

AURORA BROWSE

MEDIA ASSET MANAGEMENT



Installation and Configuration Guide
Software Version 7.0



Affiliate with the N.V. KEMA in The Netherlands



CERTIFICATE

Certificate Number: 510040.001

The Quality System of:

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

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

15655 SW Greystone Ct.
Beaverton, OR 97006
United States

10 Presidential Way
Suite 300
Woburn, MA 01801
United States

Kapittelweg 10
4827 HG Breda
The Netherlands

7140 Baymeadows Way
Ste 101
Jacksonville, FL 32256
United States

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

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

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

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

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

Spinnereistrasse 5
CH-5300 Turgi
Switzerland

Brunnenweg 9
D-64331 Weiterstadt
Germany

Carl-Benz-Strasse 6-8
67105 Schifferstadt
Germany

Including its implementation, meets the requirements of the standard:

ISO 9001:2008

Scope:

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

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

H. Pierre Sallé
President
KEMA-Registered Quality

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

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

CRT 001 073004

Accredited By:
ANAB

Experience you can trust.

AURORA BROWSE

MEDIA ASSET MANAGEMENT



Installation and Configuration Guide

Software Version 7.0

Copyright

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

Disclaimer

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

U.S. Government Restricted Rights Legend

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

Trademarks and Logos

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

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



Revision Status

Rev Date	Description
January 31, 2003	Release to part number 071-8217-00
July 21, 2003	Release for software version 1.5. Part # 071-8217-01
May 25, 2004	Release for software version 2.0. Part # 071-8307-00.
December 16, 2004	Release for software version 2.7. Info on Advanced Encoder, FlashNet archive, and DIVArchive. Part # 071-8307-01.
August 2, 2005	Release for software version 3.0. New content for NewsShare NAS. Part # 071-8424-00.
April 27, 2006	Release for software version 3.1. Part # 071-8424-01.
September 22, 2006	Release for Aurora software version 6.0b. Part # 071-8518-00.
September 5, 2007	Release for Aurora software version 6.3. Part # 071-8518-01.
November 1, 2008	Release for Aurora software version 6.5. Part # 071-8637-01.
April 6, 2010	Updated to reflect new Alloy look, simple database model, SiteConfig installation. Part # 071-8637-02.

Contents

	Preface	9
	Grass Valley Product Support	10
	Telephone Support	10
	International Support Centers	10
	Authorized Local Support Representative	10
Chapter 1	System Overview	
	The MediaFrame system.....	14
	Functional description.....	14
	MediaFrame server	14
	MDI server	15
	Encoder	16
	Low-resolution proxy NAS	16
	Archive.....	16
	Nearline system	17
	Aurora Browse client	17
	K2 BaseCamp Express	17
	Design considerations - Aurora Browse with Aurora Edit.....	17
Chapter 2	Installing the Aurora Browse system hardware	
	Rack-mount hardware components	20
	About cabling hardware components	20
	Cable hardware: MediaFrame support	21
	MediaFrame server instructions	21
	MediaFrame server instructions: HAAR platform	22
	Cabling the HAAR system servers	22
	Configuring the HAAR system network	23
	MDI Server instructions	24
	K2 BaseCamp Express instructions	25
	Cable hardware: Proxy support.....	26
	Encoder instructions	27
	Low-res proxy NAS instructions - Condor	27
Chapter 3	Understanding network system concepts	
	Control network description	29
	Streaming/FTP network description	29
	Media (iSCSI) network description	29
	Corporate LAN network	30
	Firewall considerations	30
	Networking tips	30
	About hosts files	31
	Host table tips.....	32
Chapter 4	Installing the Aurora Browse System Software	
	About SiteConfig	34
	About developing a system description.....	34
	Aurora Browse/MediaFrame installation checklists	35
	Pre-installation planning checklist	35
	Infrastructure checklist.....	36
	Network setup and implementation checklist	37
	Software update checklist.....	38
	Configuration checklist	39
	Adding proxy NAS to system description	39
	About the corporate LAN.....	42
	Configuring the corporate LAN.....	43

Adding a group	44
Adding a device to the system description	44
About device and host names	45
Establish conventions	46
Machine naming convention.....	46
MDI and Encoder logical names convention	46
Ports and services mapping	47
Modifying a device name	48
About IP configuration of network interfaces on devices	48
Placeholder device IP configuration	48
Discovered device IP configuration	49
Modifying unassigned (unmanaged) network interfaces on MediaFrame devices..	49
About SiteConfig support on MediaFrame devices	51
Discovering devices with SiteConfig	52
Assigning discovered devices	53
Modifying MediaFrame device managed network interfaces	54
Making the host name the same as the device name	57
Pinging devices from the control point PC	58
About hosts files and SiteConfig	58
Generating host tables for devices with SiteConfig.....	59
Create record of software installed on devices	60
Where to install Browse/MediaFrame software roles	60
Removing a software role from a device	62
Adding a software role to a device	62
Distribute devices into deployment groups	62
Setting deployment options	63
Configuring deployment groups	66
Install prerequisite files on the control point PC	67
About deploying software	67
Add software package to.....	
deployment group for Aurora Browse devices	68
Installing software on Aurora Browse devices	69

Chapter 5

Configuring the system

Configuration overview - K2 storage	72
Prepare for core configuration stages	73
Prepare MediaFrame Server for News systems.....	73
Prepare encoders.....	73
Add encoders to the K2 Storage System	73
Configuring encoders with the K2 System Configuration application	74
Calculating encoder bandwidth	78
Prepare NAS - Condor	79
About the administrator account.....	80
Accessing services	80
Accessing system configuration settings.....	81
MediaFrame stage	82
Configure MediaFrame ASK: Register components	84
Configuring transfer targets	87
Configuring round robin transfers.....	88
Configure ASK Location: MDI server	89
Configure Generic FTP MDI	90
Configure K2 MDI	92
Configure K2 Summit MDI.....	94
Configure M-Series MDI	97
Configure News MDIs	99
Configure Profile MDI	101
Configure Proxy MDI	103

Test: MediaFrame stage.....	104
Checklist: MediaFrame stage	104
Encoder stand-alone stage	105
Configure SmartBin Encoder.....	106
Configure Aurora Proxy Encoder.....	110
Configure multiple proxy encodes on Aurora Proxy Encoder	112
Configuring the encoder for unicode languages.....	113
Checklist: Encoder stand-alone stage	114
Encoder + Server stage.....	115
Configure Media Frame Core ASK: Encoder	115
Configure Rules Automation: Encoder	116
About configuring rules	118
Tips for configuring rules	119
Configure Assets Tab	119
About expired assets	119
Test: Encoder + Server stage - high-res source.....	120
Checklist: Encoder + Server stage	120
Configure NTFS MDI	121
Archive stage.....	123
Add archive MDI	124
Verify archive preparations.....	125
DIVA preparations	125
FlashNet preparations	126
Network connectivity - all archive types.....	127
Configure DIVA MDI	128
Configure FlashNet MDI	129
Checklist: Archive stage	130
Deploy remaining machines for full system.....	131
Test system level interactions	131
Multiple scavenge test	131
Purge test	131
Add Aurora Browse Clients	132
Connect server and NAS to customer LAN	132
Configure Aurora Browse Licenses	133
Verify license status and user sessions.....	134
Managing Aurora Browse User sessions	135
Adding custom fields and metadata mapping	136
Setting up metadata mapping.....	136
About bin and asset naming limitations.....	139

Chapter 6

Database and Recovery Planning

Database planning and maintenance strategies	141
Encoder failure considerations	141
MediaFrame server failure considerations	142
Updating the database to the simple model	142
Creating a simple maintenance plan	143
Configuring the MediaFrame maintenance plan.....	143
Using the simple maintenance plan.....	144
Verifying the database maintenance plan status.....	145
Testing the backup	146
Reconfiguring MediaFrame after renaming the server	146
Modifying the database maintenance plan	147
Modifying the maintenance plan backup location	147
Modifying the maintenance plan schedule.....	147
Restoring the MediaFrame server database	148
Updating the maintenance plan after renaming the server.....	148
Modifying the database for non-English searches.....	150

	Backup and recovery strategies	151
	About the recovery disk image process	151
	Creating a recovery disk image for storing on E:	153
	Creating a recovery disk image CD set	154
	Restoring from a system-specific recovery disk image on E:	156
	Restoring from the generic recovery disk image on E:	157
	Restoring from a recovery disk image CD set	162
	Activating the Windows operating system	163
Chapter 7	Troubleshooting the system	
	Troubleshooting tools	165
	MediaFrame troubleshooting tool	165
	Aurora Browse application troubleshooting tips	166
Appendix A	Component Interaction Diagrams	
	External Ingest Application to Transfer SmartBin	167
	External Ingest Application to Shared SmartBin	168
	Transfer SmartBin Ingest	169
	Metadata	170
	Scavenge	171
	Archive operations on Aurora system	172
	Purge	173
Appendix B	K2 BaseCamp Express	
	Configuring K2 BaseCamp Express	175
	Configuring encoders for K2 BaseCamp Express	176
	Configuring the low-res storage on the K2 BaseCamp Express server	177
	Upgrading K2 BaseCamp Express	177
	Using K2 BaseCamp Express	178
Appendix C	Legacy systems	
	NAS instructions - Fastora	180
	Prepare NAS - Windows Fastora	181
	Verify NAS access	184
	NAS instructions - Serial ATA network platform	185
	Prepare Profile Media Servers	186
	NetTime system	187
	Prepare NetTime	187
	Prepare NetTime servers	188
	Prepare NetTime clients	188
	Prepare NAS - Serial ATA network platform	189
	Prepare NAS - Linux Fastora	192
	Host table files	192
	Adding and configuring an Avalon archive	194
	Avalon archive preparations	194
	Add archive MDI	194
	Configure Avalon MDI	196
	Archive operations on Profile XP	197
Appendix D	Installing and configuring the FileZilla Server	
	Configuring the Generic FTP MDI for FileZilla	199
	Installing and configuring FileZilla	199
	Testing the FileZilla configuration	201
	Index	203

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 Payout

Grass Valley Product Support

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

Web Technical Support

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

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

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

Telephone Support

Use the following information to contact Product Support by phone.

International Support Centers

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

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

Authorized Local Support Representative

A local support representative may be available in your country. To locate a support center during normal local business hours, refer to the following list. This list is regularly updated on the website for Grass Valley Product Support (<http://www.grassvalley.com/support/contact/phone/>).

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

Region	Country	Telephone
Asia	China	+86 10 5883 7575
	Hong Kong, Taiwan, Korea, Macau	+852 2531 3058
	Japan	+81 3 6848 5561
	Southeast Asia - Malaysia	+603 7492 3303
	Southeast Asia - Singapore	+65 6379 1313
	India	+91 22 676 10300
Pacific	Australia	1 300 721 495
	New Zealand	0800 846 676
	For callers outside Australia or New Zealand	+61 3 8540 3650
Central America, South America	All	+55 11 5509 3440

Region	Country	Telephone
North America	North America, Mexico, Caribbean	+1 800 547 8949 +1 530 478 4148
Europe	UK, Ireland, Israel	+44 118 923 0499
	Benelux – Netherlands	+31 (0) 35 62 38 421
	Benelux – Belgium	+32 (0) 2 334 90 30
	France	+800 80 80 20 20 +33 1 48 25 20 20
	Germany, Austria, Eastern Europe	+49 6150 104 444
	Belarus, Russia, Tadjikistan, Ukraine, Uzbekistan	+7 095 258 09 20 +33 (0) 2 334 90 30
	Nordics (Norway, Sweden, Finland, Denmark, Iceland)	+45 40 47 22 37 +32 2 333 00 02
	Southern Europe – Italy	Rome: +39 06 87 20 35 28 ; +39 06 8720 35 42. Milan: +39 02 48 41 46 58
	Southern Europe – Spain	+34 91 512 03 50
	Switzerland	+41 56 299 36 32
Middle East, Near East, Africa	Middle East	+971 4 299 64 40
	Near East and Africa	+800 80 80 20 20 +33 1 48 25 20 20



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

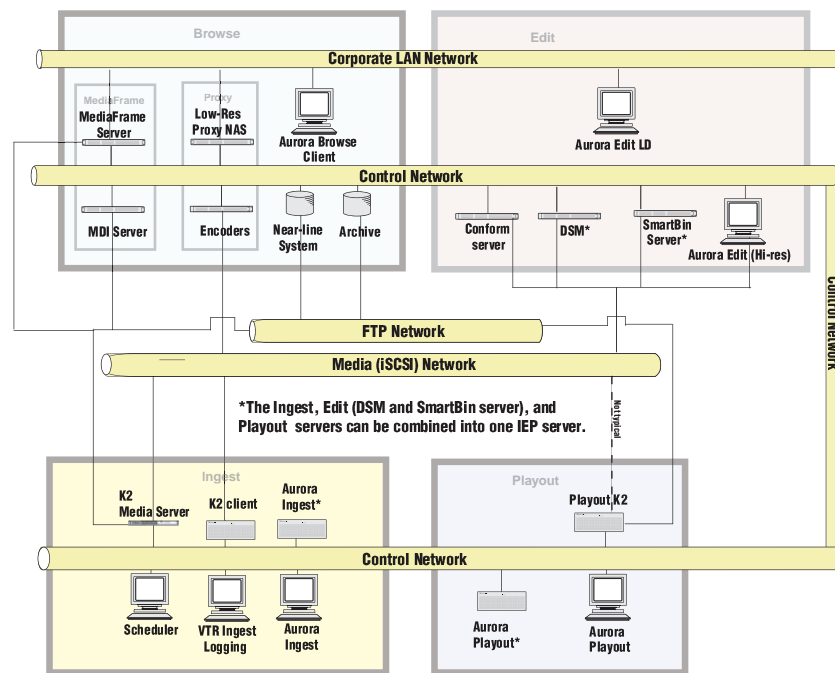


Chapter 1

System Overview

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

The following diagram illustrates the Aurora system.

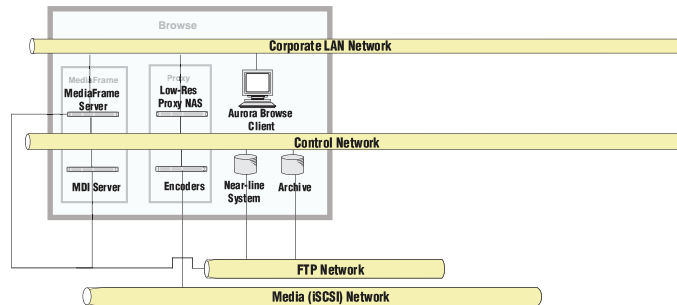


This chapter includes the following topics:

- “The MediaFrame system” on page 14
 - “Functional description” on page 14
 - “MediaFrame server” on page 14
 - “MDI server” on page 15
 - “Encoder” on page 16
 - “Low-resolution proxy NAS” on page 16
 - “Aurora Browse client” on page 17
 - “Archive” on page 16
 - “Nearline system” on page 17
 - “K2 BaseCamp Express” on page 17
- “Design considerations - Aurora Browse with Aurora Edit” on page 17

The MediaFrame system

The following diagram illustrates the MediaFrame system.



Functional description

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

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

For descriptions of software components, refer to [“Component Interaction Diagrams” on page 167](#).

MediaFrame server

The MediaFrame server contains a repository of all information about the Aurora Browse/MediaFrame system, including what devices are in the system, what the roles are for each device (for example, transfer or storage locations), and which device hosts the required software. Other devices in the system refer to the MediaFrame server for necessary information during configuration or while the system is operating.

The MediaFrame server includes:

- MediaFrame Core Services
 - Ask
 - Metadata Service
 - Resolver
 - Rules Wizard

- Subscription Manager
- Transfer Manager
- License Manager
- MediaFrame database
- Aurora Browse Application Installer
- Proxy MDI
- NTFS MDI
- Other MDIs (*see* MDI server)

MDI server

A machine that hosts an MDI (Managed Device Interface) service takes the role of an MDI server. In larger systems, a separate MDI server hosts the MDIs and connects to other devices on the control network. For smaller systems, the MDI server can be combined with the MediaFrame 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 [“The MediaFrame system” on page 14](#).

Dedicated MDI server — For medium to large MediaFrame systems, to ensure system performance, most MDI services are on a stand-alone MDI server machine. The MDI server requires only control network communication in preparation for its use in the MediaFrame system.

MediaFrame server as MDI server — For small MediaFrame systems, including the K2 BaseCamp Express, the MDI services can reside on the MediaFrame server. The MediaFrame server also has the NTFS MDI service installed, as it is required to run on the server, regardless of the size of the system.

Depending on your system, the MDI server can include:

- Archive MDI (Diva or Flashnet)
- Generic FTP MDI
- K2 MDI
- K2 Summit MDI
- M-Series MDI
- News MDI
- Profile MDI

NOTE: *The News MDI and Profile MDI cannot be on the same server.*

Encoder

The encoder creates an MPEG-1 proxy version of high-resolution video assets that already exist or are being actively recorded on a video server. The encoder also processes MPEG-1 proxy content and extracts dynamic scene detection images for storyboard/thumbnail creation.

Depending on your system, an encoder can include:

Aurora Proxy Encoder

- Aurora/MediaFrame Proxy Encoder
- Aurora FTP

SmartBin Encoder

- Aurora/MediaFrame Proxy Encoder
- Aurora FTP
- Smart Bins
- Smart Bin Encoder

For more information, see [“Encoder stand-alone stage” on page 105](#)

Low-resolution proxy NAS

The low-resolution (low-res) NAS stores the low-res assets on the network, including:

- Proxy video
- Timecode
- Storyboard
- Thumbnails

The low-res NAS maintains its own file system. For more information on preparing the NAS for the MediaFrame system, see [“Prepare NAS - Condor” on page 79](#).

Archive

Assets can be saved to or restored from archive management software. MDIs on the MediaFrame or MDI server can be configured to specify settings such as source and destination transfer locations.

Depending on your system, assets are archived to:

- Front Porch Digital Diva archive, or
- SGL FlashNet archive

For more information, see [“Archive stage” on page 123](#).

Nearline system

The nearline is a large pool of storage that high-resolution media can be stored. This is considered an “offline” system, which means it stores files only with no ability to record or play those files directly on the system. The files would have to be transferred to an online device to be played.

The nearline system is managed by the Generic FTP MDI. The K2 Nearline Condor NAS is the recommended nearline of choice. For information on how to install and configure the NAS for your K2 system, see the *K2 Storage System Instruction Manual* and the *K2 Lx0 RAID Storage Instruction Manual*.

For information on how to configure the MDI for the K2 nearline, see [“Configure Generic FTP MDI” on page 90](#). Other third-party storage systems can work if they have an FTP server capable of accessing the storage like Filezilla Server. For information on how to configure Filezilla Server for the MediaFrame system, see [Appendix D, *Installing and configuring the FileZilla Server* on page 199](#). Features and limitations may vary base on what system is used.

Aurora Browse client

The Aurora Browse client software is installed from your MediaFrame or K2 BaseCamp Express server. Depending on the roles assigned, users can use it to search for, transfer, or modify logical or physical assets on the MediaFrame server or various devices.

For information on installing or configuring the Aurora Browse client, see [“Add Aurora Browse Clients” on page 132](#). For information on operating the Aurora Browse client, see the *Aurora Browse User Guide*.

K2 BaseCamp Express

K2 BaseCamp Express is a scaled-down version of the MediaFrame system. This is a complete turnkey solution including a MediaFrame server, MDI services, low-res encoder, and low-res storage all running on one K2 BaseCamp Express Server. This solution allows on-demand proxy generation of all SD and KD K2 server assets.

The K2 BaseCamp Express system can run in two environments: a basic K2 system and a full high-resolution Aurora editing environment.

For more information, see [Appendix B, *K2 BaseCamp Express* on page 175](#).

Design considerations - Aurora Browse with Aurora Edit

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

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

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

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

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

Installing the Aurora Browse system hardware

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

The instructions in this chapter are as follows:

- [“Rack-mount hardware components” on page 20](#)
- [“About cabling hardware components” on page 20](#)
- [“Cable hardware: MediaFrame support” on page 21](#)
- [“Cable hardware: Proxy support” on page 26](#)

When you are done installing and cabling the hardware, install the software:

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 control-side LAN. Network traffic from the internal LAN is minimized.
- You may want to postpone cabling to external networks until after configuring respective IP addresses.

Cable hardware: MediaFrame support

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

- “[MediaFrame server instructions](#)” on page 21
- “[MediaFrame server instructions: HAAR platform](#)” on page 22
- “[MDI Server instructions](#)” on page 24

MediaFrame server instructions

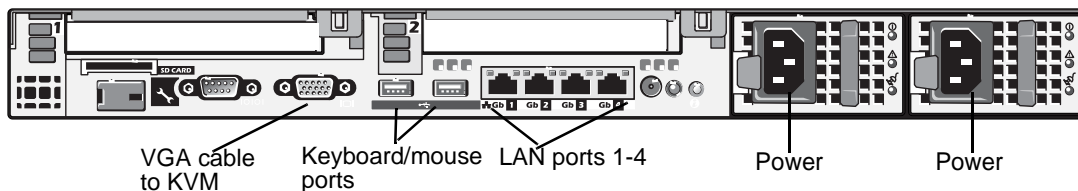
The central component of the system is the MediaFrame server. Depending on the design of your system, it can host the following software components:

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

The server connects to all encoders and the Network Attached Storage via the network. Refer to the system diagrams in [Chapter 1, System Overview](#).

For the MediaFrame server you have the option of the regular Dell-based platform, as explained in this section, or the HAAR platform, as explained in “[MediaFrame server instructions: HAAR platform](#)” on page 22.

Dell R610 server



Cable as illustrated and as follows:

- Connect port 1 to the control network.
- Connect port 2 to the FTP network.
- Connect port 3 to the Corporate LAN.

MediaFrame server instructions: HAAR platform

This topic is divided into two sections:

[“Cabling the HAAR system servers” on page 22](#)

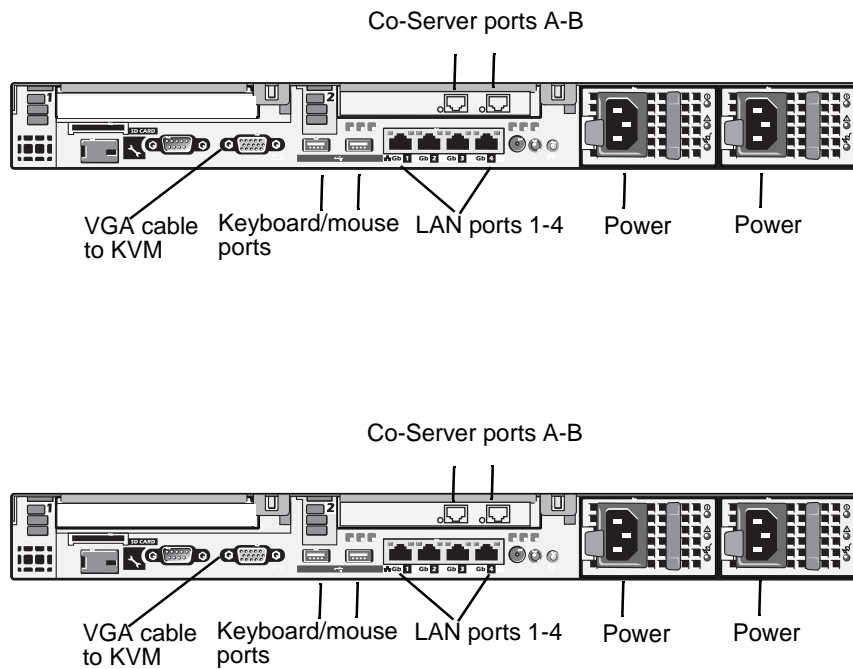
[“Configuring the HAAR system network” on page 23](#)

Cabling the HAAR system servers

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

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

HAAR platform (Dell R610 servers with an additional network card)



Cable as illustrated and as follows:

- Connect port 1 to the control network.
- Connect port 2 to the FTP network.
- Connect port 3 to the Corporate LAN.
- Use LAN port 4 for Co-Server management.
- Ports A and B of the add-on card are used for Co-Server links. Interconnect Co-Server Link ports with cross-over cables.
- Connect power cables to a power supply. Power supply units are hot-swappable.

Configuring the HAAR system network

If configuring the HAAR platform, do not add the co-servers as separate physical devices in SiteConfig. You should only add the virtual server in the SiteConfig user interface and configure it. The co-server configuration is not managed in SiteConfig.

CAUTION: Do not modify the co-server links Link A and link B on the add-on card.

To configure the HAAR platform, do the following (not in SiteConfig):

1. On either CoServer 1 or CoServer 2, configure the virtual server's network settings as follows:
 - a. Configure network connection for port 1 to the Control network.
 - b. Configure network connection for port 2 to the FTP network.
 - c. Configure network connection for port 3 to the Corporate LAN network.
 - d. Configure network connection for port 4 for Co-Server management.
2. Add the virtual server settings to SiteConfig as described in [“Modifying unassigned \(unmanaged\) network interfaces on MediaFrame devices” on page 49](#).

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

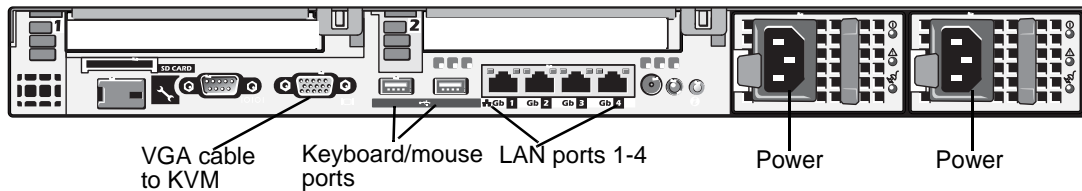
To power down the HAAR platform, right-click the system tray icon and select **Manage Endurance Configuration | Shutdown**. This process shuts down the entire configuration: one virtual and two physical servers.

MDI Server instructions

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

The MDI server is an optional component. It runs on the regular Dell-based platform.

Dell R610 server



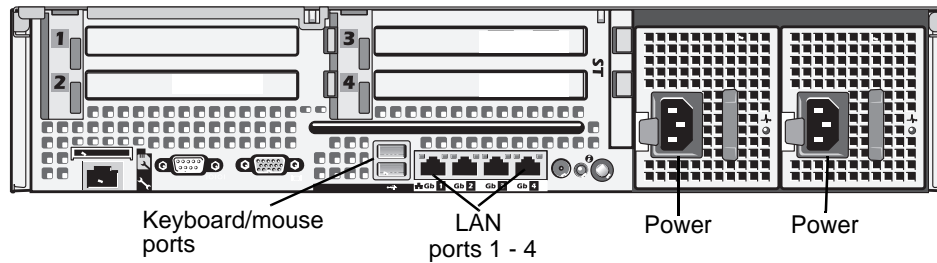
Cable as illustrated and as follows:

- Connect port 1 to the control network.
- Connect port 2 to the FTP network.

K2 BaseCamp Express instructions

The K2 BaseCamp Express is a Dell R710 server with MediaFrame system components including a low-res NAS storage, an internal RAID, the MediaFrame database, and MDIs such as Generic FTP and K2. For more information on the K2 BaseCamp Express, see [Appendix B, K2 BaseCamp Express](#).

Dell R710 server



Cable as illustrated and as follows:

- Connect port 1 to the control network.
- Connect port 2 to the FTP network.
- Connect port 3 to the Corporate LAN.

Cable hardware: Proxy support

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

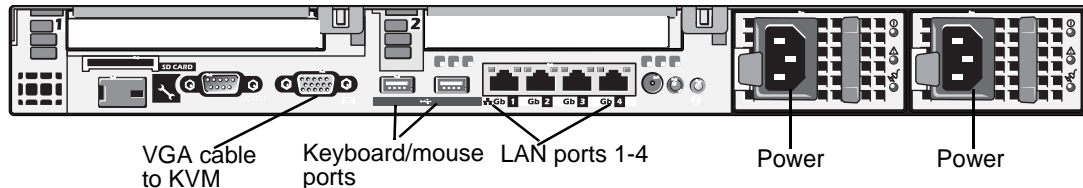
- [“Encoder instructions” on page 27](#)
- [“Low-res proxy NAS instructions - Condor” on page 27](#)

Encoder instructions

The encoder creates a low-res proxy of the high-resolution video asset. There are two types of encoders: Aurora Proxy Encoder, which creates proxy from clips on a News Share system, and SmartBin Encoder, which creates proxy from the SmartBin service while it is transferring high-resolution material from an external server to the News Share system.

The encoder runs on a Dell R610.

Dell R610 server



Cable as illustrated and as follows:

- Connect port 1 to the Control network.
- Connect port 2 to the Media (iSCSI) network.

Low-res proxy NAS instructions - Condor

The Network Attached Storage (NAS) unit provides storage for MPEG-1 proxy video, storyboards, and thumbnails. For information on how to install and configure the NAS for your K2 system, see the *K2 Storage System Instruction Manual* and the *K2 Lx0 RAID Storage Instruction Manual*. For information on how to prepare the Condor NAS for the MediaFrame system, refer to [“Prepare NAS - Condor” on page 79](#).

Understanding network system concepts

Make sure you understand the following system concepts before planning or implementing an Aurora Browse/MediaFrame system.

- “Control network description”
- “Streaming/FTP network description”
- “Media (iSCSI) network description”
- “Networking tips”
- “About hosts files”
- “Host table tips”

Control network description

The control network is for communication between devices and components. It does not have real-time media traffic or streaming/FTP media traffic. The control network must be on a different subnet than the streaming/FTP network and the Media (iSCSI) network. Static IP addresses with name resolution via host files are recommended for the control network.

The control network applies to all MediaFrame servers, Aurora Servers, Encoders, and any device managed by the MediaFrame system. Aurora Browse and Aurora Edit LD clients can also be on the control network but typically they are configured to only run on the corporate LAN.

Streaming/FTP network description

The streaming/FTP network is for media transfers and FTP traffic. It must be on a different subnet than the control network and the Media (iSCSI) network. Static IP addresses with name resolution via host files are recommended for the streaming/FTP network. Host names of network adapters that are dedicated to the streaming/FTP network must be aliased in the hosts file with the *_he0* suffix. This directs the streaming traffic to the correct port.

The streaming/FTP network applies to MediaFrame servers, MDI servers, K2 BaseCamp Express, SmartBin Encoders, and FTP servers. It also applies to Aurora Proxy Encoders using a GXF FTP server that is not hosted on the Encoder. This is the primary network for moving media between storage systems.

Media (iSCSI) network description

The media network is exclusively for real-time iSCSI traffic on a K2 SAN. It must be on a different subnet than the control network and the streaming/FTP network. Furthermore, its traffic is kept physically separate from that of other networks. This separation is provided by dedicated ports, cables, and by a dedicated VLAN on the

Ethernet switch or by separate switches. Static IP addresses are required for the media network. Name resolution is not necessary, so media network IP addresses are not required in host files.

The media network applies to Encoders and SmartBin servers connected to the online K2 SAN. It also would apply to machines hosting the News MDI if the MDI is configured to the iSCSI connection. Most systems should have the News MDI running on the MDI server using an CIFS mount connection so typically the media network is not needed for the News MDI. Nearline K2 SANs do not have a media network.

Corporate LAN network

The Corporate LAN connects the Aurora Browse/MediaFrame system to the external customer LAN. The MediaFrame server, Aurora Browse or Aurora Edit LD clients, and low-res NAS machines must have network access to the external LAN. Work with the IT personnel at the site to connect these devices to the site's Domain and network. This would include DNS, DHCP, and WINS settings.

Firewall considerations

Some sites require that there be a firewall between the MediaFrame equipment and their corporate network. The firewall should allow incoming HTTP (TCP port 80) connections to the MediaFrame server. 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.

Networking tips

- Before configuring any devices for networks, determine the full scope of IP addresses and names needed for all the machines in your Aurora Browse/MediaFrame system.
- It is recommended that you use the patterns offered in SiteConfig by default to establish a consistent convention for machine names and IP addresses. You can plan, organize, and enter this information in SiteConfig as you develop a system description. You can do this even before you have devices installed or cabled.
- If configuring a HAAR platform, bear in mind that these servers use four different subnets for the internal virtual network and co-server links. Avoid these subnets when planning a network on a HAAR platform:
 - 192.168.1
 - 192.168.2
 - 192.168.3
 - 192.168.4
- Work with the network administrator at your facility to have IP addresses and names available for your use.

About hosts files

The hosts file is used by the control network and the streaming/FTP network for name resolution, which determines the IP address of a device on the network when only the device name (hostname) is given. The hosts file is located at `C:\Windows\system32\drivers\etc\hosts` on Windows XP and Windows 2003 Server operating system computers. The hosts file must be the same on all network devices. It includes the names and addresses of all the devices on the network.

For FTP transfers on a K2 SAN, transfers go to or from K2 Media Servers that have the role of FTP server. No transfers go directly to/from the shared storage K2 clients that are on the K2 SAN. To support FTP transfers, in the hosts file the K2 Media Server hostname must have the `_he0` extension added at the end of the name and that hostname must be associated with the K2 Media Server's FTP/streaming network IP address.

Here is an example of IP addresses and names associated in a hosts file:

```
#-----
#General Host Table
#-----
127.0.0.1 localhost

192.168.100.10 root-mf-svr
192.168.101.10 root-mf-svr_he0

192.168.100.11 root-mf-mdi
192.168.101.11 root-mf-mdi_he0

192.168.100.20 root-mf-adv-1
192.168.101.20 root-mf-adv-1_he0

192.168.100.21 root-mf-adv-2
192.168.101.21 root-mf-adv-2_he0

192.168.100.30 root-mf-nas-1
```

In this example 192.168.100.xx is the control network and 192.168.101.xx is the streaming/FTP network. Each MediaFrame and MDI server has its hostname associated with its control network IP address. In addition, each Encoder that needs to transfer media over the streaming/FTP network has its `_he0` hostname associated with its streaming/FTP network address.

Use SiteConfig to define your networks and devices. When you do so, SiteConfig creates the correct hosts file and copies the hosts file to each network device. This enforces consistent hosts files across networks and reduces errors introduced by editing and copying hosts files on individual devices. You can also view hosts files from SiteConfig for troubleshooting purposes.

Host table tips

- If transferring to or from a Profile XP or Open SAN system via UIM, the hosts file must also follow UIM naming conventions for those systems. Refer to the *UIM Instruction Manual*.
- Do not enable name resolutions for media (iSCSI) network IP addresses in the hosts file, as hostname resolution is not required for the media network. If desired, you can enter media network information in the hosts file as commented text as an aid to managing your networks.

Installing the Aurora Browse System Software

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

The instructions in this chapter are as follows:

- [“About SiteConfig” on page 34](#)
- [“About developing a system description” on page 34](#)
- [“Aurora Browse/MediaFrame installation checklists” on page 35](#)
- [“Adding proxy NAS to system description” on page 39](#)
- [“Configuring the corporate LAN” on page 43](#)
- [“Adding a group” on page 44](#)
- [“Adding a device to the system description” on page 44](#)
- [“About device and host names” on page 45](#)
- [“Establish conventions” on page 46](#)
- [“Modifying a device name” on page 48](#)
- [“About IP configuration of network interfaces on devices” on page 48](#)
- [“Modifying unassigned \(unmanaged\) network interfaces on MediaFrame devices” on page 49](#)
- [“About SiteConfig support on MediaFrame devices” on page 51](#)
- [“Discovering devices with SiteConfig” on page 52](#)
- [“Assigning discovered devices” on page 53](#)
- [“Modifying MediaFrame device managed network interfaces” on page 54](#)
- [“Making the host name the same as the device name” on page 57](#)
- [“Pinging devices from the control point PC” on page 58](#)
- [“About hosts files and SiteConfig” on page 58](#)
- [“Generating host tables for devices with SiteConfig” on page 59](#)
- [“Create record of software installed on devices” on page 60](#)
- [“Removing a software role from a device” on page 62](#)
- [“Adding a software role to a device” on page 62](#)
- [“Distribute devices into deployment groups” on page 62](#)

- “Configuring deployment groups” on page 66
- “Install prerequisite files on the control point PC” on page 67
- “About deploying software” on page 67

When you are done installing the software, continue with [Chapter 5, *Configuring the system*](#) and [Chapter 6, *Database and Recovery Planning*](#) to complete the installation of your system.

About SiteConfig

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

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

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

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

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

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

About developing a system description

The topics in this manual assume that you are modifying an existing system description, such as the system description that contains your K2 SAN, in order to add and manage your Aurora Browse and MediaFrame devices.

Your system description is typically developed using one of the following taskflows:

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

stand-alone K2 systems.

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

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

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

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

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

Aurora Browse/MediaFrame installation checklists

Use the following sequence of checklists to guide the overall task flow of installing and commissioning a MediaFrame system.

Pre-installation planning checklist

	Task	Instructions	Comment
<input type="checkbox"/>	Procure existing or create new SiteConfig system description.	Refer to “About SiteConfig” on page 34 , “About developing a system description” on page 34 , and SiteConfig documentation.	This can be done before arriving at the installation site.

	Task	Instructions	Comment
<input type="checkbox"/>	Acquire Aurora Browse and Aurora Suite Software CDs or download the latest software needed for the installation.	See the <i>Aurora Browse Release Notes and Upgrade Instructions</i> for the list of required software.	The Aurora Suite software is used to install Aurora FTP on the encoder.
<input type="checkbox"/>	Install SiteConfig on a control point PC within your network operation.	See “Install prerequisite files on the control point PC” on page 67.	
<input type="checkbox"/>	Next: Infrastructure checklist		

Infrastructure checklist

	Task	Instructions	Comment
<input type="checkbox"/>	Rack and cable the system.	Follow the <i>K2 SAN Cabling Guide</i> , and other documentation that comes packaged with devices. Also refer to Chapter 2, “Installing the Aurora Browse system hardware” .	
<input type="checkbox"/>	Configure Ethernet switch(es).	Refer to Chapter 2, “Installing the Aurora Browse system hardware” and K2 documentation on setting up the Ethernet switch.	
<input type="checkbox"/>	If you have not already done so, import or create the SiteConfig System Description on the control point PC.	Refer to “About SiteConfig” on page 34, “About developing a system description” on page 34, and SiteConfig documentation: - If your system has a stand-alone K2 system, refer to the <i>K2 System Guide</i> for instructions on creating a system description. - If your system has a K2 SAN system, refer to the <i>K2 SAN Installation and Storage Manual</i> for instructions on creating a system description.	
<input type="checkbox"/>	Next: Network setup and implementation checklist		

Network setup and implementation checklist

	Task	Instructions	Comment
<input type="checkbox"/>	If you have not already done so, add the proxy NAS to the system description	“Adding proxy NAS to system description” on page 39	Modify your existing system description.
<input type="checkbox"/>	If you have not already done so, configure the proxy NAS and verify that it is operational.	Refer to the <i>K2 SAN Installation and Service Manual</i> . Follow procedures for K2 Nearline SAN.	—
<input type="checkbox"/>	Add corporate LAN to system description	“Configuring the corporate LAN” on page 43	Modify your existing system description.
<input type="checkbox"/>	Add a group for your MediaFrame devices to the system description	“Adding a device to the system description” on page 44	—
<input type="checkbox"/>	Add a placeholder device to the system description for each of your actual MediaFrame devices	“Adding a device to the system description” on page 44	—
<input type="checkbox"/>	Configure the names of the placeholder devices	“About IP configuration of network interfaces on devices” on page 48	—
<input type="checkbox"/>	Configure the network interfaces of the placeholder devices	“Placeholder device IP configuration” on page 48	Specify IP address ranges and other network details
<input type="checkbox"/>	Discover your MediaFrame devices	“Discovering devices with SiteConfig” on page 52	—
<input type="checkbox"/>	Assign each discovered device to its placeholder device	“Assigning discovered devices” on page 53	—
<input type="checkbox"/>	For each discovered and assigned device, edit each network interface. Specify network settings and apply them to the device.	“Modifying MediaFrame device managed network interfaces” on page 54	If a device connects to multiple networks, set the control network interface IP address first. Also set the hostname.
<input type="checkbox"/>	If not already set correctly, set the hostname of discovered devices	“Making the host name the same as the device name” on page 57	Make sure the device name is correct, then make the hostname the same as the device name.
<input type="checkbox"/>	Ping each MediaFrame device to test network communication	“Pinging devices from the control point PC” on page 58	—

	Task	Instructions	Comment
<input type="checkbox"/>	Generate host table information and distribute to hosts files on each device and on the control point PC	“Generating host tables for devices with SiteConfig” on page 59	Make sure you have completed network configuration of all network interfaces across all devices to ensure complete and valid host table information. You can use SiteConfig to copy hosts files to devices, or you can manage hosts files yourself.
<input type="checkbox"/>	Next: Software update checklist		

Software update checklist

	Task	Instructions	Comment
<input type="checkbox"/>	Start the SQL Server and configure the SQL services	Start the SQL Server (MSSQLSERVER) and SQL Server Agent (MSSQLSERVER) services and set them to Automatic startup .	These are not typically set from the factory to Start .
<input type="checkbox"/>	Add/remove software roles	“Adding a software role to a device” on page 62	Make sure software roles match the software that should be installed on each device, according to your system design.
<input type="checkbox"/>	Create a deployment group	“About deploying software” on page 67	
<input type="checkbox"/>	Add MediaFrame devices to the deployment group	“Distribute devices into deployment groups” on page 62	
<input type="checkbox"/>	Place software on control point PC	--	Procure the correct version of software installation files and prerequisite files. Refer to the <i>Aurora Browse Release Notes and Upgrade Instructions</i> .
<input type="checkbox"/>	Check software on devices	--	
<input type="checkbox"/>	Add software to deployment group	--	
<input type="checkbox"/>	Set deployment options	--	
<input type="checkbox"/>	Upgrade/install software to devices from control point PC		
<input type="checkbox"/>	Next: Configuration checklist		

Configuration checklist

	Task	Instructions	Comment
<input type="checkbox"/>	Prepare for core configuration	See “Prepare for core configuration stages” on page 73	--
<input type="checkbox"/>	Configure MediaFrame and MDI servers	See “MediaFrame stage” on page 82	--
<input type="checkbox"/>	Configure the encoder	See “Encoder stand-alone stage” on page 105 and “Encoder + Server stage” on page 115	--
<input type="checkbox"/>	Configure archive(s)	See “Archive stage” on page 123	--
<input type="checkbox"/>	Deploy any remaining encoders	See “Deploy remaining machines for full system” on page 131	--
<input type="checkbox"/>	Test the system	See “Test system level interactions” on page 131	--
<input type="checkbox"/>	If desired, customize the metadata.	See “Adding custom fields and metadata mapping” on page 136	--
<input type="checkbox"/>	Add Aurora Browse client PCs and users	See “Add Aurora Browse Clients” on page 132	--

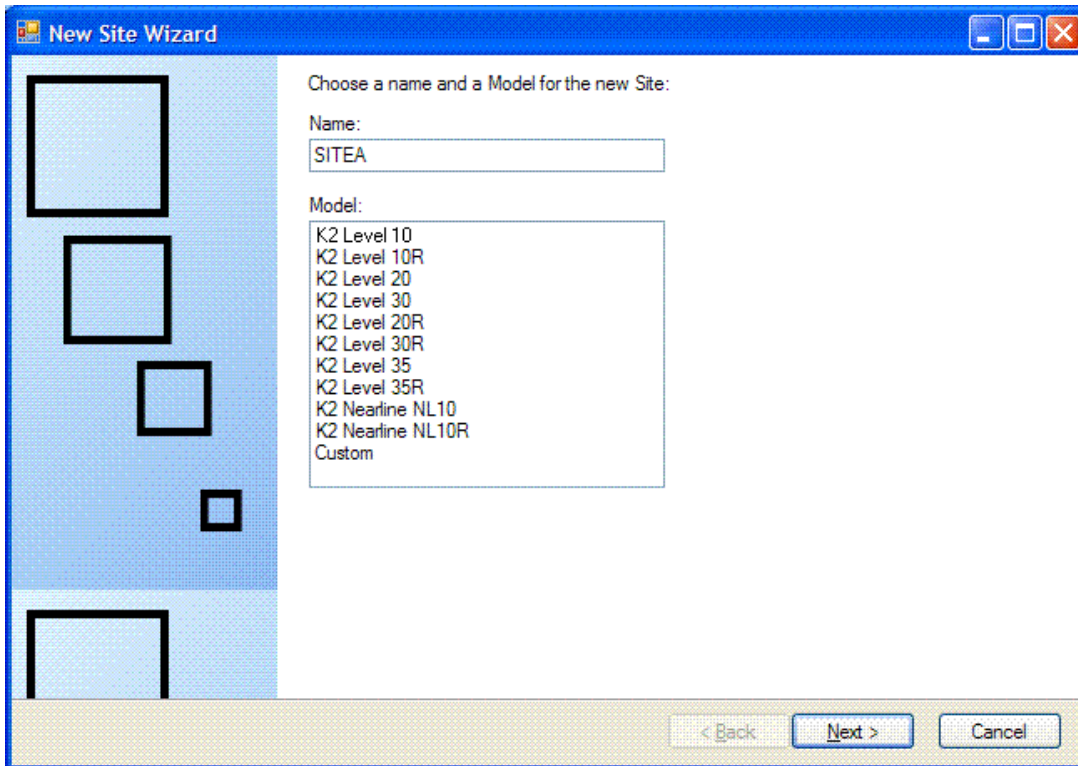
Adding proxy NAS to system description

If the proxy NAS is not already included in the SiteConfig system description, add it as follows.:

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

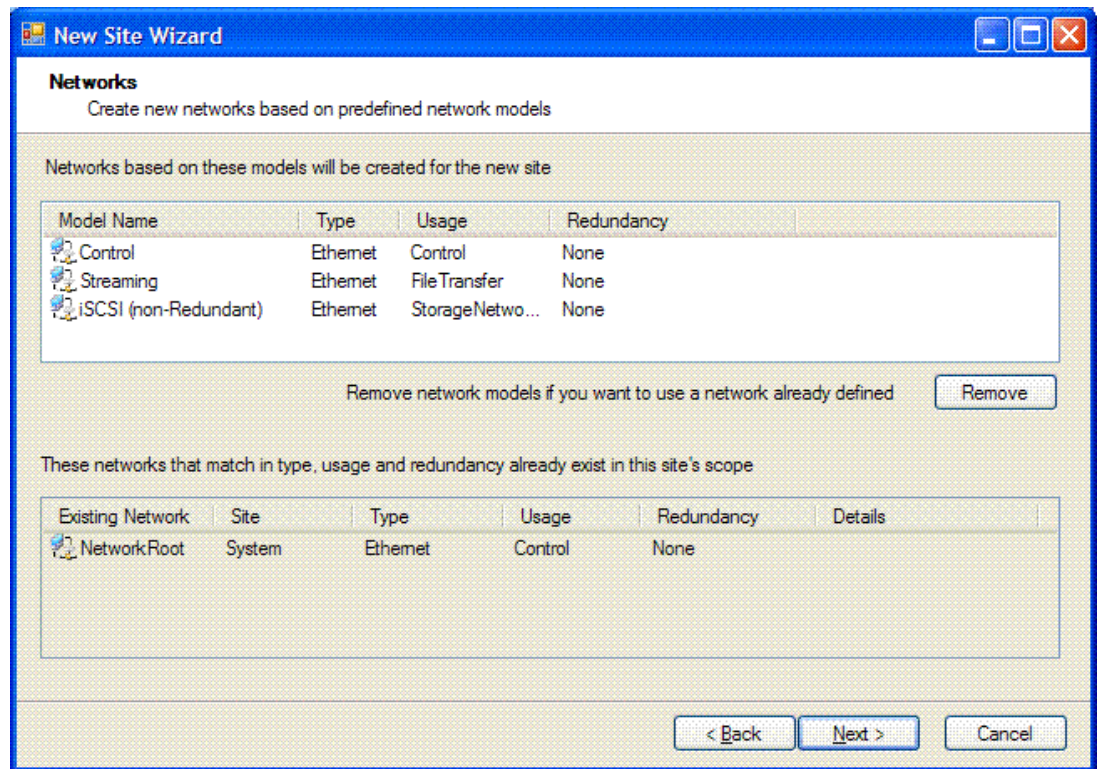
In this context, "Site" is a distinct system, such as a K2 SAN or an Aurora Browse system.

The New Site Wizard opens.



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

The Networks page opens.



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

5. Remove the control network and the streaming network.

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

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

6. Click **Next**.

The Devices page opens.

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

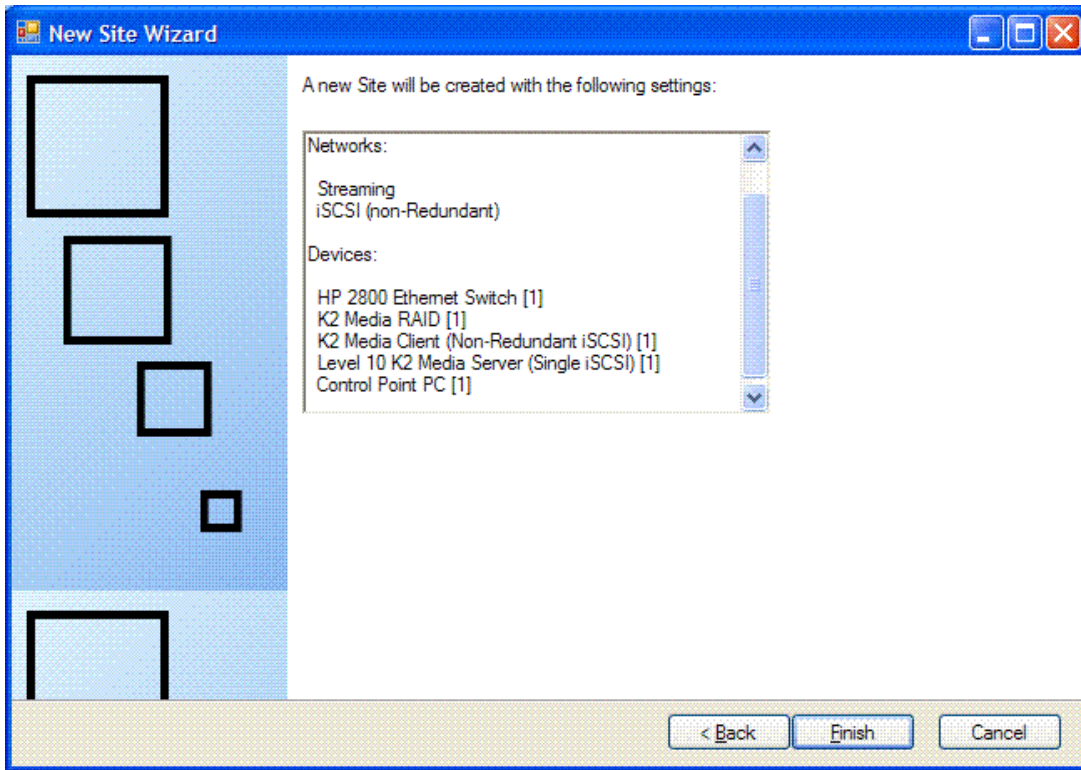
7. You can select a device model and do one or more of the following:

- Specify the number of devices of that model for the site. If the control is disabled, it means that the number of devices is constrained by the site model. For example, a site model might be constrained to have one Ethernet switch only.

- Specify the starting IP address of a set of devices of that model. SiteConfig automatically assigns IP addresses from this range. If you require a different sequence of IP addresses, you can modify them on each device after the New Site Wizard completes.

8. Click **Next**.

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



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

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

10. Add additional K2 Media Servers as necessary for the proxy NAS.

About the corporate LAN

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

- If a device, such as the MediaFrame server, is on the corporate LAN yet is a SiteConfig managed device, then SiteConfig needs to know the connection for each network interface on the device, including the corporate LAN connection. Otherwise, SiteConfig displays error messages.
- If a device uses a DNS server on the corporate LAN for name resolution,

SiteConfig needs to reference that DNS server.

- If a device has software that SiteConfig supports and the device is on the corporate LAN, such as Aurora Edit LD workstations, you can use SiteConfig to deploy software to the device via the corporate LAN.

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

Configuring the corporate LAN

If you have not already added the corporate LAN to the system description, and you have Browse/MediaFrame devices that connect to that network, use this procedure to add the corporate LAN to the SiteConfig system description.

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

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

2. Proceed as follows:

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

The Network Settings dialog box opens.

3. Configure the settings for the network as follows:

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

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

5. If you added a network, it appears in the **Network Configuration | Networks** tree view at the bottom of the list.

Adding a group

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

The group appears in the tree view.

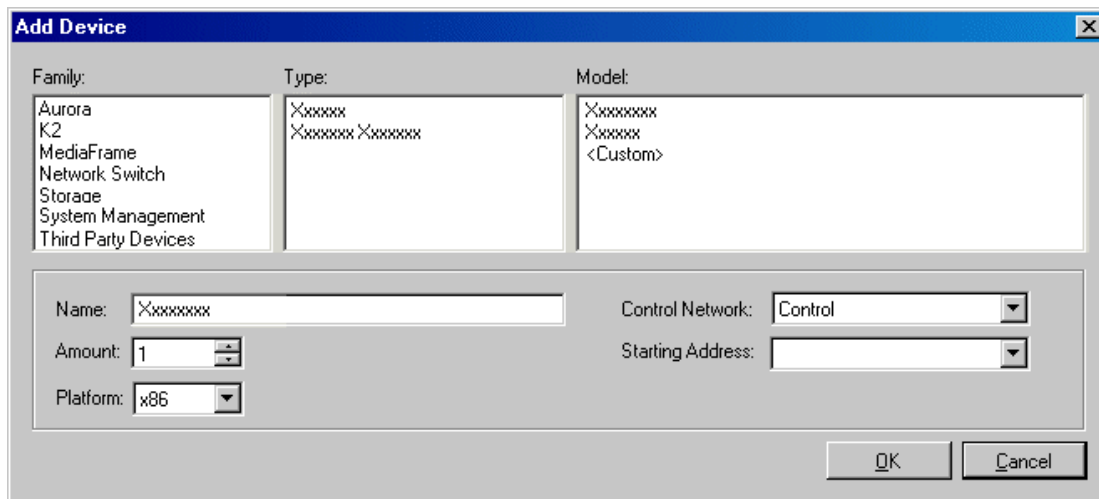
2. Right-click the group and select **Rename**.
3. Enter the desired name for the group.

Adding a device to the system description

Prerequisites for this task are as follows:

- The system description contains a group.

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



The Add Device dialog box opens.

2. Configure settings for the device you are adding as follows:

- Family – Select **MediaFrame**.
- Type – Select the appropriate type of Aurora device.
- Model – Select the appropriate model.
- Name – This is the device name, as displayed in the SiteConfig device tree view and device list view. This name can be different than the host name (network name). You can accept the default name or enter a name of your choice. Devices in the tree view are sorted alphabetically.
- Amount – You can add multiple devices, as currently defined by your settings in the Add Device dialog box. An enumerator is added to the name to create a unique name for each device added.
- Control network – Select the control network.

- Starting Address – Select from the list of available addresses on the selected control network. If adding multiple devices, this is the starting address, with addresses assigned sequentially to each device added.
3. Click **OK** to save settings and close.
 4. Repeat these steps for each of your devices.

About device and host names

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

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

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

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

SiteConfig does not allow duplicate device names or host names.

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

Establish conventions

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

Machine naming convention

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

Machine type	Name
MediaFrame machines	
MediaFrame server	<i>root-mfsvr</i>
Managed Device Interface (MDI) Server	<i>root-mf-mdi</i>
Proxy machines	
Aurora Proxy Encoder	<i>root-PXYENC-adv-1...n</i>
SmartBin Encoder	<i>root-PXYENC-sbe-1...n</i>
Network Attached Storage (NAS) ^a	<i>root-mf-nas-1...n</i>
Ingest machines	
K2 system	<i>k2-1...n</i>
Stand-alone Profile Media Server	<i>pvs-1...n</i>
M-Series iVDR	<i>ivdr-1...n</i>
Legacy machines	
Live monitor encoder	<i>root-nb-live-1...n</i>

^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 system services to the specific machines in your particular system. For this reason you should take care to create logical names that are easy to identify and interpret as they appear in the various configuration pages.

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

The software components that require logical names are as follows:

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

Ports and services mapping

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

Services	Port	Comments
MediaFrame Services		
GV Ask	9010	—
GV Asset Manager	9022 and 9023	—
GV DIVA MDI	9122	—
GV FlashNet MDI	9124	—
GV FTP MDI	9128	Formerly Thomson NLS MDI
GV K2 MDI and GV K2 Summit MDI	9160	The service manages a number of host processes, one for each K2 system that is being managed. These host processes require ports 9160 - 9169. Stopping/starting the service stops/starts all of the host processes.
GV License Manager	9012	—
GV Metadata	9014	Not visible on a configuration page
GV MSeries MDI	9140	The service manages one host process for each managed M-Series iVDR. These host processes require ports 9140 - 9149. Stopping/starting the service stops/starts all of the host processes.
GV News Share MDI	9150	—
GV NTFS MDI	9115	—
GV Profile MDI	9130	The service manages one host process for each managed Profile. These host processes require ports 9130-9139. Stopping/starting the service stops/starts all of the host processes.
GV Proxy MDI	9110	—

Services	Port	Comments
GV Resolver	9016	Not visible on a configuration page
GV RulesWizard	9018 and 9019	Not visible on a configuration page
GV Subscription Manager	9024	—
GV Transfer Manager	9020	—
Proxy Services		
GV Aurora Proxy Encoder	9230	Starting range for first control.

These services are normally distributed on different machines in the system, not on any one machine, as explained in [“Accessing services” on page 80](#). The system also depends upon Microsoft Internet Information Services (IIS) and SQL services.

Modifying a device name

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

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

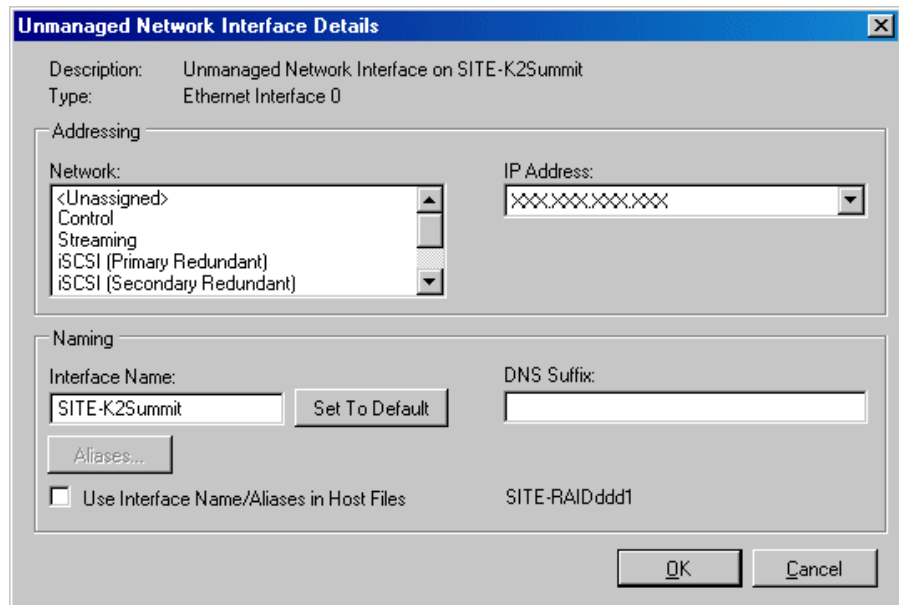
About IP configuration of network interfaces on devices

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

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

Placeholder device IP configuration

When working with a placeholder device, its network interfaces are indicated in the user interface as unmanaged interfaces — that is, IP address modification is only saved to the system description, not modified on the actual device. When you double-click on an unmanaged network interface, or if you select the interface and click the **Edit** button, the unmanaged network interfaces dialog box is displayed.



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

Discovered device IP configuration

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

Once a device has been discovered, the network interfaces are now managed interfaces; changes are made on the actual device. To edit the network configuration properties of the selected interface, double-click on the interface or click the Edit button.

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

Modifying unassigned (unmanaged) network interfaces on MediaFrame devices

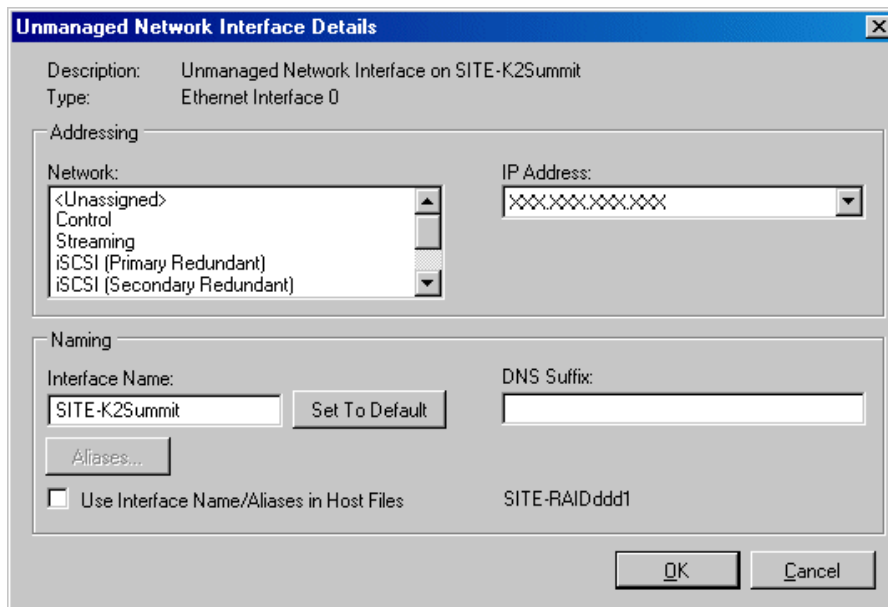
Prerequisites for this task are as follows:

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

Use this task to modify unmanaged network interfaces on a MediaFrame devices as follows:

- MediaFrame server
- MDI server
- K2 BaseCamp Express

- Encoder
 - MediaFrame server: HAAR platform
 - For HAAR platforms, SiteConfig only recognizes the virtual server, not the individual co-servers. Any modification of the HAAR network connections in SiteConfig only apply to the virtual server.
1. In the **Network Configuration | Devices** tree view, select a MediaFrame placeholder device.
 - The interfaces for that device are displayed in the interfaces list view.
 2. In the interfaces list view, right-click an interface and select **Edit**.
 - The Unmanaged Network Interface Details dialog box opens.



3. Configure the settings for the interface as follows:

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

Setting...	For control network interface
DNS Suffix	Allowed, if applicable to the network. The DNS suffix is added to the interface name.

- Click **OK** to save settings and close.
- If configuring a MediaFrame server that is also on the corporate LAN, and your device does not show a corporate LAN interface, add an interface to represent the corporate LAN connection. Then repeat the steps to configure an interface for the corporate LAN, with settings as follows:

Setting...	For corporate LAN network interface
Network	If using DHCP or external hosts file, select the unmanaged network that you configured earlier.
IP Address	Select the IP address you plan to assign to the device.
Interface Name	These settings are irrelevant, as SiteConfig does not manage this network.
Set to Default	
Use Interface Name/Aliases in Host Files	
Aliases	
DNS Suffix	For communication on some networks, a suffix, such as <i>example.com</i> , must be added to host names.

- Copy these configurations onto the virtual server.
- Do not modify the IP addresses of the CoServer Link ports (Ports 1 and 2 of the add-on card). They are used only for communication between the servers. Refer to [“MediaFrame server instructions: HAAR platform” on page 22](#).
- Click **OK** to save settings and close.

About SiteConfig support on MediaFrame devices

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

- The device must be a Microsoft Windows operating system device.
- The device must have Microsoft .NET version 2.0 installed, as reported in the Windows Add/Remove Programs control panel.
- The ProductFrame Discovery Agent service must be running on the device, as reported in the Windows Services control panel. If the Discovery Agent has not been installed, you need to install it. The installer is in the Discovery Agent Setup folder under the SiteConfig install folder.


If you suspect a problem with these requirements, do not attempt to install SiteConfig support requirements. If you must restore SiteConfig support requirements, re-image the system.

Discovering devices with SiteConfig

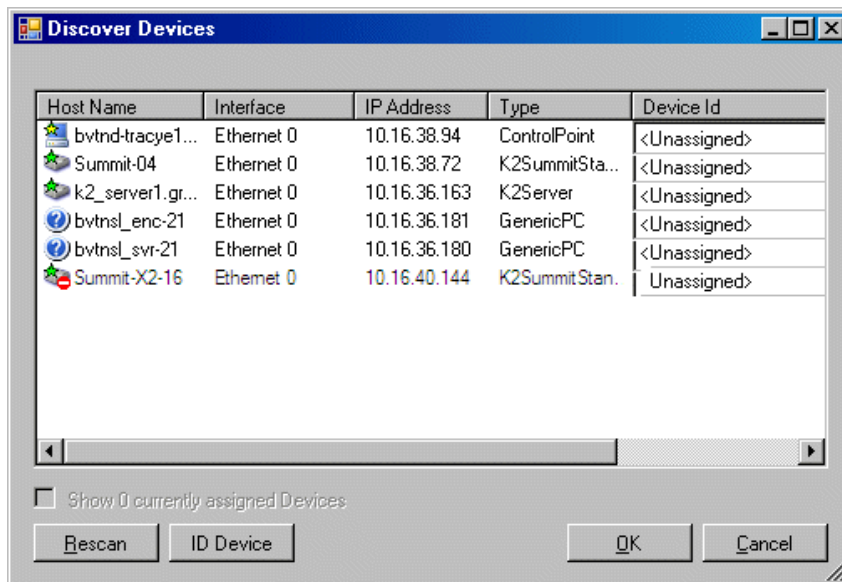
Prerequisites for this task are as follows:

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

1. Open SiteConfig on the control point PC.

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

The Discover Devices dialog box opens.




A list of discovered devices is displayed.

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

Assigning discovered devices

Prerequisites for this task are as follows:

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

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

The Discover Devices dialog box opens.

2. Identify discovered devices.

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

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

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

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

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

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

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

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

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

Modifying MediaFrame device managed network interfaces

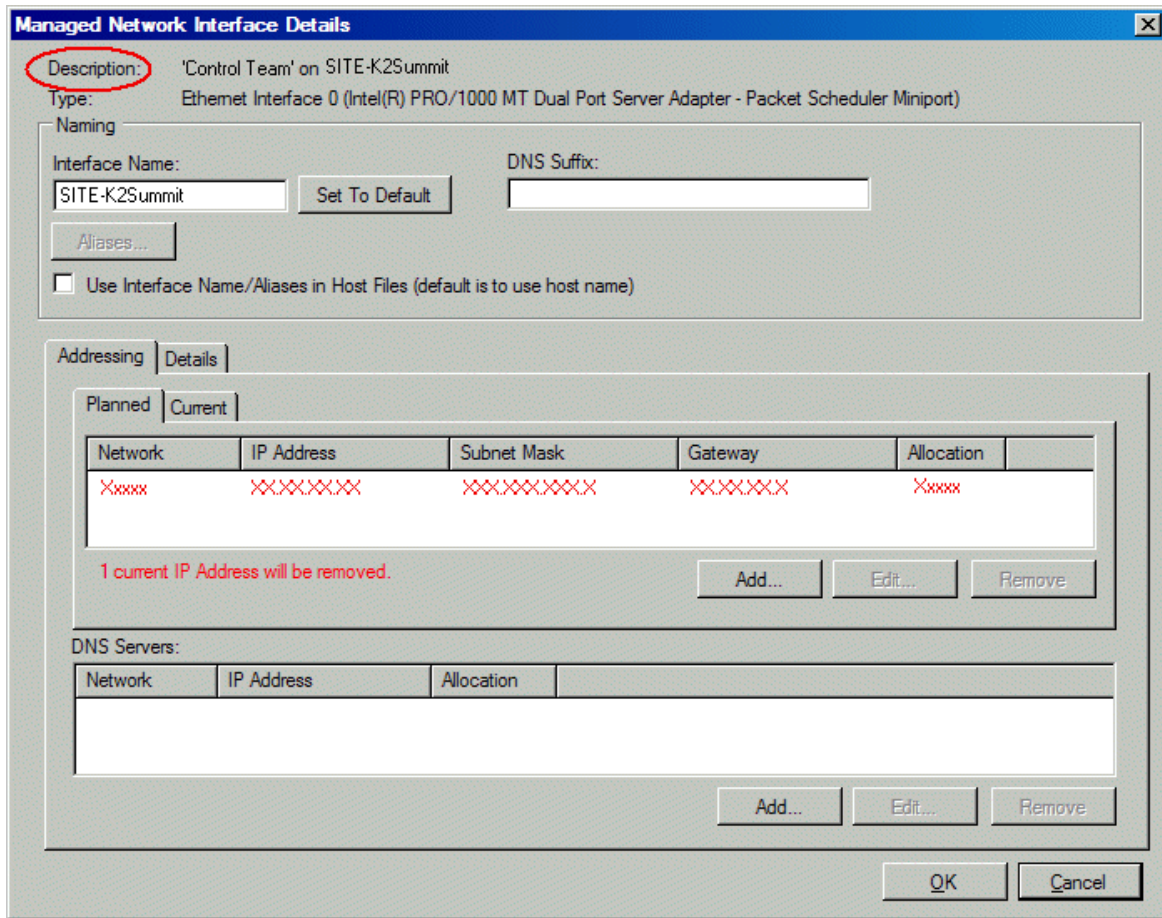
Prerequisites for this task are as follows:

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

Use this task to modify managed network interfaces on a Media-Frame devices as follows:

- MediaFrame server
 - MediaFrame server: HAAR platform
 - MDI server
 - K2 BaseCamp Express
 - Encoder
1. In the Interfaces list view determine the interface to configure, as follows:
 - Identify the interface with which SiteConfig is currently communicating, indicated by the green star overlay icon. This should be the control network interface.
 - Verify that the interface over which SiteConfig is currently communicating is in fact the interface defined for the control network in the system description. If this is not the case, you might have the control network cable connected to the wrong interface port.
 - Configure the control network interface first before configuring any of the other interfaces.
 - The control connection should always be on the first port on the motherboard on the device.
 - After you have successfully configured the control network interface, return to this step to configure each remaining interface.
 2. In the Interfaces list view, check the icon for the interface you are configuring. If the icon has a red stop sign overlay, it indicates that current settings and planned settings do not match or that there is some other problem. Hover over the icon to read a tooltip with information about the problem.
 3. In the Interfaces list view, right-click the interface you are configuring and select **Edit**.

The Managed Network Interface Details dialog box opens.



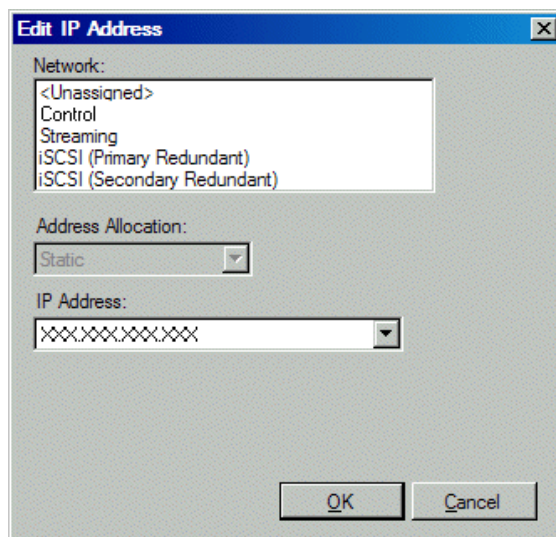
4. Identify the interface on the discovered device that you are configuring.
 - Identify Ethernet LAN adapters by their "Description" name. This is the Windows connection name. SiteConfig reads this name from the device and displays it at the top of this dialog box. This is the most accurate way to identify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

Setting...	For network interface Control Connection
Interface Name	The device host name. Required.
Set To Default	Not recommended
DNS Suffix	Allowed, if applicable to the network. The DNS suffix is added to the interface name.
Aliases	Not allowed
Use Interface Name/Aliases in Host Files	<i>Unselected</i> is required. Since not selected, the default behavior occurs, which is to use the device host name in the hosts file.

Setting...	For network interface Corporate LAN
Interface Name	The device host name. Required.
Set To Default	Not recommended
DNS Suffix	Allowed, if applicable to the network. The DNS suffix is added to the interface name.
Aliases	Not allowed
Use Interface Name/Aliases in Host Files	<i>Unselected</i> is recommended. Typically this setting has no effect, since the Corporate LAN does not use host files.

Do not modify the IP addresses of the CoServer Link ports (Ports 1 and 2 of the add-on card). They are used only for communication between the servers. Refer to [“MediaFrame server instructions: HAAR platform”](#) on page 22.

6. Evaluate settings on the Planned tab and change if necessary.
 - Compare settings on the Planned tab with settings on the Current tab.
 - If you want to keep the current settings as reported in the Current tab, click **Remove** to remove the planned settings.
 - Do not specify multiple IP addresses for the same interface. Do not use the Add button.
7. To modify planned settings, do the following:
 - a. Select the network settings and click **Edit**.
The Edit IP Address dialog box opens.



- b. Edit IP address settings as follows:

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

Setting...	For network interface Corporate LAN
Network	<i>Corporate LAN</i> is required
Address Allocation	<i>DHCP</i> is typical.
IP Address	When DHCP is selected, you cannot select an IP address.

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

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

A Contacting Device message box reports progress.

9. After configuring control network settings, do the following

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

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

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

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

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

The Ping Host dialog box opens.

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

Making the host name the same as the device name

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

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

The Edit Device dialog box opens.

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

Name.

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

4. Click **OK**.

Pinging devices from the control point PC

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

1. In the **Network Configuration | Networks** tree view, select a network, site, or system node.
2. In the Devices list view, select one or more devices. Use Ctrl + Click or Shift + Click to select multiple devices.
3. Right-click the selected device or devices and select **Ping**.

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

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

About hosts files and SiteConfig

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

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

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

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

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

Generating host tables for devices with SiteConfig

Prerequisites for this task are as follows:

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

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

2. Click **View Hosts file**.

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

3. Verify the information in the hosts file.

4. Do one of the following:

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

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

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

a. In the **Network Configuration | Devices | Devices** list view, right-click a device to

which you intend to write the hosts file and select **View Current Host File**.

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

- b. Verify that there is no information that you want to retain in the device's current hosts file that is not also in the hosts file as currently defined in the system description. If you need to save the device's current hosts file, click **Save As** and save to a different location.
- c. In the **Network Configuration | Devices | Devices** list view, right-click a device or use Ctrl + Click to select multiple devices, and select **Update Host File**.

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

Create record of software installed on devices

If you have not already done so, create a document to keep track of the software that you plan to install on each of your system devices, according to your system design. This is especially helpful for Aurora product devices.

Where to install Browse/MediaFrame software roles

The following table lists the Browse and MediaFrame software roles and the machines that each of these software roles need to be installed on. In some cases, the machine on which you install a software role differs depending upon the configuration of your particular MediaFrame or BaseCamp Express system, as well as upon the particular machines in your system.

As you proceed with subsequent tasks and remove/add software roles to devices in SiteConfig, you can refer to your table and make sure you are assigning software roles correctly.

Add roles to devices to tell SiteConfig where to deploy software when you add software cabs to the deployment group. Removing roles does not automatically remove the software from the device. To remove software using SiteConfig, you must remove the role and then uninstall the completed deployment task.

Software roles/Machine	K2 BaseCamp Express	MediaFrame Server (small system)	MediaFrame Server (large system)	MDI server	Aurora Proxy Encoder	SmartBin Encoder
Aurora Browse client application	X	X	X			
MediaFrame Core Services	X	X	X			
MediaFrame Proxy MDI	X	X	X			
MediaFrame Generic FTP MDI	X ^a	X ^a		X ^a		
MediaFrame K2 MDI	X ^b	X ^b		X ^b		
MediaFrame K2 Summit MDI	X ^b	X ^b		X ^b		
MediaFrame M-series MDI	X ^b	X ^b		X ^b		
MediaFrame Profile MDI ^c	X ^b	X ^b		X ^b		
MediaFrame News MDI	X ^d	X ^d		X ^d		
MediaFrame NTFS MDI	X ^d	X ^d	X ^d			
MediaFrame FlashNET MDI	X ^b	X ^b		X ^b		
MediaFrame DIVA MDI	X ^b	X ^b		X ^b		
MediaFrame Proxy Encoder	X ^e				X	X
Aurora FTP ^f					X	X
Smart Bins						X
SmartBins Encoder						X
GVG MLib	X ^g	X ^g		X ^g	X	X
StorNext File System Client(non K2 only)					X	X
Generic iSCSI Client (non K2 only)					X	X
NetCentral PC Monitoring	X	X	X	X	X	X

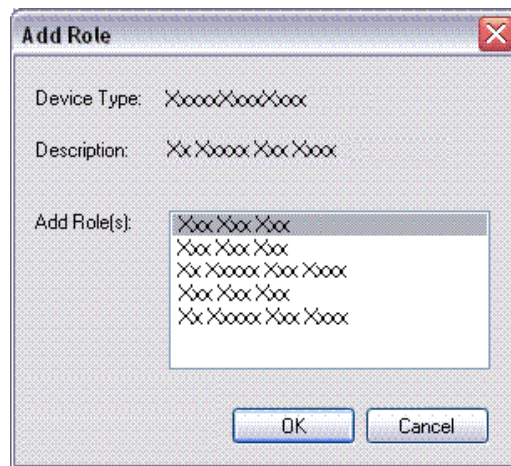
- ^a. If the system includes a nearline.
- ^b. If the system includes a machine of this type.
- ^c. When you install the Profile MDI, you also need to install the Profile XP software. You cannot install a Profile MDI and a News MDI on the same machine.
- ^d. If the system includes a NewsShare (DSM).
- ^e. If BaseCamp Express does not have a Proxy Encoder sever connected.
- ^f. News-based systems now use the K2-Aurora FTP(Aurora Assets) FTP server for transfers to and from the NewsShare system, and for News-based K2 BaseCamp Encoders
- ^g. If the MediaFrame News MDI is installed on the server.

Removing a software role from a device

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

Adding a software role to a device

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



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

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

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

Distribute devices into deployment groups

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

If you have not already done so, configure your deployment groups. To configure deployment groups, refer to [“Configuring deployment groups” on page 66](#).

The recommended deployment group distribution is as follows. Depending on your system design, your system might not have all the device types listed.

In a deployment group named "Aurora_Edit_Ingest_Playout", place the following devices:

- Aurora Edit workstation of any storage options: Shared storage, NAS storage, and stand-alone.
- Aurora Edit LD computer
- DSM
- Conform Server
- SmartBin Server
- FTP Server
- Aurora Ingest workstation
- IEP
- Aurora Playout computer

In a deployment group named "Aurora_Browse_MediaFrame", place the following devices:

- MediaFrame server
- MDI server
- Aurora Proxy Encoder
- K2 BaseCamp Express

If you have a K2 Nearline SAN (NAS), in a deployment group named for the SAN system, place the following devices:

- The Nearline SAN's K2 Media Servers.

Setting deployment options

Pre-requisites for this procedure are as follows:

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

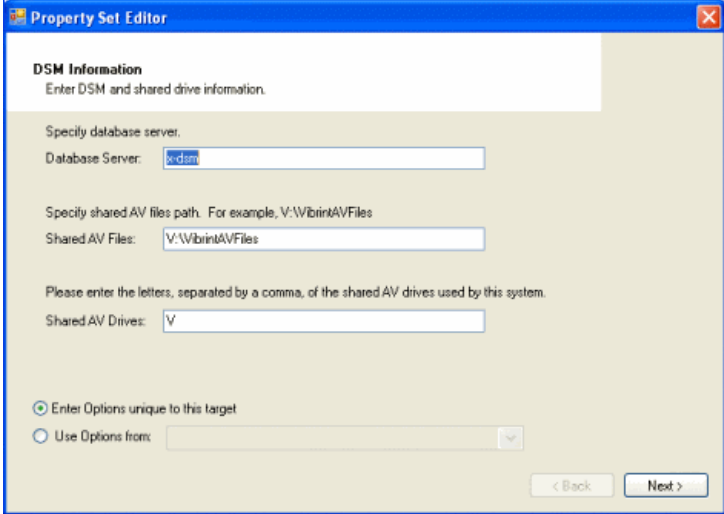
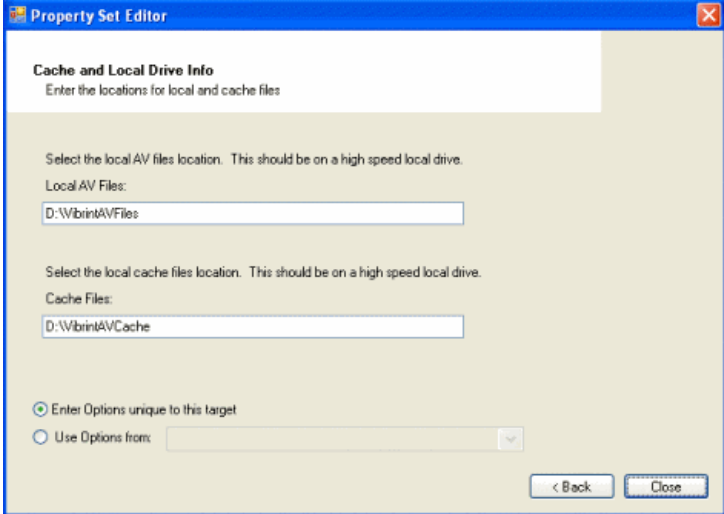
1. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.
2. In the Tasks list view, view tasks and determine if you must set deployment options. Tasks that need to have deployment options set display in the Details column a message stating "Deployment options required."

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

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

- GVG_MLib
 - MediaFrame Server
 - Proxy Encoder
 - Aurora Suite
4. Do one of the following to set deployment options:
- Double-click the task.
 - Select the task and click the **Options** button.
- A wizard opens.
5. Work through wizards and set deployment options as follows:

Software	Deployment options
GVG_MLib	Enter the name(s) of the K2 Media Server(s) with the role of file system server (FSMs)
MediaFrame Server and Proxy Encoder	<div data-bbox="704 863 1308 1293" data-label="Image"> </div> <p data-bbox="646 1308 1365 1539">Enter the service credentials to be used. You can enter a domain account or a local account in the format domain\accountname or machinename\accountname. In the case of using a local account, it is advisable to enter it as “.\accountname” where the “.” means a local account. Entering the local account in this way allows you to use the “Use Options from” feature for all other devices of the same type. Once you enter the local account in this way on the first device, it becomes the template from which options for other devices are copied.</p>

Software	Deployment options
Aurora Suite	 <p>Enter the Database server (DSM,) shared AV files, and shared AV drives.</p>  <p>Enter local AV files and cache files.</p>

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

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

Configuring deployment groups

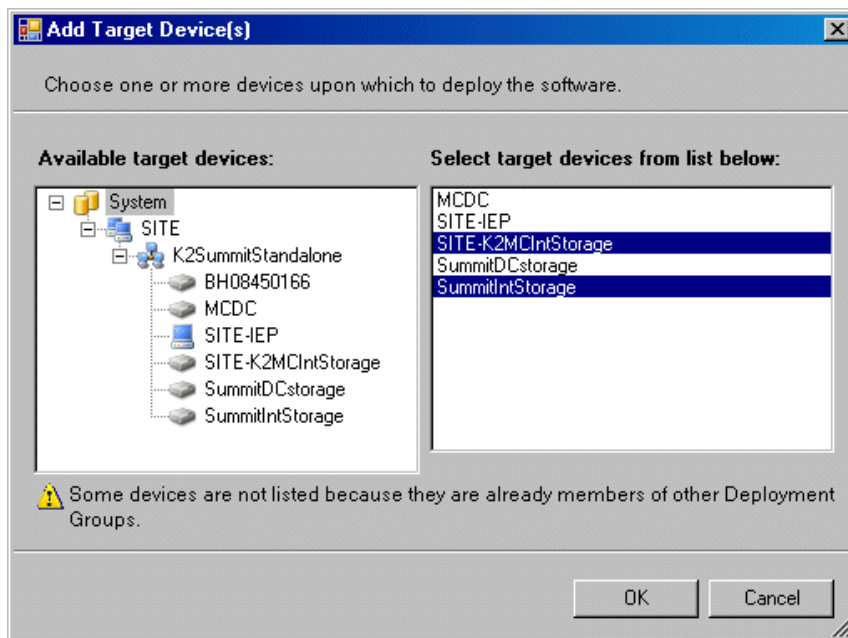
Prerequisites for this procedure are as follows:

- The device is assigned in the SiteConfig system description and network connectivity is present.
1. In the **Software Deployment | Deployment Groups** tree view, right-click the top node and select **Add Deployment Group**.

A deployment group appears in the tree view.

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

The Add Target Device(s) wizard opens.



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

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

6. Click **OK**.

The devices appear in the Deployment Groups tree view under the deployment group. Before you perform a software deployment, you must check software on the devices that will be receiving new software. If you have already added packages to the group, on the

Deployment Groups tab you will also see deployment tasks generated for every device with roles that match the package contents.

Install prerequisite files on the control point PC

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

1. Check release notes for the required version of prerequisite files, if any.
2. On the SiteConfig control point PC, open Windows Add/Remove programs and look for **Grass Valley Prerequisite Files**, then proceed as follows:
 - If the required version of prerequisite files is installed, do not proceed with this task.
 - If prerequisite files are not installed or are not at the required version, proceed with this task.
3. Procure the required prerequisite software installation file. The file name is *Prerequisite Files.msi*.
4. On the SiteConfig control point PC, run the installation file. The installation program copies prerequisite files to *C:\Program Files\Grass Valley\Prerequisite Files*.

About deploying software

You must control the sequence of tasks and device restarts as you install or upgrade software. The exact steps can vary from software version to version. The following sequence of SiteConfig tasks is typical:

1. Check currently installed software.
2. Add software package(s) to deployment group(s).
3. Set deployment options.
4. Deploy (install or upgrade) software.

Your product's release notes have the specific task flow for the version of software you are installing. The release notes are written for upgrading software on existing systems, but if you are installing software for the first time on a new system, the steps are essentially the same. The primary difference is that when installing software for the first time, the SiteConfig "uninstall" deployment tasks are not displayed.

Make sure you follow the documented task flow in the release notes for the version of software you are installing or to which you are upgrading.

Add software package to deployment group for Aurora Browse devices

Prerequisites for this task are as follows:

- You can access the software package file from the SiteConfig control point PC.
- The devices to which you are deploying software are in a deployment group.
- To review which software roles to install on which machine, see [“Where to install Browse/MediaFrame software roles”](#) on page 60.

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

- MediaFrame server
- MDI server
- Aurora Proxy Encoder
- K2 BaseCamp Express
- Aurora Suite

For this release of software, identify and add software package installation files as follows:

Software	File name
MediaFrame Server	MediaFrameServer_7.0.0.xxxx.cab
Aurora Proxy Encoder	AuroraProxyEncoder_7.0.0.xxxx.cab
Aurora Suite	AuroraSuite_7.0.x.xxxx.cab
Grass Valley Windows Monitoring SNMP agent	PCMonitoring_x.x.x.xx.cab

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

NOTE: Add files for either 3.x or 7.x. Do not add files for both 3.x and 7.x.

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

Software compatible with 3.x K2 SAN	File name
Generic iSCSI client	GenericISCI_x86_3.x.x.cab
GVG MLib software	GVG_MLib_3.x.xxxx.cab

- If your devices access storage on a K2 software version 7.x K2 SAN, add software

package installation files as follows:

Software compatible with 7.x K2 SAN	File name
Generic iSCSI client	GenericISCI_x86_7.x.xx.xxxx.cab
GVG MLib software	GVG_MLib_7.x.xx.xxxx.cab

SNFS is bundled with the Generic iSCSI cab file.

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

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

Installing software on Aurora Browse devices

Prerequisites for this task are as follows:

- The devices that you are installing are in a deployment group.
 - For the software you are installing, you have added a version of that managed software package to the deployment group.
 - Prerequisite files are installed on the control point PC.
 - You have recently done the SiteConfig "Check Software" operation on the devices you are installing.
1. In the Software Deployment | Deployment Groups tree view, select the device or the group of devices for which you are installing software.
The corresponding software deployment tasks are displayed in the Tasks list view.
 2. For the software you are installing, select the Deploy check box in the row for the install task.
 3. For installing Aurora Browse and MediaFrame and Aurora Suite devices to this release, deploy the following tasks:
 - MediaFrameServer 7.0.0.xxxx Install
 - AuroraProxyEncoder 7.0.0.xxxx Install
 - Aurora Suite 7.0.0.xxxx Install
 - GenericISCI x86 xxxx.xxxx Install (version must be compatible with K2 SAN)

- GVGMLib xxxx.xxxx Install (version must be compatible with K2 SAN)
- PCmonitoring x.x.x.xx Install

Also, you must install or upgrade SNFS with this release, so deploy the following tasks at the same time:

Managed Package	Action
SNFS nonK2 xxxxxx	Uninstall
SNFS nonK2 3.5.xxsss	Install

NOTE: The Aurora Browse Release Notes contains the latest versions of software.

When using SiteConfig for upgrades, the SNFS upgrade is required even if you are already at the current version. The upgrade resets SNFS version information for SiteConfig.

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

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

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

Deployment tasks run. If upgrading, software is uninstalled. Progress is reported and next steps are indicated in both the Status and Details columns. If an error appears regarding prerequisite software, install the prerequisite files on the control point PC and then repeat this step.
6. When the Status or Details columns indicate next steps, identify the software in the row, then proceed as follows:
 - For K2 software, when Details displays a Restart required link, click the link and when prompted "...are you sure...", click **Yes**.

The device restarts.

Deployment tasks run and software is installed. Progress is reported and next steps are indicated in both the Status and Details columns.
7. When the Status or Details columns indicate next steps, identify the software in the row, then proceed as follows:
 - For K2 software, when Details displays a Restart required link, click the link and when prompted "...are you sure...", click **Yes**.
8. Monitor progress as indicated by both the Status and Details column. When finished, the Status column indicates complete.
9. Restart all MediaFrame devices. This last restart is required, regardless of whether the Details column does or does not display "Restart required".

Configuring the system

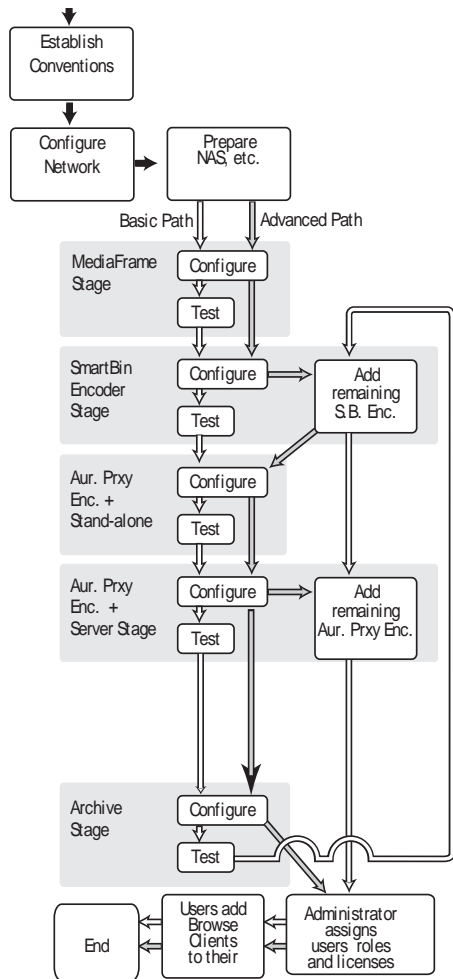
You can use the topics in this chapter in the following ways:

- **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 72](#).
- **Customizing** — After the system is functioning, you can go back to the configuration pages and modify the settings to customize the system to fit any special workflow requirements.

The topics in this chapter include the following:

- [“Configuration overview - K2 storage” on page 72](#)
- [“Prepare for core configuration stages” on page 73](#)
- [“MediaFrame stage” on page 82](#)
- [“Encoder stand-alone stage” on page 105](#)
- [“Encoder + Server stage” on page 115](#)
- [“Archive stage” on page 123](#)
- [“Deploy remaining machines for full system” on page 131](#)
- [“Test system level interactions” on page 131](#)
- [“Add Aurora Browse Clients” on page 132](#)
- [“Managing Aurora Browse User sessions” on page 135](#)
- [“Adding custom fields and metadata mapping” on page 136](#)
- [“About bin and asset naming limitations” on page 139](#)

Configuration overview - K2 storage



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

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

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

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

If you are experienced with the system and you want the fastest possible configuration, follow the **Advanced** path and configure the entire system in one pass, adding all machines at each stage.

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

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

Prepare for core configuration stages

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

- From each machine in the MediaFrame system, verify that you can ping all the devices that the MediaFrame server needs to communicate with over the control or FTP network.
- For the machines that need to communicate with an FTP server, verify you can log in to that FTP server using the credentials that the system will be using.

Prepare MediaFrame Server for News systems

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

1. In Computer Manager, select **Local Users and Groups | Users**.
2. Add the appropriate user:
 - If on a domain, user: **Vibrint Service**
 - If not on a domain (local user), user: **VibrintLocalService**
3. Enter the password: **Vibrint01801** (the password is case sensitive).
4. Add the user to both the administrator group and the iis_wpg group.
5. Add the nbadmin account. This account needs to be on every MediaFrame, K2 BaseCamp Express or MDI server and every encoder. Typically, the username and password are **nbadmin** and **newsat10**.
6. Add nbadmin to both the administrator group and the iis_wpg group.

Prepare encoders

- For K2 systems, make sure SNFS and iSCSI software is correctly installed. Refer to [“Aurora Browse/MediaFrame installation checklists”](#) on page 35.
- Add encoders to the K2 Storage System, as explained in the following section. Refer to [“Add encoders to the K2 Storage System”](#).
- On your Aurora Proxy Encoders, in the Aurora FTP configuration, make sure that the drive is mapped to the K2 or AuroraShare storage. Verify that the mapped drive is V:, unless there are multiple volumes, in which case the mapped drives are V:, W:, X:, Y:.

Add encoders to the K2 Storage System

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

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

- Make sure you’ve installed the software required for K2 support on the Aurora Proxy Encoders and SmartBin encoders. Refer to [“Aurora Browse/MediaFrame](#)

[installation checklists” on page 35.](#)

- Set up the Control Point PC.

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

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

Configuring encoders with the K2 System Configuration application

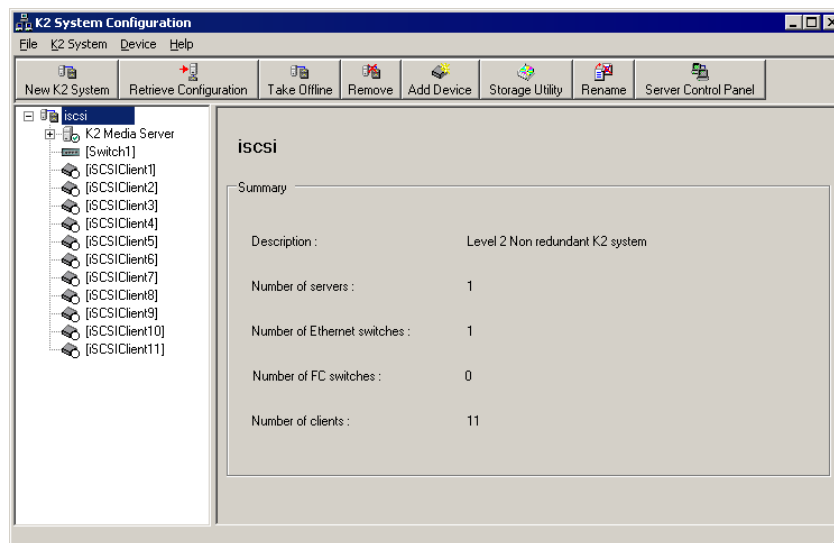
You use the K2 System Configuration application wizard to configure each of the Aurora Proxy Encoders on the iSCSI network.

NOTE: Depending on your configuration (workgroup or domain) you must have the same local or domain-supplied username and password, with administrative privileges, across all the machines in your Aurora Browse system. For more information, see [“About the administrator account” on page 80.](#)

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 Aurora Proxy Encoder or SmartBin encoder to the list, do the following:
 - a. Select the media server and click **Add Device**.

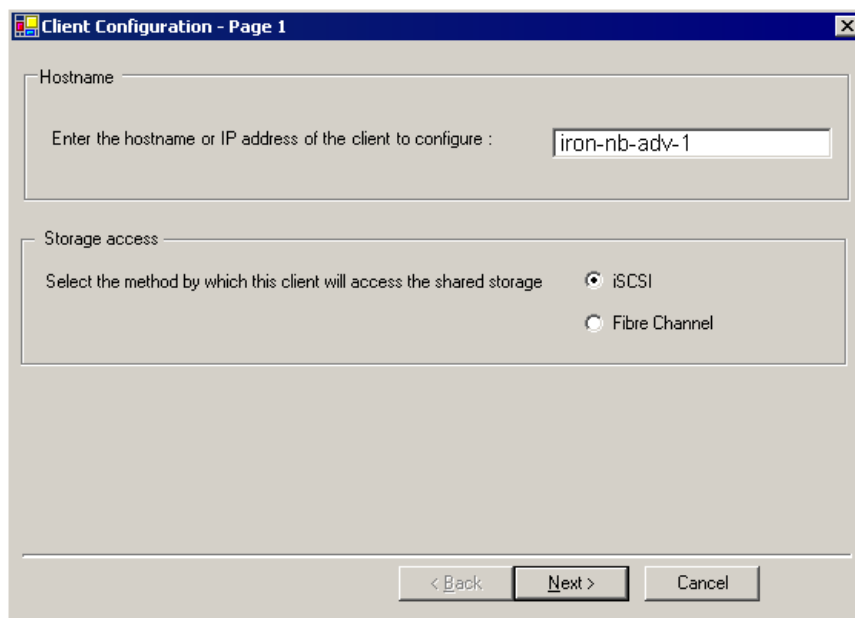


- b. In the Add Device window, click **Generic Client** and click **OK**.

A new client device gets added to the hierarchy.

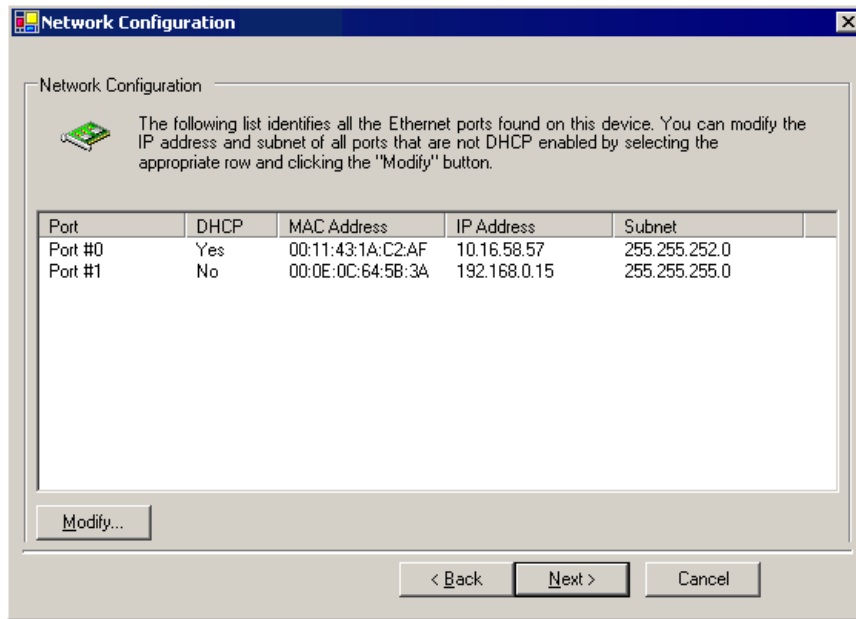
4. Select the client to be configured in the hierarchy view and click **Configure**.

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

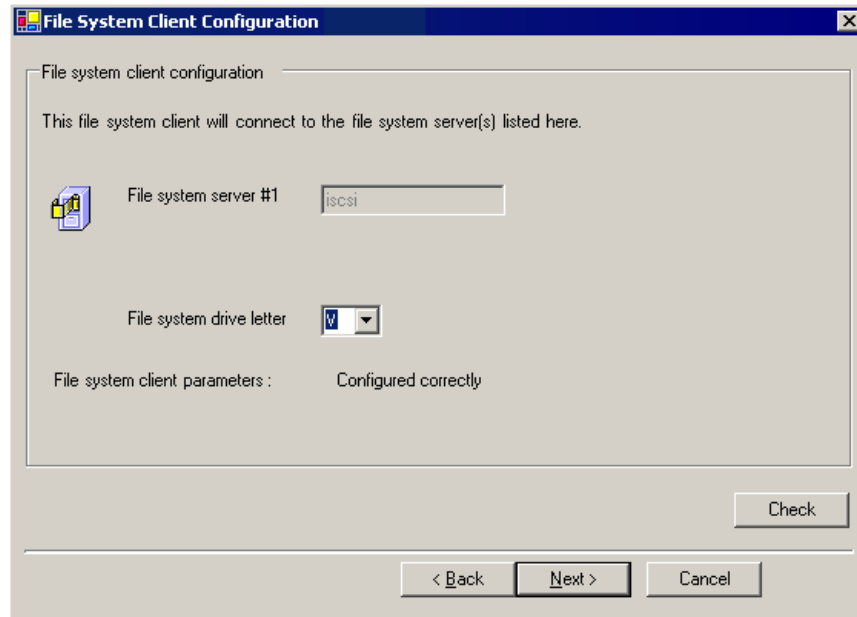


5. At the Client Configuration - Page 1 screen, do the following:

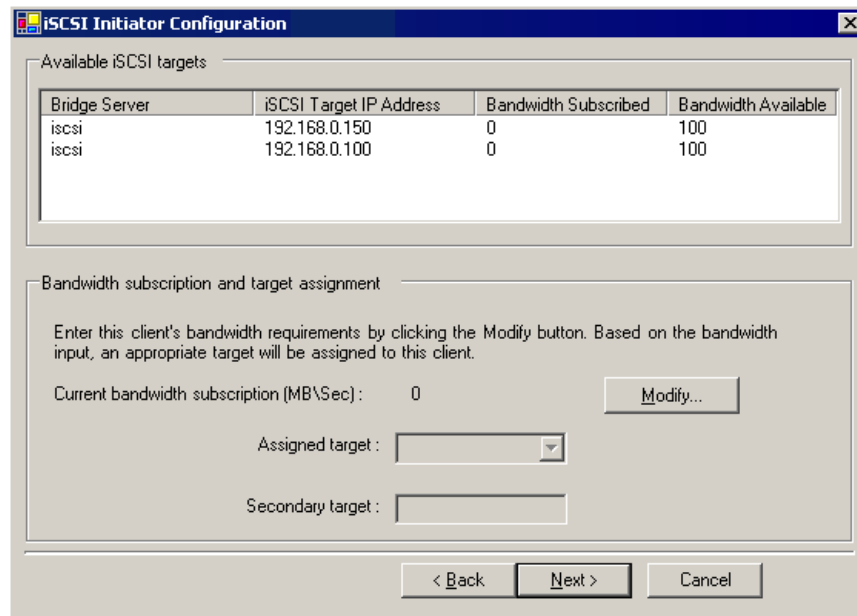
- a. Enter the machine name of the Aurora Proxy Encoder or SmartBin encoder you are configuring (such as `iron-nb-adv-1`).
- b. Select **iSCSI**.
- c. Click **Next**.



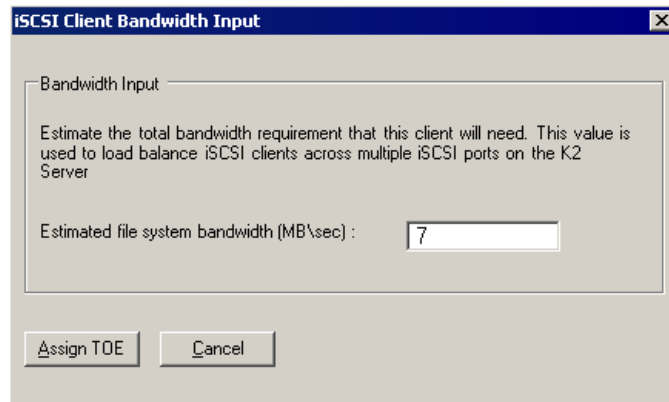
6. At the Network Configuration screen, click **Modify** to change the IP address and subnet of network adapters for this machine, and then click **Next**. You cannot configure the adapter over which the K2 System Configuration application is currently communicating.



7. At the File System Client Configuration screen, enter the drive letter you wish to configure as the iSCSI drive on the encoder machine; this letter should be the same for all machines that are iSCSI clients in this K2 Storage System.
8. Click **Check**. (If you do not click **Check**, some settings are not applied.)
9. Click **Next**.



10. 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 78](#)).
 - c. Click **Assign TOE**.
11. Click **Next**.
 4. At the Completing the Configuration Wizard screen, click **Finish**.
The wizard closes and the encoder reboots.
 5. Repeat this procedure for each Aurora Proxy Encoder or SmartBin encoder that is an iSCSI client on the K2 Storage System.

Calculating encoder bandwidth

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

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

1. Determine the highest bit rate you use on the Aurora Proxy Encoder or SmartBin encoder.
The bit rates for the DV formats are: DV25 = 28.8 Mbps; DV50 = 57.6 Mbps; and DV100 = 115.2 Mbps for the NTSC and PAL video formats.
MPEG bit rates are variable; enter the bit rate set in Aurora Edit.
2. Multiply the highest bit rate by the number of streams that are licensed on this machine.
3. Divide that number by 8 to convert Mbps to MB.
4. Round the MB number up to the nearest integer.
5. Enter this number in the iSCSI Client Bandwidth Input screen in the K2 Configuration application wizard.
6. At the conclusion of the configuration process, the K2 Configuration application restarts the encoder.

Prepare NAS - Condor

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

If you are configuring the Windows Fastora NAS for the Aurora Browse network, refer to [“NAS instructions - Fastora” on page 180](#).

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

- The MediaFrame Server and NAS need to have the clocks set to the same time, or they need to be connected to the network for NTP.
- Depending on your configuration (workgroup or domain) you must have the same local or domain-supplied username and password, with administrative privileges, across all the machines in your Aurora Browse system. For more information, see [“About the administrator account” on page 80](#).

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

1. From any Control network machine, enable the network to recognize the NAS by adding an IP address within the 192.168 range.
2. Make a share. Share name: media.
3. Assign user privileges for the media folder as follows:
 - Everyone — Modify
 - administrators — Full Control
4. Click OK.

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

- MediaFrame server/K2 BaseCamp Express
- Aurora Proxy Encoder

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

1. Open Windows Explorer and navigate to the media directory on the NAS. You can do this with the following path:
 - `\\root-nb-nas-1\Media`
2. Verify basic read/write capabilities by creating, modifying, and deleting a simple text file.

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

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

About the administrator account

Depending on your configuration (workgroup or domain) you must have the same local or domain-supplied username and password, with administrative privileges, across all the machines in your Aurora Browse system. This account is critical for most Aurora Browse proxy access, as explained in this section.

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

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

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

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

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

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

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.

Click **Start | Settings | Control Panel | Administrative Tools | Services** to access the services. All service names start with “GV...”, so they group together in the services list.

Refer to [“Ports and services mapping” on page 47](#) for a list of services.

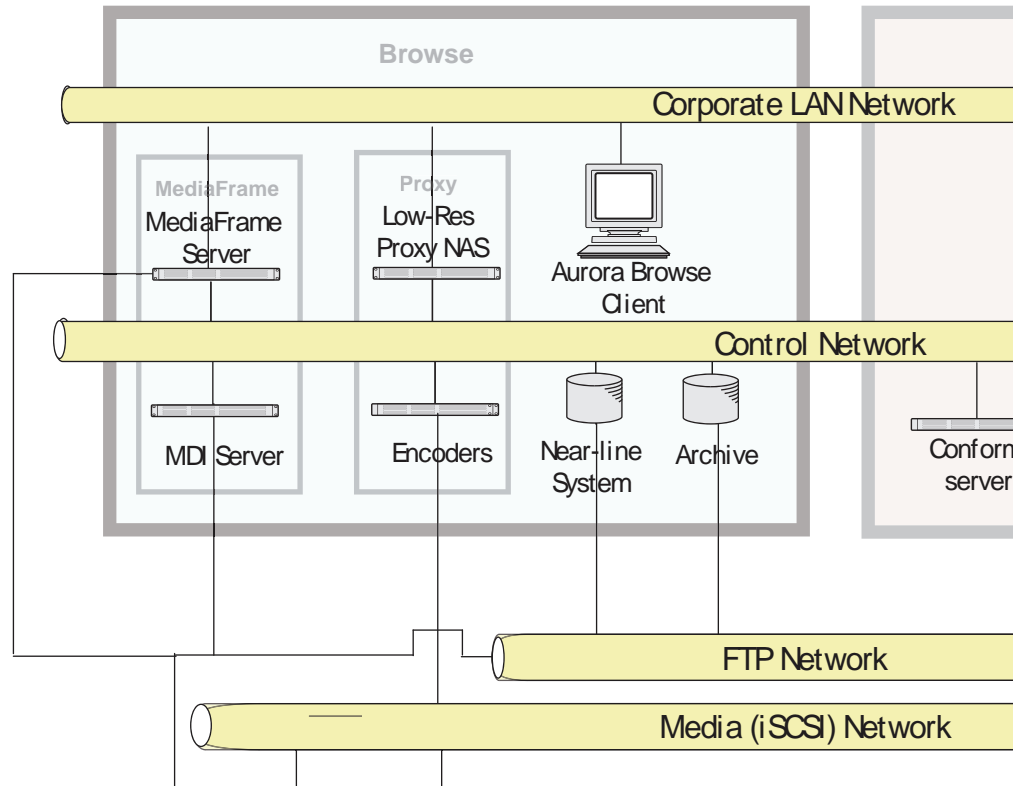
Accessing system configuration settings

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

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

NOTE: Depending on your configuration (workgroup or domain) you must have the same local or domain-supplied username and password, with administrative privileges, across all the machines in your Aurora Browse system. For more information, see [“About the administrator account” on page 80](#).

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 or K2 BaseCamp Express server. It is the central registry for all the software components of the system. As software components carry out tasks in a functioning system they regularly refer to the ASK component to establish communication and exchange commands and data. The configuration pages also refer to the ASK component to populate fields and lists and to validate the values you enter as you configure the system.
- **MDIs** — Devices have Managed Device Interfaces (MDIs) which represents the device's assets in a way that is understandable by the other components of the system. This allows the MediaFrame server to coordinate the activity of the system.

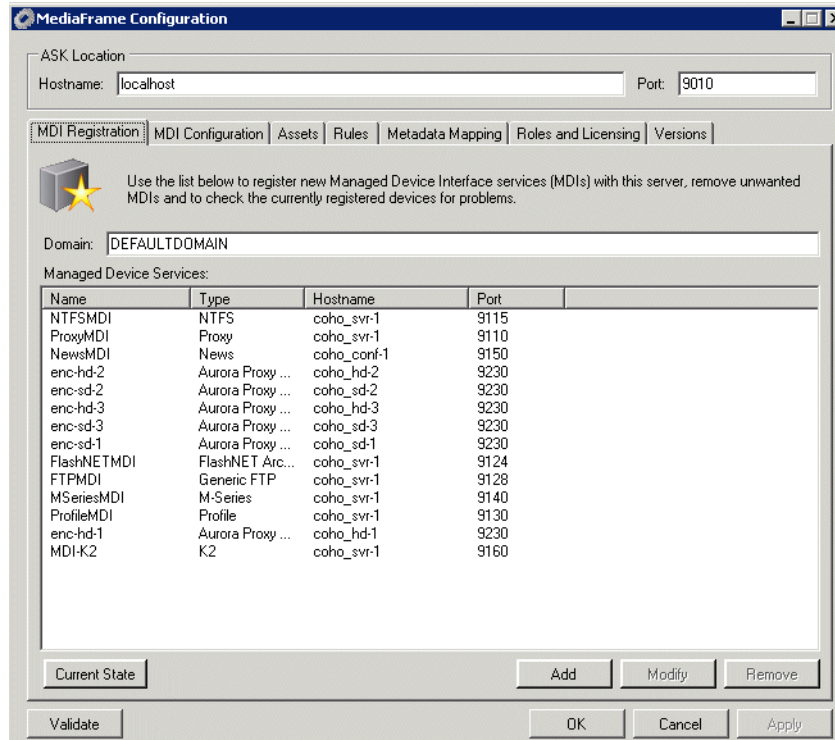
In this configuration stage you add an MDI server and then set up logical names for software components that manage devices. This brings the machines of your system on-line as managed devices. (The MediaFrame server can function as an MDI server, unless your system is very large.)

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

- [“Configure MediaFrame ASK: Register components” on page 84](#)

- “Configuring transfer targets” on page 87
- “Configure ASK Location: MDI server” on page 89
- “Configure Generic FTP MDI” on page 90
- “Configure K2 MDI” on page 92“Configure M-Series MDI” on page 97
- “Configure News MDIs” on page 99
- “Configure Profile MDI” on page 101
- “Configure Proxy MDI” on page 103

Configure MediaFrame ASK: Register components



1. To register the MediaFrame components, select **Programs|MediaFrame Config** and select the **MDI Registration** tab.
2. Port 9010 is required. Do not modify. See [“Ports and services mapping” on page 47](#).
3. All Domain names in the MediaFrame system must be identical. To add an MDI or encoder, click **Add**.
4. To put changes into effect, click **Apply**.
5. When you are finished, click **OK**.

For the conventions mentioned in the following table, refer to [“MDI and Encoder logical names convention” on page 46](#).

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 or K2 Summit MDIs. Typically the MDI Server.	9160 - 9169	These are process ports, as explained in “Ports and services mapping” on page 47 . Assign numbers in an intentional sequence, so they are easy to match in “Configure Generic FTP MDI” on page 90 .
K2 client — Internal storage (stand-alone)	K2				

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
Open SAN Profile	Profile	As per convention.	Hostname of the machine hosting the Profile MDIs. Typically the MDI server	9130 - 9139	The Open SAN Profile is not supported in 6.5, only the stand-alone. These are process ports, as explained in "Ports and services mapping" on page 47.
Stand-alone Profile	Profile				
M-Series	MSeries	As per convention.	Hostname of the machine hosting the M-Series MDIs. Typically the MDI server	9140 - 9149	These are process ports, as explained in "Ports and services mapping" on page 47.
NLS	Generic FTP	As per convention.	Hostname of the machine hosting the Generic FTP MDI. Typically the MDI server	Leave field blank. Correct port number is automatically entered on "Add MDI". Refer to "Ports and services mapping" on page 47 to verify.	—
Aurora Edit News Share (DSM)	News	As per convention.	Hostname of the machine hosting the News MDIs. Typically the MDI server.		—
NTFS storage on Windows machines	NTFS	NTFS1, as per convention.	MediaFrame server hostname, as the server is the required NTFS MDI host.		—
Aurora Proxy Encoder ^b	Aurora Proxy Encoder	As per convention	Aurora Proxy Encoder hostname		—
Proxy	Proxy	PROXY1, as per convention.	Hostname of the machine hosting the Proxy MDI. Typically the MDI server.		—
Archive device	... Archive	ARCHIVE1, as per convention.	Hostname of the machine hosting the archive MDI		—
SmartBin Encoder	SmartBin Encoder	As per convention.	SmartBin encoder hostname		

^a. For a K2 Storage System, the MDI manages one of the connected K2 clients. As per convention, name the MDI for the K2 Storage System.

^b. You need to create an encoder per stream on a machine.

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

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

Note the following distinction when entering "Hostname or IP":

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

the encoder itself.

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 client (stand-alone)	The MDI that manages the K2 client.	The FTP IP address or the user friendly name that resolves to the IP address, like K2Client_he0, of the K2 client.	root-K2_he0	—
	K2 Storage System (SAN)	The MDI that manages the one designated K2 client on the SAN	The FTP IP address(es) of the K2 Media Server(s) or the user friendly name that resolves to the IP address, with role of FTP server.	root-fsm_he0	—
Profile	Profile XP (stand-alone)	The MDI that manages the Profile XP system.	The IP address of the Profile XP system, or the user friendly name that resolves to the IP address.	root-profile_he0	Make sure that UIM addressing requirements are correct in host tables
MSeries	M-Series iVDR	The MDI that manages the iVDR.	The IP address, or the user friendly name that resolves to the IP address, of the iVDR	root-M-SERIES1_he0	
News	The AuroraShare storage system.	The MDI that manages the AuroraShare storage.	The IP address, or the user friendly name that resolves to the IP address, of the K2-AuroraFTP server.	root-mf-NEWS1_he0	If you use K2 FTP instead of AuroraFTP, make sure that you do not exceed K2 limits for the number of transfer sessions. Aurora Browse 6.5.2 and 7.0 systems use the K2-Aurora FTP.

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

Configuring round robin transfers

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

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

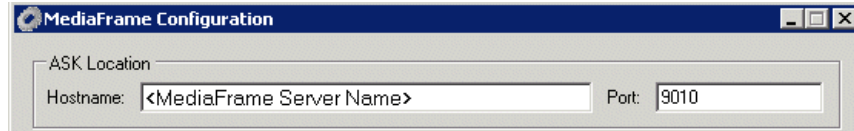
Second transfer request — handled by the second transfer server in the list.

Third transfer request — handled by the first transfer server.

Fourth transfer request — handled by the second transfer server.

Configure ASK Location: MDI server

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



1. Select **Programs | MediaFrame Config** and select the **MDI Configuration** tab.
2. Enter the name of the MediaFrame server.
3. Port 9010 is required. Do not modify. See [“Ports and services mapping” on page 47](#).

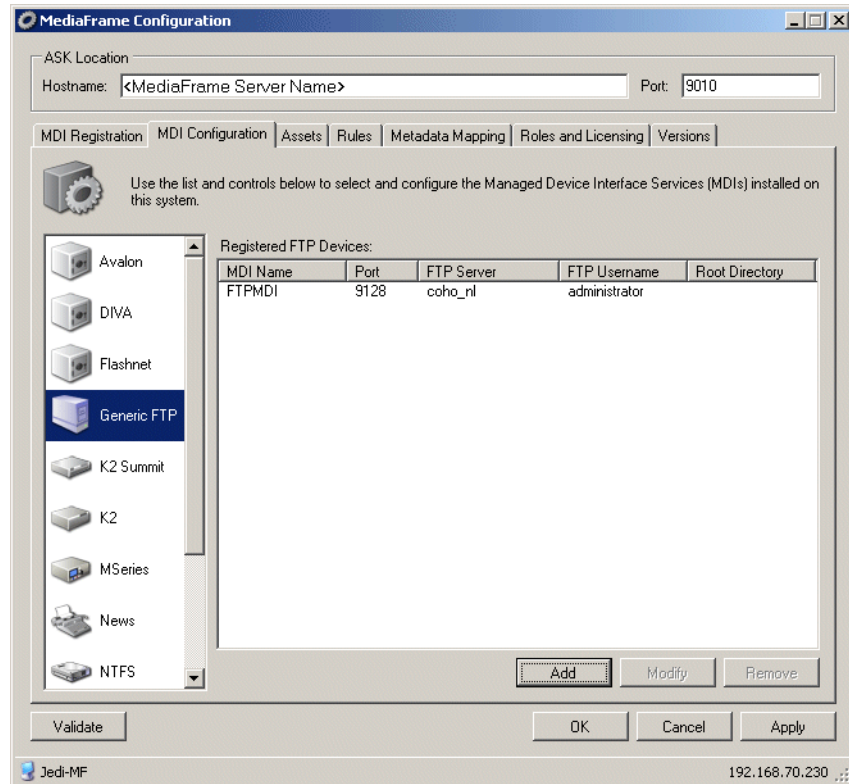
It is not necessary to restart a service to put these settings into effect.

Configure Generic FTP MDI

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

To configure the Generic FTP for FileZilla, see [Appendix D, Installing and configuring the FileZilla Server on page 201](#).

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



1. Locally on the MDI Server, select **Programs | Grass Valley | MediaFrame Config**. Select the MDI Configuration tab and the Generic FTP MDI icon.
2. Click the **Add** button. The Add FTP dialog box displays.

3. Enter the MDI name to log in to the FTP interface on the NLS device. Use the ... button to browse the list of available MDIs.
4. Port 9128 is required. See [“Ports and services mapping” on page 47](#).
5. Enter the IP Address or the name resolving to the FTP server on the FTP server network where assets will be transferred to, and the FTP username and password. If using a K2 nearline, configure the Generic FTP MDI to use the K2's nearline FTP.
6. Make sure the root directory field is blank. Otherwise, you cannot transfer between the Generic FTP MDI and another Generic FTP MDI, or between a Generic FTP MDI and Flashnet or Diva archives.

NOTE: *If you need to change the root directory to blank after the system has been configured, you must run the UpdateFTPLocations script. This script is located on the MediaFrame server under C:\Program Files\Grass Valley\MediaFrame\Database\UpdateFtpLocations.*

7. Check Passive Transfer Mode if you want to transfer assets from one server to another without having the data go through the MDI. Enable passive transfer on the FTP server first.

NOTE: *Although passive transfer mode is preferred, if the FTP server is an IIS FTP server, the Generic FTP MDI must use Active transfer mode.*

8. To put changes into effect, click **Apply**.
9. When prompted to restart the MDI, click **Yes**.

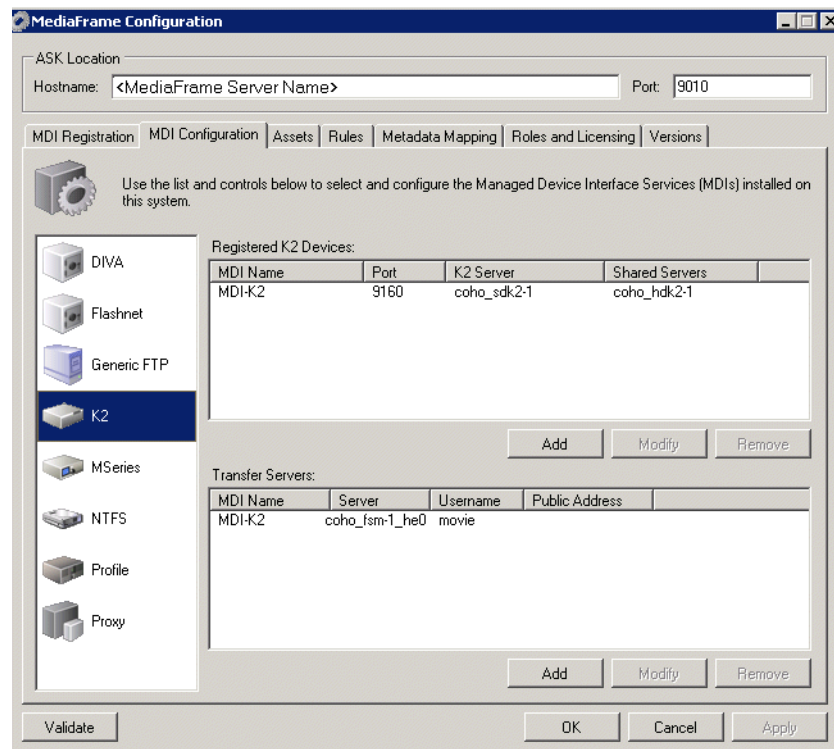
Configure K2 MDI

This page configures the Managed Device Interface (MDI) for a stand-alone K2 client or a K2 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 MediaFrame ASK: Register components” on page 84](#). To make the configurations easier to read for troubleshooting purposes, add MDIs sequentially so there is a correlation between the port number and any number in the MDI name.

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



1. On the MDI server, select **Programs| Grass Valley | MediaFrame Config**. Select the MDI Configuration tab and the K2 icon.
2. Enter the name of the MediaFrame server. Do not modify Port 9010. See [“Ports and services mapping” on page 47](#).
3. Under Registered K2 Devices, click **Add**.
4. Enter the K2 MDI. Use the ... button to choose the MDI.
5. Increment 9160-9169 so each K2 MDI has a unique process port. For each FSM, there should be one K2 MDI.

6. Enter a stand-alone K2 client or the K2 client on the K2 storage system that the MDI will use to manage the K2 SAN. For a K2 SAN, add all of the other client host names to the "Other Clients on the SAN". If Aurora Edit is setup to send directly to the K2 server, add the K2 server name to this list.
7. The default value on the Asset System Dwell Time is 120 seconds.
8. Enter the number of maximum concurrent transfers. The maximum number of concurrent transfers allowed depends on your system's configuration. For assistance determining the maximum number of allowed transfers, contact your Grass Valley representative.
9. Enter the username, domain (if necessary), and password. The username and password need to have permissions to access the K2 AppCenter application on the K2 client.
10. Click **Add** as a managed device.

The following settings enable transfers. You should add all available transfer targets, as specified in ["Configuring transfer targets" on page 87](#).

11. Under Transfer Servers, click **Add**.
12. Use the drop-down list to specify the MDI name.
13. Enter the Transfer Server for the MDI selected above. This should be configured to use the FTP network name.
14. Username: **movie**
15. Leave the Password and Public Address fields blank.
16. To put changes into effect, click **Apply**.
17. When prompted to restart the MDI, click **Yes**.

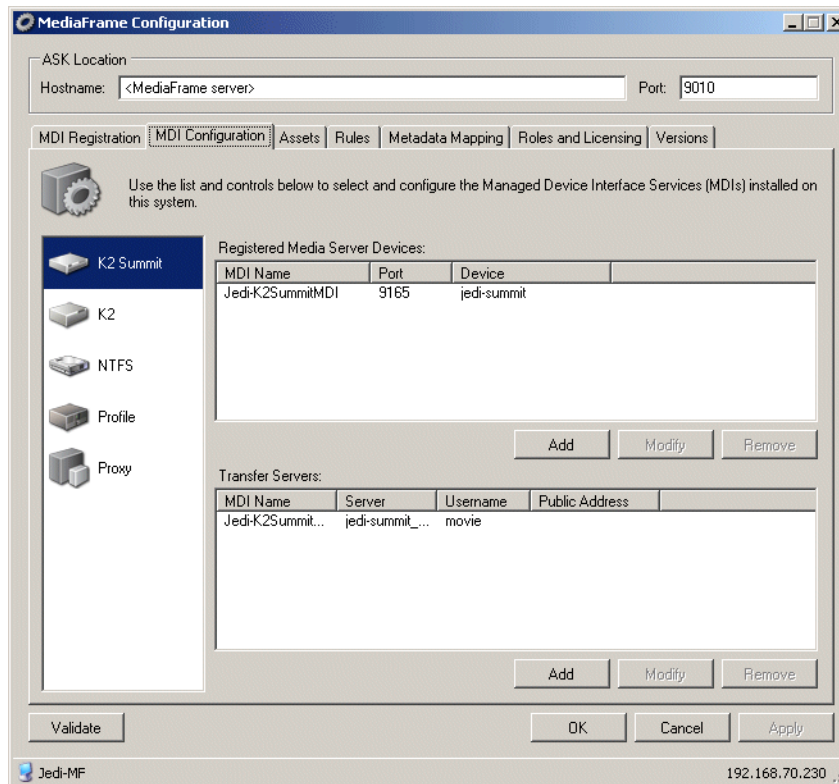
Configure K2 Summit MDI

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

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

Multiple K2 Summit 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 MediaFrame ASK: Register components” on page 84](#). To make the configurations easier to read for troubleshooting purposes, add MDIs sequentially so there is a correlation between the port number and any number in the MDI name.

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



1. On the MDI server, select **Programs | Grass Valley | MediaFrame Config**. Select the MDI Configuration tab and the K2 Summit icon.
2. Enter the name of the MediaFrame server. Do not modify Port 9010. See [“Ports and services mapping” on page 47](#).
3. Under Registered Media Server Devices, click **Add**.

4. Enter the K2 Summit MDI. Use the ... button to choose the MDI.
5. Increment 9160-9169 so each K2 Summit MDI has a unique process port. For each FSM, there should be one K2 Summit MDI.
6. The default value on the Asset System Dwell Time is 120 seconds.
7. Enter a stand-alone K2 Summit Production Client or the K2 Summit Production Client on the K2 Summit storage system that the MDI will use to manage the Summit SAN. For a K2 SAN add all of the other client host names to the "Other Clients on the SAN". If Aurora Edit is setup to send directly to the K2 Summit server, add the K2 Summit server name to this list.
8. Enter the number of maximum concurrent transfers. The maximum number of concurrent transfers allowed depends on your system's configuration. For assistance determining the maximum number of allowed transfers, contact your Grass Valley representative.
9. Enter the username, domain (if necessary), and password. The username and password need to have permissions to access the K2 AppCenter application on the K2 client.
10. Click **Add** as a managed device.

The following settings enable transfers. You should add all available transfer targets, as specified in ["Configuring transfer targets" on page 87](#).

11. Under Transfer Servers, click **Add**.
12. Use the drop-down list to specify the MDI name.
13. Enter the Transfer Server for the MDI selected above. This should be configured to use the FTP network name.
14. Username: **movie**
15. Leave the Password and Public Address fields blank.
16. To put changes into effect, click **Apply**.

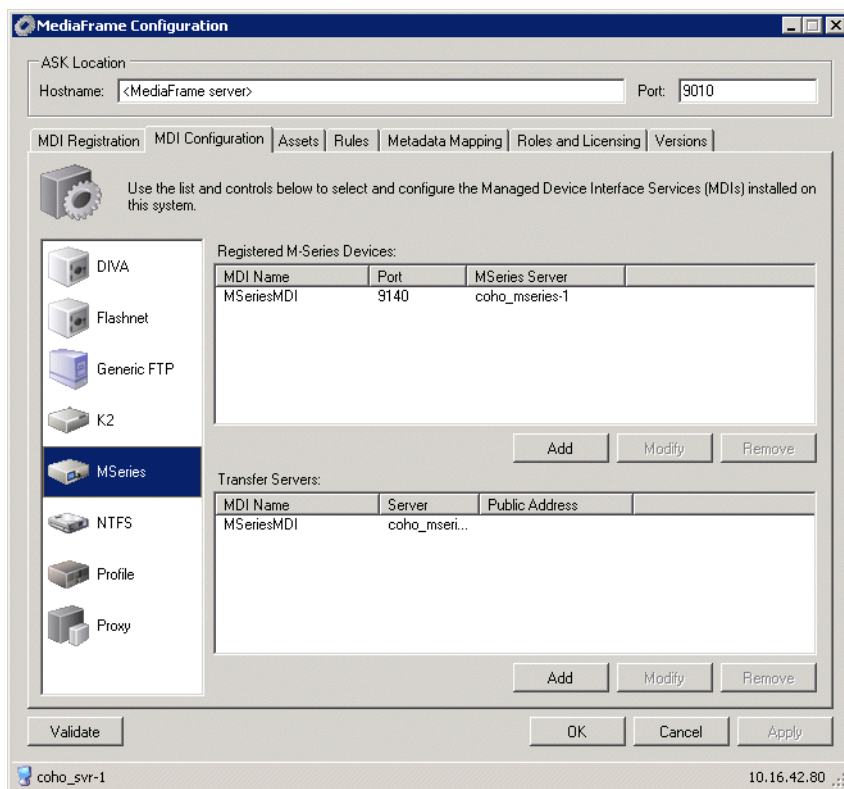
17. When prompted to restart the MDI, click **Yes**.

Configure M-Series MDI

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

Multiple M-Series MDIs run on a single machine (the MDI Server), but they each need their own process port number. For this purpose, enter incrementing numbers in the “Port” field. The MDIs and their port numbers must match settings as in [“Configure MediaFrame ASK: Register components” on page 84](#). To make the configurations easier to read for troubleshooting purposes, add MDIs sequentially so there is a correlation between the port number and any number in the MDI name.

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

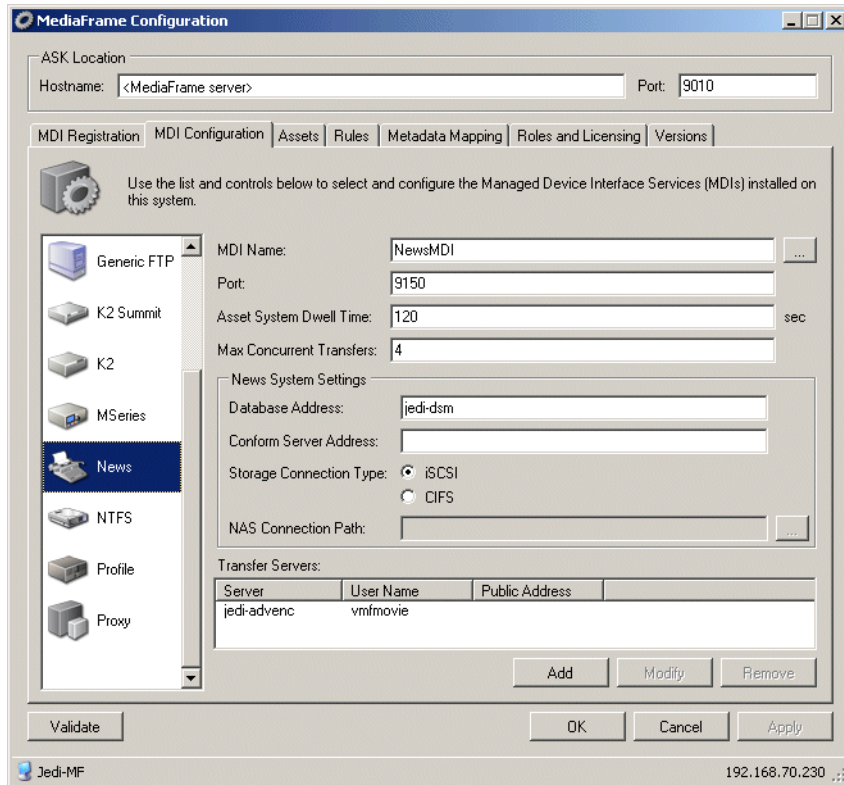


1. Locally on the MDI server, select **Programs | Grass Valley | MediaFrame Config**. Select the MDI Configuration tab.
2. Enter the name of the MediaFrame server. Do not modify Port 9010. See [“Ports and services mapping” on page 47](#).
3. Select the M-Series MDI tab.
4. Under Registered M-Series Devices, click **Add**.
5. Enter the MDI name or click ... to browse for the M-Series MDI.
6. Enter the port number 9140.

7. Enter the name of the M-Series server.
 8. The default value on the Asset System Dwell Time is 120 seconds.
 9. Click **Add** as a managed device.
 10. If adding an additional M-Series MDI, increment the port number, e.g. enter 9141.
- The following settings enable transfers. You should add all available transfer targets, as specified in [“Configuring transfer targets” on page 87](#).
11. Under Transfer Servers, click **Add**.
 12. Use the drop-down list to specify the MDI name.
 13. Enter the Transfer Server for the MDI selected above.
 14. Leave the Public Address field blank.
 15. To put changes into effect, click **Apply**.
 16. When prompted to restart the MDI, click **Yes**.

Configure News MDIs

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



1. Locally on the DSM or MDI server, select **Programs | Grass Valley | MediaFrame Config**. Select the MDI Configuration tab.
2. Enter the name of the MediaFrame server. Do not modify Port 9010. See [“Ports and services mapping” on page 47](#).
3. Select a News MDI.
4. Port 9150 is required. See [“Ports and services mapping” on page 47](#).
5. Asset System Dwell Time — The time that the News MDI waits before it informs the MediaFrame system that a clip has finished recording. Leave at 120 seconds.
6. Enter the number of maximum concurrent transfers.
7. Enter the machine that hosts the Aurora Edit database (the DSM).
8. Enter the machine that hosts the conform service (typically the Conform Server). If Aurora Edit has not been installed, leave blank.
9. The V: drive must be mapped on the machine that hosts the News MDI. Typically, the News MDI uses the CIFS mount. Specify the NAS connection path; the News MDI then maps the drive for the News MDI service account.

NOTE: *If an (iSCSI or Fibre Channel) SNFS mount of the V: drive is available on the News MDI host, the News MDI will use the mount as required to fulfill the MDI's service requests for the V: drive, regardless of the Storage Connection Type and NAS Connection Path entries.*

If using Aurora Edit LD in No-V mode, if voiceover and graphic media are stored on the proxy NAS, the NAS must be mapped on the News MDI.

For example, if the NAS Server media path for a No V Aurora LD is \\K2-proxy-nas\vo-graphics, the NAS connection path on the News MDI would be Z:\\K2-proxy-nas\vo-graphics.

If you need to configure multiple NAS systems in the MediaFrame Configuration tool, use this format:

```
V:\\k2-highres-share\V | Z:\\K2-proxy-nas\vo-graphics
```

The following settings enable transfers. You should add all available transfer targets, as specified in [“Configuring transfer targets” on page 87](#).

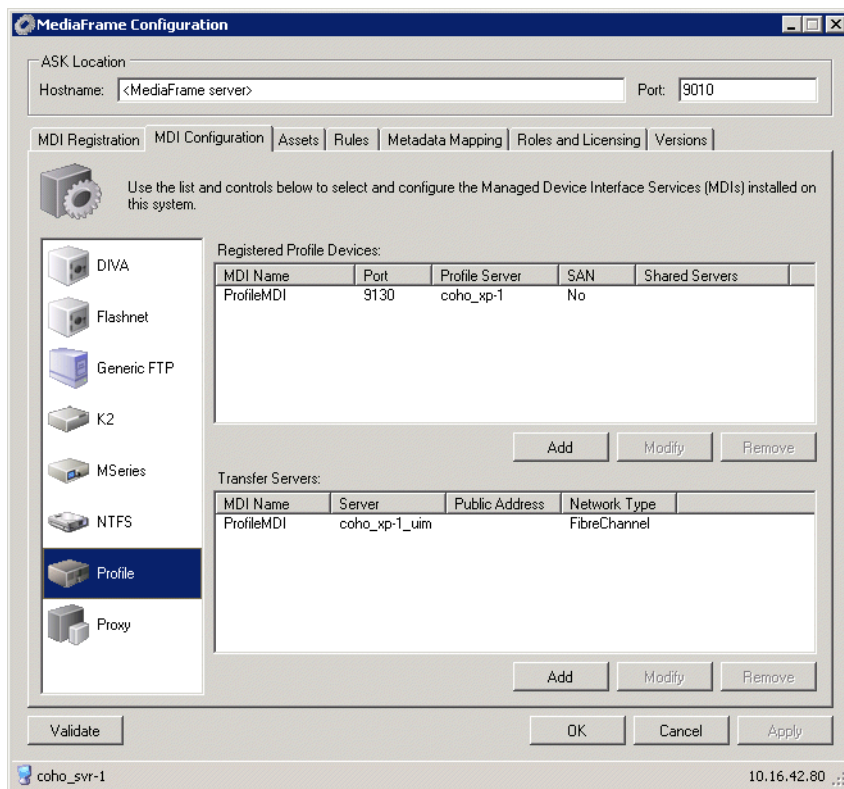
10. Under Transfer Servers, click **Add**.
11. Enter a username and the Transfer Server for the MDI selected above. This should be configured to use the FTP network name.
12. Leave the Password and Public Address fields blank.
13. Click **Validate** to test the configuration settings. To put changes into effect, start or restart News MDI Service on the MDI server (DSM).

Configure Profile MDI

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

Multiple Profile MDIs run on a single machine (the MDI Server), but they each need their own process port number. For this purpose, enter incrementing numbers in the “Port” field. The MDIs and their port numbers must match settings as in [“Configure MediaFrame ASK: Register components” on page 84](#).

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.

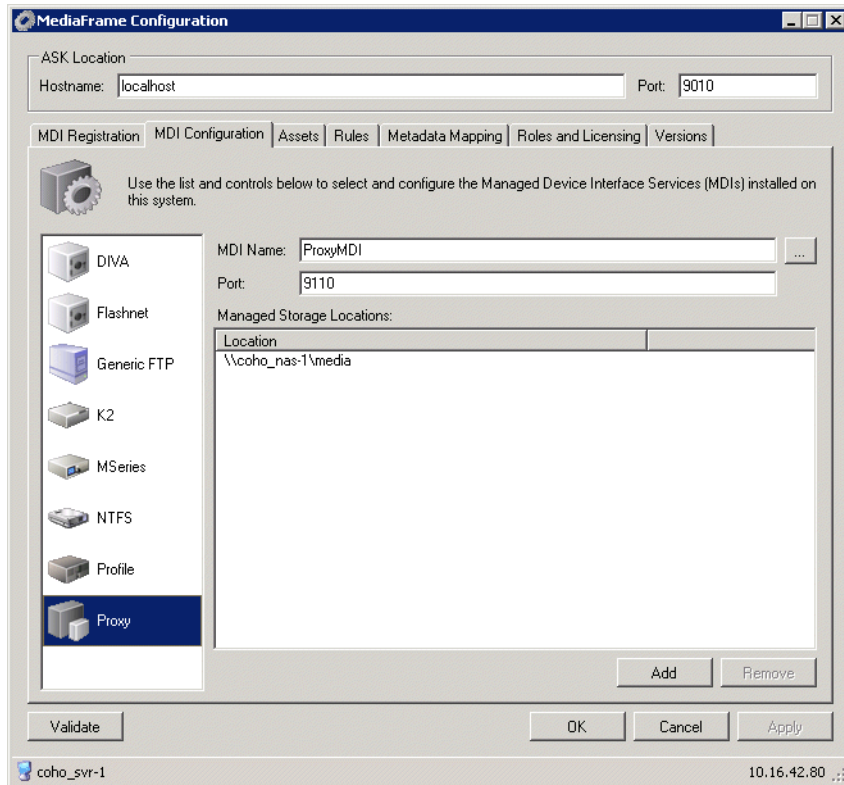


1. Locally on the MDI server, select **Programs | Grass Valley | MediaFrame Config**. Select the MDI Configuration tab.
2. Enter the name of the MediaFrame server. Do not modify Port 9010. See [“Ports and services mapping” on page 47](#).
3. Select the Profile MDI tab.
4. Under Registered Profile, click **Add**.
5. Enter the MDI name or click ... to browse for the Profile MDI.
6. Enter the port number 9130.
7. Enter the primary and secondary profile names.

8. The default value on the Asset System Dwell Time is 120 seconds.
 9. Make sure the StandAlone radio button is checked.
 10. Click **Add** as a managed device.
 11. If adding an additional Profile MDI, increment the port number, e.g. enter 9131.
- The following settings enable transfers. You should add all available transfer targets, as specified in [“Configuring transfer targets” on page 87](#).
12. Under Transfer Servers, click **Add**.
 13. Use the drop-down list to specify the MDI name.
 14. Enter the Transfer Server for the MDI selected above.
 15. Use the drop-down list to specify the network type.
 16. Leave the Public Address field blank.
 17. To put changes into effect, start or restart the Profile MDI service on the MDI Server.

Configure Proxy MDI

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



1. Select **Programs| MediaFrame Config**. Select the MDI Configuration tab and the Proxy icon.
2. In the Ask Location hostname field, enter the name of the MediaFrame server. Do not modify Port 9010. See [“Ports and services mapping” on page 47](#).
3. Set the MDI name.
4. Port 9110 is required. See [“Ports and services mapping” on page 47](#).
5. To add a storage location, click **Add**.
6. For each Proxy NAS machine, enter the UNC path to the “Media” folder. This is the location to which the system writes the proxy media.¹ Click **Add**.
7. Click **Apply** or **OK** after you’ve finished making changes.
8. To put changes into effect, start or restart the Proxy MDI Service on the MediaFrame server.

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

Test: MediaFrame stage

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

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

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

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

Checklist: MediaFrame stage

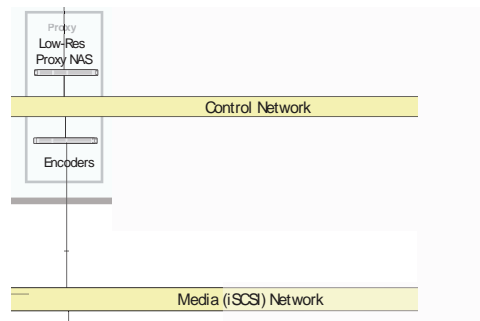
Use the following check list to verify that the basic configuration and testing of the MediaFrame stage is complete.

- All logical MDI names and Encoder service names are registered with ASK.
- All machines taking the role of MDI server have the appropriate MDI services installed and running.

Encoder stand-alone stage

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

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



Refer to [“The MediaFrame system” on page 14](#) for a view of the entire system.

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

1. Configure the encoder:
 - [“Configure SmartBin Encoder” on page 106](#)
 - or
 - [“Configure Aurora Proxy Encoder” on page 110](#)
2. [“Checklist: Encoder stand-alone stage” on page 114](#)

Configure SmartBin Encoder

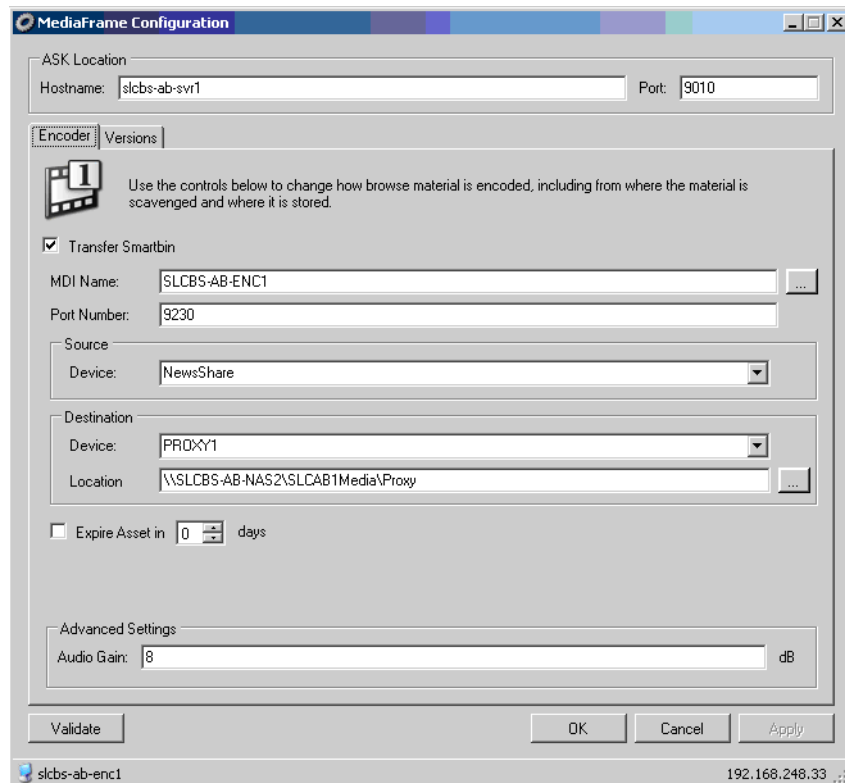
This section describes configuring the SmartBin Encoder. To configure an Aurora Proxy encoder, see [“Configure Aurora Proxy Encoder” on page 110](#).

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

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

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

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



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

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

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

It is recommended that you dedicate at least one SmartBin Encoder to scavenge newly edited material that you place in an “Outbox” folder. Refer to [“Design considerations - Aurora Browse with Aurora Edit” on page 17](#).

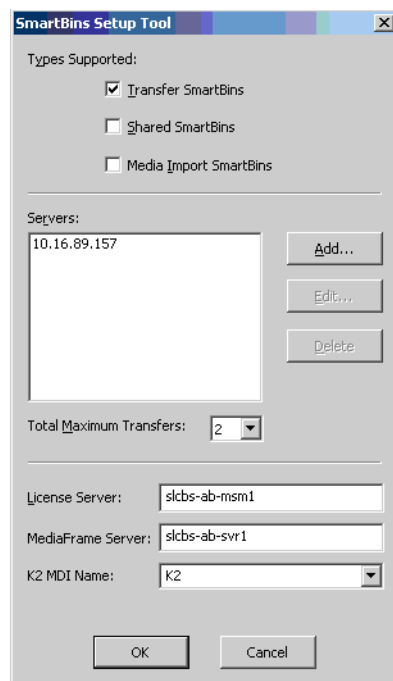
You can dedicate the SmartBin Encoder to a particular low-res proxy NAS location.

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

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

To configure the SmartBin Encoder, do the following.

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



2. Under Types Supported, check the Transfer SmartBins box. Do not check the other boxes.
3. Click the **Add** button. The Edit Server Settings dialog box appears.
4. Enter the name of the Profile, M-Series, or K2 client that you are using.
5. Select the Server Type from the drop-down list and click **OK**.
6. Specify the license server. This is the server where the MOV generation license is located.
7. Specify the MediaFrame server, and K2 MDI and click **OK**. The SmartBins Setup Tool closes, and the SmartBin service restarts.

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

8. Select **Programs | Grass Valley | MediaFrame Config** and select the Encoder tab.
9. Enter the host name of the machine that hosts the ASK location. If this service is on the same machine as the SmartBin Encoder, enter *localhost*. Port 9010 is required. See [“Ports and services mapping” on page 47](#).
10. Use the ... button to select the MDI. For the first encoder, port 9230 is required. See [“Ports and services mapping” on page 47](#). For any additional encoders, the port number is automatically incremented, e.g. 9231.
11. In the Source section, use the drop-down list to select a source Device. For MDI Name, select the News Share MDI name.
12. In the Destination section, use the drop-down list to select a destination Device.
 - To configure the Aurora Proxy Encoder to process proxy media on one location, select that location as the Proxy Storage Location. Use the ... button to browse to the folder (\Media) on the NAS (or other storage location) that receives the MPEG this encoder creates.¹
 - You can only select one low-res destination; you cannot specify multiple locations.
13. Optionally, you can check the Expire Asset box. If unchecked, the MediaFrame asset is not set to expire. If checked, the encoder sets the MediaFrame asset to expire in the specified number of days.

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

14. In the Advanced Settings section, you can adjust the Audio Gain Level to calibrate Aurora Edit LD audio, or to improve the quality of the desktop audio (e.g. if the source is 'too hot').
15. In the MediaFrame Config tool, click **Apply**.
16. Press the **Validate** button to test the status of the current configurations. If the configurations are valid, click **OK** to exit the MediaFrame Config tool.

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

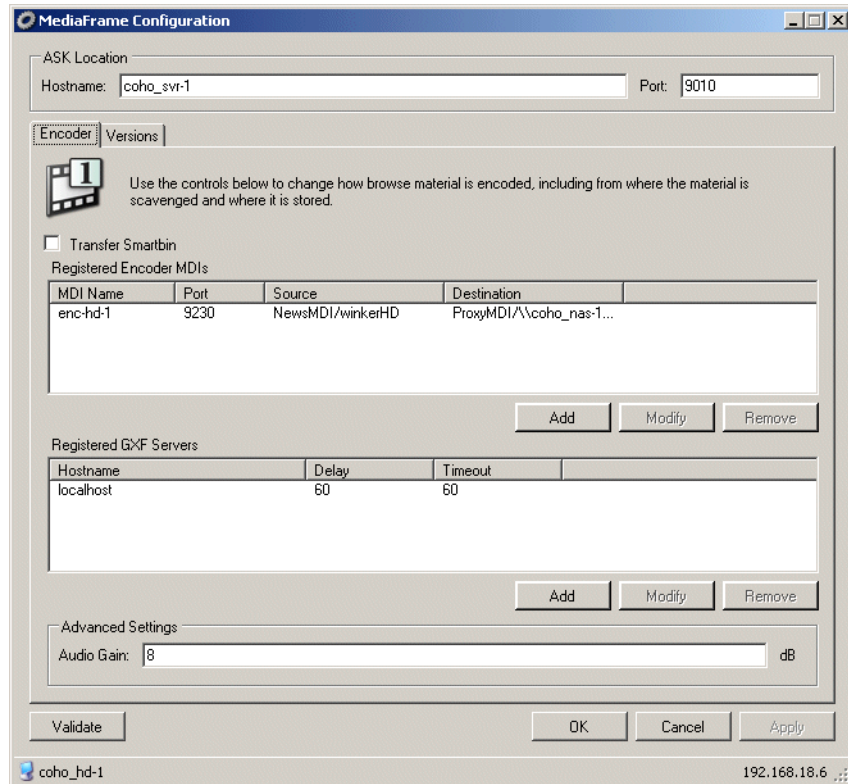
If configuring the encoder for unicode languages, see [“Configuring the encoder for unicode languages”](#) on page 113.

Configure Aurora Proxy Encoder

This section describes configuring the Aurora Proxy Encoder. To configure a SmartBin encoder, see [“Configure SmartBin Encoder” on page 106](#).

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

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



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

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

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

It is recommended that you dedicate at least one Aurora Proxy Encoder to scavenge newly edited material that you place in an “Outbox” folder. Refer to [“Design considerations - Aurora Browse with Aurora Edit” on page 17](#).

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

To configure the Aurora Proxy Encoder, do the following.

1. On the Aurora Proxy Encoder machine, select **Programs | Grass Valley | MediaFrame Config** and select the Encoder tab.
2. For the ASK location, enter the name of the MediaFrame server. Port 9010 is required. See [“Ports and services mapping” on page 47](#).
3. On the Encoder tab under Registered Encoder MDIs, click **Add**.
4. Use the ... button to select the MDI. For the first encoder, port 9230 is required. See [“Ports and services mapping” on page 47](#). For any additional encoders, the port number is automatically incremented, e.g. 9231.
5. In the Source section, use the drop-down list to select a source Device:
 - For MDI Name, select a valid MDI Name.
 - To scavenge material in an “Outbox” folder on a K2 Storage System, select the K2 MDI.
6. In the Source section, use the ... button to select a source location:
 - For Storage Location, select a valid Storage Location.
 - To scavenge material in an “Outbox” folder on a K2 Storage System, select the specific folder.
7. In the Destination section, use the drop-down list to select a destination Device.
 - To configure the Aurora Proxy Encoder to process proxy media on one location, select that location as the Proxy Storage Location. Use the ... button to browse to the folder (\Media) on the NAS (or other storage location) that receives the MPEG this encoder creates.¹
8. To configure the GXF Server and MPEG encoder options, click **Add** in the Registered GXF Servers section. The Add GXF Server dialog box displays.
 - a. Enter the GXF Server Host Name. This is usually set to localhost. For an encoder used with K2 BaseCamp Express, set the GXF server to point to the K2 FTP server.
 - b. Max Startup Delay — Enter the maximum time the encoder waits for recording to begin after a clip is created in the database. 60 seconds is the recommended setting.²
 - c. Stream Timeout — Enter the maximum time the encoder waits for a break in the

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

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

media stream to be restored. 60 seconds is the recommended setting.¹

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

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

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

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

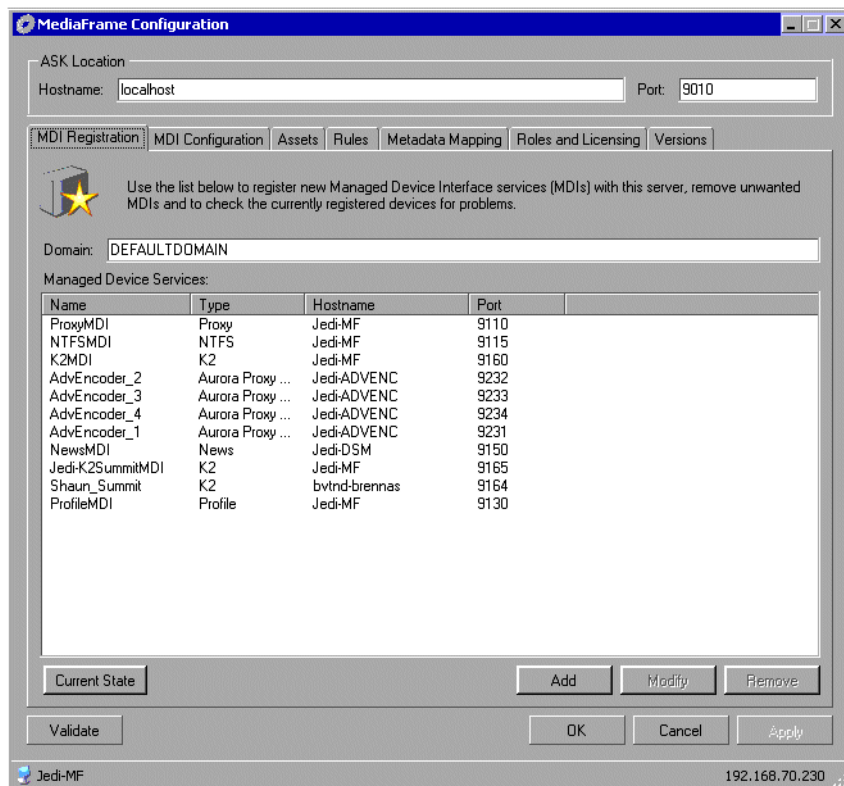
If configuring the encoder for unicode languages, see [“Configuring the encoder for unicode languages”](#) on page 113.

Configure multiple proxy encodes on Aurora Proxy Encoder

If you are configuring multiple proxy encodes on an Aurora Proxy Encoder server, make sure there is a unique MDI name for each encode.

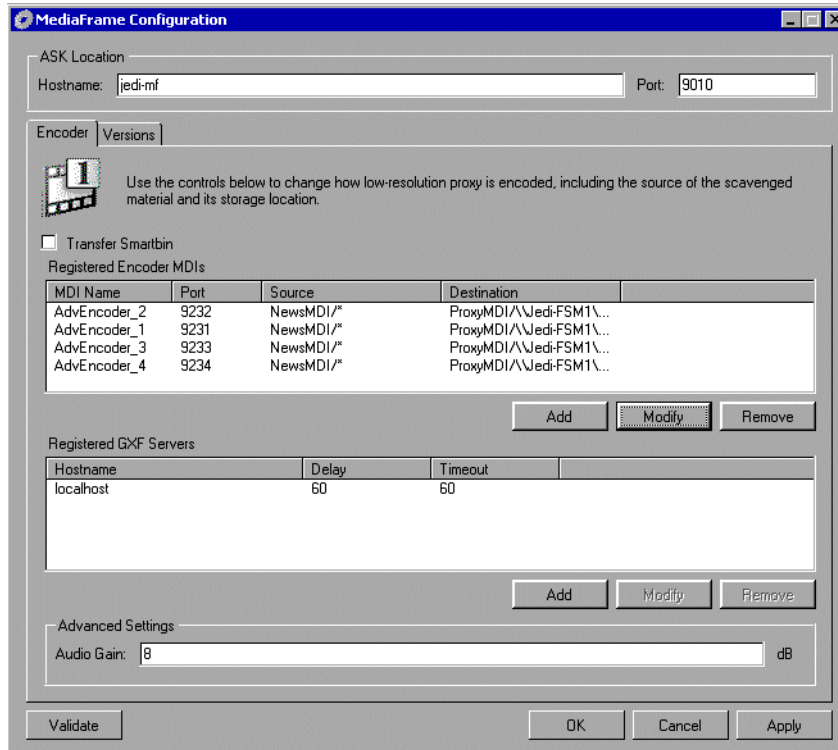
NOTE: An encoder license is required for each stream.

On the MediaFrame Server, configure in the following manner:



1. 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.

On the Encoder, configure in the following manner:

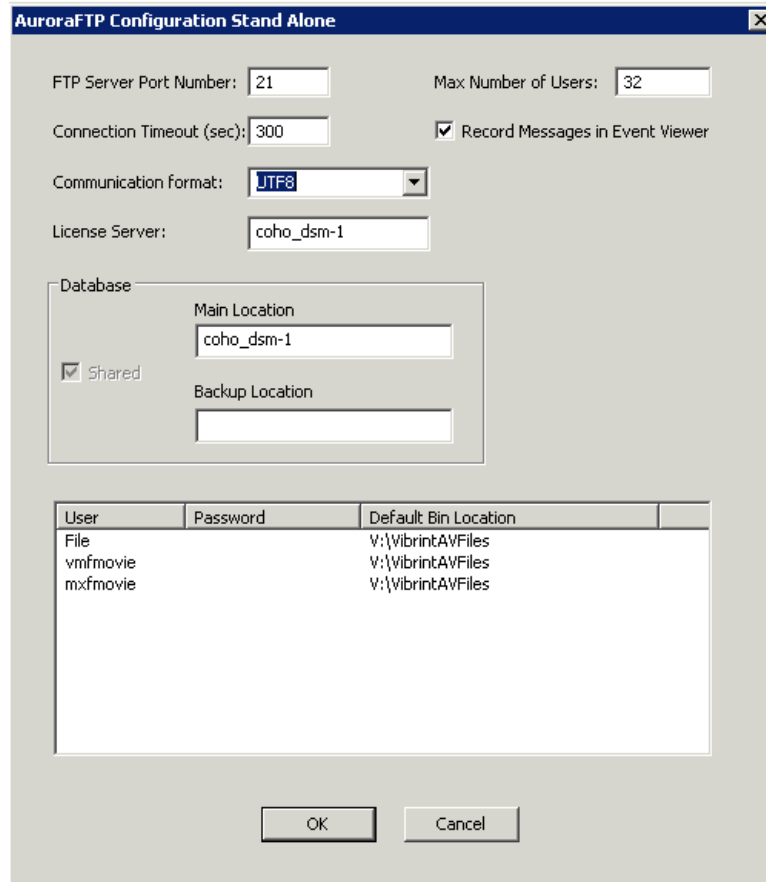


Configuring the encoder for unicode languages

If your system is encoding assets that use unicode languages, the Aurora FTP communication format needs to be set to UTF8.

To configure the encoder for unicode, follow these steps.

1. From the Start menu on the encoder, select **Programs | Grass Valley | Aurora FTP**.
2. In the AuroraFTP configuration dialog box, click the Communication format drop-down list.
3. Select **UTF8**.



Checklist: Encoder stand-alone stage

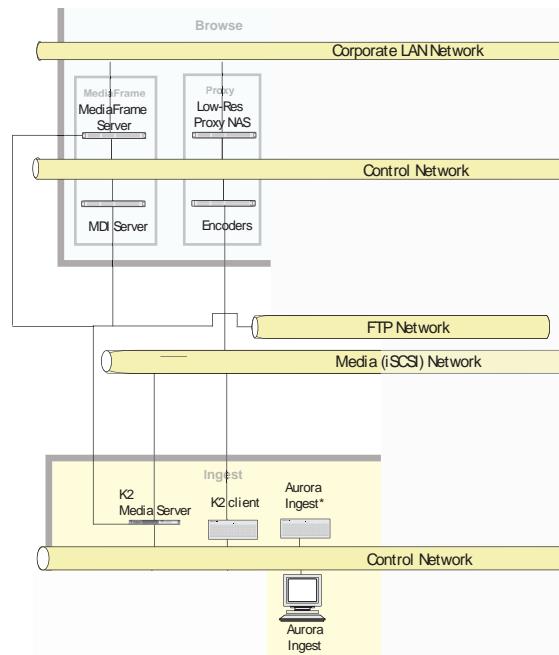
Use the following check list to verify that the basic configuration and testing of the stand-alone encoder is complete.

- Encoder is connected to NAS
- Encoder writes to NAS
- MPEG created
- MPEG playback with audio
- Storyboard files are created.

Encoder + Server stage

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

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



Refer to “[The MediaFrame system](#)” on page 14 for a view of the entire system.

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

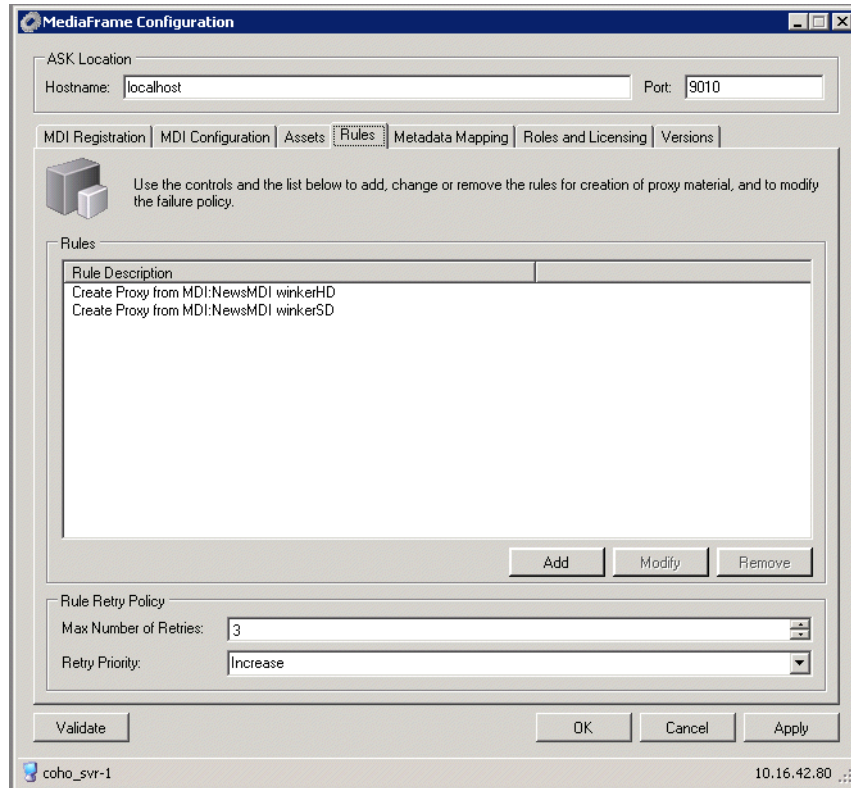
1. “[Configure Media Frame Core ASK: Encoder](#)” on page 115
2. “[Configure Rules Automation: Encoder](#)” on page 116
3. “[Test: Encoder + Server stage - high-res source](#)” on page 120

Configure Media Frame Core ASK: Encoder

Make sure the encoder’s proxy transfer service is registered with the ASK software component with a logical name, as explained in “[Configure MediaFrame ASK: Register components](#)” on page 84. If ASK is down, you need to manually enter the names, and they must match exactly. Therefore, where possible, use the drop-down list to ensure the exact name.

Configure Rules Automation: Encoder

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

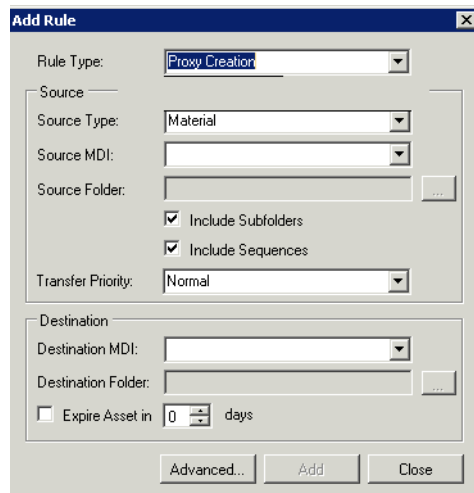


To scavenge newly edited material in an “Outbox” folder on a K2 Storage System, for MDI Name, select the K2 MDI and location as in [“Configure Aurora Proxy Encoder” on page 110](#).

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. Configure the rules after you have all the MDIs configured with their correct names.*

Before configuring rules, make sure to apply all previous configuration changes. To configure a rule defining the creation of proxy assets, do the following:

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



2. Using the Rule Type drop-down list, select the Rule Type:
 - **Proxy creation** — this rule creates a MediaFrame asset and associates the source material to it, if it does not already exist. If the asset does not have proxy already associated, this rule causes proxy to be created.
 - **Asset creation** — this rule only creates a MediaFrame asset and associates the source material to it, if it does not already exist. It does not create proxy. This rule is useful for systems that don't have proxy encoders, or systems that don't want to create proxy for everything (such as systems that only want to create proxy for archived material).
3. Using the Source Type drop-down list, select the Source MDI.
4. Use the ... button to select or type in the source folder on the machine that the system monitors for new material.

NOTE: You must use forward slashes for this path.

5. Check the Include Subfolders box to also monitor for material in folders nested in "MDI Storage Location".
6. Check the Include Sequences box to include Aurora Edit sequences.
7. In the Destination section, use the drop-down list to select a destination MDI.
8. Use the ... button to select or type in the destination folder.
9. Expired assets are purged from the system after this many days. Leave blank to never expire. Refer to ["About expired assets" on page 119](#).
10. To modify the Proxy Types and Creation Options, click the **Advanced...** button.
By default, the following are selected:

- Create while recording
- Recreate proxy if content modified

For further information about these options, refer to ["About configuring rules" on page 118](#). Click **OK** when done to exit the Advanced dialog box.

11. **Add** adds the above settings as a new Proxy Creation rule.
12. The **Update Rule** button only appears if an existing rule is selected in the Existing Rules box below, in which case the button puts into effect any changes you have made to the existing rule.
13. In the MediaFrame Config tool, all currently added rules are displayed. When a rule is selected, the options above are automatically loaded with the settings for the selected rule. You can then modify the rule and update it, or modify the rule and add it as a new rule, or remove the currently selected rule
14. The Rule Retry Policy section specifies how many times the system retries a failed rule. Keep this setting at 3 or below for most rules (3 for single or dual streamed encoder, and 4 for quad-stream encoders) to prevent degradation of system performance. If all the rules have the same setting, jobs are handled in the order they were put in the database.
15. When a failed rule is retried, its priority can be changed in relation to other rules currently being processed. Set to **Increase** to promote timely processing.
16. Always click **OK** after making changes
17. You must start or restart the GV Rules Wizard service on the MediaFrame server to put changes into effect, but if you are doing the initial configuration of the Aurora Proxy Encoder + Server stage, don't start the service until instructed to do so in the Aurora Proxy Encoder + Server stage test.

The following sections explain rules.

About configuring rules

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

Rules when the source is high-res material

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

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

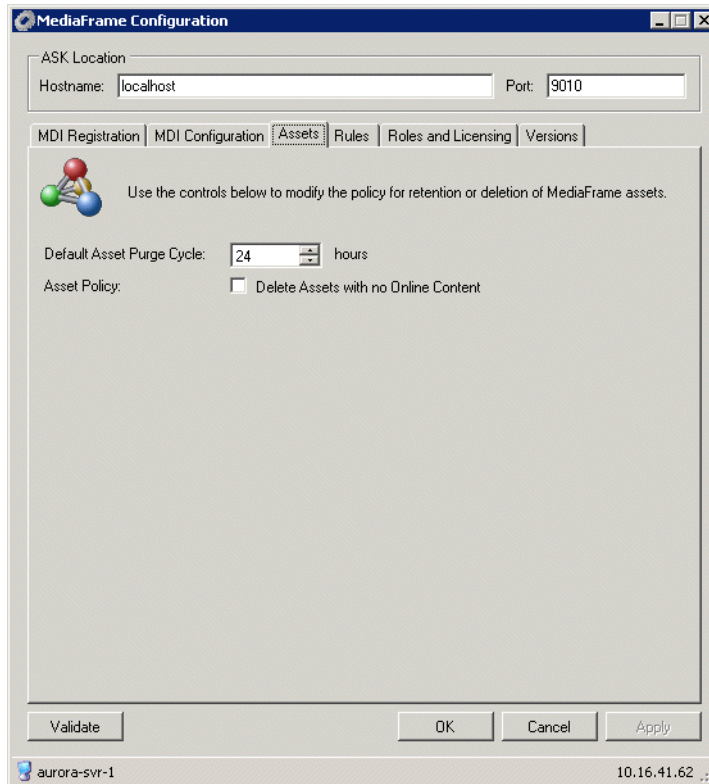
The following takes place by default with both these types of rules:

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

Tips for configuring rules

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

Configure Assets Tab



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

About expired assets

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

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

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

Recommendation:

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

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

Test: Encoder + Server stage - high-res source

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

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

Run the test as follows:

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

Checklist: Encoder + Server stage

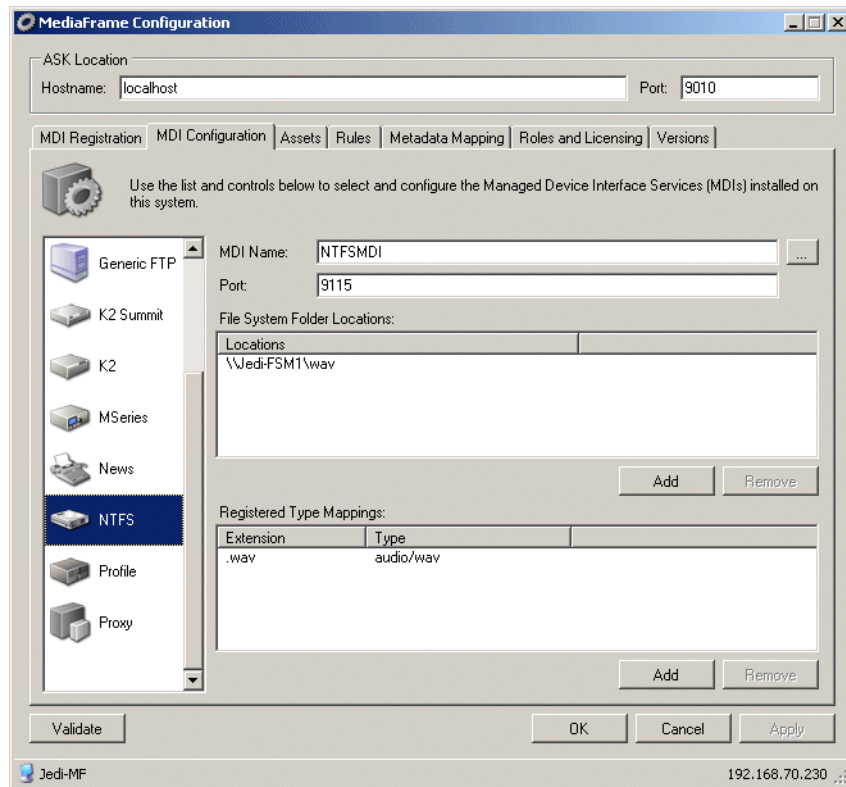
Use the following check list to verify that the basic configuration and testing of the single-channel encoder plus MediaFrame server is complete.

- When the Rules Wizard starts up, rules work as configured for the creation of

MPEG and storyboard proxy.

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

Configure NTFS MDI



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

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

1. Select **Programs | Grass Valley | MediaFrame Config**. Select MDI Configuration tab and the NTFS icon.
2. Use the ... button. Enter the name of NTFS MDI, as registered with ASK. Refer to [“Configure MediaFrame ASK: Register components” on page 84](#).
3. Port **9115** is required. See [“Ports and services mapping” on page 47](#).
4. Click the **Add** button to specify the location of the folder managed by the NTFS MDI. This must be a UNC path. The machine must have NTFS storage. (You can optionally specify the folder.)

The Locations section lists currently added machines/folders accessible by the NTFS MDI. For example, for configuring No V Aurora Edit LD systems the location for the .wav voiceover files would be something like
\\k2-proxy-nas\wav

5. The Registered Type Mappings section defines the types of files accessible by the NTFS MDI.

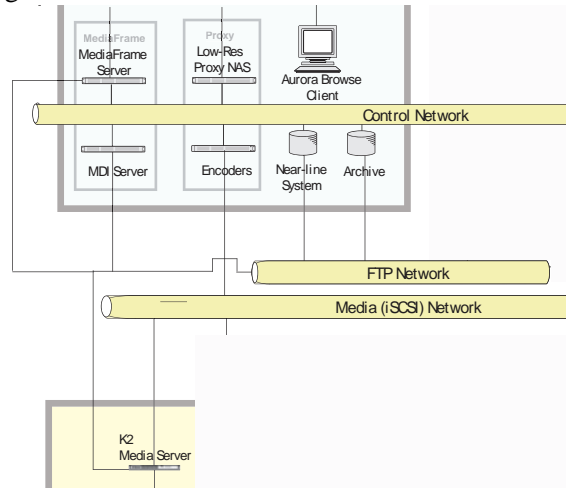
NOTE: *Do not map the edl/xml.LiteEdit type.*

6. To put changes into effect, click **Apply**.
7. When prompted to restart the MDI, click **Yes**.

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 configure and test the Archive stage, do the following:

1. [“Add archive MDI” on page 124](#)
2. [“Verify archive preparations” on page 125](#)
3. Configure your archive:
 - a. [“Configure DIVA MDI” on page 128](#)
 - b. [“Configure FlashNet MDI” on page 129](#)
 - c. [“Checklist: Archive stage” on page 130](#)
4. [“Checklist: Archive stage” on page 130](#)

Add archive MDI

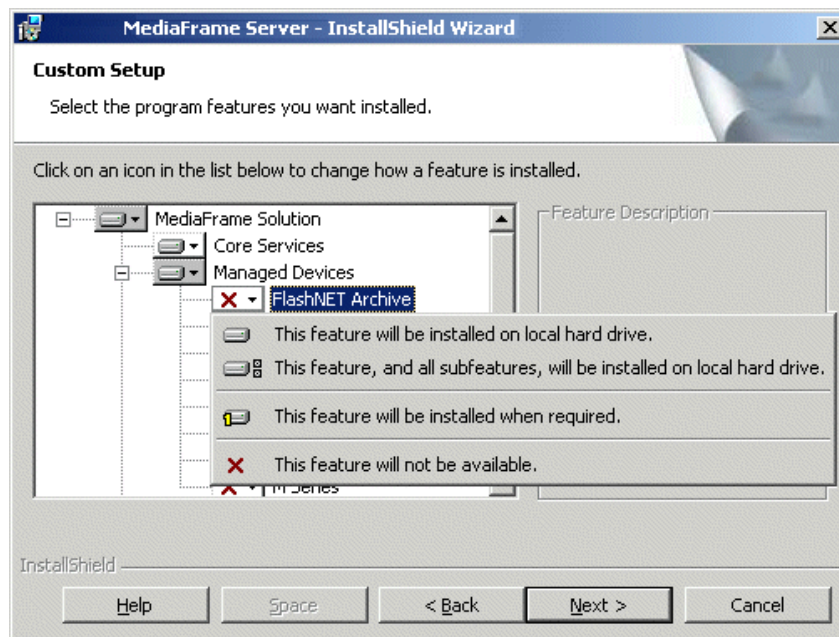
The archive MDI software component runs as a service. The archive MDIs available are as follows:

- DIVA
- FlashNet

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

NOTE: Before archiving News assets, the Aurora FTP software must be installed on the K2-Aurora FTP server.

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

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

DIVA preparations

Check the following on the machine that runs DIVA software:

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

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

- The DIVA MDI does not take any user specified name for a full restore. The clips

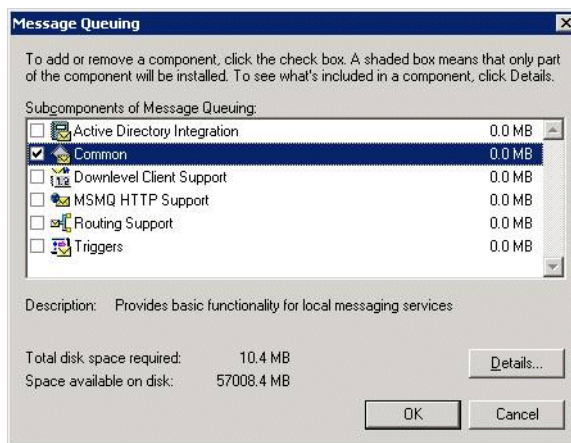
are restored using the original name (from archive). The DIVA MDI does, however, allow a user specified name for a partial restore.

- DIVA has no fixed limit for concurrent transfers.
- If archiving from a Profile XP standalone, take the concurrent transfer limit into consideration. DIVA's setting for concurrent transfers applies to specific source/destination pairs. With the configuration utility/tool you can specify the concurrency limit on a server-by-server basis.
- The DIVA MDI makes an the assumption that the MDI is the only gateway to the entire DIVA file system. Any changes made outside the scope of the MDI will not be reflected in MDI immediately.
- Renaming of an asset is not supported in DIVA.
- The MDI will use whatever priority the user chooses.
- The source name must be the same as the host name specified in the Transfer Server, not the actual machine. Under that name, specify the host name or IP address of the actual machine in the IP Address field.
- If the DIVA server is rebooted, the DIVA MDI service must be restarted. Refer to [“Accessing services” on page 80](#).

FlashNet preparations

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

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



Check the following on the Flashnet server:

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

3. Make sure the FlashNet services are up and running.

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

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

Network connectivity - all archive types

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

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

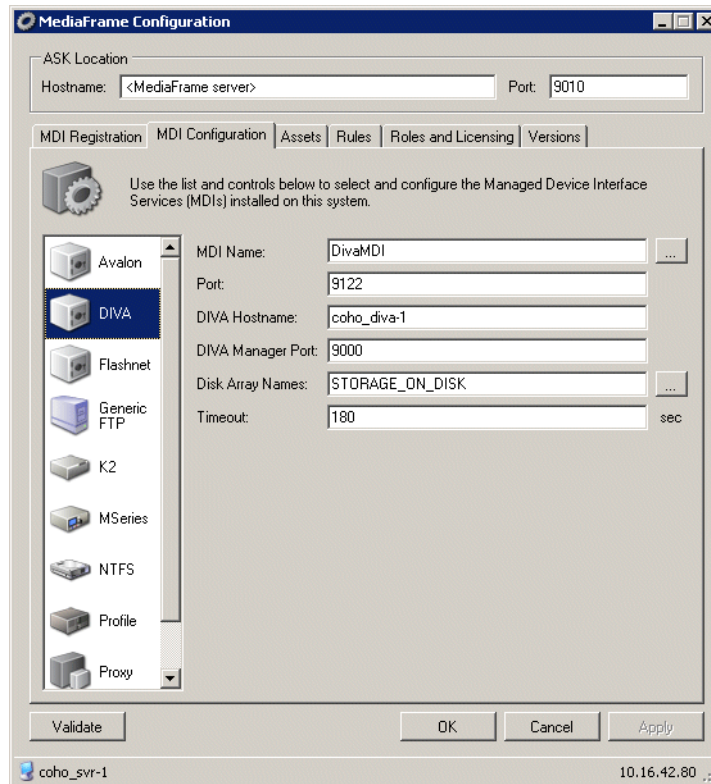
If archiving from the Aurora Share, verify that you can FTP from the DIVA or Flashnet server to the K2-Aurora FTP server through the FTP network using the `vmfmovie` login account.

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

Configure DIVA MDI

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

To configure the DIVA MDI, do the following.

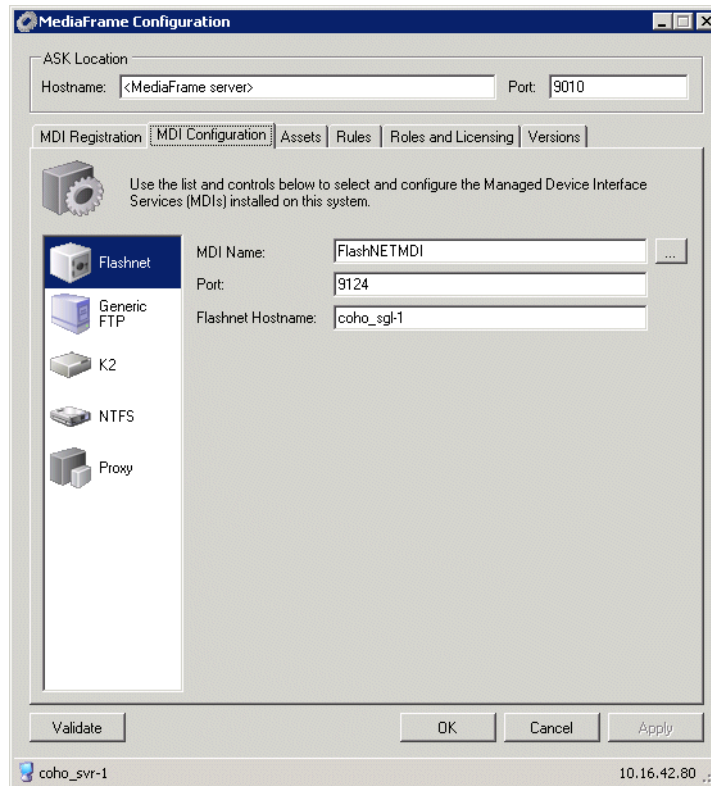


1. Select **Programs | Grass Valley | MediaFrame Config**. Select the MDI Configuration tab and the DIVA icon.
2. Use the ... button to location the name of the DIVA MDI.
3. Port 9122 is required.
4. Enter the hostname or IP address of the DIVA machine.
5. The default value for the Diva manager port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

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

Configure FlashNet MDI

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



To configure the Flashnet MDI, do the following.

1. Select **Programs | Grass Valley | MediaFrame Config**. Select the MDI Configuration tab and the Flashnet icon.
2. Enter the name of the MediaFrame server.
3. Port 9010 is required. Do not modify.
4. Use the ... button to location the name of the FlashNet MDI.
5. Port 9124 is required. See [“Ports and services mapping” on page 47](#).
6. Enter the name or IP address of the FlashNet machine.
7. Click **OK**.

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

Checklist: Archive stage

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

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

Deploy remaining machines for full system

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

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

- Deploy remaining Aurora Proxy Encoders. Refer to “[Encoder stand-alone stage](#)” on page 105 and “[Encoder + Server stage](#)” on page 115.

Test system level interactions

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

Multiple scavenge test

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

To test multiple scavenge operations, do the following:

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

Purge test

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

in the past.

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

Add Aurora Browse Clients

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

If the Aurora Browse user has administrator privileges you can use *setup.exe* to install the Aurora Browse application on the client PC. The executable file installs the prerequisites and the Aurora Browse application.

If the Aurora Browse user does not have administrator privileges, an administrator needs to install all the prerequisites for the user. The user then can install the Aurora Browse application by using the AuroraBrowse.application installer.

You can find the installer on the MediaFrame server share:

`\\MediaFrameServer\AuroraBrowse.`

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 132](#)
- [“Configure Aurora Browse Licenses” on page 133](#)
- [“Managing Aurora Browse User sessions” on page 135](#)

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.

If you have MediaFrame client applications on a different Windows domain from the MediaFrame server, you need to define a trust relationship (one way or two way). For example, you could have your MediaFrame system on Windows domain A with a trust in the B domain. Applications running on Windows domain B can then connect to the MediaFrame server on Windows domain A.

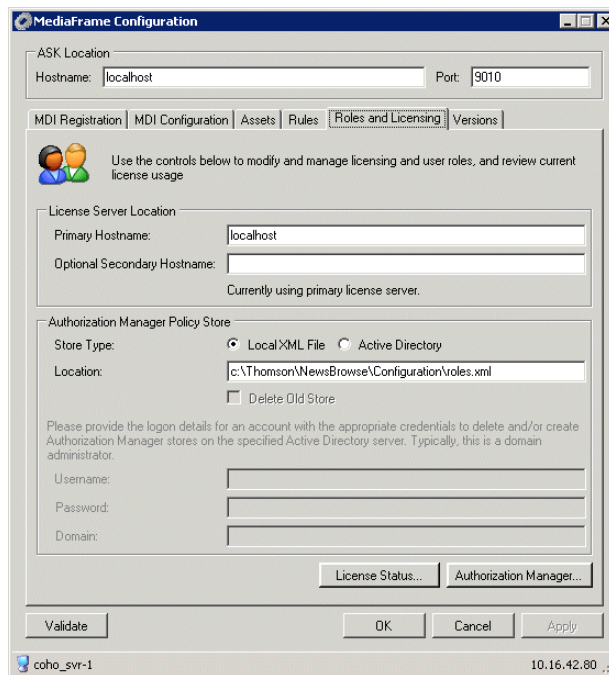
Also, make sure that permissions are correct for access to the MediaFrame server website, which serves the Aurora Browse application. The website uses Integrated Windows Authentication.

Configure Aurora Browse Licenses

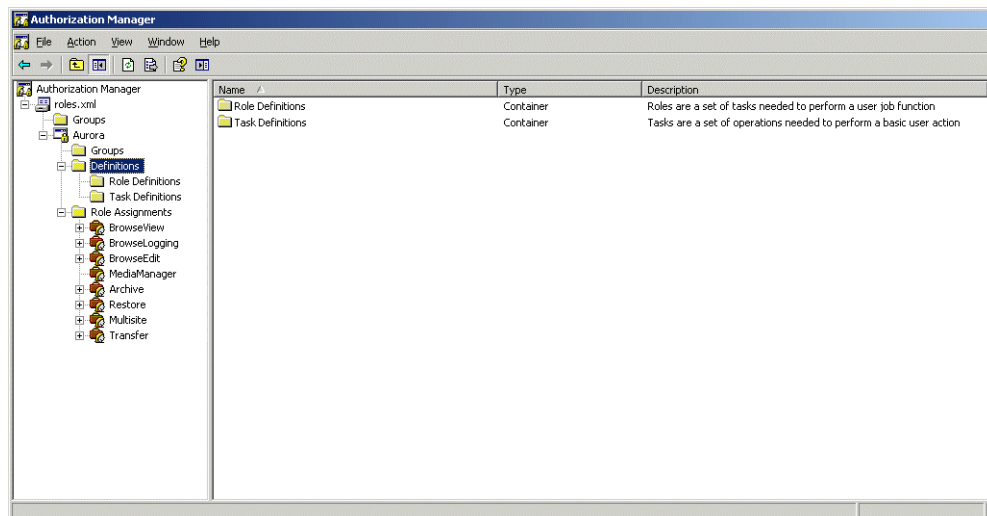
You must configure the MediaFrame server, as per your Aurora Browse license, to allow user access to Aurora Browse application features. Roles and Licensing is managed centrally from the MediaFrame server. This requires that you log in as Aurora Browse administrator. A role can be leased if the user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

To configure for Aurora Browse licenses, do the following.

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



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



3. Configure according to the Microsoft Windows documentation: add a group, then add users to that group.
4. Enter the following:
 - Username — This must match the account with which the Aurora Browse client accesses the Aurora Browse application.
 - Roles — Select the Aurora Browse application functionality to which the user needs access. The Roles listed are dependent upon current licensing.

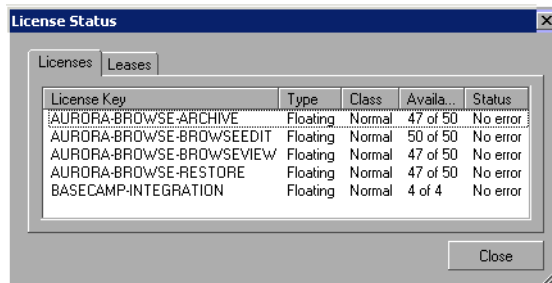
The following table defines the Roles:

Role	Description
BrowseView	Lets you search, browse, and explore assets and view them.
BrowseLogging	Lets you search, browse, edit and explore metadata.
BrowseEdit	LD editing, search, browse and explore.
MediaManager	In addition to all the other privileges in this table, MediaManager lets you search, browse, explore, delete, rename, change custom metadata schema, and create proxy.
Archive	Lets you transfer high-res assets from a K2 system to an archive device and optionally delete the high-res assets from the K2 system.
Restore	Lets you restore high-res assets from an archive device to a K2 system.
Transfer	Lets you transfer locally on the Aurora Browse system. You need to add this role even if the user has the MediaManager role.
Encoder	As of 7.0, there is no longer an Encoder role. An encoder license is used to license each encoding stream.

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

Verify license status and user sessions

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

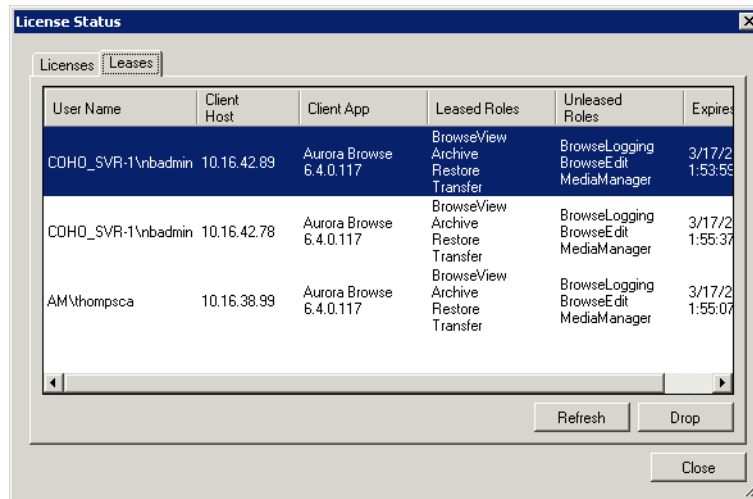


The Aurora Browse administrator sets up Aurora Browse users and can restrict their access to Aurora Browse application features and assets, as explained in the following procedures.

Managing Aurora Browse User sessions

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

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



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

Adding custom fields and metadata mapping

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

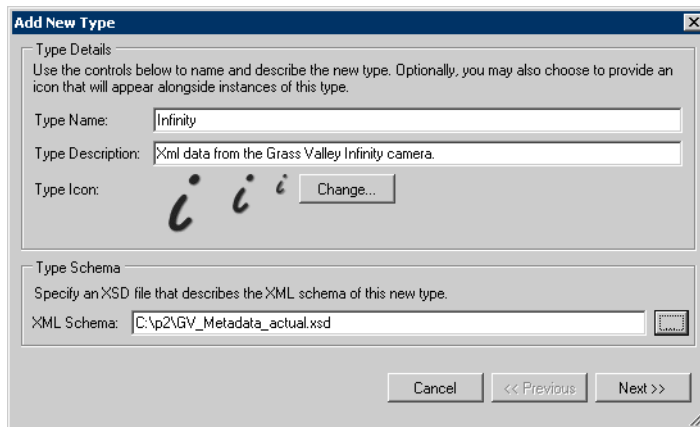
The user of the Aurora Browse application can then assign metadata to an asset by entering text or making a selection in the custom field. Adding custom fields is optional. If you have administrator-level privileges, you can add custom metadata fields in the Aurora Browse client. For more information,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

Setting up metadata mapping

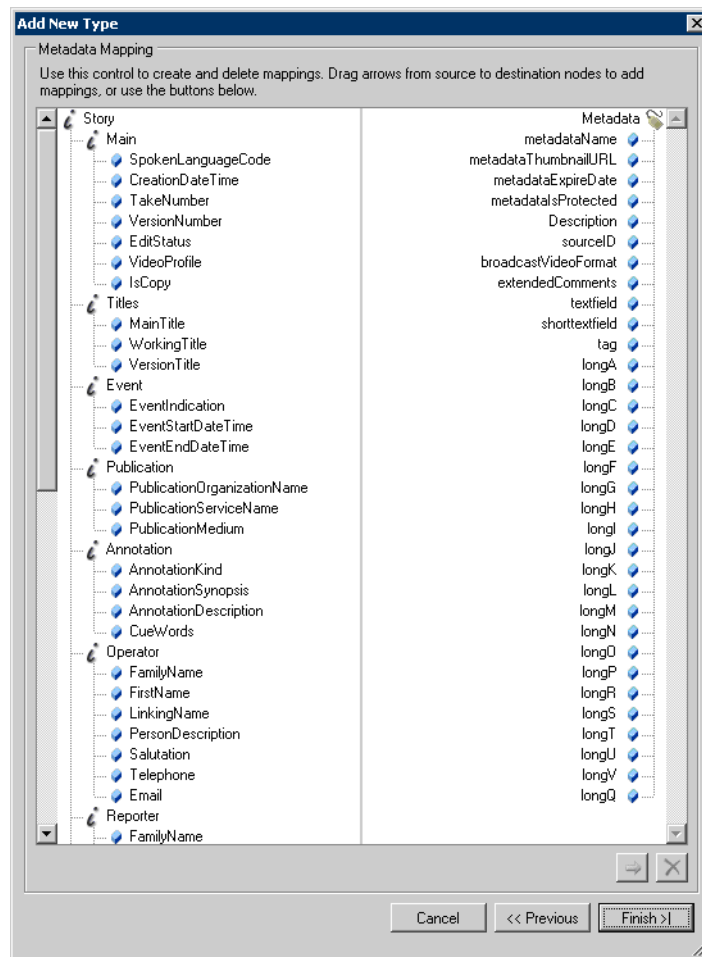
Metadata mapping registers and maps any foreign metadata (such as metadata from a camera) into the MediaFrame system. Since it is in XML format, an XML schema is needed.

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

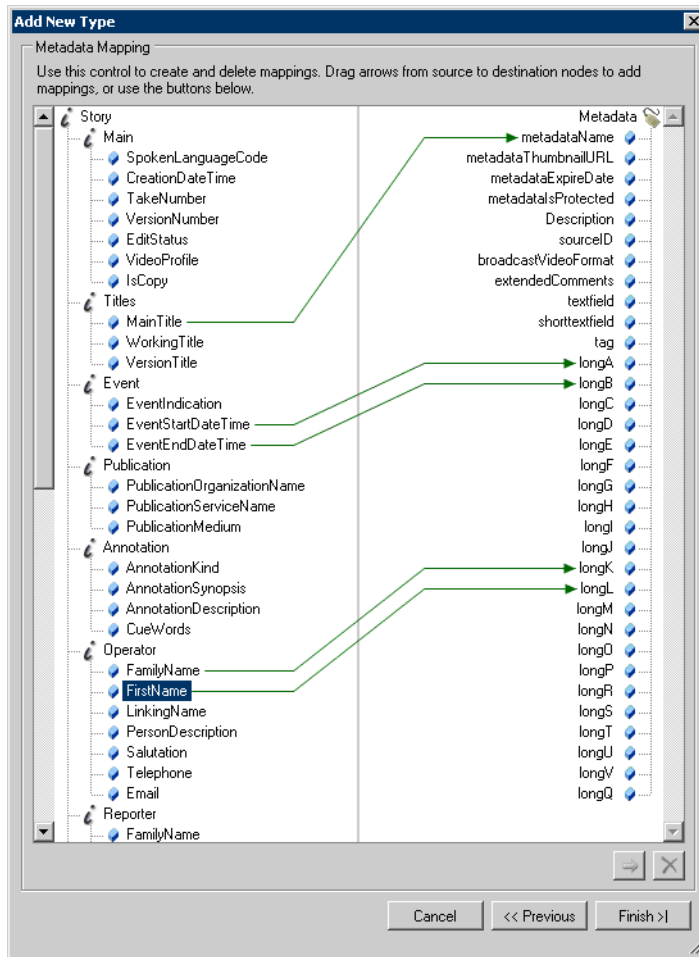
1. Select **Programs | Grass Valley | MediaFrame Config**. Select the Metadata Mapping tab.
2. Click **Add**. The Add New Type —Type Details dialog box displays.



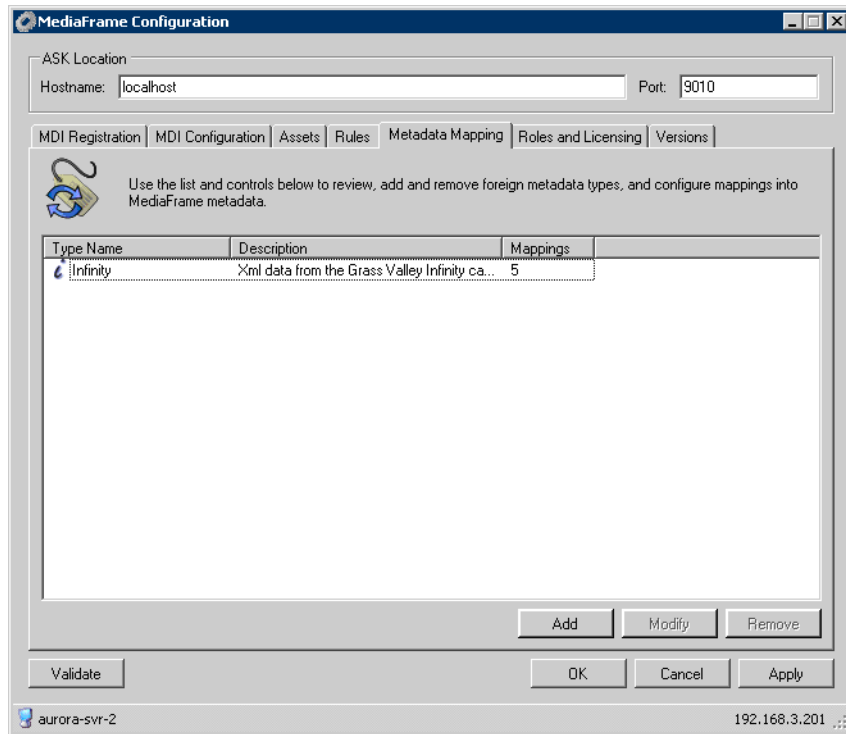
3. Enter the type name and description. If you want to change the type icon, click the **Change...** button.
4. Click the ... button to select the XML schema for this type.
5. Click **Next**. The Add New Type — Metadata Mapping dialog box displays.



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



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



About bin and asset naming limitations

The asset name, bin name, and path can include up to 259 characters (including separators such as \). Some parts of the file path are not visible in AppCenter or Aurora applications.

The file system limits the number of bytes in a name as well as the number of characters. The full count of 259 characters applies to names in English and other languages referred to in ISO 8859-1. The number of characters might be less than 259 with some other character sets.

NOTE: Try to limit path names to less than 150 characters.

The following table breaks down the character length restrictions for the sample file system path of `\media\mybin1\mybin2\MyVideo.cmf\MyVideo.xml`.

	Asset name, bin name, and path (up to 259 ^a characters, including separators such as \))			
Section of an asset/path name	The rest of the path name (i.e. everything apart from the bin and asset names)	Bin name	Asset media directory and extension	Asset name and extension

	Asset name, bin name, and path (up to 259^a characters, including separators such as \))			
Naming limitation	This part of the path name is not visible in AppCenter or Aurora applications.	The bin name can be up to 227 characters (which would leave room for only a 1-character asset name)	This part of the path name is not visible in AppCenter or Aurora applications. The directory name is the same as the asset name. 4 characters are reserved for the extension.	The extension is not visible in AppCenter or Aurora applications. At least 25 characters are reserved for the asset name and extension, even if they are not all used.
File system example	\media	\mybin mybin2	\MyVideo.cmf	\MyVideo.xml

^aThe full count of 259 characters might not be available with some character sets.

Database and Recovery Planning

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

This chapter describes strategies for planning and maintaining the database and recovery images. It is divided into two sections:

- [“Database planning and maintenance strategies”](#)
- [“Backup and recovery strategies”](#)

Database planning and maintenance strategies

Procedures in this section are as follows:

- [“Encoder failure considerations” on page 141](#)
- [“MediaFrame server failure considerations” on page 142](#)
- [“Updating the database to the simple model” on page 142](#)
- [“Creating a simple maintenance plan” on page 143](#)
- [“Verifying the database maintenance plan status” on page 145](#)
- [“Testing the backup” on page 146](#)
- [“Modifying the database maintenance plan” on page 147](#)
- [“Restoring the MediaFrame server database” on page 148](#)
- [“Updating the maintenance plan after renaming the server” on page 148](#)
- [“Reconfiguring MediaFrame after renaming the server” on page 146](#)

Encoder failure considerations

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

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

MediaFrame server failure considerations

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

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.

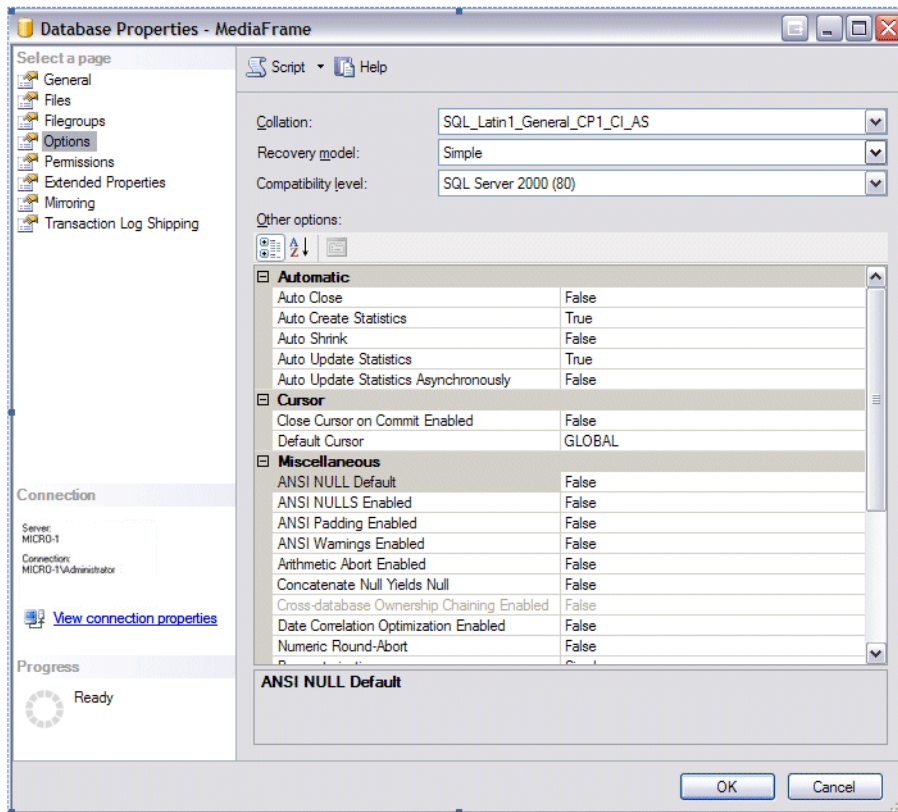
Newer systems have redundant power supplies and mirrored disks to further protect the integrity of the system.

Updating the database to the simple model

As of Aurora Browse 6.5.2, the MediaFrame database needs to be updated to the simple model. If your database is not using the simple model, it needs to be updated before you run the maintenance plan.

To update the database to the simple model, follow these steps:

1. On the MediaFrame server, open SQL Server Management Studio.
2. Connect with the administrator credentials.
3. Expand the left-hand tree view to
`<machine name> Databases | MediaFrame.`
4. Right click on **MediaFrame** and select **Properties**.
5. In the Select a page pane, select the **Options** page.
6. From the Recovery Model drop-down list, select **Simple**.
7. Verify that the rest of the settings match the following screenshot, and click **OK**.



Creating a simple maintenance plan

Maintenance plans automate database tasks necessary to ensure database integrity and recovery in case of data loss. As part of the installation process, an application was downloaded that creates a simple maintenance plan.

Before you run the MediaFrame maintenance plan application, it must be configured for your system.

Configuring the MediaFrame maintenance plan

Before you can run the MediaFrame maintenance plan, you need to change the backup location. By default, it is set for `C:\MediaFrame\Backup`, which is a folder that is not automatically set up on the system. Modify the database backup location to a network storage, preferably one that is backed up or has some kind of RAID protection.

To configure the plan, follow these steps:

1. Open the executable file in an editor application, such as Notepad. The MediaFrame maintenance plan is installed along with the MediaFrame database files:

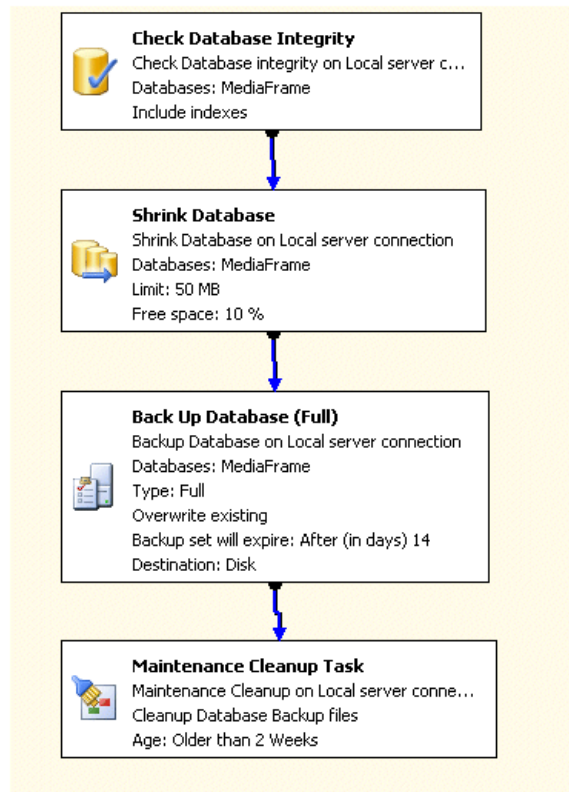
```
C:\ProgramFiles\GrassValley\MediaFrame\Database\MaintenancePlan.exe
```

2. Modify the backup location <add key="BackupLocation" value="C:\MediaFrame\Backup" /> .

3. If the database is backed up to a network share, modify the account that the SQL Server (*MSSQLSERVER*) and SQL Server Agent (*MSSQLSERVER*) run as. It needs to run using an account that has permission to write to the network shared location for the database backup.

Using the simple maintenance plan

Once you have configured the maintenance plan, you can run the executable file and it will automatically configure SQL Server to run maintenance tasks shown in the following workflow at the scheduled time.

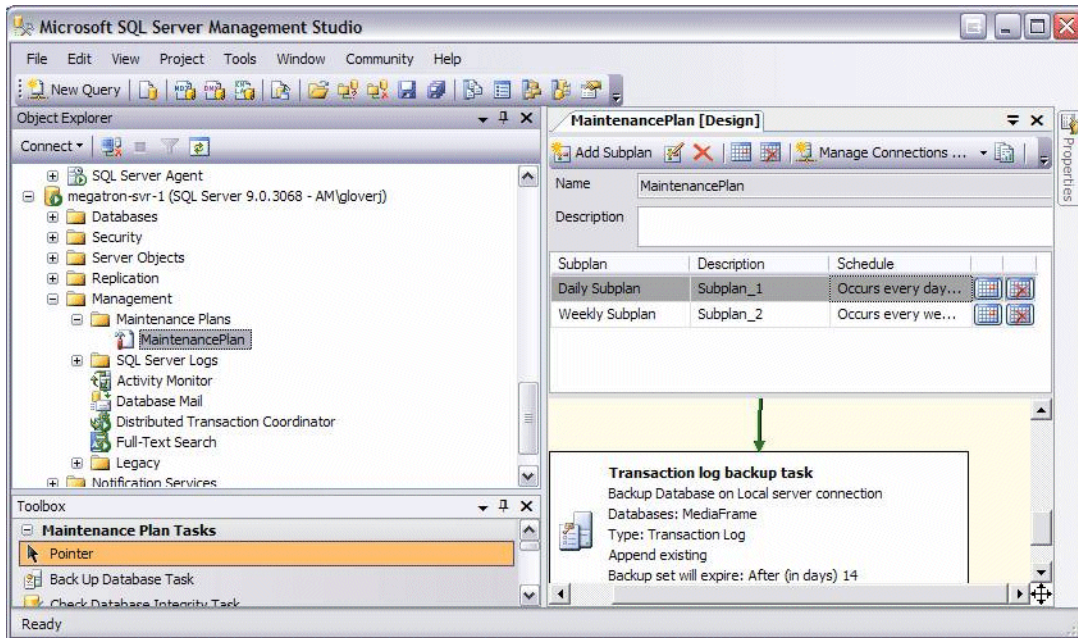


CAUTION: When you run the maintenance plan, it deletes any previously created maintenance plans and all associated jobs and schedules. To retain these files, save them under a different name before running the maintenance plan.

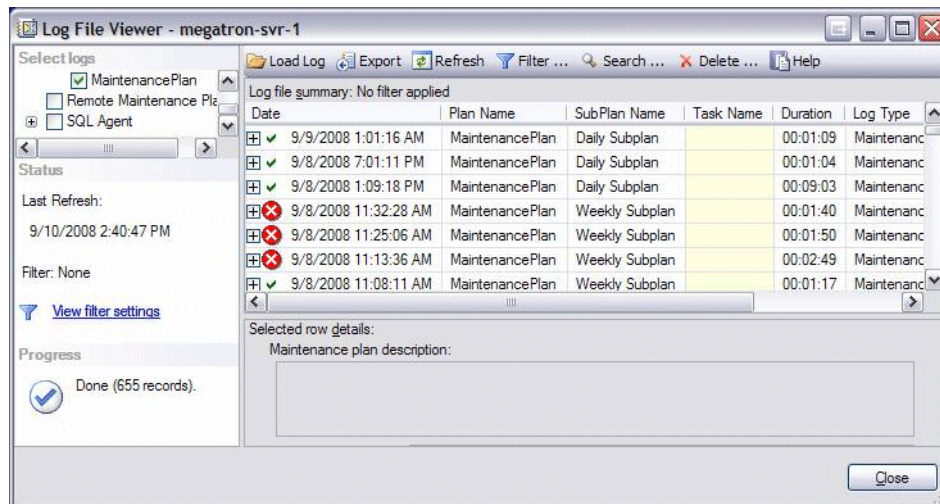
To customize the maintenance plan, use SQL Server Management Studio (SSMS) under **<server name> + Management + Maintenance Plans**. If the SSMS is open while the maintenance plan is running, the SSMS will not reflect the latest scheduling information. Restart the SSMS to display the correct information.

Verifying the database maintenance plan status

1. To determine the maintenance plan status, look in SQL Server Management Studio under **<server name> + Management + Maintenance Plans**.
2. Right-click on the plan and select **View History**.



3. Verify the status:
 - Green check mark — everything is good
 - Red X — indicates an error



Testing the backup

Database performance can be downgraded while this test is in progress, but the database will remain operational during the test.

Prerequisite: Verify that logging is turned off for IIS.

1. Right-click on MediaFrame maintenance plan.
2. Click **Execute**.

NOTE: To check for errors, view the history. See [“Verifying the database maintenance plan status” on page 145](#).

Reconfiguring MediaFrame after renaming the server

Renaming the MediaFrame server after installation can affect the operation of the system. If you rename the MediaFrame server or K2 BaseCamp Express server after the software has been installed or configured, follow these steps.

1. To update SQL with the name change, run the *ChangeServerName.bat* script found in C:\Program Files\Grass Valley\MediaFrame\Database\ChangeServerName. Follow the Readme.txt instruction located in the same folder.
2. Redo the database maintenance plan as described in [“Updating the maintenance plan after renaming the server” on page 148](#).
3. Update MediaFrame Configuration:
 - a. Make a backup copy of the configuration file:
C:\Thomson\MediaFrame\Configuration\MediaFrameCore.config
 - b. In the Configuration file, update the server name in each of the URL lines that contain the old server name.

For example:

```
<Ask Url="tcp://OldMediaFrameServerName:9010/
AskService" />
<Resolver Url="tcp://OldMediaFrameServerName:9016/
ResolverService" />
<Metadata Url="tcp://OldMediaFrameServerName:9014/
MetadataService" />
<LicenseManager Url="tcp://
OldMediaFrameServerName:9012/LicenseManagerService" />
<TransferManager Url="tcp://
OldMediaFrameServerName:9020/TransferManagerService" /
>
<SubscriptionManager Url="tcp://
OldMediaFrameServerName:9024/
SubscriptionManagerService" />
<AssetManager Url="tcp:// OldMediaFrameServerName:9022/
AssetMangerService">
```

4. In the MediaFrame Config tool, update any MDI running on the server.
5. On any other machines that access the MediaFrame server, update the configuration to use the new server name.

Modifying the database maintenance plan

The following section is based on a database maintenance plan created using the steps in [“Creating a simple maintenance plan” on page 143](#).

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 the *weekly_maintenance* subplan.

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. 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.

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.

Updating the maintenance plan after renaming the server

If you rename the MediaFrame server, you must update the maintenance plan. Renaming the server does not alter the maintenance plan.

Before updating the maintenance plan, verify that you have has SQL Server Integration Services (SSIS) installed. SSIS is part of the typical SQL Server installation.

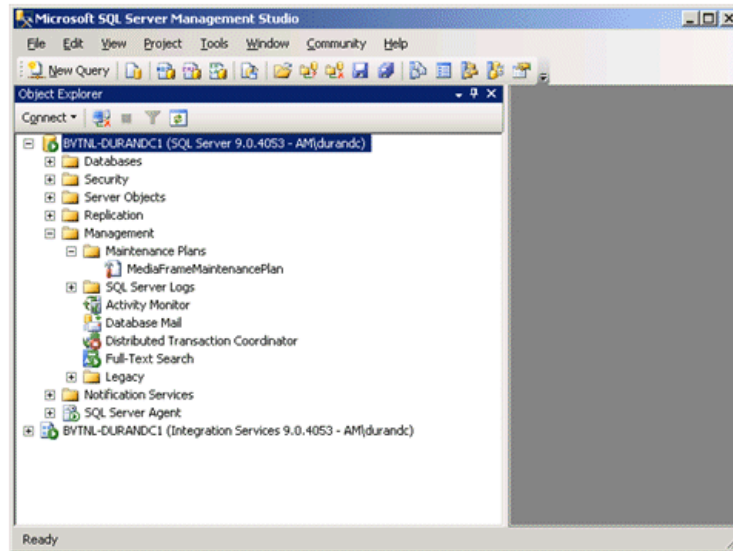
The maintenance plan update can be divided into three main sections:

- Stage 1: Exporting the maintenance plan to a file
- Stage 2: Updating the file with the new server name
- Stage 3: Importing the modified plan

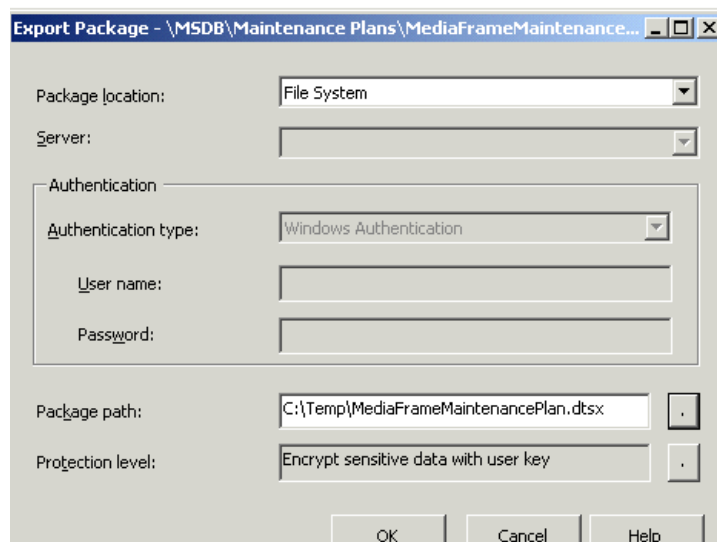
To update the maintenance plan, follow these steps:

1. Open SQL Server Management Studio (SSMS) on the server.

2. Open a connection to the local Database Engine and to the local Integration Services. (Use the Connect drop down button in SSMS.)

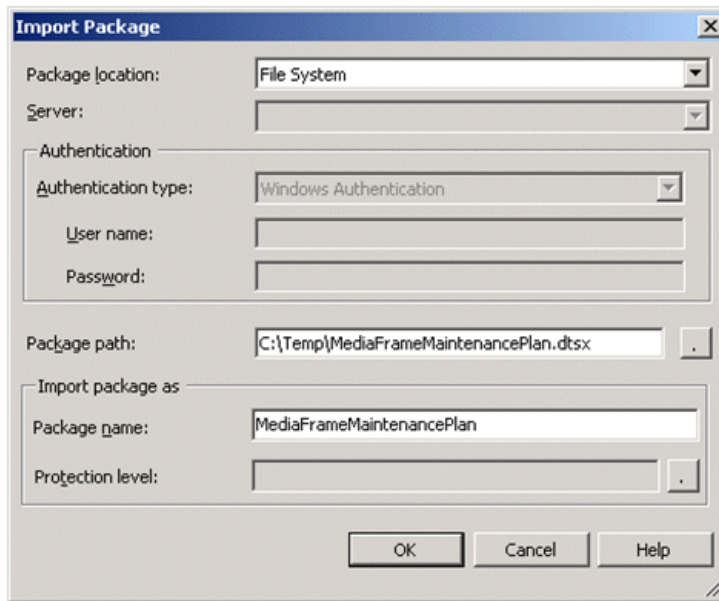


3. Locate the MediaFrameMaintenancePlan under **Integration Services|Stored Packages|MSDB| Maintenance Plans**.
4. Right-click on the maintenance plan to bring up the context menu, and select **Export Package**.
5. Select **File System** in the Package Location drop-down list.



6. Enter or browse to a desired location in the Package Path text box.
7. Click **OK** and verify that the file was created by navigating to the specified location.
8. Open the file in a text editor, such as Notepad.

9. Replace all occurrences of the old server name with the new server name, and save the file.
10. In SSMS, right-click on **Integration Services Stored Packages | MSDB | Maintenance Plans**.
11. From the context menu, select **Import Package**.
12. Specify the same path as you did in step 6.



13. If the modified maintenance plan has the same name as the original, a warning is displayed indicating that the Maintenance Plan will be overwritten. Click **OK**.

CAUTION: Do not import the package file (e.g. *MediaFrameMaintenancePlan.dtsx*) into another maintenance plan.

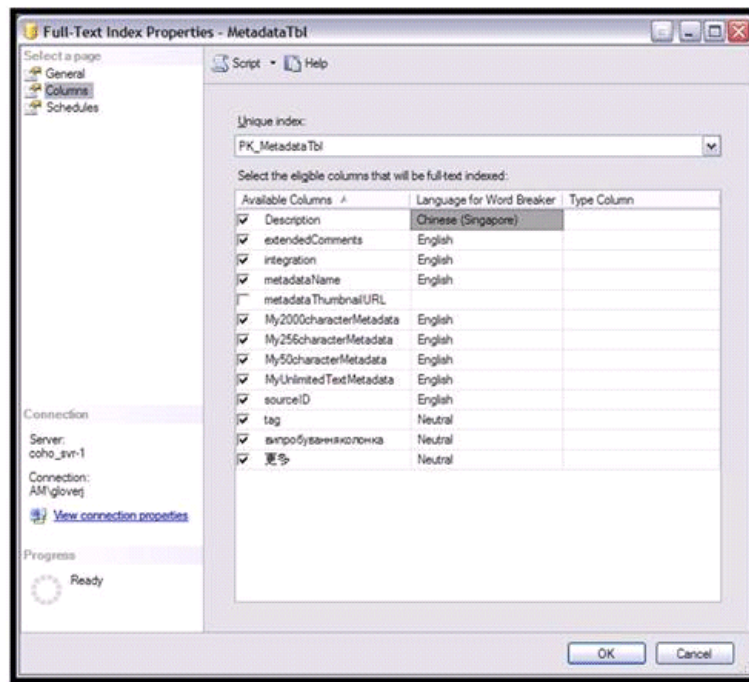
Modifying the database for non-English searches

To enable the MediaFrame database to allow searches in languages such as Chinese, the database needs to be modified. Because it will take some time to re-index the data, this procedure should be performed when the system is not in prime use. This procedure will not affect operations aside from search functionality.

To modify the database for non-English searches, follow these steps.

1. Open the Microsoft SQL Server Management Studio tool.
2. Select **Databases | MediaFrame | Tables**.
3. Right-click on the **dbo.MetadataTbl** table.
4. Select **Full-Text Index | Properties**. The Full-Text Index Properties dialog box displays.
5. Select the **Columns** page.
6. For every column that has a check box, change the language in the Language for

Word Breaker column to the appropriate language.



7. Once all the values are correct, click **OK**.

The indexes will rebuild with the new word breaker.

Backup and recovery strategies

Procedures in this section are as follows:

- “About the recovery disk image process” on page 151
- “Creating a recovery disk image for storing on E:” on page 153
- “Creating a recovery disk image CD set” on page 154
- “Restoring from a system-specific recovery disk image on E:” on page 156
- “Restoring from the generic recovery disk image on E:” on page 157
- “Restoring from a recovery disk image CD set” on page 162
- “Activating the Windows operating system” on page 163

About the recovery disk image process

On the MediaFrame server, there are three partitions on the system drive to support backup and recovery strategies as follows:

- The C: drive is for the Windows operating system and applications.

- The D: drive is for the data files. This allows you to restore the Windows operating system on the C: drive, yet keep the files on the D: drive intact. You can also restore the D: drive.
- The E: drive is for storing a system image of the other partitions. From the E: drive you can restore images to the C: and D: drives.

When you receive a MediaFrame server from the factory, the machine has a generic image on the E: drive. This image is not specific to the individual machine. It is generic for all machines of that type.

You receive a recovery CD with your MediaFrame server. This recovery CD does not contain a disk image. Rather, the recovery CD is bootable and contains the Acronis True Image software necessary to create and restore a disk image.

After your MediaFrame server is installed, configured, and running in your system environment, you should create new recovery disk images for the machine to capture settings changed from default. These “first birthday” images are the baseline recovery image for the machine in its life in your facility. You should likewise create new recovery disk images after completing any process that changes system software or data, such as a software upgrade. In this way you retain the ability to restore to a recent “last known good” state.

For the highest degree of safety, you should create a set of disk image recovery CDs, in addition to storing disk images on the E: partition. Since system drives are RAID protected, in most failure cases the disk images on the E: partition will still be accessible. But in the unlikely even of a catastrophic failure whereby you lose the entire RAID protected system drive, you can use your disk image recovery CDs to restore the system.

NOTE: Recovery disk images do not back up the media files themselves. You must implement other mechanisms, such as a redundant storage system or mirrored storage systems, to back up media files.

The recommended recovery disk image process is summarized in the following steps.

At the MediaFrame server first birthday...

1. Boot from the Recovery CD.
2. Create a set of disk image recovery CDs. These CDs contain the C:, D:, and E: partitions.
3. Create a disk image, writing the disk image to the E: partition. This disk image contains the C: and D: partitions.
4. Copy the disk image from the E: partition to another location, such as a network drive.

At milestones, such as after software upgrades...

1. Boot from the Recovery CD.
2. Create a disk image, writing the disk image to the E: partition. This disk image contains the C: and D: partitions.
3. Copy the disk image from the E: partition to another location, such as a network drive.

If you need to restore the MediaFrame server...

1. Boot from the Recovery CD.
2. If the E: partition is accessible, read the image from the E: partition to restore the C: partition, restore the D: partition, or restore both partitions.
3. If the E: partition is not accessible, do the following:
 - a. Read the disk image from your set of CDs and restore all three partitions.
 - b. Restart into Windows.
 - c. Copy your most recent disk image to the E: partition.
 - d. Boot from the Recovery CD.
 - e. Read the image from the E: partition to restore the C: partition, restore the D: partition, or restore both partitions.

Plan a recovery strategy that is appropriate for your facility, then refer to the following procedures as necessary to implement your strategy.

Creating a recovery disk image for storing on E:

Do the following at the local MediaFrame server to create a disk image of the C: partition and the D: partition and store the image file on the E: partition:

1. Make sure that media access is stopped and that the MediaFrame server on which you are working is out of service.
2. If you have not already done so, connect keyboard, monitor, and mouse to the MediaFrame server.
3. Insert the Recovery CD and restart the machine.

The machine boots from the disc. The Acronis True Image program loads.
4. At the startup screen, select **True Image Server (Full Version)**.

- The Acronis True Image program loads.
The Acronis True Image main window appears.
5. In the Acronis True Image main window, click **Backup**.
The Create Backup Wizard opens.
 6. On the Welcome page, click **Next**.
The Select Backup Type page opens.
 7. Select **The entire disk contents or individual partition** and then click **Next**.
The Partitions Selection page opens.
 8. Select the **OS (C:)** and the **Data (D:)** partitions and then click **Next**.
The Backup Archive Location page opens.
 9. In the tree view select the **Backup (E:)** partition and then enter the name of the image file you are creating. Create the file name using the MediaFrame server hostname and the date. Name the file with the .tib extension. For example, if the hostname is *mfServer*, in the File name field you would have `E:\mfServer1_20051027.tib`. Click **Next**.
The Backup Creation Options page opens.
 10. Do not change any settings on this page. Click **Next**.
The Archive Comment page opens.
 11. If desired, enter image comments, such as the date, time, and software versions contained in the image you are creating. Click **Next**.
The "...ready to proceed..." page opens.
 12. Verify that you are creating images from the C: and D: partitions and writing to the E: partition. Click **Proceed**.
The Operation Progress page opens and displays progress.
 13. When a "Backup archive creation has been successfully completed" message appears, click **OK**.
 14. Click **Operations | Exit** to exit the Acronis True Image program.
The MediaFrame server device restarts automatically.
 15. Remove the Recovery CD while the MediaFrame server device is shutting down.
 16. Upon restart, log on to Windows.
 17. Open Windows Explorer and find the image file on the E: partition.

Creating a recovery disk image CD set

Do the following at the local MediaFrame server to create a disk image of the entire system drive, which includes the C:, D:, and E: partitions, and store the image file on a set of CDs:

1. Make sure that media access is stopped and that the MediaFrame server on which you are working is out of service.

2. If you have not already done so, connect keyboard, monitor, and mouse to the MediaFrame server.
3. Insert the Recovery CD and restart the machine.
The machine boots from the disc. The Acronis True Image program loads.
4. At the startup screen, select **True Image Server (Full Version)**.
The Acronis True Image program loads.
The Acronis True Image main window appears.
5. In the Acronis True Image main window, click **Backup**.
The Create Backup Wizard opens.
6. On the Welcome page, click **Next**.
The Select Backup Type page opens.
7. Select **The entire disk contents or individual partition** and then click **Next**.
The Partitions Selection page opens.
8. Select **Disk 1** to select the OS (C:), the Data (D:), and the Backup (E:) partitions and then click **Next**.
The Backup Archive Location page opens.
9. In the tree view select **CD-RW Drive (F:)** and then enter the name of the image file you are creating. Create the file name using the MediaFrame server hostname and the date. Name the file with the .tib extension. For example, if the hostname is *mfServer*, in the File name field you would have `F:\mfServer_20051027.tib`. Click **Next**.
The Backup Creation Options page opens.
10. Do not change any settings on this page. Click **Next**.
The Archive Comment page opens.
11. If desired, enter image comments, such as the date, time, and software versions contained on the image you are creating. Click **Next**.
The "...ready to proceed..." page opens.
12. Remove the Recovery CD and insert a blank CD.
13. Verify that you are creating an image from Disk 1 and writing to the CD-RW Drive (F:). Click **Proceed**.
The Operation Progress page opens and displays progress.
14. Remove and insert CDs as prompted. As you remove each burned CD make sure you label it correctly to show the sequence of CDs.
15. When a "Backup archive creation has been successfully completed" message appears, click **OK**.
16. Click **Operations | Exit** to exit the Acronis True Image program.
The MediaFrame server restarts automatically.
17. Remove any CD that is still in the CD drive while the MediaFrame server is

shutting down.

Restoring from a system-specific recovery disk image on E:

The following procedure can be used on a MediaFrame server that needs its image restored, if the image was made from that specific machine. If the image is the generic factory-default image, refer to the next procedure [“Restoring from the generic recovery disk image on E:”](#)

1. Make sure that media access is stopped and that the MediaFrame server on which you are working is out of service.
2. If you have not already done so, connect keyboard, monitor, and mouse to the MediaFrame server.
3. Insert the Recovery CD and restart the machine. If there is a problem restarting, hold the standby button down for five seconds to force a hard shutdown. Then press the standby button again to startup.

The machine boots from the disc. The Acronis True Image program loads.

4. At the startup screen, select **True Image Server (Full Version)**.

The Acronis True Image program loads.

The Acronis True Image main window appears.

5. In the Acronis True Image main window, click **Recovery**.

The Restore Data Wizard opens.

6. On the Welcome page, click **Next**.

The Archive Selection page opens.

7. In the tree view expand the node for the E: partition and select the image file, then click **Next**:

The Verify Archive Before the Restoring page opens.

8. Leave the selection at **No, I don't want to verify** and then click **Next**.

The Partition or Disk to Restore page opens.

9. Select **OS (C:)** and then click **Next**.

The Restored Partition Location page opens.

10. Select **OS (C:)** and then click **Next**.

The Restored Partition Type page opens.

11. Leave the selection at **Active** and then click **Next**.

The Restored Partition Size page opens.

12. Leave settings at their defaults. The size reported in the upper pane is the size detected of the actual C: partition. This should be the same as that reported in the Partition size field in the middle of the page. Free space before and Free space after should both be reported at 0 bytes. Click **Next**.

The Next Selection page opens.

13. Depending on the partitions you are restoring, do one of the following:

- If you are restoring only the C: partition, select **No, I do not** and then click **Next**.
The "...ready to proceed..." page opens.
Skip ahead to step 20.
 - If you are also restoring the D: partition, select **Yes, I want to restore another partition or hard disk drive** and then click **Next**.
The Partition or Disk to Restore page opens. Continue with the next step in this procedure.
14. Select **Data (D:)** and then click **Next**.
The Restored Partition Location page opens.
 15. Select **Data (D:)** and then click **Next**.
The Restored Partition Type page opens.
 16. Leave the selection at **Primary** and then click **Next**.
The Restored Partition Size page opens.
 17. Leave settings at their defaults. The size reported in the upper pane is the size detected of the actual D: partition. This should be the same as that reported in the Partition size field in the middle of the page. Free space before and Free space after should both be reported at 0 bytes. Click **Next**.
The Next Selection page opens.
 18. Select **No, I do not** and then click **Next**.
The Restore Operation option page opens.
 19. Do not make any selections. Click **Next**.
The "...ready to proceed..." page opens.
 20. Verify that you are restoring the correct partition or partitions. Click **Proceed**.
The Operation Progress page opens and displays progress.
 21. When a "The data was successfully restored" message appears, click **OK**.
 22. Click **Operations | Exit** to exit the Acronis True Image program.
The MediaFrame server restarts automatically.
 23. Remove any CD currently in the CD drive while the MediaFrame server is shutting down.
 24. If restoring a MediaFrame or K2 BaseCamp Express server, follow the procedure described in ["Updating the maintenance plan after renaming the server"](#) on [page 148](#).

Restoring from the generic recovery disk image on E:

There can be multiple versions of the generic recovery disk image on the MediaFrame server's E: partition. Refer to *Aurora Browse Release Notes* to determine which version you should use.

This procedure can be used on a MediaFrame server that needs to be restored to its factory default state. For example, if you neglected to make a first birthday image, you might need to use this procedure. If the image from which you are restoring was made from the specific machine, refer to the previous procedure [“Restoring from a system-specific recovery disk image on E:”](#).

NOTE: *This procedure restores the MediaFrame server (both C: and D: partitions) to its factory default condition. Passwords and other site-specific configurations are reset to factory defaults.*

1. Make sure that media access is stopped and that the MediaFrame server on which you are working is out of service.
2. If you have not already done so, connect keyboard, monitor, and mouse to the MediaFrame server.
3. Insert the Recovery CD and restart the machine. If there is a problem restarting, hold the standby button down for five seconds to force a hard shutdown. Then press the standby button again to startup.

The machine boots from the disc. The Acronis True Image program loads.

4. At the startup screen, select **True Image Server (Full Version)**.

The Acronis True Image program loads.

The Acronis True Image main window appears.

5. In the Acronis True Image main window, click **Recovery**.

The Restore Data Wizard opens.

6. On the Welcome page, click **Next**.

The Archive Selection page opens.

7. In the tree view expand the node for the E: partition and select the image file, then click **Next**:

The Verify Archive Before the Restoring page opens.

8. Leave the selection at **No, I don't want to verify** and then click **Next**.

The Partition or Disk to Restore page opens.

9. Select **OS (C:)** and then click **Next**.

The Restored Partition Location page opens.

10. Select **OS (C:)** and then click **Next**.

The Restored Partition Type page opens.

11. Leave the selection at **Active** and then click **Next**.

The Restored Partition Size page opens.

12. Leave settings at their defaults. The size reported in the upper pane is the size detected of the actual C: partition. This should be the same as that reported in the Partition size field in the middle of the page. Free space before and Free space after should both be reported at 0 bytes. Click **Next**.

The Next Selection page opens.

13. Depending on the partitions you are restoring, do one of the following:
 - If you are restoring only the C: partition, select **No, I do not** and then click **Next**.
The "...ready to proceed..." page opens.
Skip ahead to step 20.
 - If you are also restoring the D: partition, select **Yes, I want to restore another partition or hard disk drive** and then click **Next**.
The Partition or Disk to Restore page opens. Continue with the next step in this procedure.
14. Select **Data (D:)** and then click **Next**.
The Restored Partition Location page opens.
15. Select **Data (D:)** and then click **Next**.
The Restored Partition Type page opens.
16. Leave the selection at **Primary** and then click **Next**.
The Restored Partition Size page opens.
17. Leave settings at their defaults. The size reported in the upper pane is the size detected of the actual D: partition. This should be the same as that reported in the Partition size field in the middle of the page. Free space before and Free space after should both be reported at 0 bytes. Click **Next**.
The Next Selection page opens.
18. Select **No, I do not** and then click **Next**.
The Restore Operation option page opens.
19. Do not make any selections. Click **Next**.
The "...ready to proceed..." page opens.
20. Verify that you are restoring the correct partition or partitions. Click **Proceed**.
The Operation Progress page opens and displays progress.
21. When a "The data was successfully restored" message appears, click **OK**.
22. Click **Operations | Exit** to exit the Acronis True Image program.
The MediaFrame server restarts automatically.
23. Remove any CD currently in the CD drive while the MediaFrame server is shutting down.
24. Upon restart the Windows Setup Wizard automatically opens. Do Windows setup as follows:
 - a. Set the Regional and Language Options and click **Next**.
 - b. Fill in the Personalize Your Software information. (For example, set the Name and Organization to **gv**.)
 - c. Enter in Windows Product Key and click **Next**.
The Product Key is on a sticker on the top of the machine near the front right corner.

- d. Enter the name of the machine.
The password is pre-set to the factory default. Leave the password as is.
- e. Click **Next**
- f. Set Time and click **Next**.

Windows loads network components and restarts the MediaFrame server.

25. Label network connections as follows:

- a. On the Windows desktop right-click **My Network Places** and select **Properties**.
The Network Connections window opens.
- b. Rename the connection associated with port 1 on the back of the PC to *Control Connection*. If unsure which connection is associated with port 1, try one of the following procedures
 - Plug and unplug a cable into the port on to see which connection gets connected/disconnected.
 - Check the NIC Location:
 - i. On the Windows desktop right-click **My Network Places** and select **Properties**.
 - ii. In the Local Area Connection Properties dialog click the **Configure...** button.

A Broadcom property dialog opens. In the Location line, it shows the PCI bus, device, and function. Concatenate the numbers after the bus, device, and function. This represents an index of the NIC card where the bus is the highest order number and the function is the lowest. For example in the below picture the index would 100.



- iii. Do steps i and ii for all Network connections. The lowest index should be associated to Port 1, the next lowest should be associated to Port 2, etc.
- c. For the connection that is associated to Port 2 on the back of the PC, rename it as follows:

- If the machine is a MediaFrame Server, MDI Server, or K2 BaseCamp Express, rename the connection to *FTP Connection*.
 - If the machine is an encoder, rename the connection to *Media Connection*.
- d. If the machine is a MediaFrame Server or a K2 BaseCamp Express, rename the connection that is associated to Port 3 to *Corporate LAN Connection*.
 - e. For all other connections rename them to *Unused* and disable the connection.
 - f. On the menu bar at the top of the window, select **Advanced**, then **Advanced Settings...**
 - g. Select **Control Connection** in Connections field.
 - h. Use the up arrow button, move the Control Connection to the top of the list (TOP priority - 1st).
 - i. Ensure that FTP Connection is below the Control Connection.
If not, select FTP Connection, and move it below the Control Connection.
 - j. Ensure that Corporate LAN Connection is below the Control Connection.
If not, select Corporate LAN Connection, and move it below the Control Connection.
 - k. Click **OK** to save settings and close.
26. Set power management settings as follows:
- a. On the Windows desktop right-click **My Network Places** and select **Properties**.
The Network Connections window opens.
 - b. Right-click a network connection and select **Properties**.
The ...Connection Properties dialog box opens.
 - c. Click **Configure**.
The ...Properties dialog box opens.
 - d. On the **Power Management** tab, uncheck all checkboxes, if they are not already unchecked.
 - e. On the ...Properties dialog box, click **OK**.
 - f. Repeat these steps on the remaining network connections in the Network Connections window.
27. Install the Discovery Agent software.
- If this machine is a MediaFrame, MDI, or K2 BaseCamp Express server, select the **MediaFrameServer** option.
 - If this machine is an encoder, select the **ProxyEncoder** option.
28. Start the SQL Server (*MSSQLSERVER*) and SQL Server Agent (*MSSQLSERVER*) services and set them to **Automatic startup**.
29. Install MediaFrame server software as described in [Chapter 4, Installing the Aurora Browse System Software on page 33](#). Also install related software, such as SNFS, if required for the latest upgrade. Refer to your latest *Aurora Browse Release Notes* for detailed instructions.

30. You must activate the Windows operating system within 30 days. Refer to [“Activating the Windows operating system” on page 163](#)

The MediaFrame server is now restored to its factory-default state. However, you still need to configure the server. If it is a MediaFrame server or K2 BaseCamp Express, you need to restore the SQL database. For more information, see [Chapter 5, *Configuring the system on page 71*](#) and [“Restoring the MediaFrame server database” on page 148](#).

Restoring from a recovery disk image CD set

The following procedure can be used on a MediaFrame server that needs all three partitions on the system drive restored.

This procedure assumes that the image on the CD set is the system-specific image, for the particular machine that you are restoring.

NOTE: *At any step in this procedure if a message appears asking for disc/volume, insert CDs as prompted until you can proceed to the next step.*

1. Make sure that media access is stopped and that the MediaFrame server on which you are working is not being used.
2. If you have not already done so, connect keyboard, monitor, and mouse to the MediaFrame server.
3. Insert the Recovery CD and restart the machine. If there is a problem restarting, hold the standby button down for five seconds to force a hard shutdown. Then press the standby button again to startup.

The machine boots from the disc. The Acronis startup screen appears.

4. At the startup screen, select **True Image Server (Full Version)**.

The Acronis True Image program loads.

The Acronis True Image main window appears.

5. Insert the last CD (volume) in your recovery disk image CD set. For example, if there are three CDs that make up the disk image, insert the third CD.
6. In the Acronis True Image main window, click **Recovery**.

The Restore Data Wizard opens.

7. On the Welcome page, click **Next**.

The Archive Selection page opens.

8. In the tree view expand the node for the CD ROM drive and select the image file, then click **Next**:

The Restoration Type Selection page opens.

9. Select **Restore disks or partitions** and then click **Next**.

The Partition or Disk to Restore page opens.

10. Select **Disk 1**. This selects all three partitions to be restored.

If you do not want to restore all three partitions, refer to similar steps in [“Restoring from a system-specific recovery disk image on E:” on page 156](#).

Click **Next**.

The Restored Partition Sizing page opens.

11. Select **No, I don't want to resize source partitions** and then click **Next**.

The Restored Hard Disk Drive Location page opens.

12. Select **Disk 1** and then click **Next**.

The Non-Empty Destination Hard Disk Drive page opens.

13. Select **Yes...delete all partitions...** and then click **Next**.

If messages appear asking for disks, insert CDs sequentially and click **Retry** until you can proceed to the next step.

The Next Selection page opens.

14. Select **No, I do not** and then click **Next**.

The Restore Operation option page opens.

15. Do not make any selections. Click **Next**.

The "...ready to proceed..." page opens.

16. Verify that you are restoring partitions. Click **Proceed**.

The Operation Progress page opens and displays progress.

17. Insert CDs as prompted. As messages appear asking for disks, insert CDs sequentially and click **Retry**.

18. When a "The data was successfully restored" message appears, click **OK**.

19. Click **Operations | Exit** to exit the Acronis True Image program.

The MediaFrame server restarts automatically.

20. Remove the Recovery CD while the MediaFrame server is shutting down.

Activating the Windows operating system

If a MediaFrame server is restored to its factory default state or otherwise has the Windows operating system re-applied, you might need to activate the operating system. This procedure provides instructions for doing this while the machine is connected to the Internet. The Activation wizard provides other options, which you can also choose if desired.

To activate the Windows operating system on a K2 device, do the following:

1. Make sure the machine is connected to the Internet.
2. From the Windows desktop, in the system tray double-click on the key symbol icon. The Activate window opens.
3. Select **Yes, let's activate Windows over the Internet now** and click **Next**.
4. When prompted, "If you want to register with Microsoft right now.", select **No**.
5. Wait for the connection. If the system times out, you are prompted for entering information in the Internet Protocol Connection dialog. Enter the proxy address and port number as appropriate for your facility's connections.

6. Ensure that “You have successfully activated your copy of Windows” message appears in Activate Windows.
7. Click **OK** to close the Activate Windows.

Troubleshooting the system

Troubleshooting tools

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

MediaFrame troubleshooting tool

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

Aurora Browse application troubleshooting tips

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

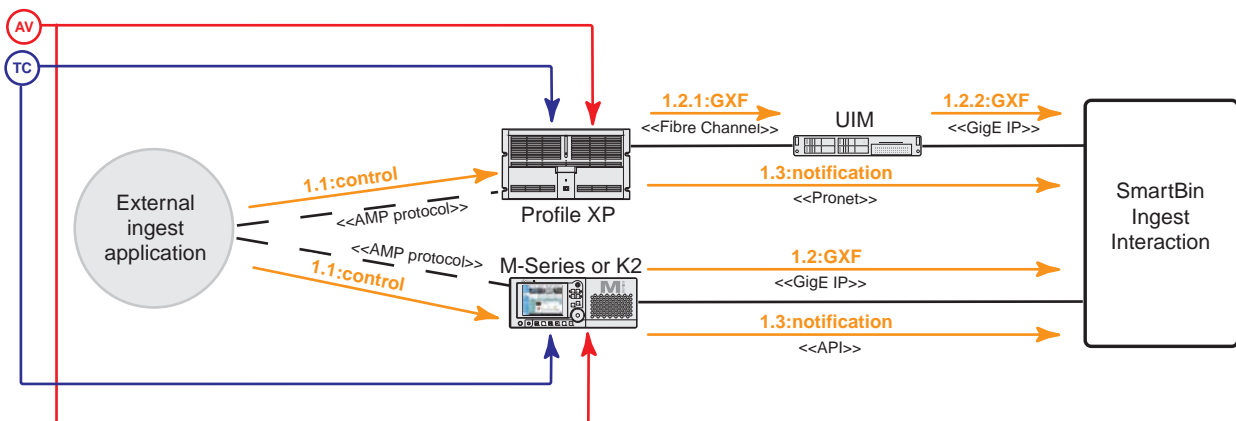
Symptom	Solution
Problem searching for specific words in the Aurora Browse search	<p>Verify that the word or words you are searching for is not in the noise words list that SQL automatically screens out of search terms.</p> <p>To modify the list of noise words, edit the file that is contained at <code>\$\$SQL_Server_Install_Path\Microsoft SQL Server\MSSQL.1\MSSQL\FTDATA\</code> on your SQL Server host.</p> <p>Be aware that modifying this list might affect expected execution times.</p>
Problem accessing the Aurora Browse system.	<p>Check the Status window. Verify ASK and the other components are running.</p> <p>Check that the server is running.</p> <p>Check that the server is connected to the client network.</p> <p>Check that connections are secure.</p> <p>Check that IIS is running on the server.</p>
Problem searching for or opening proxy	<p>Check to make sure the low-res NAS location is a mapped drive.</p>
MediaFrame server is accessible using IP address but not server name	<p>Host tables or DNS entries must be set to map name to IP address. This should be coordinated with facility IT personnel.</p>
Problem Accessing the Aurora Browse application - permission denied	<p>Check that the account used to log into the client workstation is licensed on the server. See “Configure Aurora Browse Licenses” on page 133.</p>

Appendix A

Component Interaction Diagrams

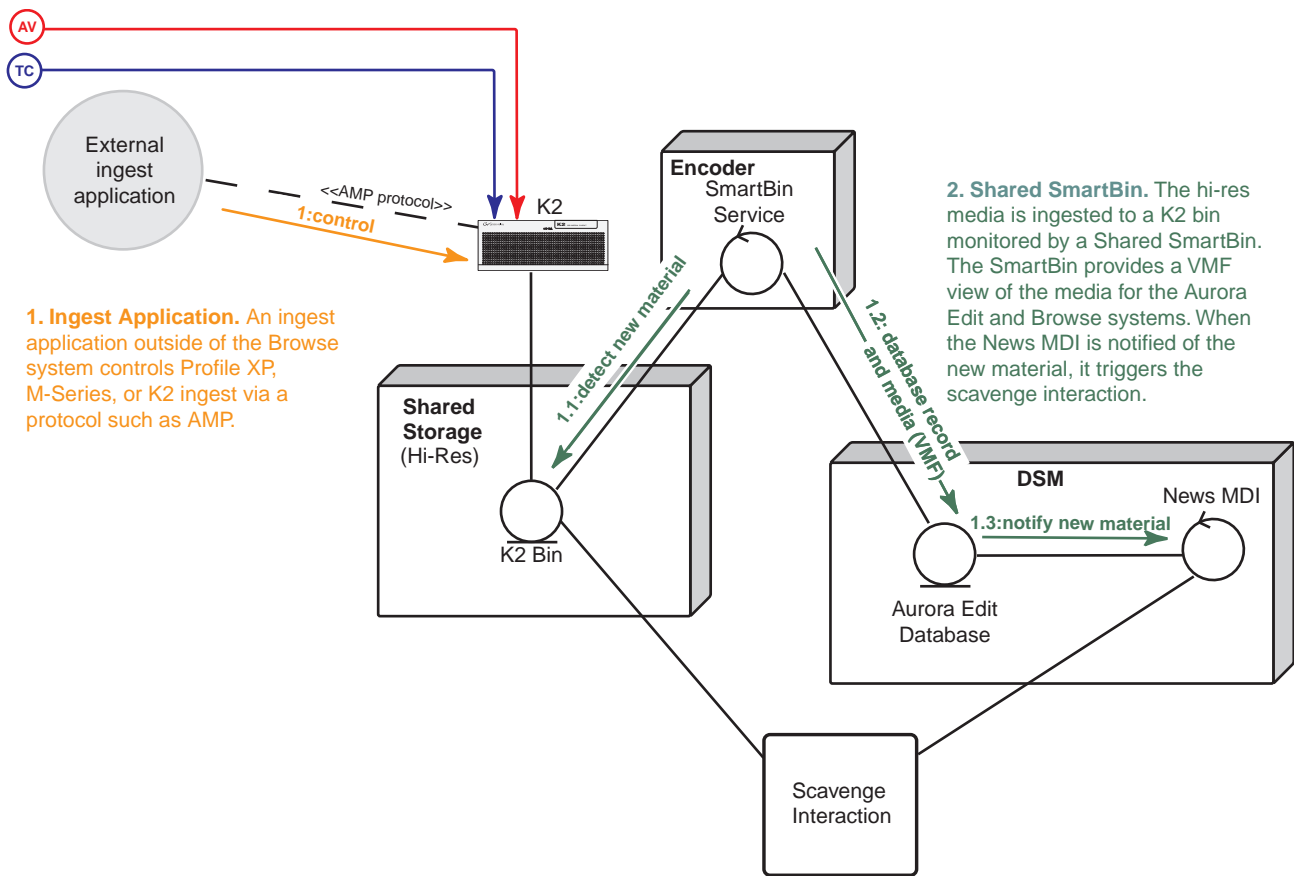
This appendix provides diagrams and explanations of how the system software components interact.

External Ingest Application to Transfer SmartBin

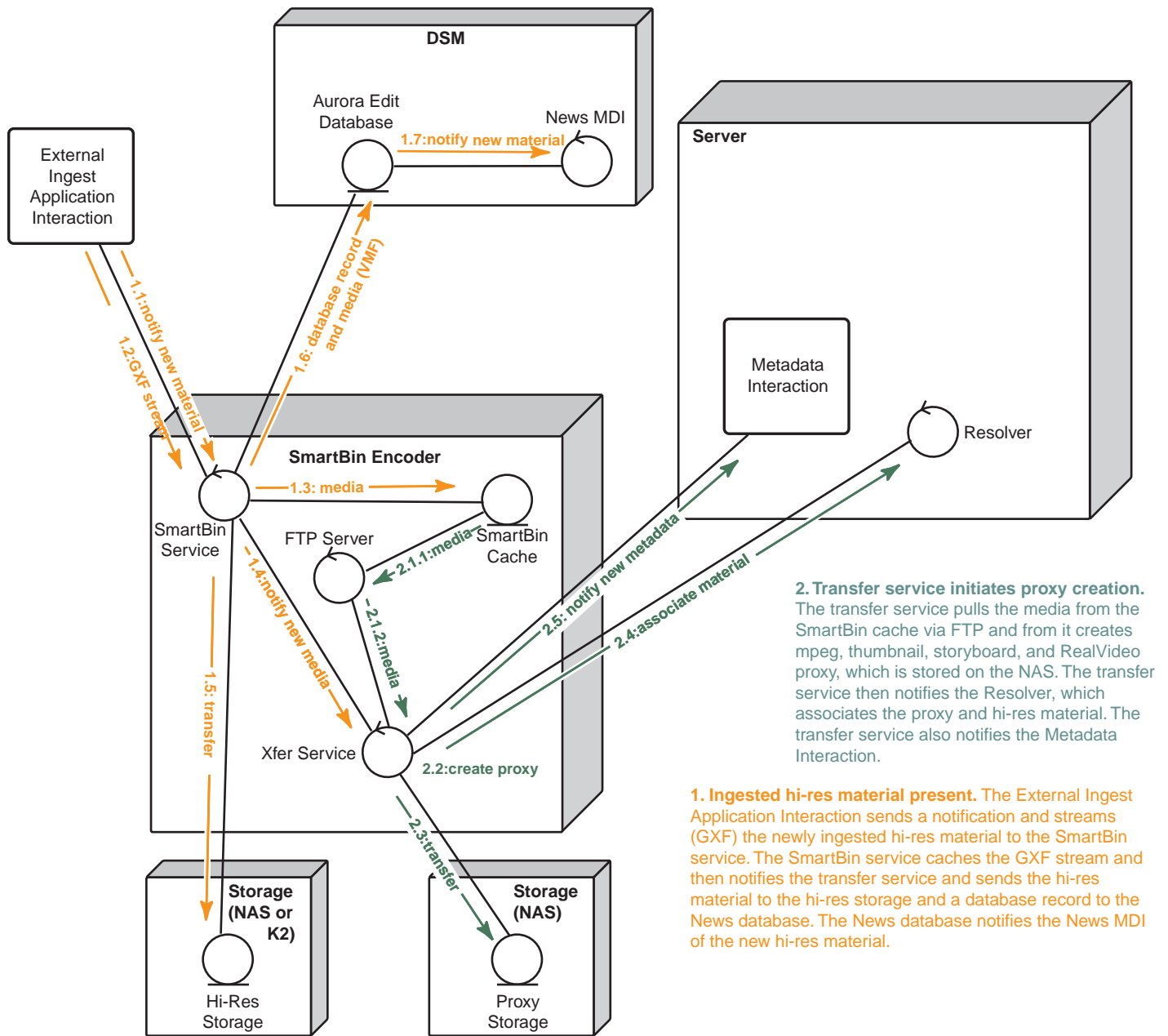


1. Ingest Application. An ingest application outside of the Browse system controls Profile XP, M-Series, or K2 ingest via a protocol such as AMP. When hi-res media is ingested, the Profile XP or M-Series sends the media as a GXF stream and sends a notification about the newly ingested media to the SmartBin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

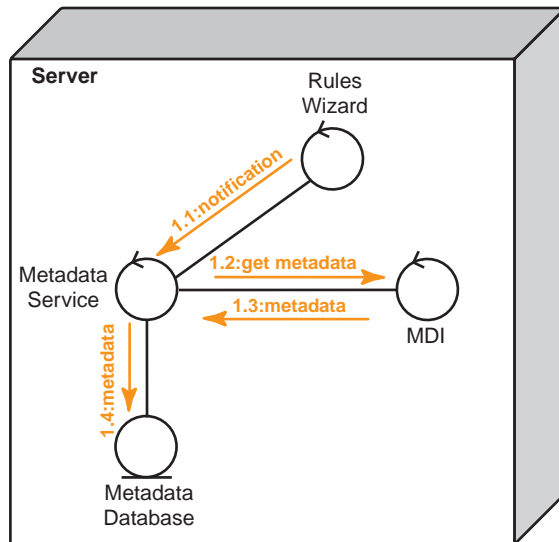
External Ingest Application to Shared SmartBin



Transfer SmartBin Ingest



Metadata



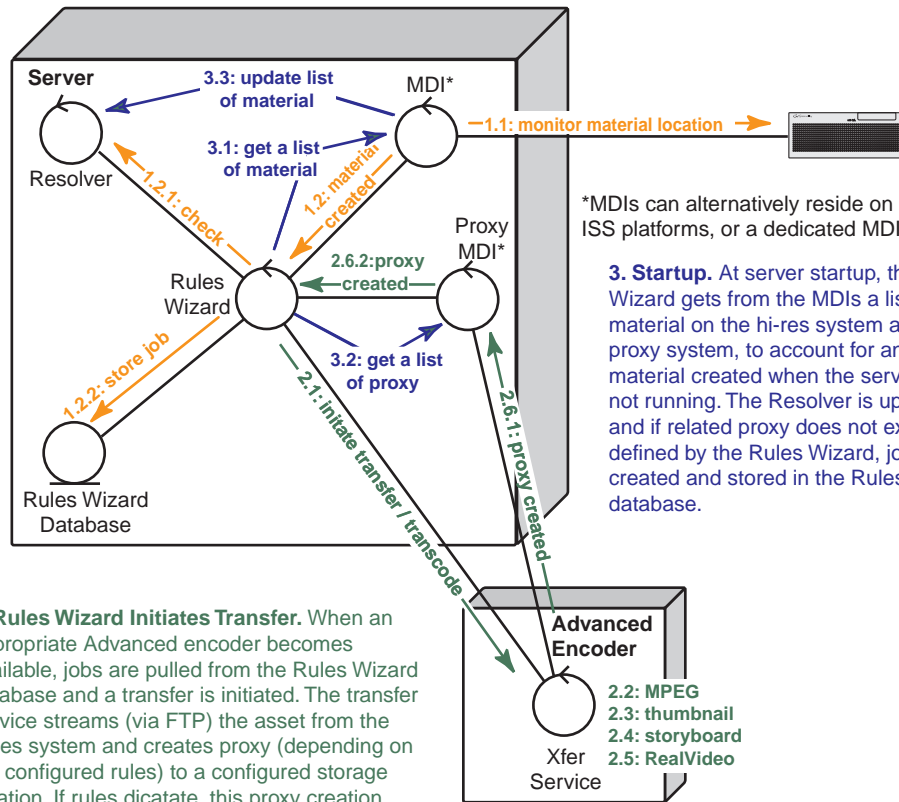
1. Metadata. When the Rules Wizard or transfer service initiates the creation or modification of proxy, it notifies the Metadata Service. The Metadata Service gets the new or modified metadata from the MDI that has knowledge of the associated hires material and puts it in the metadata database.

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.

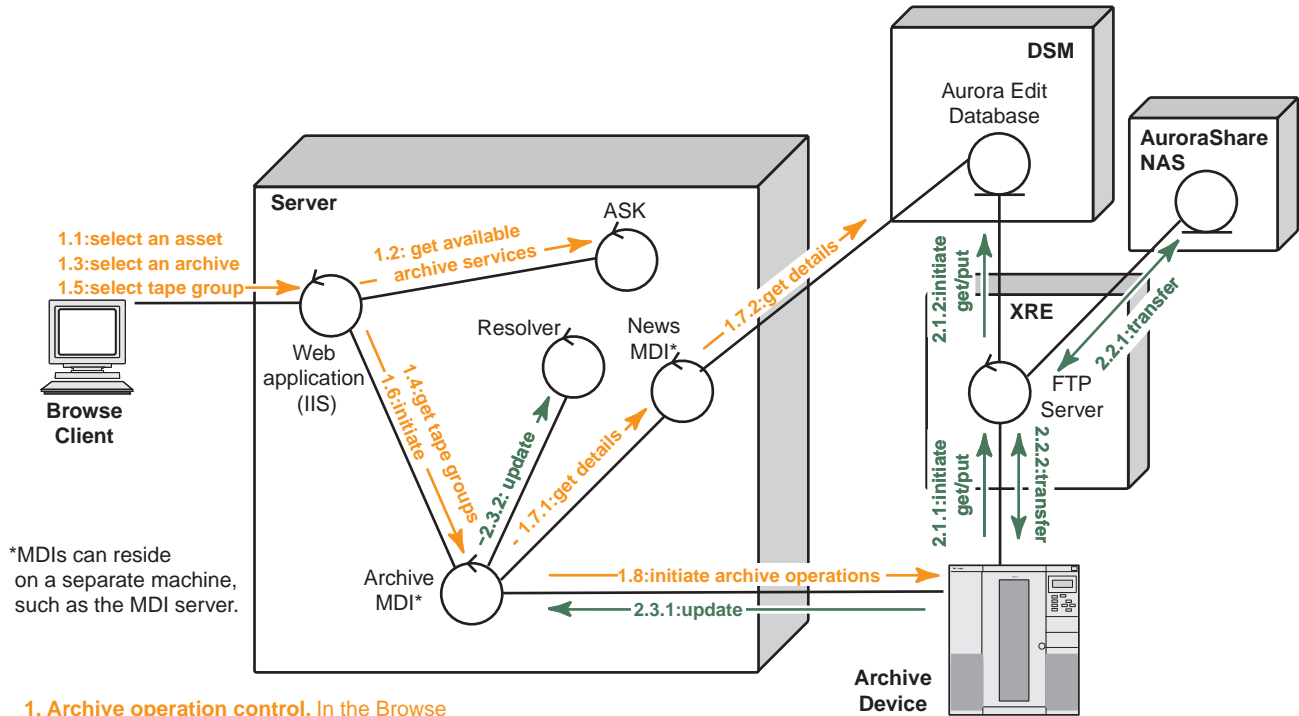


*MDIs can alternatively reside on encoders, ISS platforms, or a dedicated MDI server.

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 dictate, this proxy creation occurs while the high-res material is still recording. Then the transfer service communicates to the Resolver to associate the proxy and hi-res material. Once the proxy is created the transfer service notifies the Proxy MDI.

Archive operations on Aurora system

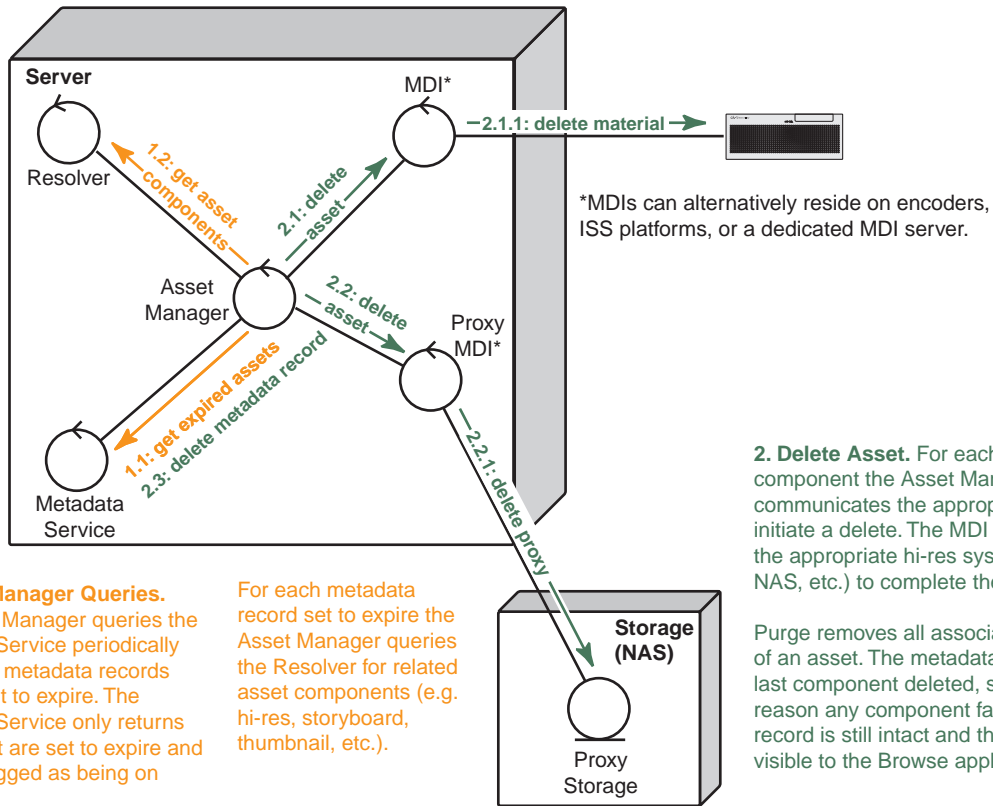


1. Archive operation control. In the Browse application, the user selects an asset, navigates to the management tab, and selects the archive option. The system queries the ASK for available archive devices. (Also filters out for hi-res material that already exists in archive by querying the Resolver).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



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.

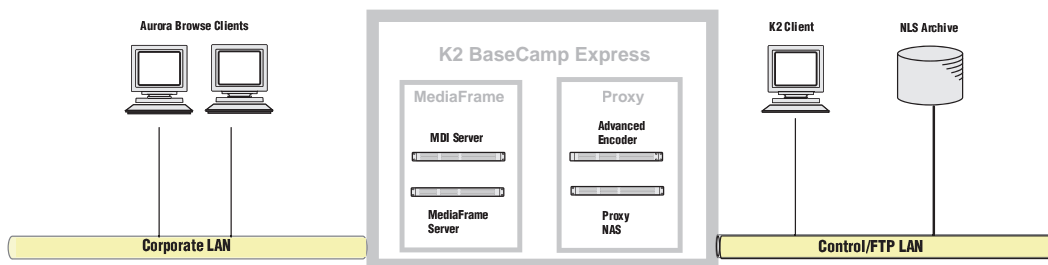
For each metadata record set to expire the Asset Manager queries the Resolver for related asset components (e.g. hi-res, storyboard, thumbnail, etc.).

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.

K2 BaseCamp Express

K2 BaseCamp Express is a Dell R710 server with MediaFrame system components including a low-res NAS storage, an internal RAID, the MediaFrame database, and MDIs such as Generic FTP and K2.



K2 BaseCamp Express does not scavenge assets; proxy is created on demand. It can utilize multiple encode streams. The speed of the encoder is “throttleable;” that is, it can be slowed to less than real time. However, the encoder maintains one real-time encode of 100mb/s 1080i MPEG.

NOTE: Multiple encoder streams can affect encoder performance.

Configuring K2 BaseCamp Express

K2 BaseCamp Express does not come from the factory with the Aurora system components already installed. You need to cable the system as described in [Chapter 2 Installing the Aurora Browse system hardware on page 19](#). You must then install the MediaFrame and Proxy Encoder software as described in [Chapter 4 Installing the Aurora Browse System Software on page 33](#).

Depending on your system configuration you might need to install some dependency software:

- If BaseCamp Express will host the News MDI and connect to an Aurora DSM, you must install the GVG_MLIB software.
- If BaseCamp Express will host the Profile MDI, you must manually install the Profile XP software.

CAUTION: You cannot host both the News MDI and Profile MDI on the same server.

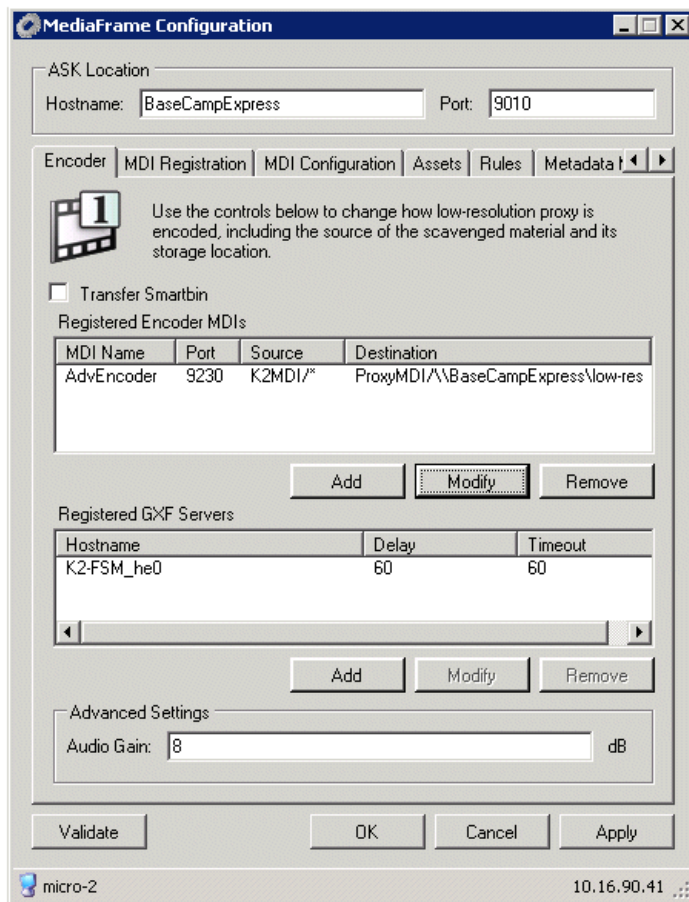
K2 BaseCamp Express is not an iSCSI client. The encoder uses an external FTP server to generation low-res material. If a BaseCamp Express server is used with an external encoder, disable the internal encoder on the BaseCamp Express server.

Configuring encoders for K2 BaseCamp Express

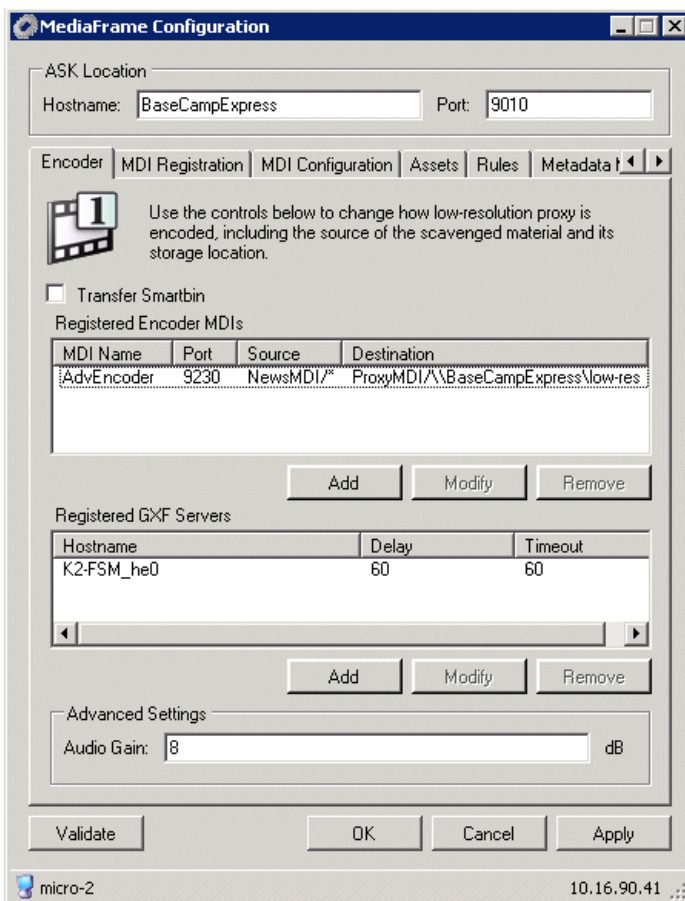
If your system includes a K2 Storage System and Aurora Proxy Encoders, you need to point the encoder to the K2 FTP server.

The encoders used with K2 BaseCamp Express uses an external FTP server for low-res generation. When using the BaseCamp Express server for low-res generation, it can only have one encode stream configured. If a Proxy Encoder server is used, it can have up to 4 SD encode streams configured. You must create and configure an Encoder MDI for each stream on the encoder.

For K2 BaseCamp Express servers running in a basic K2 system-only configuration, configure the encoder to use the K2 FTP server as shown in the following illustration.



In an Aurora System environment, the encoder need to access the K2-Aurora FTP server. The K2-Aurora FTP server has the Aurora Asset software installed on the K2 FTP server. The encoder configuration for the Aurora setup is show in the following illustration.



Configuring the low-res storage on the K2 BaseCamp Express server

The low-res storage is typically already configured before being shipped. If you need to re-image your system, as described in [“Backup and recovery strategies”](#) on page 151, then you will need to configure the low-res storage.

To configure the low-res storage, follow these steps:

1. If BaseCamp Express has been restored from the factory image, and all existing partitions were removed, create a partition for all remaining unused disk space.
2. Create two shared folders: *Media* and *Audio*.
3. Configure the NTFS MDI, as described in [“Configure NTFS MDI”](#) on page 121.
4. Prepare the NAS, as described in [“Prepare NAS - Condor”](#) on page 79.

Upgrading K2 BaseCamp Express

You can add additional encoders to K2 BaseCamp Express. For more information, see your Grass Valley support representative.

Using K2 BaseCamp Express

You can access 2 BaseCamp Express using the Aurora Browse application on client PCs exactly as you would access the MediaFrame server, to search for or archive assets. Up to 18 users can access a BaseCamp Express server at one time. For more information, see the *Aurora Browse User Guide*.

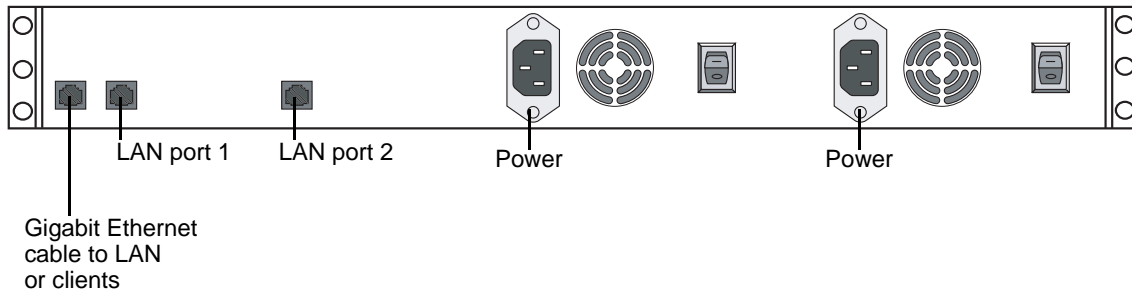
Legacy systems

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.

NAS instructions - Fastora

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

Aurora Browse Proxy NAS (Fastora 104)



Cable as illustrated and as follows:

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

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

Prepare NAS - Windows Fastora

For the Linux version, refer to “[Prepare NAS - Linux Fastora](#)” on page 192.

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).

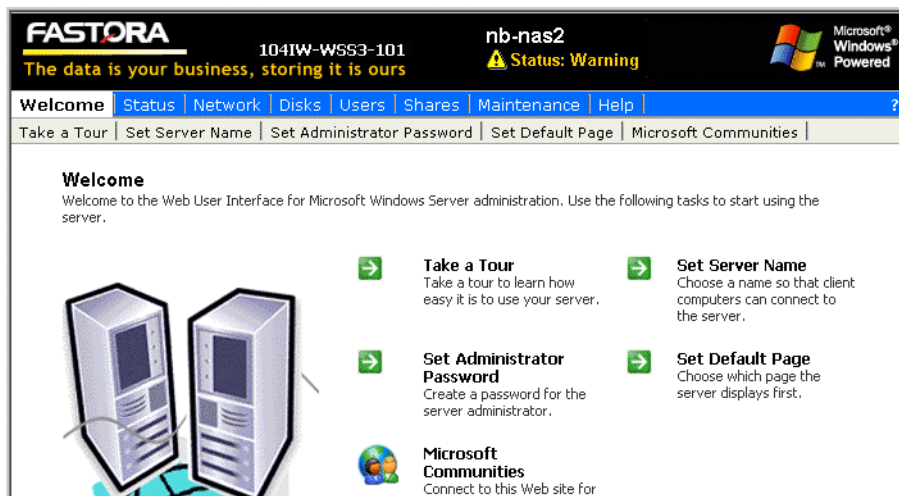
If you received your NAS unit directly from Fastora, the default Fastora IP address is 192.168.1.11.

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.

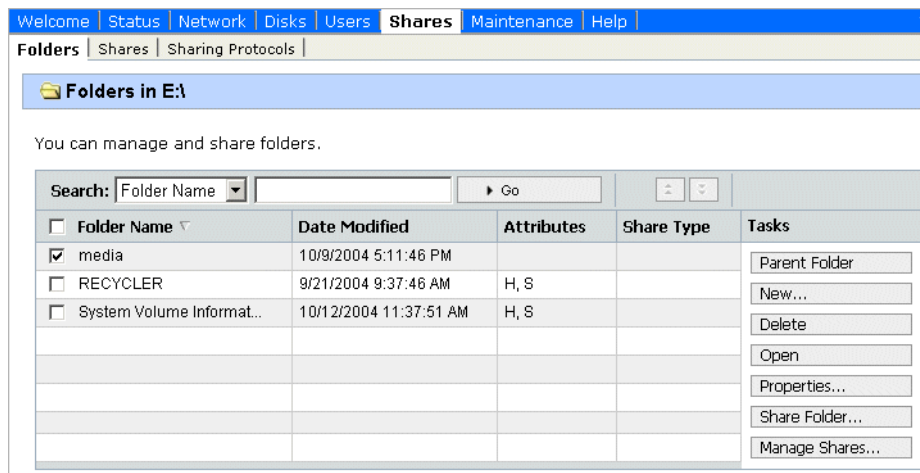
If you make a change, click **OK**.

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

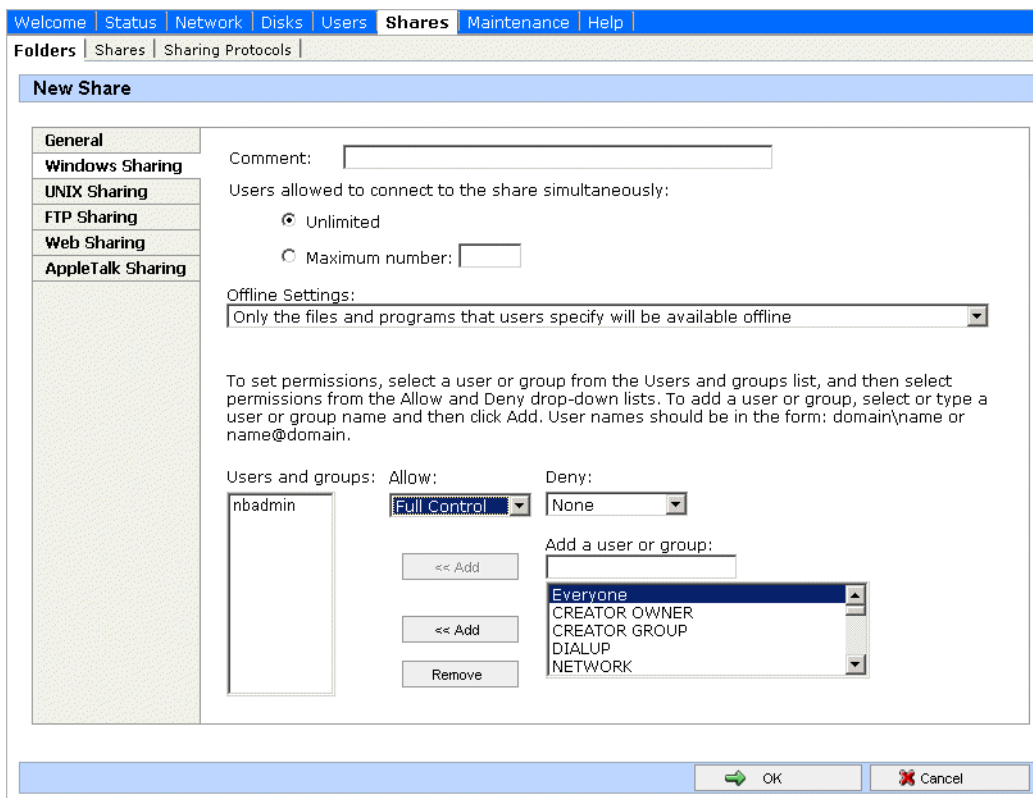
6. Click **Set Administrator Password**.

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
- Aurora Proxy Encoder
- SmartBin encoder

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

1. Open Windows Explorer and navigate to the media directory on the NAS. You can do this with the following path:
 - \\root-nb-nas-1\Media
2. Verify basic read/write capabilities by creating, modifying, and deleting a simple text file.

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

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

\\root-nb-nas-1\Media

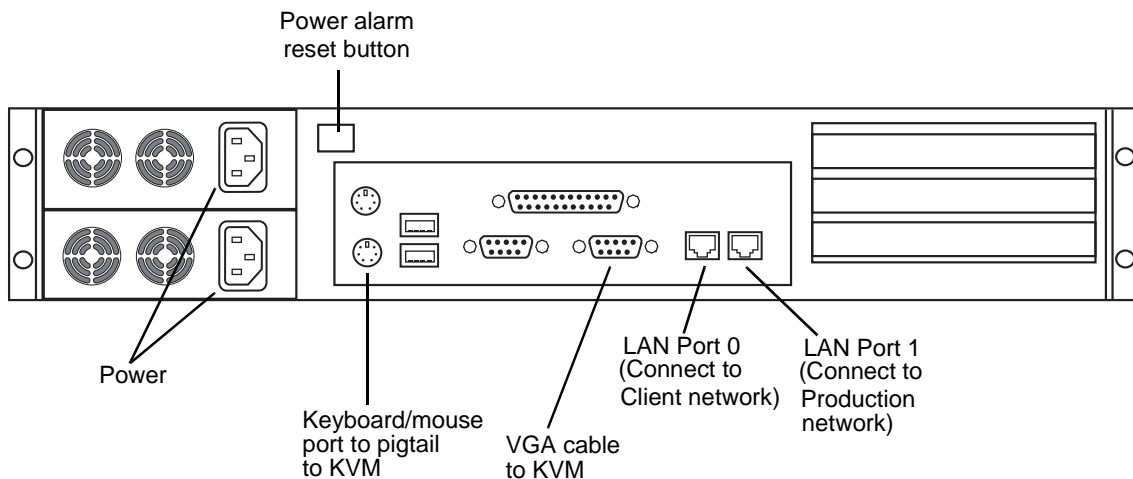
Verify that Aurora Browse client PCs will have read only rights.

NAS instructions - Serial ATA network platform

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

Platform Specifications are as follows:

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



Make cable connections as illustrated.

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

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

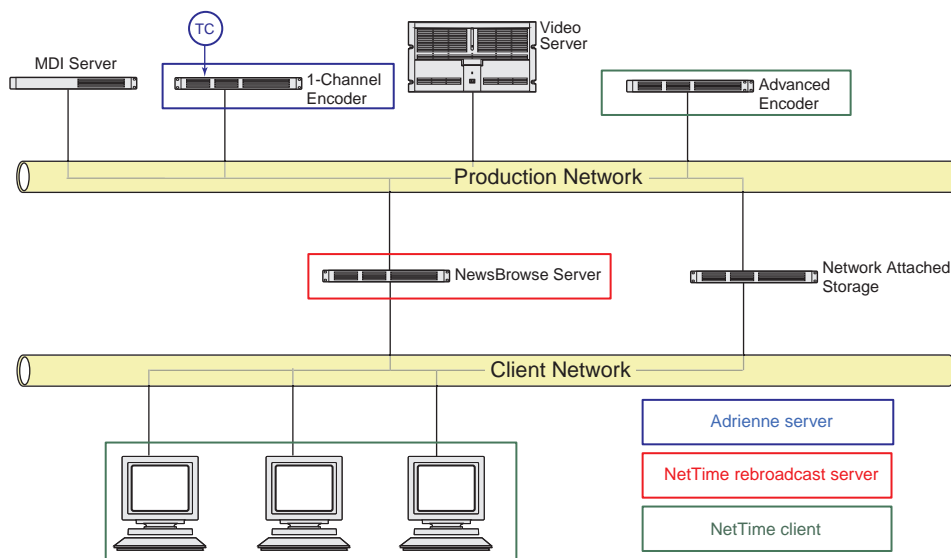
Prepare Profile Media Servers

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

1. Set up as a NetTime client. Refer to preceding procedures.
2. Click **Start | Run**, enter *regedit* and press **Enter**. The Registry Editor opens.
3. In the Registry Editor open the following key:
HKEY_LOCAL_MACHINE/SOFTWARE/Tektronix/Profile/ShuttleAtMode
Set the key to **TRUE**.
4. On the Profile XP, start **PortServer**.
5. Add a shortcut to PortServer to the startup folder. This ensures that PortServer always runs on the Profile XP, as it is required for Aurora Browse operation.
6. Verify that the following account has been added to the Profile system:
 - username: nbadmin
 - password: (contact Grass Valley Support for password)

NetTime system

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



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

Prepare NetTime

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

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

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

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

Set up NetTime with the following procedures:

- “Prepare NetTime servers” on page 188
- “Prepare NetTime clients” on page 188

Prepare NetTime servers

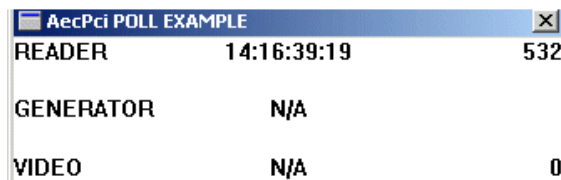
You use one single-channel encoder as the primary Adrienne Absolute Time Server, and another single-channel encoder as the secondary (redundant) Adrienne Absolute Time Server. A LTC connection to house timecode is required for single-channel encoders functioning as Adrienne Absolute Time Servers.

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

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

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

C:\AecPciPoll.exe



READER	14:16:39:19	532
GENERATOR	N/A	
VIDEO	N/A	0

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

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

Prepare NetTime clients

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

Some clients need special configuration to ensure time synchronization throughout the system. Since your single-channel encoder Adrienne Absolute Time Server is on the Production Network, only NetTime clients on the Production Network have

access. You must provide access for the external (Client Network) NetTime clients as well. To do this, you configure a NetTime client machine (in this case, the MediaFrame server) which has access to both Production and Client Networks to rebroadcast the time sync to external networks. NetTime clients on external networks can then look to the MediaFrame server as their NetTime server.

To prepare a NetTime client, do the following:

1. Open the following folder:
C:\Time Sync Software\Client
2. Open *NetTime-2b6.exe* and click **Yes** to install. Choose the defaults, including **configure as service**.
3. Set Net Time options as follows:
 - a. Enter the host name for the primary and secondary server according to the following table:

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

- b. Select the **RFC868(TCP)** protocol for both servers
 - c. For the MediaFrame server, select **Allow other computers to sync to this computer**.
 - d. Leave other fields at the defaults and click **Okay**.
4. The PC clock should automatically update to match the server. If not, check network connectivity and review install steps. All machines must be set for the same time zone to function properly.

Prepare NAS - Serial ATA network platform

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

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

1. From any Production network machine, enable the network to recognize the NAS by adding an IP address within the subnet range of 192.168.50.0.
2. For the first NAS machine (*nb-nas-1*), open the NAS configuration software in Internet Explorer by entering the following in the browser address bar:
<https://192.168.50.31:9890>

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

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

The NAS Administration Tool window opens at the Welcome page.

3. Enter the password. The default password is *triton*. The Status page opens.
4. In the tree view click **Network | Network Ports**. The Configure Network Ports page opens.
5. Configure network ports as follows:
 - a. **Port 0 Client Network** - Set the IP address and subnet mask for the Client network as specified by the local network administrator.

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

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

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

- c. Click **Save**, then select the **Restart** option to restart. Reboot takes 2-10 minutes. Do not power-down the enclosure during reboot.
6. After the NAS reboots, access the NAS configuration software as described earlier in step 2 and step 3, except this time, enter the following in the browser address bar:
`https://<Client IP Address>:9890`
The Status page appears.
7. In the Status page tree view, click **Network | Names/IPs**. The Names and IPs page opens.
8. Set the following:
 - **Domain name** - Enter the Client network Domain name.
 - **Gateway** - Enter the IP address for the Client network gateway. Consult the network administrator.
 - **Node Name** - For example: (*root-nb-nas-n*)
9. In the tree view click **System | System Administration | Date/Time**. The Date/Time page opens.
10. Select the correct time zone, date, and time.
11. Click **Save**, then select the **Restart** option to restart.
Reboot takes 2-10 minutes. Do not power-down the enclosure during reboot.
12. After the NAS reboots, access the NAS configuration software again as described

- in step 6. The Status page appears.
13. In the Status page tree view, click **Storage | Shares | Create** and then click the **Next** button. The CIFS Share page opens.
 14. Specify CIFS options as follows:
 - a. Enter *Media* as the share name.
 - b. Set user privileges. Select all of the following options:
 - Writeable
 - Public
 - Browseable
 - Available(Do not select Case Sensitive)
 - c. Click **Save**.
 15. Close the NAS Administration Tool.

Prepare NAS - Linux Fastora

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

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

Host table files

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

Devices share a common host table, which lists out the Production Network IP settings. For security purposes, the IP addresses should be non-routable (e.g. 192.168.xxx.xxx) and be part of the same subnets used by the Profile/Open SAN systems. The customer may request a particular subnet (routable or not) depending on

the needs of the facility. The only client side IP address needed in the host table is for the client switch itself, which is useful for accessing the web management page from the Aurora Browse devices.

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

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

#MediaFrame server

192.168.30.21      iron-nb-svr

#Browse MDI server

192.168.30.101    iron-nb-mdi

#Browse NAS

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

#Browse Advanced encoders

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

#Browse single-channel encoders

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

#NB Router Gateway

192.168.30.111    iron-nb-rtr

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

#Browse live monitor encoder

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

```
10.16.37.92      iron-nb-live-2      #Client LAN
#Browse Ethernet Switch
10.16.37.20      iron-nb-2950-client-1  #Client LAN
192.168.30.200   iron-nb-2950-prod-1
```

Host table tips:

- If you are exporting EDLs to Aurora Edit, the Aurora Edit workstation must be able to resolve the Profile MDI name (present in the EDL) to the IP address of the Profile XP system to which the MDI connects. The recommended solution is to map the MDI name to the Profile IP address in the Aurora Edit workstation’s host table. Refer to [“MDI and Encoder logical names convention” on page 46](#).
- 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.example.net”, then the host table entry in the MDI server(s) must match; if the entry is “NB-SERVER1.EXAMPLE.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.

Adding and configuring an Avalon archive

Avalon archive management software has reached end of service. The following information on adding and configuring an Avalon archive to a Mediaframe system is included here for reference only.

Avalon archive preparations

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

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

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

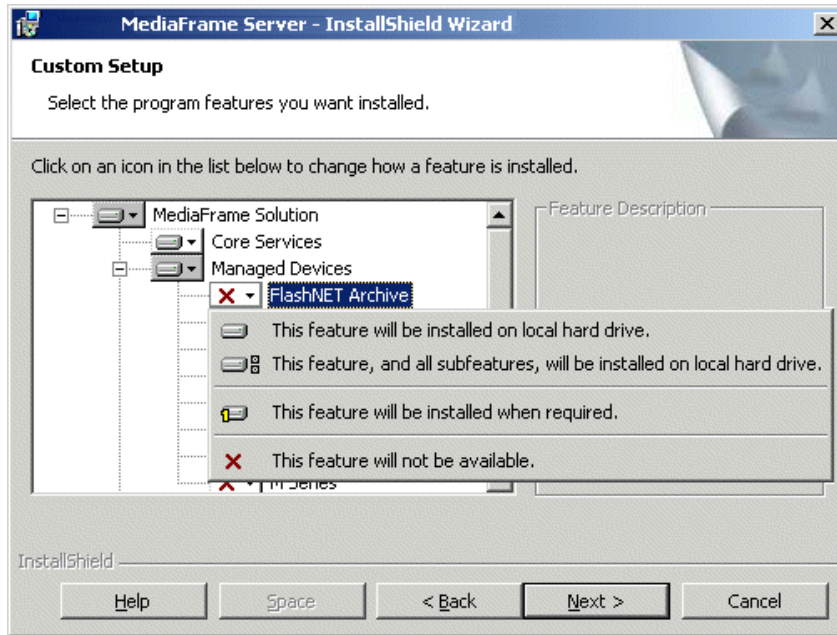
- Avalon archive has no fixed limit for concurrent transfers.

Add archive MDI

The archive MDI software component runs as a service, GV Avalon Archive MDI.

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.

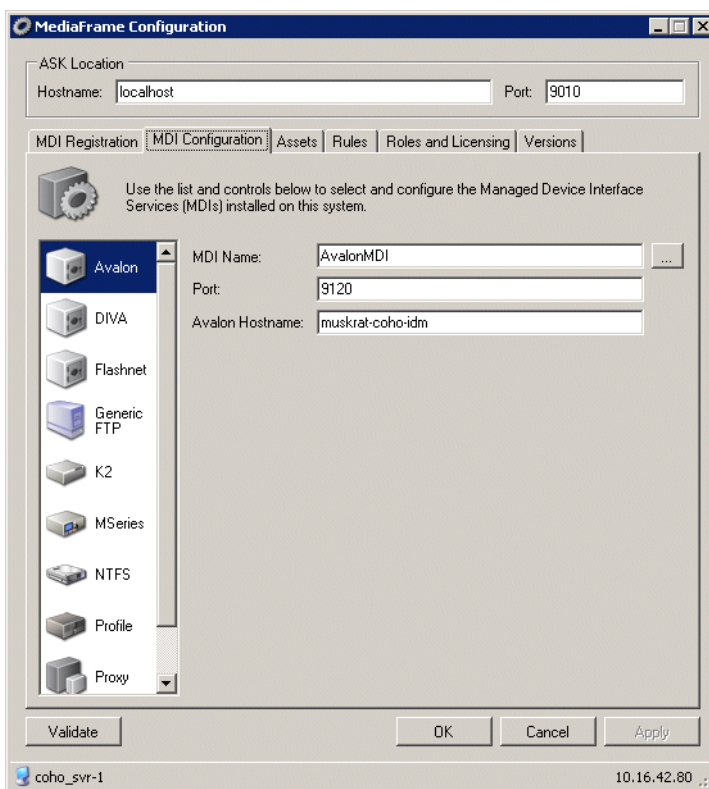
You can install the archive MDI software component from the MediaFrame server installation program. Select the component for your archive from the Custom setup page.



Configure Avalon MDI

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

To configure the Avalon MDI, do the following.

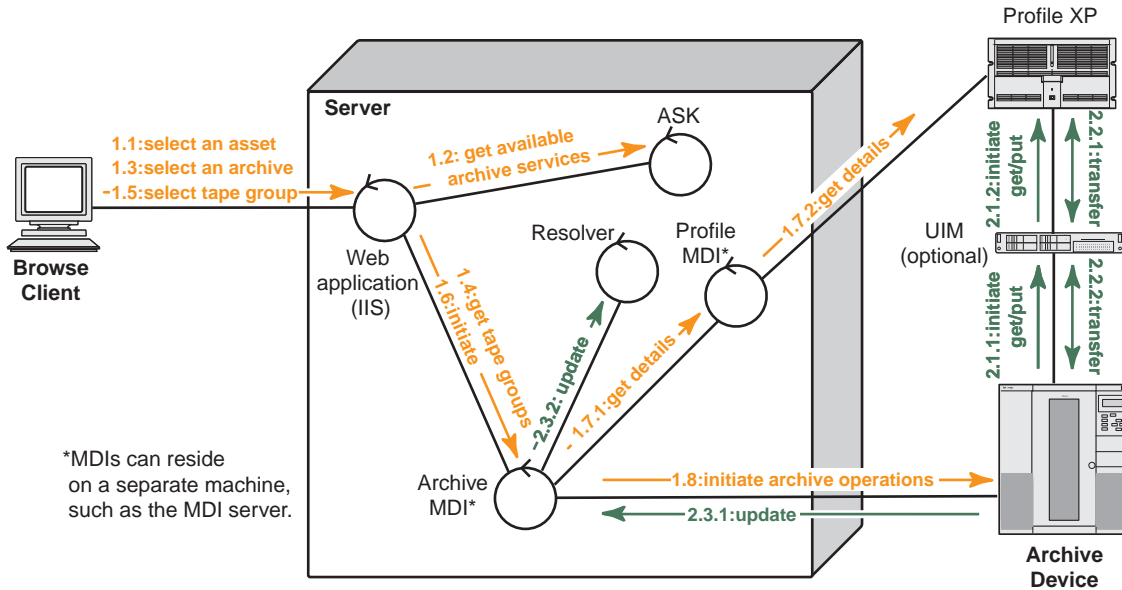


1. Select **Programs | Grass Valley | MediaFrame Config**. Select the MDI Configuration tab and the Avalon icon.
2. Enter the name of the MediaFrame server.
3. Port 9010 is required. Do not modify.
4. Use the ... button to location the name of the Avalon MDI.
5. Port 9120 is required.
6. Enter the name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

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

Archive operations on Profile XP

If archiving from the M-Series, Profile, or K2 server side, verify that you can FTP from the DIVA or Flashnet server to the K2 FTP through the FTP network using the movie login account.



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 initiates 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 transferred 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.

Appendix **D**

Installing and configuring the FileZilla Server

Third-party servers such as the FileZilla FTP server can be used for nearline storage. The Generic FTP MDI must be configured for FileZilla before you can use FileZilla with the MediaFrame system.

This chapter contains the following topics:

- [“Configuring the Generic FTP MDI for FileZilla”](#)
- [“Installing and configuring FileZilla”](#)
- [“Testing the FileZilla configuration”](#)

Configuring the Generic FTP MDI for FileZilla

To use FileZilla with the MediaFrame system, follow these steps.

1. Install the Generic FTP MDI on the MediaFrame server.
2. In the MediaFrame Config tool, select the MDI Registration tab.
3. Under Managed Device Services, highlight FTPMDI.
4. Click the **Add** button. The Add MDI Service dialog box displays.
5. In the MDI Server Hostname text field, enter the name of the MediaFrame server and click **OK**.
6. In the MediaFrame Config tool, select the MDI Configuration tab.
7. Click on the Generic FTP icon.
8. Click the **Add** button. The Add FTP dialog box displays.
9. Enter the FTP Server Address. This is the name from the host table of the FTP network on the machine running FileZilla. Be sure to include the `_he0` suffix.
10. Leave FTP Root Directory blank.
11. Enter the FTP username and password. This is the username and password of an administrator-level user that created on the machine that is running FileZilla.

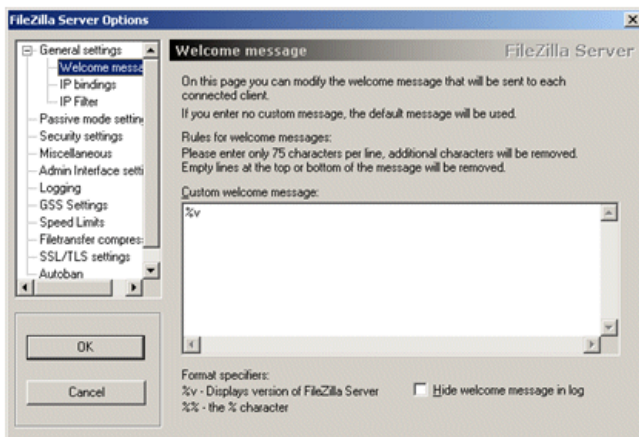
Installing and configuring FileZilla

On the machine chosen to run the FTP service (FileZilla), check to see if IIS is installed. If it is, either uninstall it or disable it.

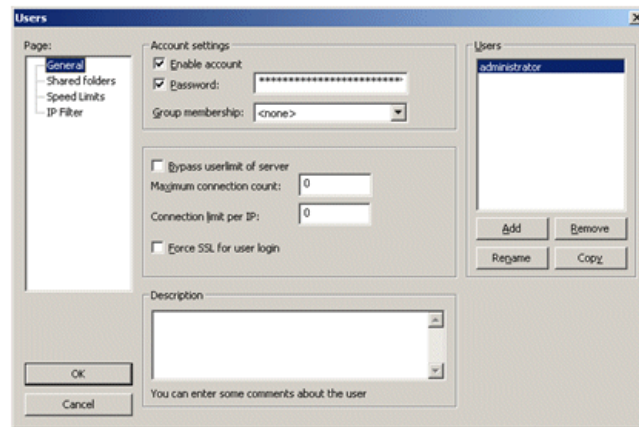
IIS can be uninstalled through **Control Panel | Add Remove Programs | Windows Components**. To disable IIS, follow the Microsoft Windows documentation for your version of IIS.

On the machine that is going to run FileZilla, follow these steps:

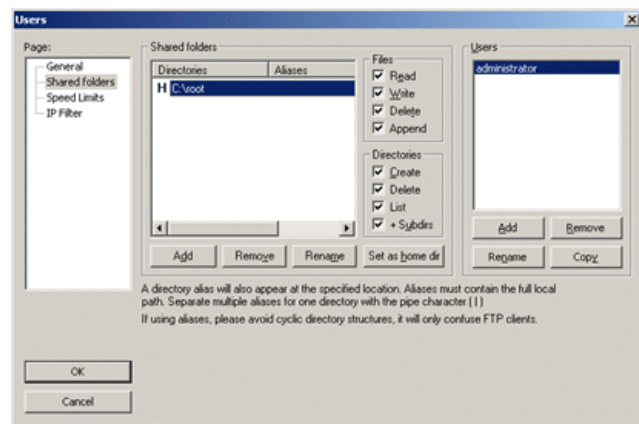
1. On the C:\ drive, create a folder and name it *root*.
2. Create an administrator-level user with the same values used in step 11 of “Configuring the Generic FTP MDI for FileZilla” on page 199.
3. Install the FileZilla Server software.
4. Open the FileZilla application.
5. Under **Edit | Settings**, highlight the Welcome message.
6. From the Custom welcome message window, delete all characters except **%v**



7. Click **OK** to close.
8. Under **Edit | Users | General**, click **Add** on the right-side of the pane.
9. Add the username that you used in the FTP MDI config dialog.
10. Select **General**, then check **Enable account and Password**.
11. In Password field, enter the password for that user, same as in FTP MDI Config window.



12. Under **Edit | Users**, select **Shared folders**.
13. Under Shared folders window, select **Add**.
14. Add the *root* folder created on the C:\ drive. Check all boxes.



15. Select **Set as home dir**.
16. Click **OK** to close.

Testing the FileZilla configuration

1. Open the Aurora Browse client application.
2. Select the **Explore** pane.
3. Right-click on **FTP-MDI** and select **New Folder**.
4. Create a folder named *Archive*.
5. Archive an asset.
6. Open **Transfer Monitor** to follow the progress of the transfer.

Index

Symbols

_he0 31

A

archive

- configuring 123
- enter MDI name 85
- MDI installed on platforms 124, 194
- MDI service 47
- preparing for MediaFrame 125
- round robin 88
- using Profile XP 197

ASK

- configuring 82
- service 47

assets, naming conventions 139

Aurora Browse clients

- adding 132

Aurora Browse users 134

Aurora Edit LD

- mapping the NAS for no V mode 100
- no V configuration for voiceover files 122

Aurora Proxy Encoder

- cabling 27

Axiom platform 185

B

backup and recovery 151

bins, naming conventions 139

C

cabling

- HAAR platform 22
- MDI server 24, 25, 27
- MediaFrame Server 25
- NAS 21, 22, 180, 185

canonical names 194

clock, synchronizing 189

component interaction diagrams 167

configuration

- FileZilla 199
- K2 BaseCamp Express 175, 177
- K2 BaseCamp Express encoders 176
- overview 72

configuration pages

accessing 81

ASK settings 84

FlashNet MDI 129

Generic FTP MDI 90

K2 MDI 92, 94

News MDI 99

NTFS MDI 121

proxy MDI 103

rules automation Aurora Proxy Encoder 116

control network description 29

conventions

machine naming 46

MDI naming 46

naming assets 139

naming bins 139

custom fields, adding 136

D

D drive 152

database

configuring the maintenance plan 143

creating a maintenance plan 143

modifying a maintenance plan 147

modifying for non-English searches 150

recovery plan 142

SQL 21

testing the backup 146

updating to the simple model 142

verifying maintenance plan status 145

device

adding with SiteConfig wizard 41

DNS 132, 192, 194

Domains and nbadmin 80

E

encoder, test 120

F

fields, custom 136

FileZilla

configuring 199

installing 199

test 201

first birthday 152

FlashNet archive

- configuring MDI 129
- Flashnet Archive
 - MDI service 47
- FTP network description 29
- functional description 14

G

- Generic FTP MDI, configuring 90

H

- HAAR platform
 - cabling 22
 - configuring 23
- hardware platforms
 - Axiom and Dell 185
 - K2 BaseCamp Express 25
 - MDI server 24
 - MediaFrame server 21
 - NAS 27, 180
- hosts files
 - example 192
 - explanation 31
 - writing to devices 59

I

- ingest
 - to a shared SmartBin 168
 - to a transfer SmartBin 167
- installation
 - cabling 20
 - FileZilla 199
 - rack-mounting 20
 - software 33
- Integrated Windows Authentication 132
- IP addresses
 - NAS 190, 192
- iSCSI network description 29

K

- K2 14
 - adding encoder to K2 system 73
 - configuring ASK 84
 - configuring MDI 92, 94
 - ingest 14
 - installing supporting software 176
 - nbadmin account 80
 - overview description 14

- K2 BaseCamp Express
 - about 17
 - configuring 175
 - encoders 176
 - low-res storage 177

L

- Legacy systems 179
- logons
 - NAS 190, 192
- LogViewer 165
- LTC 188

M

- maintenance plan
 - configuring 143
 - creating 143
 - modifying 147
 - testing 146
 - using 144
 - verifying status 145
- Marathon, see HAAR platform 22
- MDI, cabling the MDI server 24
- media (iSCSI) network description 29
- Media Frame Core ASK, configure 84
- MediaFrame server
 - renaming 146
 - test 120
- metadata
 - about 170
 - mapping 136
 - service 47

N

- name resolution 194
- naming conventions
 - assets 139
 - bins 139
 - machines 46
 - MDI 46
- NAS
 - cabling 27, 180
 - configuring multiple systems 100
 - mapping systems for Aurora Edit LD no V
 - mode 100
 - preparing 189
- nbadmin and Domains 80

NetTime 187
network
 canonical names 194
 connecting to customer LAN 132
 control 29
 creating with SiteConfig wizard 41
 DNS lookup 194
 Domain 132
 Domains and nbadmin 80
 FTP/streaming 29
 media (iSCSI) 29
 NAS test 79, 184
 zoning 20
new site wizard
 SiteConfig 39
News
 configure MDI 99
NLS MDI, see Generic FTP MDI 90
NTFS MDI
 configure 121
 service 47

P

partitions 151
passwords
 NAS 190, 192
ports
 K2 MDI 92
 mapping to services 47
 M-Series MDI 97
 News MDI 99
 Profile MDI 94, 101
 Proxy MDI 103
 Summit MDI 94
PortServer 186
power management settings
 on K2 Media Server 161
power supplies, NAS 22, 180, 185
ProductFrame
 definition 34
Profile
 MDI service 47
 Portserver 186
 preparations necessary for Aurora
 Browse 186
Proxy MDI
 configure 103
 service 47

proxy transfer
 service 48
purge
 about 173
 test 131

R

rack mounting 20
recovery 151, 152
recovery plan 141
registry key 186
renaming the MediaFrame server 146
Resolver service 48
Restoring from the generic recovery disk
 image 157
roles 134
round robin 88
rules
 configure rules automation 116
rules wizard
 on server 21
 service 48
 test 120

S

scavenge
 about 171
 test 131
searches, non-English 150
security
 Aurora Browse website 132
 NAS 192
services
 accessing 80
 mapping to ports 47
sessions, dropping 135
ShuttleAtMode 186
site
 creating in SiteConfig 39
site wizard
 SiteConfig 39
software
 SiteConfig 67
software components, interactions explained 167
SQL
 recovery plan 142
streaming/FTP network description 29
system

- creating in SiteConfig 39
- functional description 14
- system description
 - Siteconfig 35

T

- timecode,LTC 188
- transfer
 - round robin 88
- troubleshooting
 - tips 166
 - tools 165

U

- UIM
 - hosts file 32
- upgrade software
 - SiteConfig 67

W

- website, Aurora Browse security 132
- Windows Product Key 159
- WINS 192
- wizard
 - new site SiteConfig 39

Z

- zoning, network 20