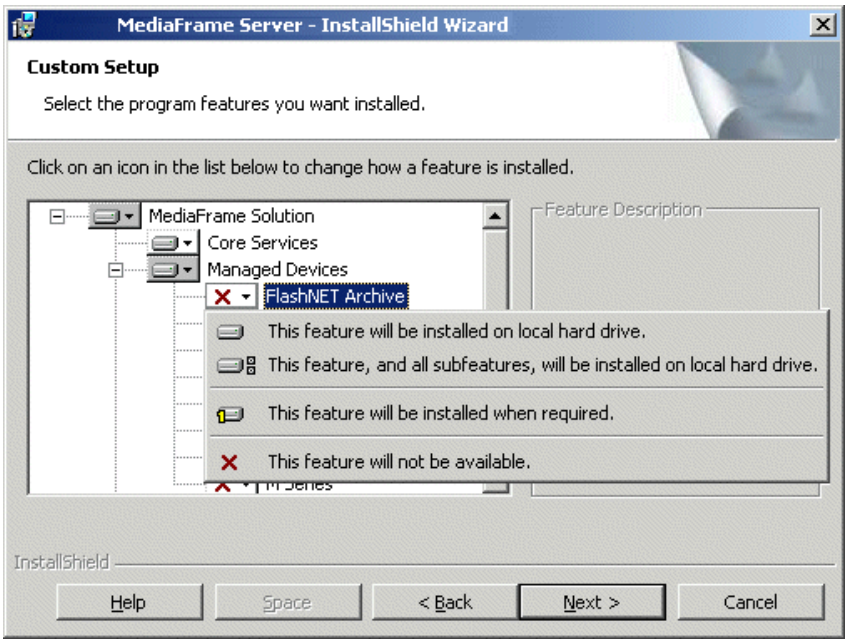
Add archive MDI

The archive MDI software component runs as a service. The archive MDIs that are available for the different types of archive devices are as follows:

- Avalon Archive MDI — runs as the Thomson Avalon Archive MDI service
- FlashNet MDI — runs as the Thomson FlashNet MDI service
- DIVA MDI — runs as the Thomson DIVA MDI service

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.



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 (either stand-alone or on a Open SAN system), 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 which runs Avalon IDM Software (Archive):

1. Login to the machine and go to /avalon/aam/utils
2. Run stataam and verify all services running properly.
3. Make sure host tables are set correctly. Verify for the machine name/IP which IDM will talk to.
4. If archiving from a Profile XP or Open SAN system, make sure the Fiber 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.

FlashNet preparations

Check the following on the machine which runs the FlashNet software:

1. Login to the machine.
2. If archiving from a Profile XP or Open SAN system, verify that you can telnet to the Profile XP Ethernet IP address on port 8192 (`telnet keystone2_le0 8192`).
3. Verify that you can FTP from the FlashNet server to the high-res storage machine:
   - If archiving from a Profile XP or Open SAN, verify that you can FTP from the FlashNet server to the Profile on the Fibre Channel address and login as user *movie*.
   - 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 Gigabit Ethernet and login as user *vmfmovie*.

4. Make sure the “FlashNet Socket Listener” and “FlashNet Automation” services are up and running.
5. Use the FlashNet “Jukebox” application to test that a drive can be successfully accessed from FlashNet. Refer to *“User Guide for FlashNet running on Windows NT and Windows 2000 platforms”*.

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

- The FlashNet MDI does not take any user specified name for a full restore. The clips are restored using the original clip name (from archive). The FlashNet MDI does, however, allow a user specified name for a partial restore.
- If archiving from a Profile XP or Open SAN system, take the concurrent transfer limit into consideration. FlashNet’s setting for concurrent transfers applies globally to all source/destination pairs. There is no setting on a server-by-server basis. To make the setting for “maximum number of concurrent transfers”, you use a file named *C:\.dtool_env* where you can specify “API_MAX_BACKUPS” and “API_MAX_RESTORES”. The following is an example for an eight drive system:

  ```
  API_MAX_BACKUPS     2
  API_MAX_RESTORES    4
  ```

  This example specifies that two concurrent jobs could be used for automation ingest into the archive, four concurrent jobs could be allowed for automation restore of archives, leaving two drives spare for emergency use or another function.
- 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.
- Renaming of an asset is not supported in FlashNet.
- The FlashNet server installation must have the GENERATE UNIQUE NAME entry set to FALSE. Use *Configurator.exe* for FlashNet server configuration.
- A restore operation always defaults to highest “Time Critical” priority and archive operation defaults to “normal” priority.

DIVA preparations

Check the following on the machine which 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 a Profile XP or Open SAN, 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*.

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 or Open SAN system, 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.
- A restore operation always defaults to highest "Time Critical" priority and an archive operation defaults to "normal" priority.
- The source name specified in the DIVA configuration utility must be the same as the host table name of the machine with high-res online material.
- If the DIVA server is rebooted, the Thomson DIVA MDI service must be restarted. Refer to "Accessing services" on page 53.

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 GigaBit 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

If archiving to/from Profile XP/Open SAN systems, ping these machines on the GigaBit network:

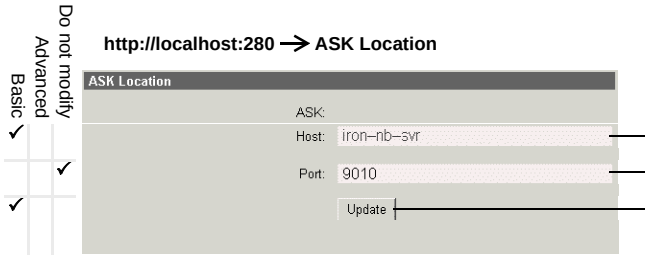
- MediaFrame server
- Archive MDI host
- Profile MDI host (MDI server)
- Archive machine
- All Profile XP or Open SAN systems from/to which media is archived/restored

If archiving to/from Profile XP/Open SAN systems, also use Fibre Channel IP addresses and ping these machines:

- Archive server

- All Profile systems from/to which media is archived/restored

Configure ASK Location: Archive MDI host



Open this page locally on the machine that hosts the Archive MDI.

Enter the name of the MediaFrame server

Port 9010 is required. See "Ports and services mapping" on page 38.

Saves changes. Changes are lost if you leave the configuration page without updating.

Always click **Update...** buttons after making changes

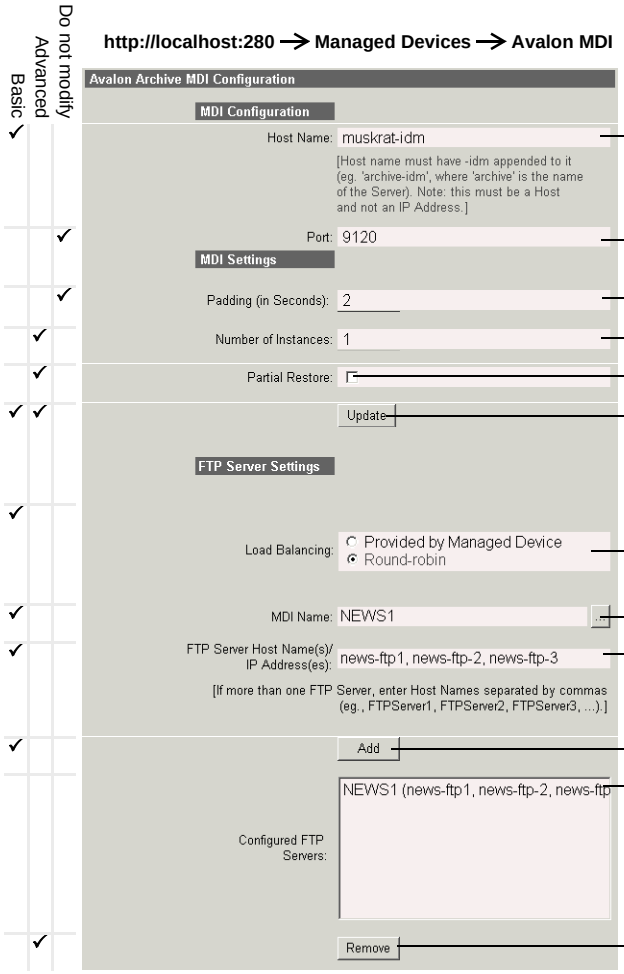
It is not necessary to restart a service to put these settings into effect.

This page tells the Archive MDI host where to look for the ASK service, which runs on the MediaFrame server. If the Archive MDI host is a MDI server or other Aurora Browse machine this configuration has likely already been done.

Configure Media Frame Core ASK: Archive

Make sure the Archive MDI is registered with the ASK software component, as explained in "Configure Media Frame ASK: Register components" on page 57.

Configure Avalon Archive MDI



Open this page locally from the Avalon Archive MDI host.

Name of the Avalon Archive machine. Append *-idm* to the end of the name. This name (with *-idm* appended) must also be in the host table.

Enter **9120**. See "Ports and services mapping" on page 38.

Adds media to the clip to ensure correct long GOP structure. Leave at 2.

The number of archive devices controlled by the MDI.

Select if using partial restore feature.

Saves changes. Changes are lost if you leave the configuration page without updating.

The following settings define FTP for archive sources/destinations.

Select **Provided by Managed Device**. Requires netsem configuration on Avalon. The remainder of this page is disabled.[a]
-OR-
Select **Round-robin**. Requires configuration in the following fields[b]:

Select the News MDI name.

Enter the hostname of the machine hosting the Aurora FTP service. If multiple hostnames, enter with commas separating.[c]

Adds a FTP server as a source/destination for archive operations.

Currently added FTP servers.

Deletes the currently selected device.

Always click **Update…** buttons after making changes

To put changes into effect, start or restart the Thomson Avalon Managed Device service.

a. With Avalon configuration, you define FTP Servers and load balance when you configure netsem, so it is not necessary to enter any information on this page.

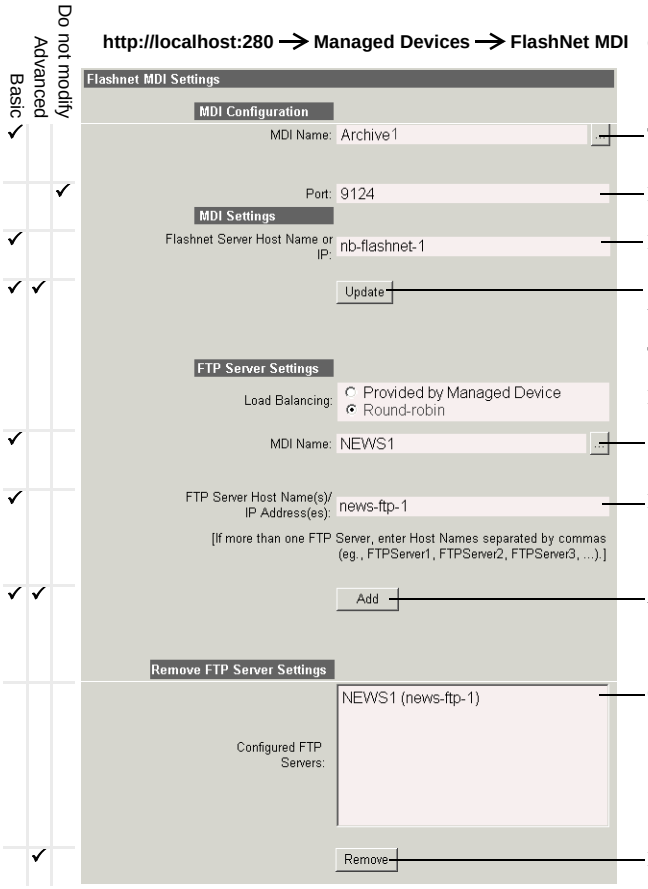
b. If you do not use Avalon configuration, you must define FTP servers and load balance on this page.

c. This defines the load balancing. The order of servers entered here is the order in which the MDI seeks an open channel for an archive job.

Open this page locally on the machine that hosts the Avalon Archive MDI software component. In this example settings are shown for archiving to/from a AuroraShare NAS. This page tells the Avalon Archive MDI where to look for FTP transfer of high-res material.

Typically load balancing is configured using Round Robin on this page. If load balancing is provided by the managed device, when configuring netsem, make sure the netsem FTP server logical name matches the same FTP server MDI name.

Configure FlashNet MDI



Open this page locally from the FlashNet MDI host.

The name of the FlashNet MDI.

Enter **9124**. See "Ports and services mapping" on page 38.

Name or IP address of the FlashNet machine.

Saves changes. Changes are lost if you leave the configuration page without updating.

The following settings define FTP for archive sources/destinations.

Load balancing settings are disabled as only Round Robin is supported.

Select the MDI name for the News MDI.

Enter the hostname of the machine hosting the Aurora FTP service.

Adds a FTP server as a source/destination for archive operations.

Currently added FTP servers.

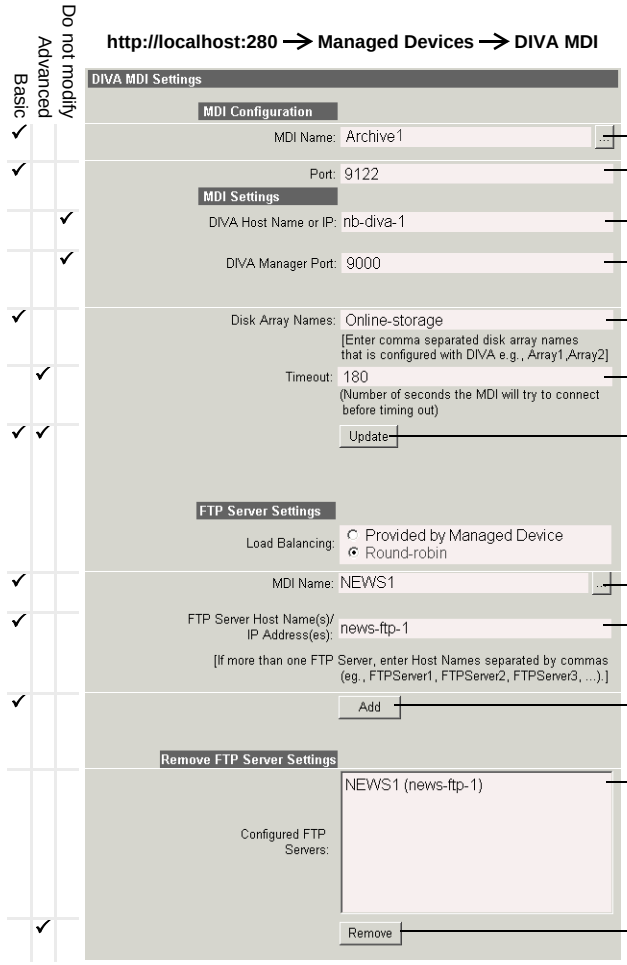
Deletes the currently selected device.

Always click **Update...** buttons after making changes

Open this page locally on the machine that hosts the FlashNet MDI software component.

This page tells the FlashNet MDI where to look for FTP transfer of high-res material. In this example settings are shown for archiving to/from a AuroraShare NAS. For K2 storage or AuroraShare NAS systems, archive transfers are handled by a single FTP server.

Configure DIVA MDI



Open this page locally from the DIVA MDI host.

Name of the DIVA MDI.

Enter **9122**. See "Ports and services mapping" on page 38.

Name of IP address of the DIVArchive machine.

The port at which DIVA Manager listens for any active connection. By default this port is set to 9000.

Specify the name of the disk arrays that are currently configured with the DIVA system.[a]

The timeout value that controls any communication with the DIVA manager. Default value is set to 180 seconds.

Saves changes. Changes are lost if you leave the configuration page without updating.

The following settings define FTP for archive sources/destinations.

Load balancing settings are disabled as only Round Robin is supported.

Select the News MDI name.

Enter the hostname of the machine hosting the Aurora FTP service.

Adds a FTP server as a source/destination for archive operations.

Currently added FTP servers.

Deletes the currently selected device.

Always click **Update...** buttons after making changes

a. An array designates a collection of disks designated by their name as they are declared in the DIVArchive configuration.

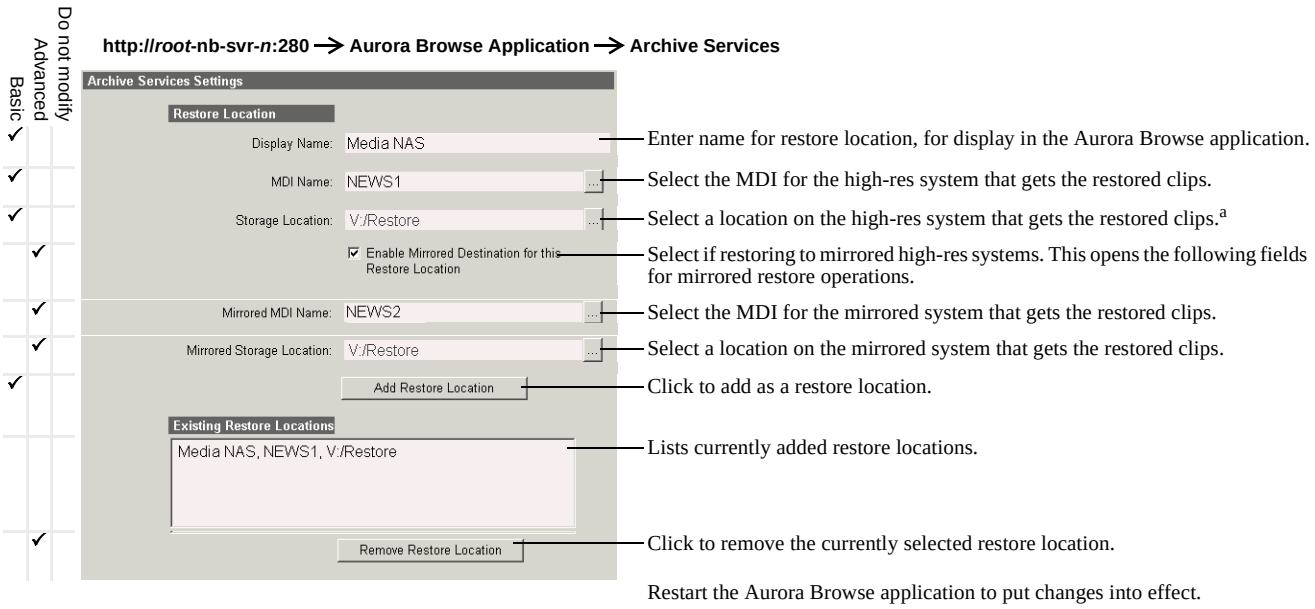
Open this page locally on the machine that hosts the DIVA MDI software component.

This page tells the DIVA MDI where to look for FTP transfer of high-res media assets. In this example settings are shown for archiving to/from a AuroraShare NAS. For K2 storage or AuroraShare NAS systems, archive transfers are handled by a single FTP server.

Configure NLS MDI

Refer to "Configure NLS MDIs" on page 67.

Configure Archive Services.



a. Profile location lists are automatically populated by reading bins and volumes, as in Media Manager, from the Profile whose MDI is selected from the field above.

This page tells the Archive MDI where to place high-res assets as they are restored from the archive device.

When you select "Enable Mirrored Destination…", you can then enter the MDI and location for the mirrored high-res system. This allows you to define the pair of mirrored systems as a single restore location. When this single location is selected in the Aurora Browse application, clips are restored or deleted on both high-res systems simultaneously.

Test: Archive stage

The following test exercises archive functionality. A successful test verifies that the archive configurations are correct.

Test description: Using the Aurora Browse application, archive and restore high-res media.

Run the test as follows:

1. Make sure that the system is not in use.
2. From the MediaFrame server, open the Aurora Browse application.
3. From the **Find** tab, load an asset. After a short pause, the asset appears in the application interface.
4. On the **related** tab, verify that **online media** is listed as a Related Asset Component.

5. On the **mgmt** tab, verify the presence of the following links:
   - Modify Group Membership
   - Archive Selected Asset

   The following links might also be present if the asset has already been archived:
   - Restore Selected Asset
   - Delete from Archive

   Archive and Restore links are not present if the user currently logged on is not assigned Archive and Restore roles. See "Configure Aurora Browse Users" on page 111.
6. On the **mgmt** tab, click **Archive Selected Asset**. The Archive Selected Asset settings are displayed on the tab.
7. Select an **Archive Group**. This list comes from the archive device. This is the location to which the high-res clip is archived.
8. Select **delete online media following archive**.
9. Click **Submit**, then **Yes** to confirm and **Close**.
10. On the Aurora Browse launch page, click **Archive Status** to track the progress of the transfer. Once the transfer is complete the status reports as DONE and 100%.
11. On the Aurora Browse application **Find** tab, click **Go**. The asset list reloads. Verify that an amber dot is listed with the asset. Select the asset to reload it, then click the **related** tab and verify that **offline media** is now listed.
12. On the **mgmt** tab, click **Restore Selected Asset**. The Restore Selected Asset settings are displayed on the tab.
13. Select from the **Restore to Location** list. This is the location to which the archived clip is transferred.
14. Click **Submit**, then **Yes** to confirm and **Close**.
15. On the Aurora Browse launch page, click **Archive Status** to track the progress of the transfer. Once the transfer is complete the status reports as DONE and 100%.
16. On the Aurora Browse application **Find** tab, click **Go**. The asset list reloads. Verify that the amber dot is no longer listed with the asset. Select the asset to reload it, then click the **related** tab and verify that both **online media** and **offline media** are now listed.

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 Advanced encoders. Refer to "Advanced encoder stand-alone stage" on page 73 and "Advanced encoder + Server stage" on page 82.
- Deploy remaining SmartBin encoders. Refer to "SmartBin encoder stage" on page 69.

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 Advanced 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 Advanced encoders in your system. For example, if you have four Advanced 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 Thomson Event Viewer.
3. Prepare a bin or folder (preferably one that is currently empty) for monitoring by the system for scavenge operations. On the Advanced 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 advanced 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 sections in the remainder of this chapter apply to the use of the web-based Aurora Browse application. If you are using the Aurora Edit LD application, also refer to the Aurora Edit LD Readme file, which you can find on the Aurora Edit LD Installation CD.

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 107
- "Set up client PCs" on page 108
- "Configure Aurora Browse Licenses" on page 109
- "Testing Aurora Browse client operations" on page 115

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.

Continue with the next procedure "Set up client PCs".

Set up client PCs

The requirements for a Aurora Browse client PC are as follows:

- Network access to the MediaFrame server
- Network access to NAS machines. Refer to "Prepare NAS - Windows Fastora" on page 48 for test procedures.
- DirectX 9.0c or higher. Enable "Download signed ActiveX controls" in Internet Explorer.
- NetTime is required if Aurora Browse controls ingest on Profile XP/Open SAN.

It is no longer necessary to install Live Feed Filter or Flash Player. They are now bundled together with the Aurora Browse Clip Player. Live Feed Filter and Flash Player automatically download when the application first runs.

To set up a PC to satisfy these requirements, do the following:

1. From a client PC, open Internet Explorer 6 and click **Tools | Internet Options**. The Internet Options dialog box opens.
2. Click **Security | Local intranet | Custom Level**. The Security Settings dialog box opens.
3. Under "Download signed ActiveX controls", click **Enable**.
4. Browse to the following URL to open the Aurora Browse launch page:

   http://*root*-nb-srv/nbui.
5. From the Aurora Browse Launch page, click **Client Setup**. Follow the Client Setup on-screen instruction for Browser, DirectX, and (if necessary) for NetTime. Also refer to "Prepare NetTime" on page 140. For K2 storage or AuroraShare NAS systems, NetTime is not required on Aurora Browse client machines.

After installation be sure to clear the browser cache on client machines to insure updated components are downloaded. To clear the browser cache in Internet Explorer go to **Tools | Internet Options**, from the **General** tab select the **Delete Files** button, check **Delete all offline content**, and click **OK**.

If the PC runs the Aurora Edit LD application, additional requirements are as follows:

- The PC must have a video card that supports DirectX 9.0c and that has 32 MB to 128 MB DDR. Recommended video cards that meet this requirement are as follows:
  - GeForce FX 5200 AGP (Note: Use for Dual Monitor Support)
  - ATI Radeon 7500
  - ViewSonic G771 nVidea Quadro PCI-E Series (Quadro NVS 280)
  - PNY Verto GeForce FX5500 Graphics Adapter AGP
  - PNY Verto GeForce FX5500 Graphics Adapter PCI
  - Asus Extreme N6600 Graphics Card

  An incompatible video card displays the following symptoms upon launch of Aurora Edit LD:

- The Timeline Video Display is grayed out. No clips can be loaded into the Timeline or Source Tool.
- The Timeline Video Display is black even after a clip is loaded into the Source Tool or a Timeline EDL is opened from the bin.

Also refer to the Aurora Edit LD Readme file, which you can find on the Aurora Edit LD Installation CD.

Continue with the next procedure "Configure Aurora Browse Licenses".

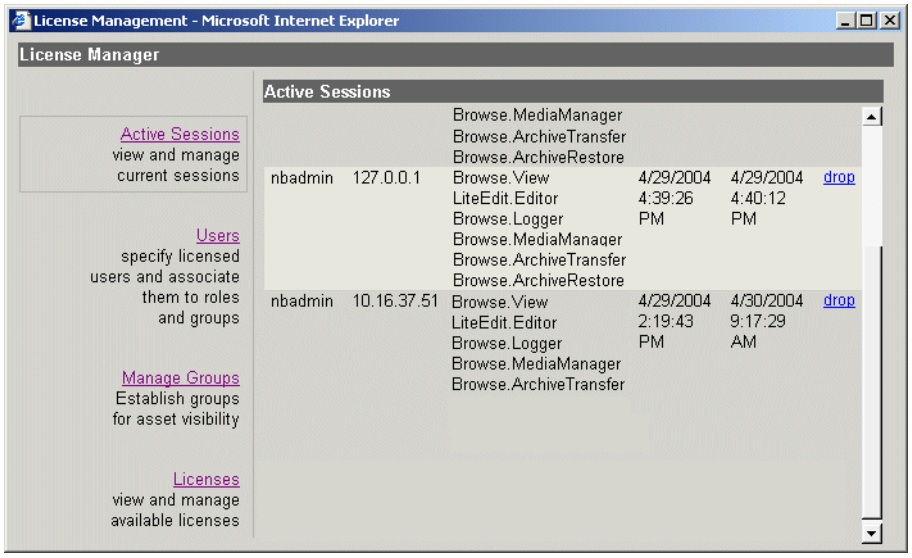
Configure Aurora Browse Licenses

You must configure the MediaFrame server as per your Aurora Browse license to allow user access to Aurora Browse application features.

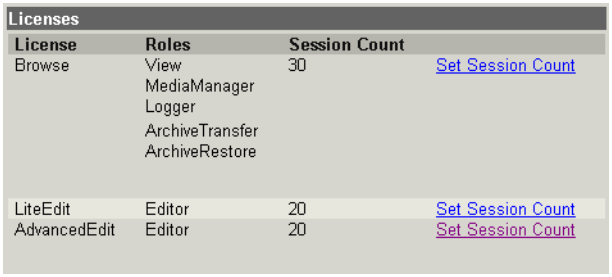
To configure for Aurora Browse licenses, do the following:

1. From the Aurora Browse Launch page, click **License & User Management**. This requires that you log in as Aurora Browse administrator.
   - Login: `root-nb-srv\nbadmin`
   - Password: (contact Grass Valley Support for password)

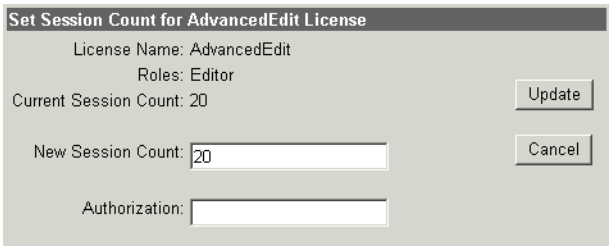
   The License Manager page opens.



2. Click **Licenses**. The Licenses page is displayed.



3. Click **Set Session Count** next to the applicable license. The Set Session Count for … page is displayed.



4. Enter the appropriate number of licenses purchased (be sure to include any previously purchased license counts). You must provide the proper password to change this value. Click **Update** to save changes.
5. On the MediaFrame server, restart ISS services. Click **Start | Run** and run `issrestart`.

Users must be set up to allow access to the Aurora Browse application from a Aurora Browse client PC. To do this, you must continue with the next section "Administering Aurora Browse user access".

Administering Aurora Browse user access

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:

- "Configure Aurora Browse Groups" on page 110
- "Configure Aurora Browse Users" on page 111
- "Managing Aurora Browse User sessions" on page 113

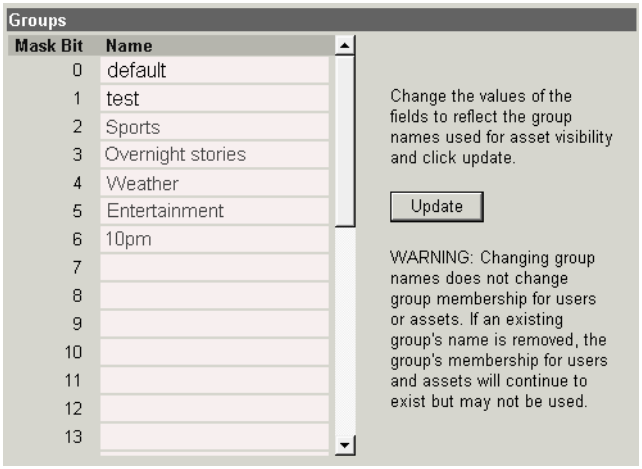
Configure Aurora Browse Groups

The purpose of Aurora Browse groups is to manage a user's access to assets. The Aurora Browse administrator can create groups and assign the groups individually to users. Using the Aurora Browse application, groups can also be assigned to individual assets. In this way each user's access is restricted to the assets in their assigned groups.

Configuring Aurora Browse groups is optional. If you do not configure Aurora Browse groups, users and assets are all assigned to the default group, so all users have access to all assets.

To configure Aurora Browse groups, do the following:

1. From the License Manager page, click **Manage Groups**. The Groups page is displayed.



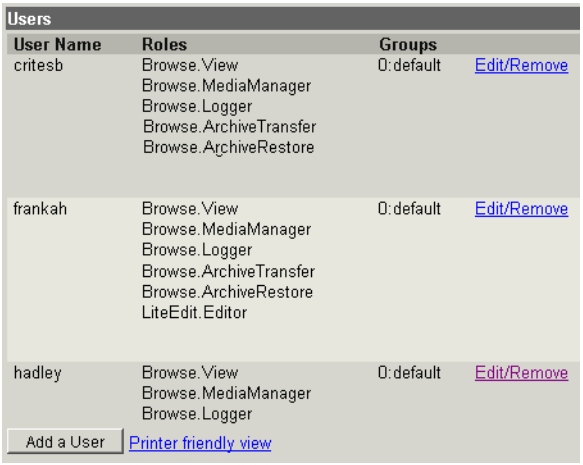
2. Enter names to define groups according to the workflow with which the system is used.
3. Click **Update** to save changes.

Continue with the next procedure "Configure Aurora Browse Users".

Configure Aurora Browse Users

You must add Aurora Browse users before using the Aurora Browse application from any Aurora Browse client PC. The Aurora Browse application only allows access by users that have been added, as explained in the following procedure.

1. From the License Manager page, click **Users**. The Users page is displayed.



2. To add new Aurora Browse User, click **Add a User**. To modify an existing Aurora Browse user, click the **Edit/Remove** link for the user. The Update User page is displayed.

3. 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 will have access. The Roles listed are dependent upon current licensing.The following table defines the Roles:

Role	Description
Browse.View	Lets you browse for video clips and view them.
Browse.MediaManger	Also lets you change the metadata including clip expiration; you can schedule and execute purge.
Browse.Logger	Also lets you modify custom fields and keywords.
Archive.SendToArchive	Lets you transfer high-res assets from a Profile system to an archive device and optionally delete the high-res assets from the Profile system.
Restore.RestoreFrom Archive	Lets you restore high-res assets from an archive device to a Profile system.

Role	Description
LiteEdit.Editor	Lets you do cuts-only editing.
AdvancedEdit.Editor	Lets you use the Aurora Edit LD program, which lets you use the editing features of Aurora Edit.

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.

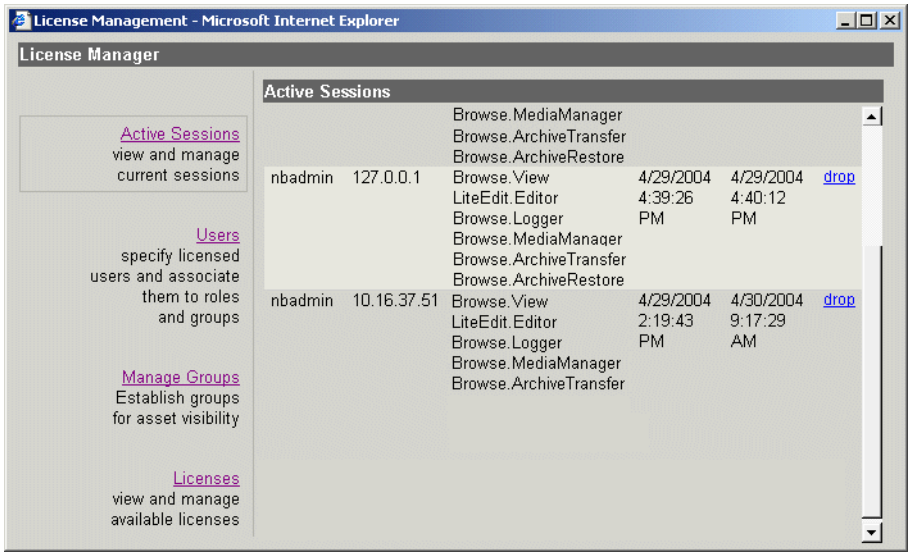
- Groups — Select the groups for which the user will be allowed to access media assets.

4. Click **Add** for new users, or **Update** to modify existing users. You can also click **Delete** to remove a user from the Aurora Browse system.
5. Repeat the previous two steps to add additional users.
6. Click **Update** to save changes.
7. On the MediaFrame server, restart ISS services. Click **Start | Run** and run `issrestart`.

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. From the License Manager page, click **Active Sessions**. The Active Sessions page is displayed.



2. Click the **drop** link to drop a user's current active session.

Adding custom fields

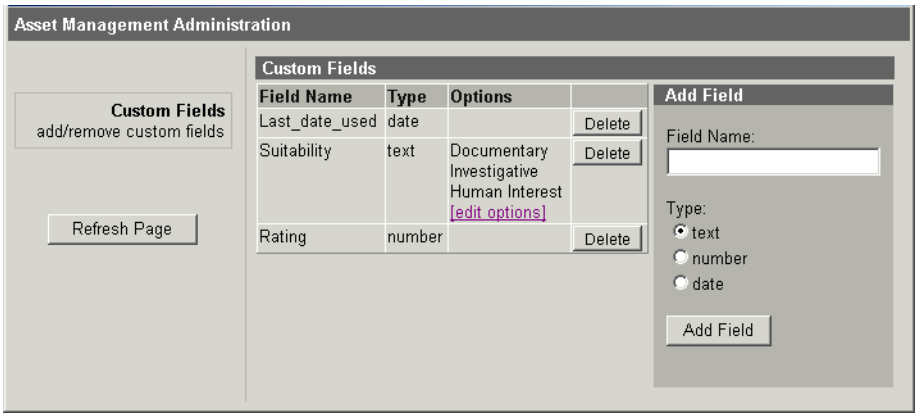
The purpose of custom fields is to enhance site-specific management of assets. The Aurora Browse administrator defines a custom field to create an asset metadata-type that uniquely fits the site's workflow. The user of the Aurora Browse application can then assign metadata to an asset by entering text or making a selection in the custom field.

Adding custom fields is optional.

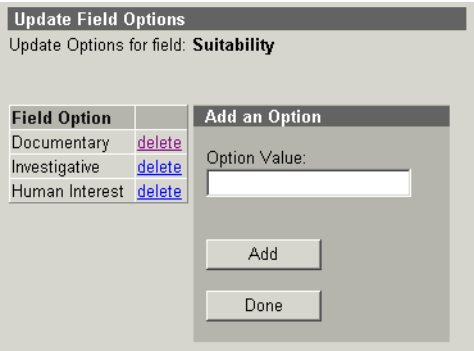
To configure custom fields, do the following:

1. From the Aurora Browse Launch page, click **Asset Management Administration**. This requires that you log in as Aurora Browse administrator.
   - Login: *root*`-nb-srv\nbadmin`
   - Password: (contact Grass Valley Support for password)

   The Asset Management Administration page opens.



2. For each custom field you add, do the following:
   a. Enter a field name.
   b. Select the type of field as follows:
      - Text — A free-entry text field or a drop down list of selections that you define, as explained in the next step in this procedure.
      - Number — A field in which only numbers can be entered.
      - Date — A field that, when clicked, opens a calendar from which a date can be selected.
   c. Click **Add Field**.
3. If you are adding a text field, you have the following options:
   - To allow text to be freely entered in the field, no further configurations are necessary. Skip to the next step in this procedure.
   - To provide a pre-defined list of selections for the field, click **Edit Options** for the field. The Update Field Options page opens.



For each selection that is to be on the list, enter its text and click **Add**. You can also click **Delete** to remove a selection from the list. When the list is complete, click **Done**.

4. Click **Add Field** and **Delete** as necessary to complete your custom fields. To view your latest changes, click **Refresh Page**.
5. Open the Aurora Browse application, select an asset, and click **Custom**. Your custom fields are available to assign metadata to the asset.

Testing Aurora Browse client operations

To perform a quick check that the web and database services are accessible to a client PC, do the following:

1. Log in to a client machine.
2. Open Internet Explorer 6 and browse to the following URL:

   http://iron-nb-svr/nbui.

   In this example, **iron-nb-svr** is the host name or IP address of the MediaFrame server.
3. Click **Launch Aurora Browse Application**. You are now logged into the Aurora Browse application website and should have assets available for browsing.

Chapter 4

Recovery Planning

Establish a recovery plan in the event an Aurora Browse and/or MediaFrame machine 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 and/or 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 Advanced Encoder. N+1 redundancy is achieved by adding an extra Advanced 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 shipping 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.

Modifying the database maintenance plan

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

The MediaFrame server utilizes 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.

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. 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 | Thomson**.

MediaFrame troubleshooting tools

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

Asset System Client — This utility on the MDI server provides a view of the events generated by Managed Device Interface services configured in the system.

Configuration Tool — This tool can check network connectivity (ping) from the MediaFrame server to all the machines in the system. Open the configuration tool on the MediaFrame server at **Start | Thomson | Aurora Browse | Utilities**.

Remoting Host Controller — This utility on the MDI server manages Profile Managed Device processes.

Aurora Transfer — This is an application by which you have visibility via the MDIs to the media files on managed devices. You can do a manual drag-and-drop transfer between devices in Aurora Transfer. Refer to the *Aurora Transfer Instruction Manual*.

Proxy troubleshooting tools

Transfer Client — This encoder utility is used to test scavenge and transcode operations. Refer to "Test: Advanced encoder stand-alone stage - high-res source" on page 77.

Smart Bin Encoder Status — On the Aurora Browse launch page, this page displays the status of all Smart Bin Encoders in the system. This page displays the list of all jobs attempted by the Smart Bin Encoders. For each job, the following are provided:

- encoder name
- the source and destination file names
- the time the job was run
- job status (with error information if the job was unsuccessful)
- job completion percentage (if job is currently running)

Proxy troubleshooting tips

Use the following table to identify and resolve problems related to the creation and storage of low-res proxy assets.

Symptom	Solution
An operational Browse scavenge system (on an Open SAN) suddenly stops working or there is a drop in scavenge performance for more than an hour.	Debug as follows: 1. Copy and paste a short test clip into the scavenge folder, **note the name and time**. 2. Profile MDI stage: Use the Browse event viewer on the machine running the Profile MDI, verify that the Profile MDI service reports the creation of the new clip. Look for a CREATE_CLOSE message. - If the message doesn't show up, or there are errors in the MDI's log, restart the Profile MDI service. 3. Rules Wizard Stage: Look at the events on the NB server. You're looking for a message from the rules wizard that it received a CREATE_CLOSE message from the Profile MDI. You should then see follow-up messages as a new job is being created and sent to the Sequential encoder. - If the message does not arrive, or the Rules Wizard does not send the job, restart the Rules Wizard service. 4. Sequential Encoder: Look at the events on the Sequential encoder. You'll see a new job showing up and the sequential encoder starting. - If the job does not arrive, restart the Proxy Transfer Service. 5. Server: If the job arrives, but the sequential encoder can't start, check the connection to the target Profile: a. Ping the Profile host name, make sure the ProLink server is running, make sure no other application (i.e. VdrPanel or ConfigManager) is trying to use the playout channel. b. If the connection the Profile appears okay, restart the ProxyTransfer service and run the test again with a new test clip. c. If scavenge still fails, there are a couple of possibilities: - Profile is too busy to respond to request. This can happen if several MediaManager sessions are running in full refresh mode. If so, shut down these sessions. - ProNet is wedged. Restart the Profile. In general, don't reboot the system components such as the encoder or the NB server until you've tried the above
The Aurora Browse client browse comes up with results but thumbnails are missing (broken link indicators where thumbnails should be). Video is also inaccessible.	Check Ethernet connections from NAS to the client network. Check that the client account exists on the NAS. This is the account used to log into the client browse machine.
The Aurora Browse client play back video but scrubbing is poor.	There is too much traffic on the network. Try to isolate Aurora Browse from other network activity. Use a switch rather than a hub for connectivity.
Recording does not start as scheduled for ingest.	Check that encoder, server and client workstation PC clocks are synchronized to house timecode feed (reference NetTime setup instructions). Check that all Thomson services are running on server and encoders (use windows services panel from administrative tools).

Symptom	Solution
Storyboard displays permissions denied error.Timecode does not display with video in clip player.	Check that the server has permissions to access the NAS. Make an initial connection from the server to the NAS by mapping a drive. This establishes the connection for subsequent use - the mapped drive is not used directly.
Video does not load/play in the clip player.	Check that MPEG-1 exists by navigating to the “related” tab in the details display area. If an MPEG link appears, click on it. If video plays then install the “live feed filter” on the client. This can be found from the Client setup link on the Aurora Browse launch page. If video does not display, check that the client has permissions on the NAS.

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.

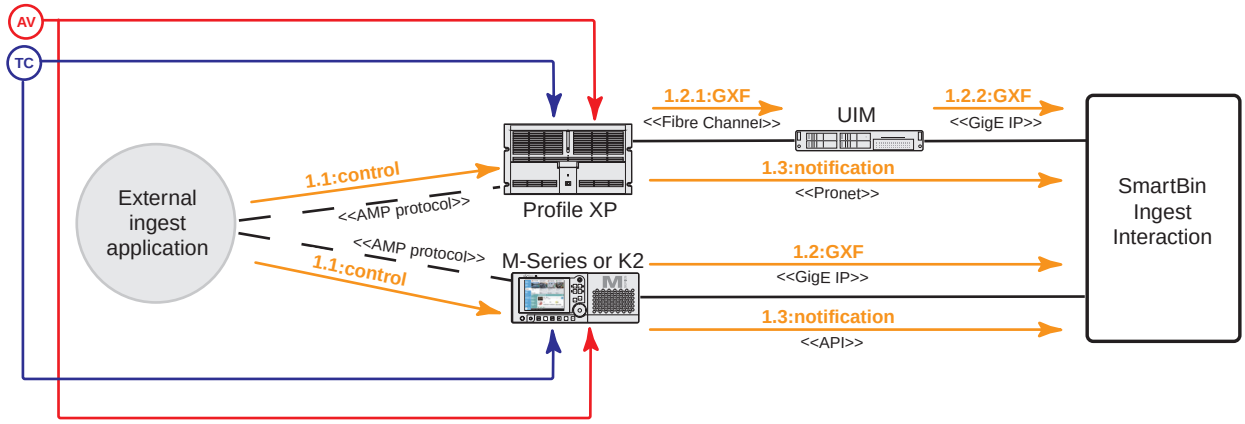
Symptom	Solution
Problem accessing the Aurora Browse application with Internet Explorer - cannot find server or DNS error.	Check the server name or IP address used in the browse address. Check that the server is running. Check that the server is connected to the client network. Check that connections are secure. Check that IIS is running on the server.
Web application 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 also exists on the server. This is done through the windows administrative tools.
General Browser Issues (esp. after reinstall).	Be sure to clear the browser cache by selecting Tools > Internet Options from the menu. Then from the General tab select the Delete Files button. Check the Delete all offline content checkbox and click OK. Also be sure to update components from the client setup page provided with the Aurora Browse application. The client setup page can be accessed from the Aurora Browse launch page.

Appendix **A**

Component Interaction Diagrams

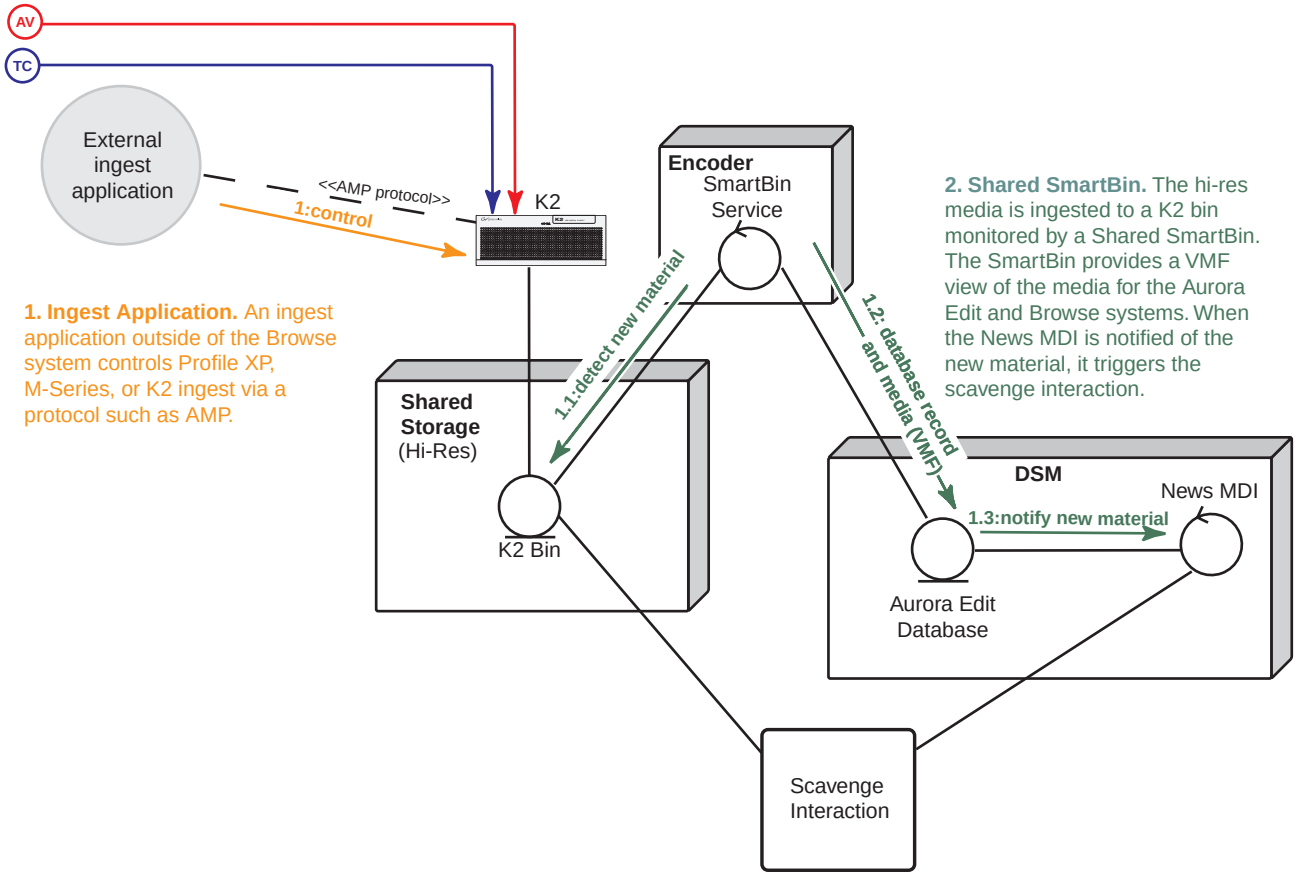
This appendix provides diagrams and explanations of how the system software components interact.

External Ingest Application to Transfer SmartBin

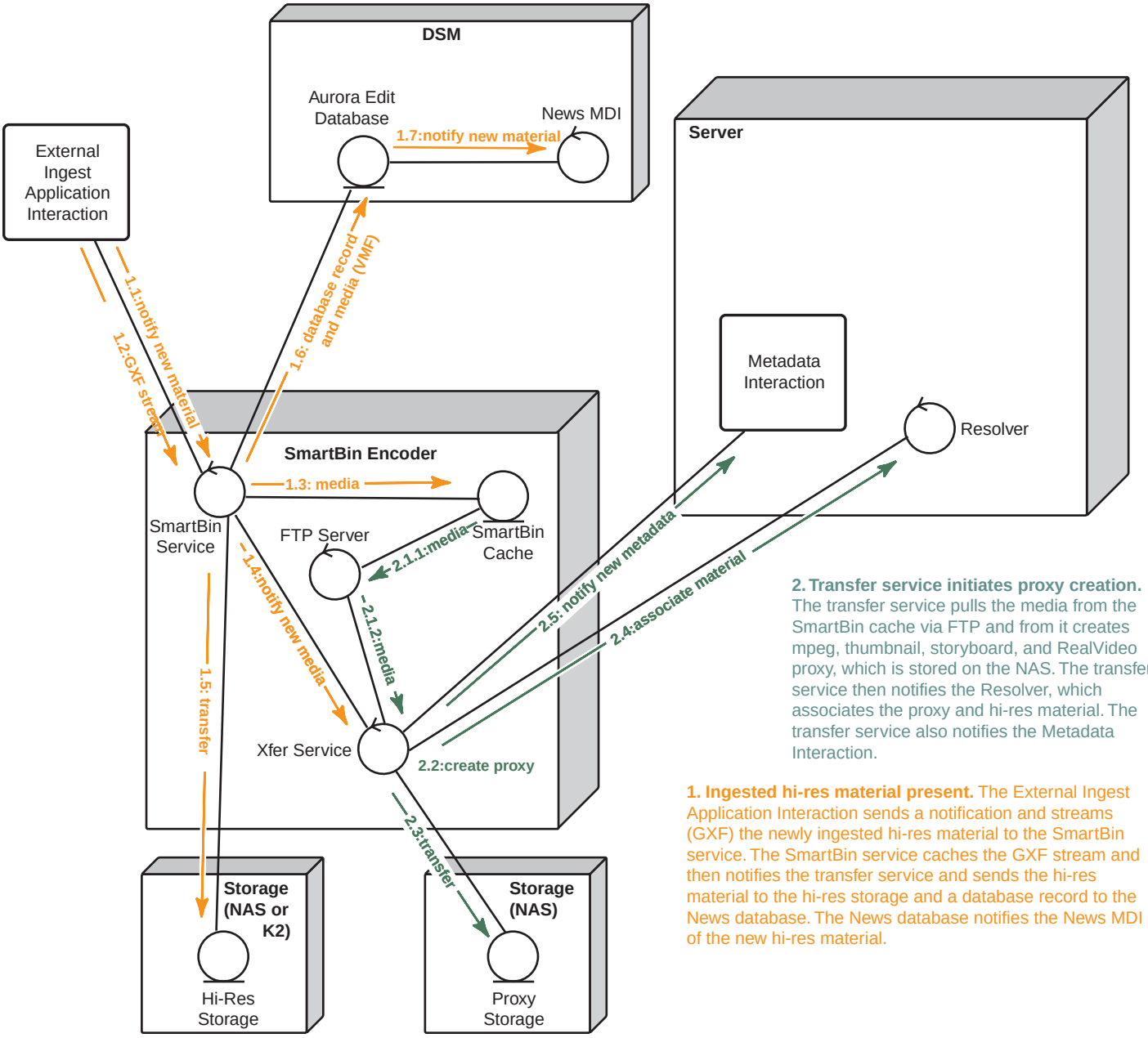


1. Ingest Application. An ingest application outside of the Browse system controls Profile XP, M-Series, or K2 ingest via a protocol such as AMP. When hi-res media is ingested, the Profile XP or M-Series sends the media as a GXF stream and sends a notification about the newly ingested media to the SmartBin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

External Ingest Application to Shared SmartBin



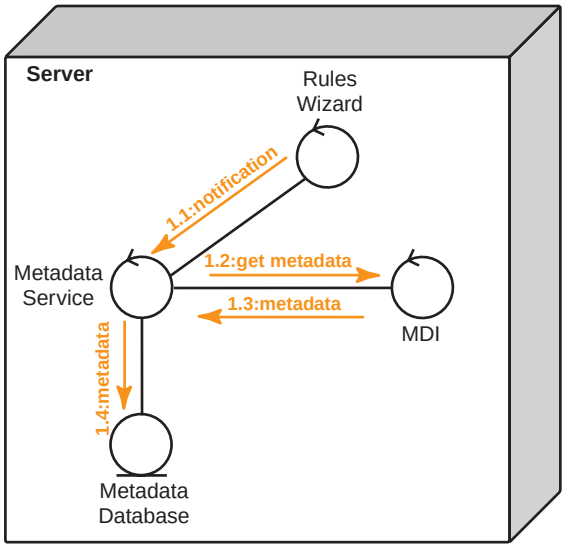
Transfer SmartBin Ingest



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

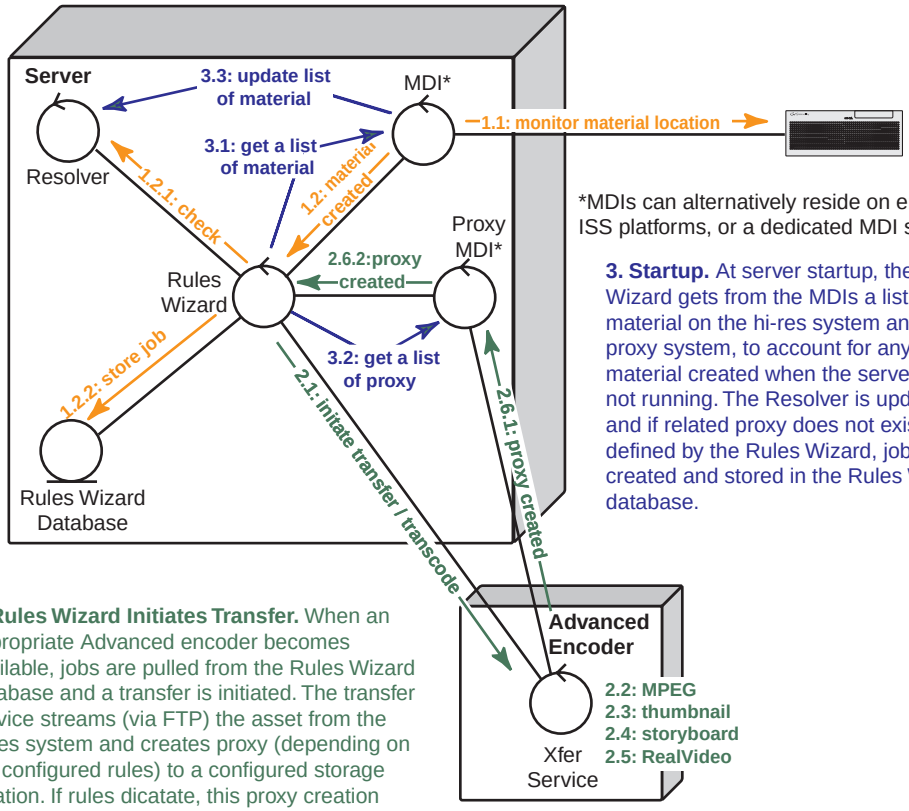


1. Metadata. When the Rules Wizard or transfer service initiates the creation or modification of proxy, it notifies the Metadata Service. The Metadata Service gets the new or modified metadata from the MDI that has knowledge of the associated hi-res material and puts it in the metadata database.

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.



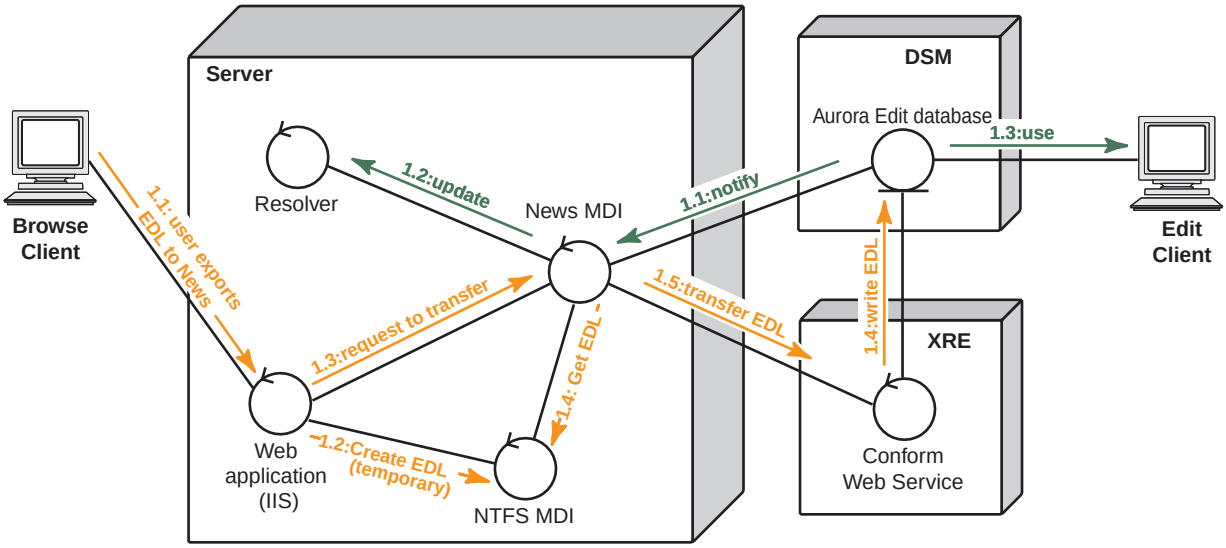
*MDIs can alternatively reside on encoders, ISS platforms, or a dedicated MDI server.

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.

EDL Export to Aurora Edit database

This export functionality converts the Aurora Browse EDL into a Aurora Edit sequence. After the conversion the EDL is available to Aurora Edit for modification.

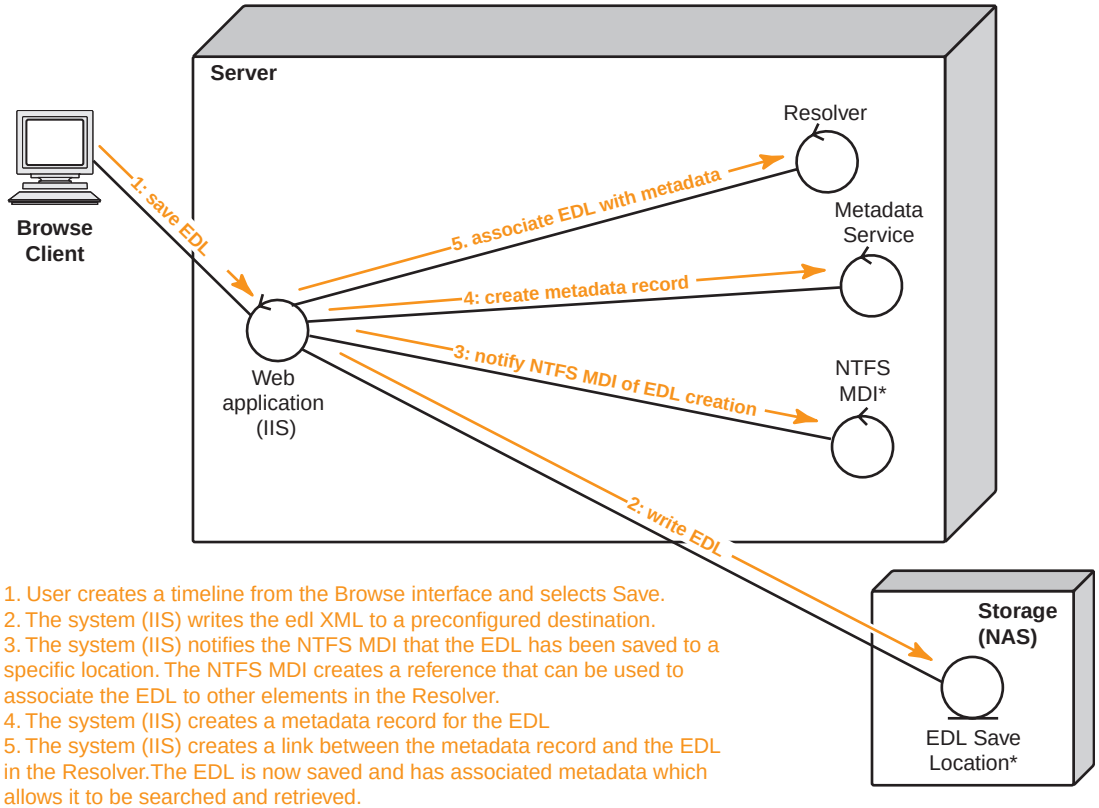


1. Export. User creates a timeline from the Browse interface and exports it to Edit. The system (IIS) requests that the News MDI transfers the EDL to the Conform Web Service. The Conform Web Service converts the Browse EDL to a Edit compatible EDL and pushes the EDL to the Aurora Edit database.

2. Identify as Browse asset. The Aurora Edit database notifies the News MDI of the EDL. The News MDI updates the Resolver so the EDL asset, now on Edit, is visible to Browse. The EDL is also available to Edit.

EDL Browse save

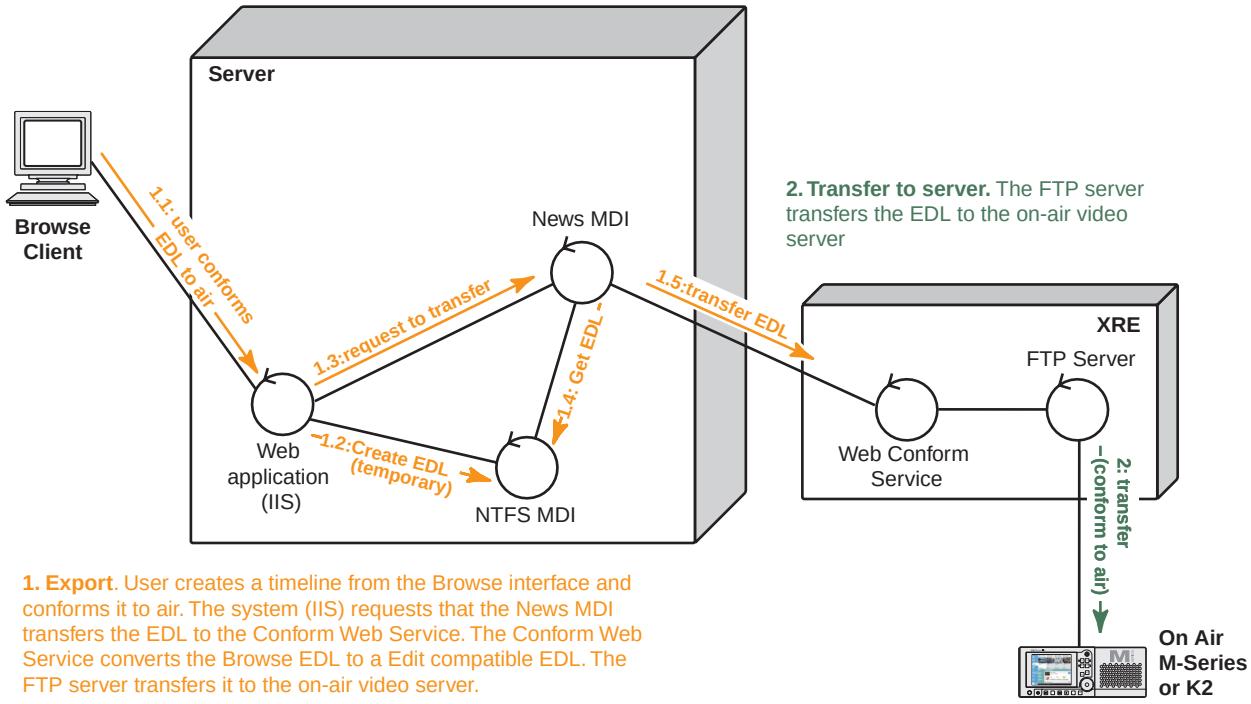
This save functionality retains the EDL in the Browse domain for further modification with the Aurora Browse application.



1. User creates a timeline from the Browse interface and selects Save.
2. The system (IIS) writes the edl XML to a preconfigured destination.
3. The system (IIS) notifies the NTFS MDI that the EDL has been saved to a specific location. The NTFS MDI creates a reference that can be used to associate the EDL to other elements in the Resolver.
4. The system (IIS) creates a metadata record for the EDL
5. The system (IIS) creates a link between the metadata record and the EDL in the Resolver.The EDL is now saved and has associated metadata which allows it to be searched and retrieved.

EDL Conform via Aurora Edit

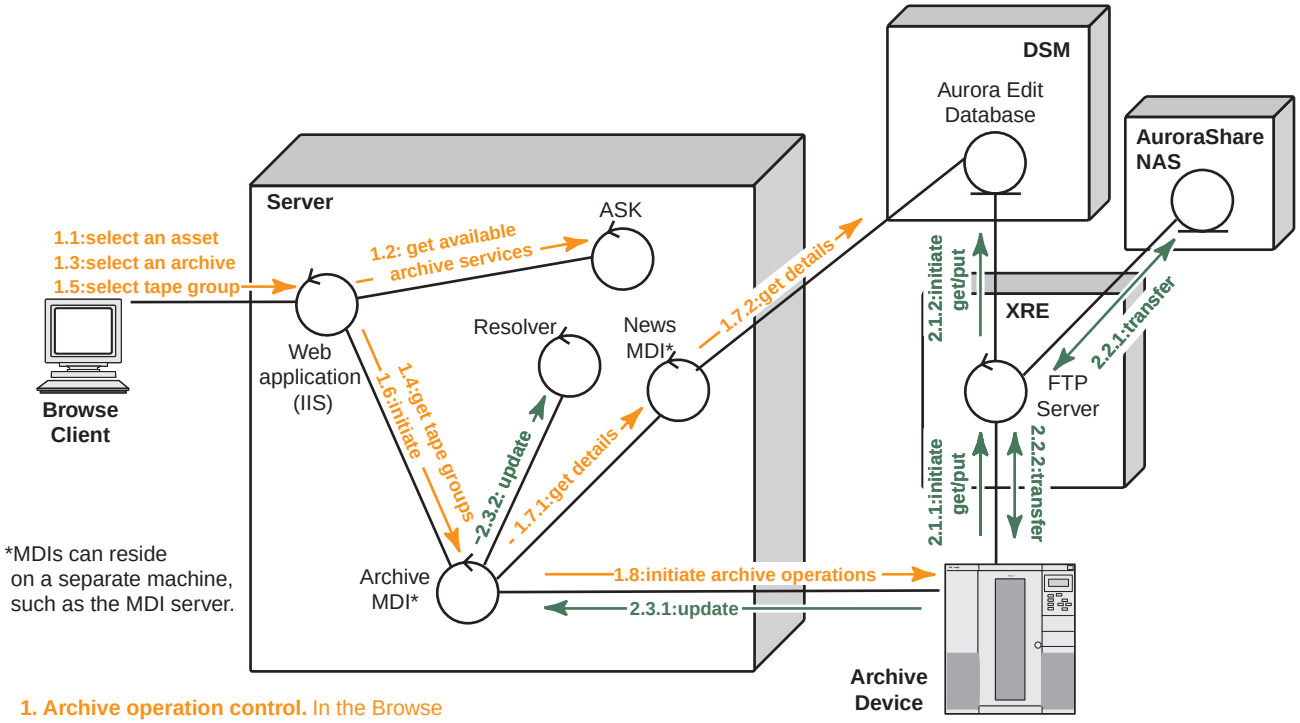
This conform functionality converts the EDL into a Aurora Edit EDL and automatically places it on the designated on-air video server.



2. Transfer to server. The FTP server transfers the EDL to the on-air video server

1. Export. User creates a timeline from the Browse interface and conforms it to air. The system (IIS) requests that the News MDI transfers the EDL to the Conform Web Service. The Conform Web Service converts the Browse EDL to a Edit compatible EDL. The FTP server transfers it to the on-air video server.

Archive operations on Aurora system

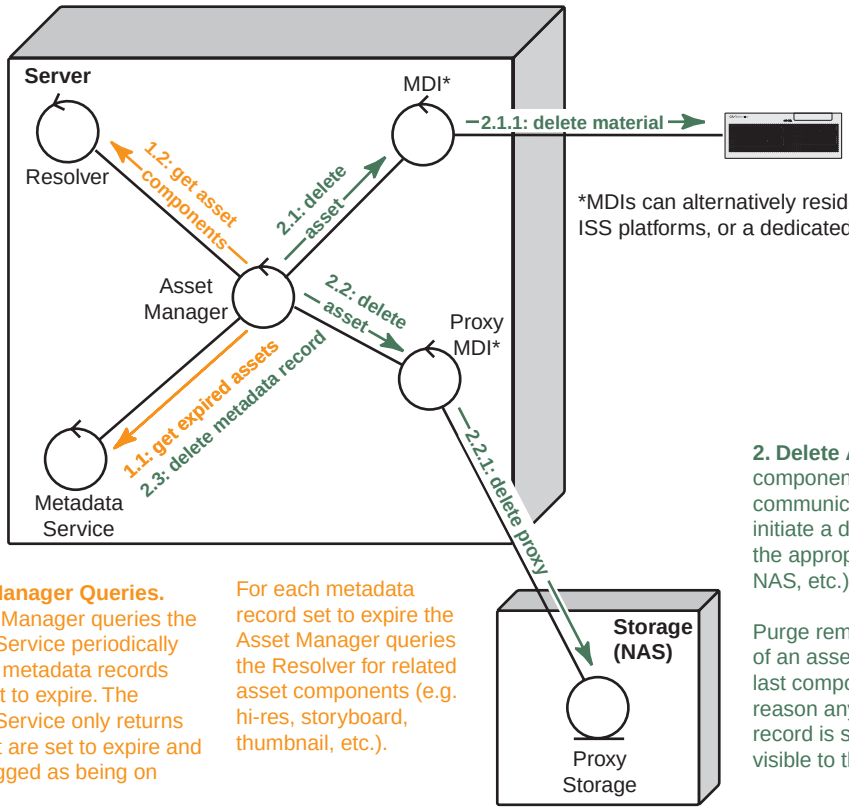


1. Archive operation control. In the Browse application, the user selects an asset, navigates to the management tab, and selects the archive option. The system queries the ASK for available archive devices. (Also filters out for hi-res material that already exists in archive by querying the Resolver). 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**

Legacy systems

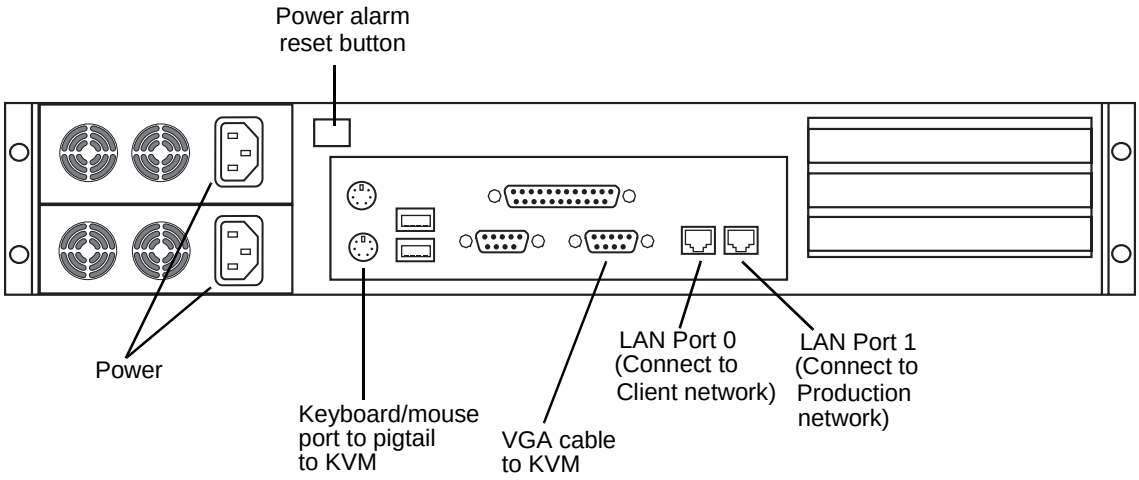
This appendix documents system architectures, hardware platforms, and software components that are no longer recommended for new systems, but that are retained in existing systems and supported by current software releases.

NAS instructions - 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



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:

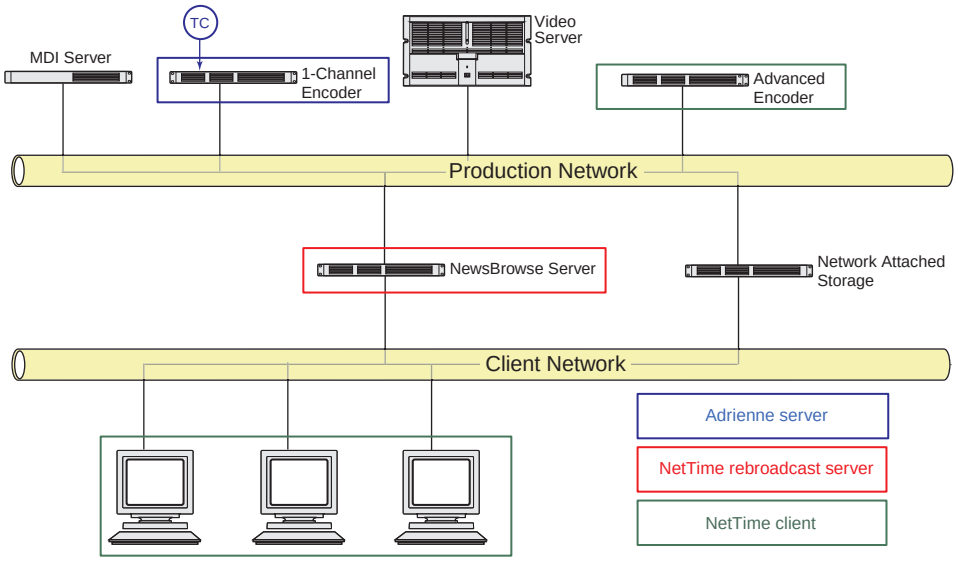
   HKEY_LOCAL_MACHINE/SOFTWARE/Tektronix/Profile/ShuttleAtMode

   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

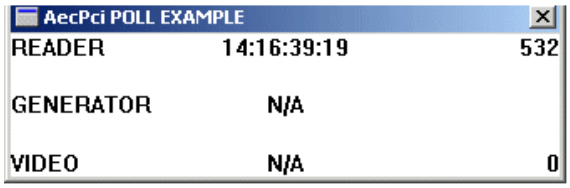
You use one single-channel encoder as the primary Adrienne Absolute Time Server, and another single-channel encoder as the secondary (redundant) Adrienne Absolute Time Server. A LTC connection to house timecode is required for single-channel encoders functioning as Adrienne Absolute Time Servers.

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



   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 (i.e. 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.

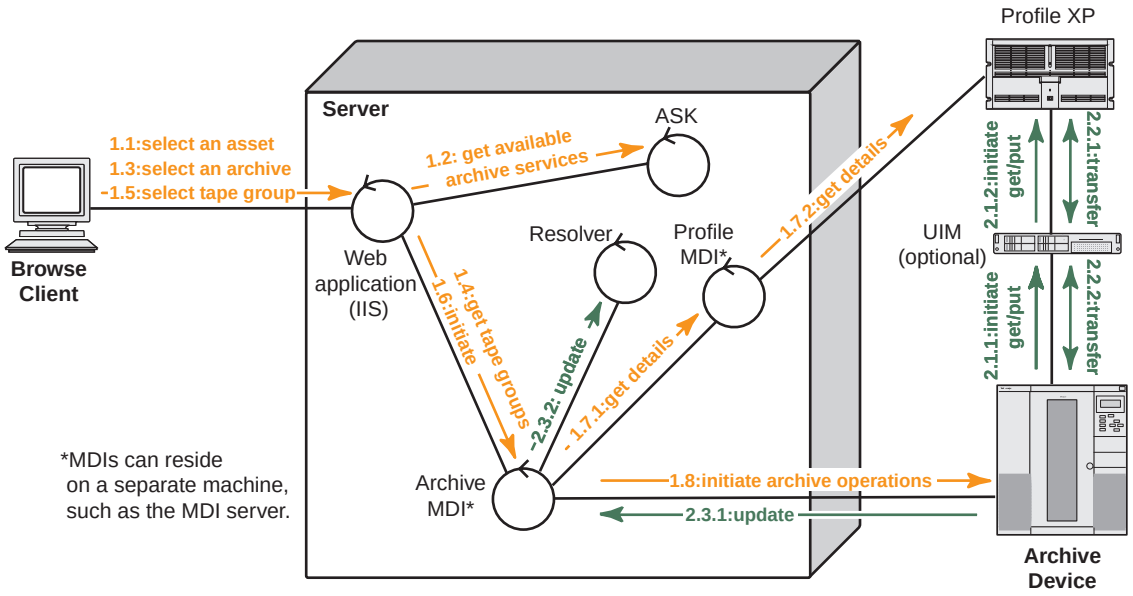
```
#-------------------------------------------------------
#General Host Table
#-------------------------------------------------------

#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 35.
- 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



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

P

R

S

T

U

W

Z