071-8705-00

SiteConfig Migration Instructions

This document contains the most recent information and supersedes previous publications, as of 02 July 2009. Check the Grass Valley website at *www.grassvalley.com/docs* for an updated version that contains additional important information.

Contents

Grass Valley Product Support

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

Web Technical Support

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

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

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

Telephone Support

Use the following information to contact Product Support by phone.

International Support Centers

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

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

Authorized Local Support Representative

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

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

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

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

Region	**County**	**Telephone**
	Southeast Asia - Singapore	+65 6379 1769
	Indian Subcontinent	+91 11 515 282 502; +91 11 515 282 504
Pacific	Australia, New Zealand	+61 1300 721 495
Central America, South America	All	+55 11 5509 3440
North America	North America, Mexico, Caribbean	+1 800 547 8949; +1 530 478 4148
Europe	UK, Ireland, Israel	+44 118 923 0499
	Benelux – Netherlands	+31 (0) 35 62 38 421
	Benelux – Belgium	+32 (0) 2 334 90 30
	France	+800 80 80 20 20; +33 1 48 25 20 20
	Germany, Austria, Eastern Europe	+49 6150 104 444
	Belarus, Russia, Tadzhikistan, Ukraine, Uzbekistan	+7 095 258 09 20; +33 (0) 2 334 90 30
	Nordics (Norway, Sweden, Finland, Denmark, Iceland)	+45 40 47 22 37
	Southern Europe – Italy	+39 02 24 13 16 01; +39 06 87 20 35 42
	Southern Europe – Spain	+34 91 512 03 50
Middle East, Near East, Africa	Middle East	+971 4 299 64 40
	Near East and Africa	+800 80 80 20 20; +33 1 48 25 20 20

Prepare for SiteConfig migration

NOTE: There might be a newer version of this document available. Check your product's release notes and the Grass Valley website at www.grassvalley.com/docs for references to an updated version that contains additional important information.

Work through the following topics to plan and procure the items necessary to manage your existing system with SiteConfig.

About system descriptions

You have several options for starting and developing a SiteConfig system description, as follows:

Start with an existing system description

You can obtain a system description for a system similar to the one you are installing. Some system descriptions are provided with SiteConfig as templates for specific system types. You can import the system description into SiteConfig, and then modify it until it matches your specific system. You can define the entire system including defining sites, groups, networks, devices and even the planned IP assignments before you arrive at the installation site.

You can save your work as a system description file (*.scsd*) file and when onsite at the installation site, you can import the file into SiteConfig as your starting point.

Once you import the system description you can make changes as appropriate and proceed to discover the connected physical devices.

Start with a new system description

You can create new system description using SiteConfig on your PC before you arrive at the installation site, or as part of the commissioning process at the installation site.

Typically, if you are starting with a new system description, you use the site wizard to add one or more sites based on appropriate site models, define networks and their IP ranges, and add device placeholders. Then you discover devices and perform appropriate network configuration, followed by software deployment.

Start with a K2 System Configuration file

If you are using SiteConfig at a system that has already been commissioned and if the system has a K2 SAN, you can import or merge the K2 System Configuration

(K2Config) application's XML file into SiteConfig to add the K2 SAN networks and devices to your system description.

When you import or merge the K2Config XML, SiteConfig opens a dialog box in which you provide additional information about the devices connected to your SAN. This allows SiteConfig to create the groups and devices in the system description that most accurately represent your SAN.

About system migration types

For the purposes of migrating an existing system to SiteConfig management, systems are categorized into system types that share similar characteristics. Systems of each type share common migration taskflows, especially as it concerns the development of the initial system description. System types and taskflows are described as follows:

System	Definition	System description	Other tasks	Comments
Type I	One or more K2 SANs (not mirrored), plus additional devices.	Merge K2Config XML into SiteConfig.	Add additional devices, such as MediaFrame systems.	—
Type II	A mirrored K2 SAN, plus additional devices.	Import a mirrored SAN system description template.	Add devices to the system description.	Mirrored SANs require a special hierarchy that is best achieved by starting with a system description template.
Type III	Not Type I or Type II. Systems range from small to large.	Choose the appropriate method.	Choose the appropriate tasks.	Use topics in this document as examples. Also find topics in *SiteConfig Help Topics* and *SiteConfig User Manual*.

Identify the type that matches your existing system, then use checklists and topics in this document as appropriate for your system type.

Type I migration checklist

Use the following sequence of tasks as a guideline to migrate an existing Type I system to SiteConfig management.

	Task	Comment
□	Procure SiteConfig software.	—
□	Verify that your existing control point PC meets the requirements for a SiteConfig control point PC.	Review system requirements and network access requirements about installing SiteConfig.
□	Install SiteConfig on the control point PC	—
□	If you have an Aurora Browse/MediaFrame system at a version lower than 6.5.0, you must upgrade the system to support 6.5.0 and higher software.	Refer to the section at the end of this document.
□	Merge the K2 SAN's K2Config XML into the SiteConfig system description.	Use the default blank system description that SiteConfig provides when it opens. Merge the K2Config XML into the system description.
□	If necessary, modify networks.	Make the networks in the system description match your actual system networks. You can also configure a unmanaged network for software deployment only. This is useful if you have devices, such as Aurora Edit LD workstations, that are on a network that should not be managed by SiteConfig.
□	Add one or more groups to the system description, if additional groups are needed.	Group similar devices together.
□	Add a placeholder device to the system description for each of your system devices that do not already have a placeholder device.	Select Family, Type, and Model to create a placeholder device based on the standard device model.
□	Evaluate actual devices and determine their readiness for SiteConfig.	Check SiteConfig support software, network interfaces, and software roles.
□	Install SiteConfig support on system devices as necessary.	—
□	Set credentials on system devices.	Verify that SiteConfig can access the device via administrator username/password.

	Task	Comment
□	Remove and add network interfaces on placeholder devices as necessary.	Make network interfaces on placeholder devices match the network interfaces on actual devices.
□	Remove and add software roles on placeholder devices as necessary.	Make software roles on placeholder devices match the software on actual devices.
□	Make any further modifications to the system description as necessary to represent your actual system.	—
□	Discover system devices.	If configuring for software deployment only, device discovery is not used for Aurora Edit LD workstations.
□	Assign each discovered device to its placeholder device.	—
□	For each discovered and assigned device, evaluate managed network interfaces.	—
□	Remove planned settings, if present, from network interfaces.	***NOTE: Do not apply planned settings.***
□	Add a control point PC placeholder device to the system description.	—
□	Discover the control point PC and assign it to the placeholder control point PC.	—
□	Ping each device and the control point PC to test network communication.	—
□	View and verify host table information for future use	Do not update hosts files on devices, as this overwrites your existing hosts files.
□	Configure deployment groups	—
□	Uninstall software as necessary	If software was previously installed manually (without using SiteConfig), you might need to manually uninstall the software before first using SiteConfig to deploy software.

Type II migration checklist

Use the following sequence of tasks as a guideline to migrate an existing Type II system to SiteConfig management.

	Task	Comment
□	Procure SiteConfig software.	—

	Task	Comment
□	Procure the SiteConfig mirrored SAN system description template.	Find system description template XML files in the templates directory on the SiteConfig software CD or on the Grass Valley website.
□	Verify that your existing control point PC meets the requirements for a SiteConfig control point PC.	Review system requirements and network access requirements about installing SiteConfig.
□	Install SiteConfig on the control point PC	—
□	If you have an Aurora Browse/MediaFrame system at a version lower than 6.5.0, you must upgrade the system to support 6.5.0 and higher software.	Refer to the section at the end of this document.
□	Import the mirrored SAN system description template	—
□	If necessary, modify networks.	Make the networks in the system description match your actual system networks, but do not change the position of networks in the tree view hierarchy.
□	Add one or more groups to the system description, if additional groups are needed.	Group similar devices together.
□	Add a placeholder device to the system description for each of your system devices that do not already have a placeholder device.	Select Family, Type, and Model to create a placeholder device based on the standard device model.
□	Evaluate actual devices and determine their readiness for SiteConfig.	Check SiteConfig support software, network interfaces, and software roles.
□	Install SiteConfig support on system devices as necessary.	—
□	Set credentials on system devices.	Verify that SiteConfig can access the device via administrator username/password.
□	Remove and add network interfaces on placeholder devices as necessary.	Make network interfaces on placeholder devices match the network interfaces on actual devices.
□	Remove and add software roles on placeholder devices as necessary.	Make software roles on placeholder devices match the software on actual devices.
□	Make any further modifications to the system description as necessary to represent your actual system.	—

	Task	Comment
□	Discover system devices.	If configuring for software deployment only, device discovery is not used for Aurora Edit LD workstations.
□	Assign each discovered device to its placeholder device.	—
□	For each discovered and assigned device, evaluate managed network interfaces.	—
□	Remove planned settings, if present, from network interfaces.	***NOTE: Do not apply planned settings.***
□	Add a control point PC placeholder device to the system description.	—
□	Discover the control point PC and assign it to the placeholder control point PC.	—
□	Ping each device and the control point PC to test network communication.	—
□	View and verify host table information for future use	Do not update hosts files on devices, as this overwrites your existing hosts files.
□	Configure deployment groups	—
□	Uninstall software as necessary	If software was previously installed manually (without using SiteConfig), you might need to manually uninstall the software before first using SiteConfig to deploy software.

Type III migration checklist

Use the following sequence of tasks as a guideline to migrate an existing Type III system to SiteConfig management.

	Task	Comment
□	Procure SiteConfig software.	—
□	Verify that your existing control point PC meets the requirements for a SiteConfig control point PC.	Review system requirements and network access requirements about installing SiteConfig.
□	Install SiteConfig on the control point PC	—
□	If you have an Aurora Browse/MediaFrame system at a version lower than 6.5.0, you must upgrade the system to support 6.5.0 and higher software.	Refer to the section at the end of this document.

	Task	Comment
□	Develop your system description as neccessary to represent your system	—
□	Create or modify networks as necessary	Make the networks in the system description match your actual system networks. You can also configure a unmanaged network for software deployment only. This is useful if you have devices, such as Aurora Edit LD workstations, that are on a network that should not be managed by SiteConfig.
□	Add one or more groups to the system description, if additional groups are needed.	Group similar devices together.
□	Add a placeholder device to the system description for each of your system devices that do not already have a placeholder device.	Select Family, Type, and Model to create a placeholder device based on the standard device model.
□	Evaluate actual devices and determine their readiness for SiteConfig.	Check SiteConfig support software, network interfaces, and software roles.
□	Install SiteConfig support on system devices as necessary.	—
□	Set credentials on system devices.	Verify that SiteConfig can access the device via administrator username/password.
□	Remove and add network interfaces on placeholder devices as necessary.	Make network interfaces on placeholder devices match the network interfaces on actual devices.
□	Remove and add software roles on placeholder devices as necessary.	Make software roles on placeholder devices match the software on actual devices.
□	Make any further modifications to the system description as necessary to represent your actual system.	—
□	Discover system devices.	If configuring for software deployment only, device discovery is not used for Aurora Edit LD workstations.
□	Assign each discovered device to its placeholder device.	—
□	For each discovered and assigned device, evaluate managed network interfaces.	—
□	Remove planned settings, if present, from network interfaces.	***NOTE: Do not apply planned settings.***

	Task	**Comment**
□	Add a control point PC placeholder device to the system description.	—
□	Discover the control point PC and assign it to the placeholder control point PC.	—
□	Ping each device and the control point PC to test network communication.	—
□	View and verify host table information for future use	Do not update hosts files on devices, as this overwrites your existing hosts files.
□	Configure deployment groups	—
□	Uninstall software as necessary	If software was previously installed manually (without using SiteConfig), you might need to manually uninstall the software before first using SiteConfig to deploy software.

Related Links

About system descriptions on page 6

Procure SiteConfig software

1. Determine your source location for SiteConfig software, as follows:

Location	**Description**
SiteConfig Software CD	Contains software installation files and documentation. Obtain from Grass Valley.
Grass Valley website	Provides access for downloading software installation files and documentation.

2. Make the following files available to your system devices and to the control point PC.

Software	**Location**
SiteConfig application	Find in the `Release` directory
SiteConfig Discovery Agent	Find in the `Discovery Agent Setup` directory
Microsoft .NET	Find in the `Release\DotNetFX` directory
SiteConfig system description templates	Find in the `Templates` directory

Install SiteConfig on control point PC

NOTE: There might be a newer version of this document available. Check your product's release notes and the Grass Valley website at www.grassvalley.com/docs for references to an updated version that contains additional important information.

Work through the following topics to install the SiteConfig application on the control point PC.

About installing SiteConfig

SiteConfig uses a protocol that involves sending Ethernet broadcast messages to discover and configure devices. To enable this protocol to work correctly, there must be unrestricted network access between the control point PC and the devices to be discovered.

This is achieved if control network interfaces are all connected to the same switch or to multiple switches interconnected with ISLs/trunks. If your site requires that other switches and/or routers be in the network path, you must make sure that no restrictions are in place that block SiteConfig protocols.

Also, do not install SiteConfig on a PC on which a drive from a managed device is mapped as an administrative share (C$). For example, if you have a PC set up to run anti-virus software and for this purpose you have network drives set up on the PC mapped to C$ shares on devices, then do not use that PC as the SiteConfig control point PC that manages those devices.

System requirements for SiteConfig control point PC

The PC on which SiteConfig is installed must meet the following requirements:

Requirements	**Comments**
Operating system	Microsoft Windows (Must be a U.S. version): XP Professional Service Pack 2, Server 2003, or Vista Enterprise Service Pack 1.
RAM	Minimum 512 MB, 1 GB recommended
Graphics acceleration	Must have at least 128 MB memory
Processor	Pentium 4 or higher class, 2 GHz or greater
Hard disk space	400 MB
Microsoft .NET Framework	Version 2.0

Requirements	Comments
Java JRE	1.3.1_12 and 1.4.2_05 or higher. Required for the HP Ethernet Switch configuration interface, which is used for K2 Storage Systems (shared storage).
XML	Microsoft XML 4 Service Pack 2 is required. You can install it from the msxml4sp2 file on the K2 System Software CD.

Installing SiteConfig

Connect a PC with the appropriate system requirements to the LAN on which all the devices to be managed are connected. Take into consideration the requirement that there be no routed paths to the devices.

1. Install the SiteConfig application on the PC. The SiteConfig application can be downloaded from the Grass Valley website or from the SiteConfig CD.
2. Open the Windows operating system Services control panel on your Control Point PC and look for an entry called " ProductFrame Discovery Agent".

   The Discovery Agent is also known as the Network Configuration Connect Kit.

   The Discovery Agent must be installed on the control point PC so that the control point PC can be discovered by SiteConfig and added to the system description as a managed device. This is necessary to ensure name resolution in SiteConfig's hosts file.

3. Proceed as follows:

   - If the Discovery Agent is not installed, navigate to the SiteConfig install location's Discovery Agent Setup subdirectory and double-click the *DiscoveryAgentServiceSetup.msi* file. This launches the setup program and installs the Discovery Agent. Follow the setup wizard to complete installation. A restart is required after installation. Then continue with the next step in this procedure.
   - If the Discovery Agent is already installed, continue with the next step in this procedure.

4. If not already configured, configure the control point PC with a valid Ethernet IP address for the LAN using Windows Network Connections.
5. If you are not going to be using SiteConfig to manage system hosts files, put the system hosts file on the control point PC.

Start system description

NOTE: There might be a newer version of this document available. Check your product's release notes and the Grass Valley website at www.grassvalley.com/docs for references to an updated version that contains additional important information.

Use the topics in this section as appropriate for your system type to get started with your SiteConfig system description.

NOTE: Refer to the migration checklist for your system type to determine the appropriate topics and other system-specific information.

Related Links

Type I migration checklist on page 8

Type II migration checklist on page 9

Type III migration checklist on page 11

Opening SiteConfig

1. Use the SiteConfig shortcut on the Windows desktop or in the Start menu to open SiteConfig.
2. SiteConfig opens as follows:
   - If you have previously opened SiteConfig, the SiteConfig main window opens with the most recently used system description loaded.
   - If you have not previously used SiteConfig or if SiteConfig does not have access to a system description file, you are prompted to create a new system description or to import an existing system description.
3. Respond as appropriate.

About the mirrored SAN system description template

Mirrored K2 SANs introduce an additional level to the network hierarchy in the SiteConfig system description. Because of the rules for networks, the placement of networks in a mirrored SAN system is critical for device connectivity. Therefore it is recommended that you start by importing a SiteConfig system description template designed specifically for a mirrored K2 SAN system to achieve the required network hierarchy.

The mirrored SAN system description template provides a Site node for the X SAN and a Site node for the Y SAN. The K2 clients (K2 Media Clients and/or K2 Summit Production Clients) and K2 Media Servers for each SAN must be under their Site node. For your existing mirrored SANs, you add groups and devices to the appropriate Site node. As you modify the system description template to match your specific K2 SAN mirrored system, do not change the position of the SAN Site nodes or the networks in the tree view hierarchy.

Rules for networks

When adding networks to sites, you are indicating that all devices under that site can connect to the network. If you edit the network interfaces of any device that you add to that site, SiteConfig shows you only the networks that are within "scope", which are networks defined in each immediate site parent going up the hierarchy to the System node.

Importing a system description

Prerequisites for this task are as follows:

- The SiteConfig PC has access to the system description file you are importing.

1. Open SiteConfig and proceed as follows:
   - If a dialog box opens that gives you the choice of creating or importing a system description, it means SiteConfig does not have access to a system description file. Click **Import**.
   - If the SiteConfig main window opens, click **File | Import**.

   The Import System Description dialog box opens.
2. Browse to and select a system description file (`*.scsd`) and click **Open**.

The current system description is closed and the system description you are importing is displayed in SiteConfig.

Merging a K2 System Configuration file

You can merge a K2 SAN's K2 System Configuration (K2Config) application XML file into your system description. You should do this just once for a particular K2 SAN, as there are no features in SiteConfig or K2Config to keep subsequent changes synchronized.

1. Click the **File | Merge** menu item.

   The Merge System Description dialog box opens.
2. From the **Files of type** drop-down list select **K2 SAN Config (.xml)**, browse to the location of the XML file, select the file, and click **Open.**
3. If SiteConfig opens a dialog box asking you to resolve devices to equivalent device models in SiteConfig, choose the appropriate device model.

SiteConfig creates a Site under the top-level System node with networks and groups representing the K2 SAN it finds in the XML file. SiteConfig adds placeholder devices for each device in the K2 SAN.

Creating a system description for stand-alone K2 clients

Do not do this task if:

- You already have or are developing a SiteConfig system description managing other devices in your facility and that system description has the correct networks and connectivity for your stand-alone K2 clients. In this case, skip ahead to the task in which you add a group to the system description for your stand-alone K2 clients.

Do this task if:

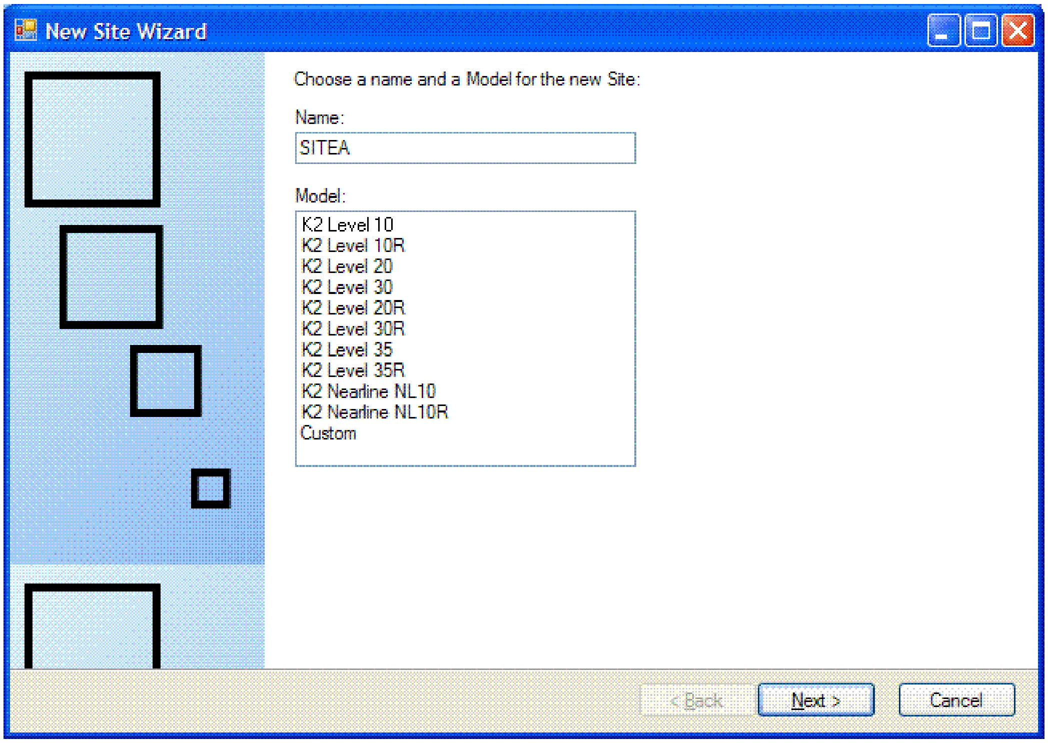
- You do not yet have a system description appropriate for managing your stand-alone K2 clients.

1. Open SiteConfig and proceed as follows:
   - If a dialog box opens that gives you the choice of creating or importing a system description, it means SiteConfig does not have access to a system description file. Click **Create**.
   - If the SiteConfig main window opens, click **File | New**.

   The Create New System Description dialog box opens.
2. In the Create New System Description dialog box, enter the name of the file for the system description you are creating.
   It is recommended that you store the system description file in the default location, rather than browsing to store the file in a different location. SiteConfig always accesses the default location.
3. Click **OK**.

   A blank system description loads, which displays just the top-level System node in the tree view.
4. In the **Network Configuration | Devices** tree view, right-click the **System** node or a **Site** node and select **Add Site**.

   The New Site Wizardopens.



Choose a name and a Model for the new Site:

Name: SITEA

Model:
K2 Level 10
K2 Level 10R
K2 Level 20
K2 Level 30
K2 Level 20R
K2 Level 30R
K2 Level 35
K2 Level 35R
K2 Nearline NL10
K2 Nearline NL10R
Custom

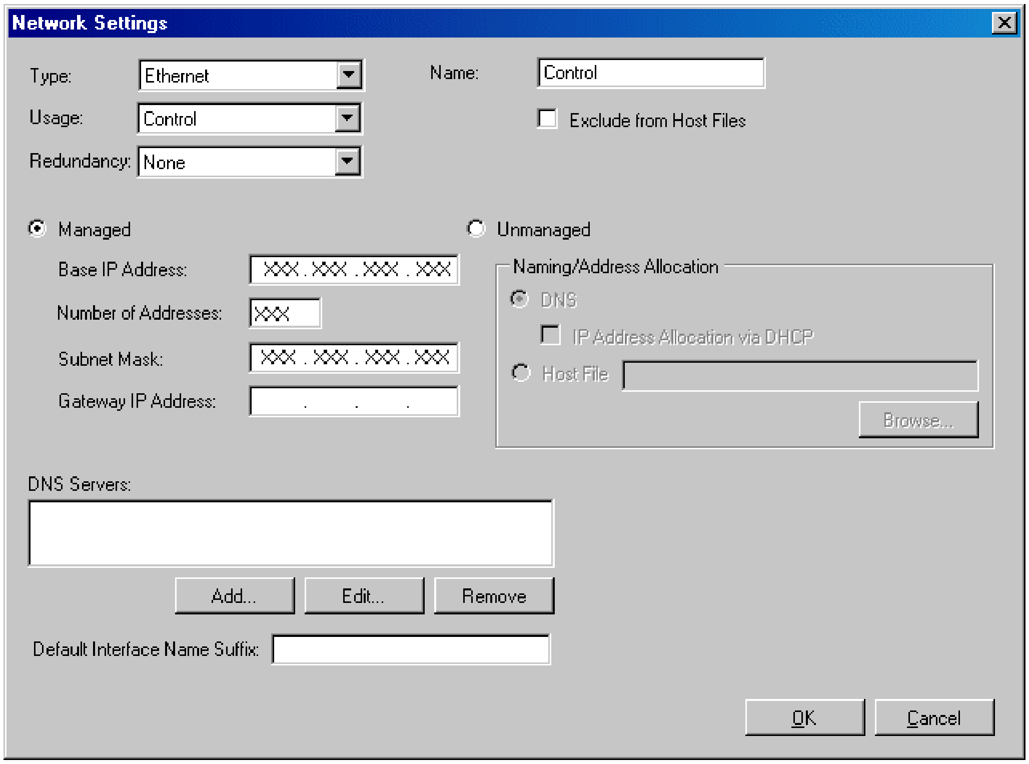
5. Enter a name for the site you are creating, considering the following:
   - Keep the site name short, as it becomes the root identifier that is the default prefix for device and network names.
   - Sites in the tree view are automatically sorted alphabetically.
6. Select **Custom** and click **Next**.
7. Click **Finish** to create the site.

The site is displayed in SiteConfig in the tree view with groups and device placeholders displayed under the site node. New networks are displayed in the tree view of networks in the Networks tab.

Creating the control network for stand-alone K2 clients

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



Type: Ethernet

Usage: Control

Redundancy: None

Name: Control

☐ Exclude from Host Files

● Managed

Base IP Address: XXX . XXX . XXX . XXX

Number of Addresses: XXX

Subnet Mask: XXX . XXX . XXX . XXX

Gateway IP Address: . . .

○ Unmanaged

Naming/Address Allocation

● DNS

☐ IP Address Allocation via DHCP

○ Host File

DNS Servers:

Default Interface Name Suffix:

3. Configure the settings for the network as follows:

Setting...	**For control network**
Type	*Ethernet* is required
Usage	*Control* is required
Redundancy	*None* is required. This is true even on a redundant K2 SAN. (Only the iSCSI network is redundant on a redundant K2 SAN.)
Name	*Control* is recommended
Exclude from Host Files	*Unselected* is required
Managed	*Selected* is required
Base IP Address	The first (lowest) IP address in the range of IP addresses managed by SiteConfig. Required.
Number of Addresses	The number of IP addresses in the range managed by SiteConfig. Required.
Subnet Mask	The network's subnet mask. Required.
Gateway IP Address	Additional network settings managed by SiteConfig. Allowed.

Setting...	For control network
Unmanaged	*Unselected* is required. Related settings are disabled.
DNS Servers	Servers providing DNS for name resolution. Allowed.
Default Interface Name Suffix	Not allowed

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

Creating the FTP/streaming network for stand-alone K2 clients (optional)

If you transfer media to/from the stand-alone K2 client, create a FTP/streaming network.

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

Setting...	For FTP/streaming network
Type	*Ethernet* is required
Usage	*FileTransfer* is required
Redundancy	*None* is required. This is true even on a redundant K2 SAN. (Only the iSCSI network is redundant on a redundant K2 SAN.)
Name	*Streaming* is recommended
Exclude from Host Files	*Unselected* is required
Managed	*Selected* is required
Base IP Address	The first (lowest) IP address in the range of IP addresses managed by SiteConfig. Required.
Number of Addresses	The number of IP addresses in the range managed by SiteConfig. Required.
Subnet Mask	The network's subnet mask. Required.
Gateway IP Address	Additional network settings managed by SiteConfig. Allowed.
Unmanaged	*Unselected* is required. Related settings are disabled.

Setting...	**For FTP/streaming network**
DNS Servers	Servers providing DNS for name resolution. Allowed.
Default Interface Name Suffix	*_he0* is required

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

Creating or modifying a network

Compare the networks in the system description with your actual system networks. Create or modify networks in the system description as necessary to match your actual system networks.

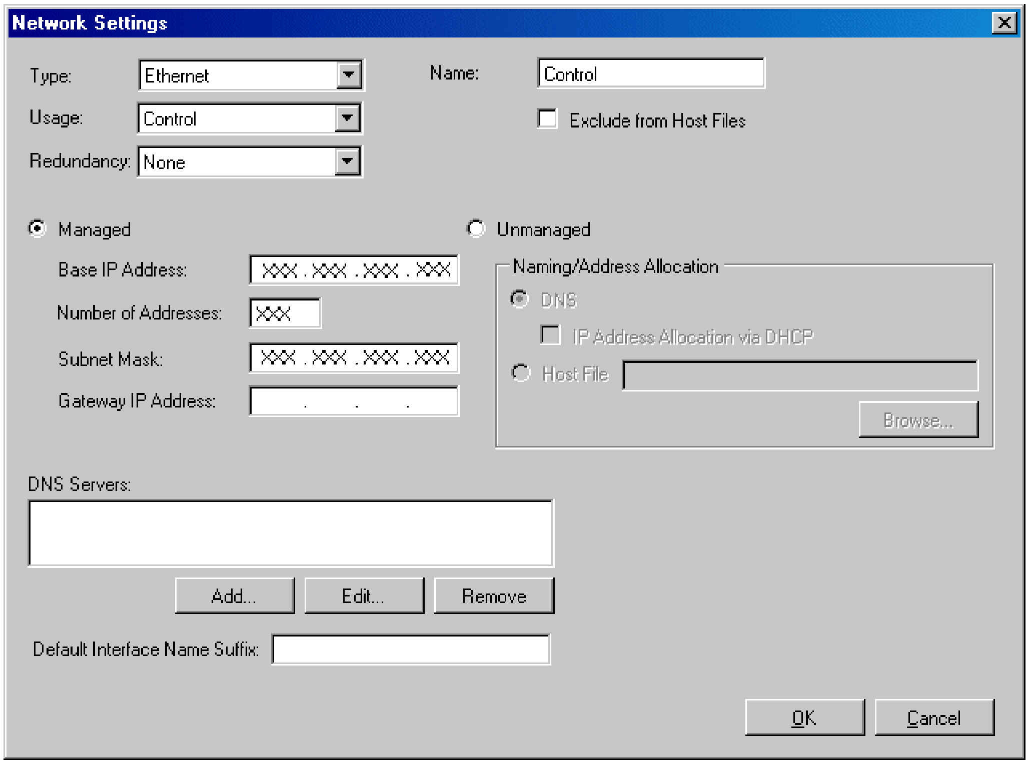
You might also want to create an unmanaged network in the system description. You do this to represent a network that SiteConfig does not manage, such as your corporate LAN that is managed by your IT department. This is the case if you have devices, such as Aurora Edit LD workstations, that are on your corporate LAN, yet you want to use SiteConfig to deploy software to those devices.

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**.
   - To modify a network, in the list view right-click a network and select **Details**.

   The Network Settings dialog box opens.



Network Settings

Type: Ethernet

Usage: Control

Redundancy: None

Name: Control

☐ Exclude from Host Files

● Managed

Base IP Address: XXX . XXX . XXX . XXX

Number of Addresses: XXX

Subnet Mask: XXX . XXX . XXX . XXX

Gateway IP Address: . . .

○ Unmanaged

Naming/Address Allocation

● DNS

☐ IP Address Allocation via DHCP

○ Host File

DNS Servers:

Default Interface Name Suffix:

3. Configure the settings for the network as follows:

   - Type – The link layer of the protocol stack, such as Ethernet or Fibre Channel.
   - Usage – The function of the network, related to the type of traffic the network carries, such as control or file transfer.
   - Redundancy – Specifies if the network supports redundancy and if the network is primary or secondary.
   - Name – The name of the network, as it is displayed in SiteConfig and identified in host files.
   - Exclude from Host Files – If selected, SiteConfig does not write the network's hostnames and IP addresses to the host files that it copies to networked devices.
   - Managed – Network settings are managed by SiteConfig.
   - Base IP Address – The first (lowest) IP address in the range of IP addresses managed by SiteConfig.
   - Number of Addresses – The number of IP addresses in the range managed by SiteConfig.
   - Subnet Mask/Gateway IP Address – Additional network settings managed by SiteConfig.
   - Unmanaged – Network settings are managed by mechanisms external to SiteConfig.

- DNS – Name resolution is provided by a DNS server for the unmanaged network.
- IP Address Allocation via DHCP – IP addresses are assigned by DHCP for the unmanaged network.
- Host File – Name resolution is provided by host files for the unmanaged network. If you want SiteConfig to copy the contents of the unmanaged network's host file into a managed network's host file, enter the location of the unmanaged network's host file. This allows host names of devices on the unmanaged network to be resolved on the managed network.
- DNS Servers – Servers providing DNS for name resolution. These DNS server can be for both managed and unmanaged networks.
- Default Interface Name Suffix – The suffix added to the end of host names to identify interfaces on this network.

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

Related Links

Configuring for software deployment only on page 25

Adding a group

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

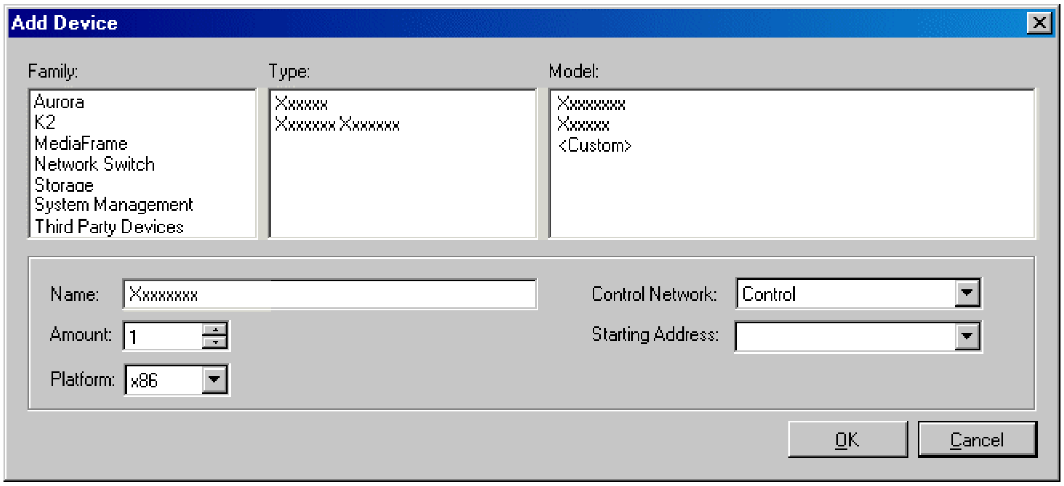
   The group appears in the tree view.
2. Right-click the group and select **Rename**.
3. Enter the desired name for the group.

Adding a device

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**.
   If a device supports sub-devices, you can right-click the device and select **Add Sub-Device**.



Name: Xxxxxxxx

Amount: 1

Platform: x86

Control Network: Control

Starting Address:

The Add Device dialog box opens.

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

   - Family, Type, Model – Based on your selection, the device is pre-defined in Product Frame, with interfaces added and networks assigned. For Model, if you select <Custom>, no interfaces are added or networks assigned.
   - Name – Enter the host name (network name) of the actual device.
   - 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.
   - Platform type - Select x86 if the device has a 32 bit OS, x64 if it has a 64 bit OS.
   - Control Network – If multiple control networks are available in the system description, you can select the control network for the device you are adding.
   - 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.

Configuring for software deployment only

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

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

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

   The networks under that node are displayed in the list view.
2. Proceed as follows:

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

   The Network Settings dialog box opens.
3. Configure the settings for the network as follows:

   - Type – Select Ethernet
   - Usage – Select Control
   - Redundancy – Select None
   - Name – Enter a name to identify the network in the system description
   - Exclude from Host Files – Select the checkbox
   - Unmanaged – Select the radio button. If name resolution via DNS or hosts file, configure Naming/Address Allocation appropriately for DNS or hosts file
   - Base IP Address - If static IP network, enter the first (lowest) IP address in the range that the Aurora Edit LD workstations have their IP addresses
   - Number of IP Addresses – If static IP network, enter the number of IP addresses in the range that the Aurora Edit LD workstations have their IP addresses
   - 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.
6. Add a placeholder device for an Aurora Edit LD workstation.
7. Select the placeholder device.
8. In the interfaces list view, right-click an interface and select **Edit**.

   The Unmanaged Network Interface Details dialog box opens.

9. Configure the settings for the interface as follows:
   - Network – If using DHCP or external hosts file, select the unmanaged network that you configured earlier in this procedure.
   - IP Address – Select the IP address currently configured on the Aurora Edit LD workstation.
   - DNS Suffix – For communication on some networks, a suffix, such as *`mycorp.com`*, must be added to host names.
   - Remaining settings are irrelevant, as SiteConfig does not manage this device's network.
10. Configure for the device name as follows:
    a) In the tree-view select the placeholder device.
    b) In the Device list view right-click the device and select **Edit**.

    The Edit Device dialog box opens.

    c) Edit the hostname.
    d) If using DHCP, specify a domain name.
    e) Click OK to save settings and close.
11. Click **OK** to save settings and close.
12. From the control point PC, ping the Aurora Edit LD workstation to verify communication.

Evaluate and prepare devices for SiteConfig

NOTE: There might be a newer version of this document available. Check your product's release notes and the Grass Valley website at www.grassvalley.com/docs for references to an updated version that contains additional important information.

Use the following topics to answer the following questions for each of your system devices:

- Is SiteConfig support software installed?
- Are network cables connected and settings configured as SiteConfig expects?
- Is software installed and configured as specified by SiteConfig software roles?

Then, if necessary, install support software and make other preparations so that your devices are ready for SiteConfig discovery and configuration.

NOTE: Refer to the migration checklist for your system type to determine the appropriate topics and other system-specific information.

Related Links

Type I migration checklist on page 8

Type II migration checklist on page 9

Type III migration checklist on page 11

Create record of software installed on devices

if you have not already done so, create a document on which you can keep track of the software installed on each of your system devices. This is especially helpful for Aurora product devices. The following table is an example of this type of document. As you evaluate each of your system devices, verify the software currently installed on the device and fill in the table. Then, as you proceed with subsequent tasks and assign software roles to devices in SiteConfig, you can refer to your table and make sure you are assigning software roles correctly.

Software	SVR-1	HD-1, 2, 3	CONF-1	EDIT-1	DSM-1	ING-1	FSM-1	HDK2-1	FTP-1
MF Server	X								
+ K2 MDI	X								
+ News MDI			X						
+ NTFS	X								
+ FlashNET MDI	X								
+ Proxy MDI	X								

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

About SiteConfig support on managed 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.

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

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

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

Installing SiteConfig support

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

1. Open the Windows Services Control Panel and look for the following required item:
   - ProductFrame Discovery Agent
2. Open the Windows Add\Remove Programs Control Panel and look for the following required item:
   - Microsoft .NET Framework 2.0 Service Pack 2
3. Proceed as follows:
   - On Aurora Edit, Aurora Share, Aurora SmartBins, Aurora FTP, and Aurora Conform Server devices, if the ProductFrame Discovery Agent is installed, use the Windows Add\Remove Programs Control Panel and uninstall it. On these devices you must uninstall and then install version 1.1 or higher, as instructed in next steps.

     NOTE: The Discovery Agent can be named the ProductFrame Discovery Agent, the SiteConfig Discovery Agent, or the SiteConfig Network Configuration Connect Kit.
   - On other devices, if the ProductFrame Discovery Agent is already installed, you can leave it installed as is.
   - On all devices, if either the ProductFrame Discovery Agent or .NET is not installed, install the required software as instructed in next steps.
4. Navigate to your SiteConfig files or to the SiteConfig install location.
5. To install the ProductFrame Discovery Agent Service do the following:

   a) Copy the `Discovery Agent Setup` subdirectory to the device.

   b) In the `Discovery Agent Setup` directory, double-click the `DiscoveryAgentServiceSetup.msi` file.
   The setup program launches to install the SiteConfig Discovery Agent.

   c) Follow the setup wizard.
   The setup wizard presents a list of devices types similar to the following:
   - K2Server
   - GigESwitch
   - FCSwitch

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

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

e) Complete the setup wizard.

f) Restart.

The restart is required after the installation.

6. To install .NET 2.0 do the following:

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

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

Related Links

Qualifying software roles on page 37

Verifying Discovery Agent installation on page 53

Set credentials

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

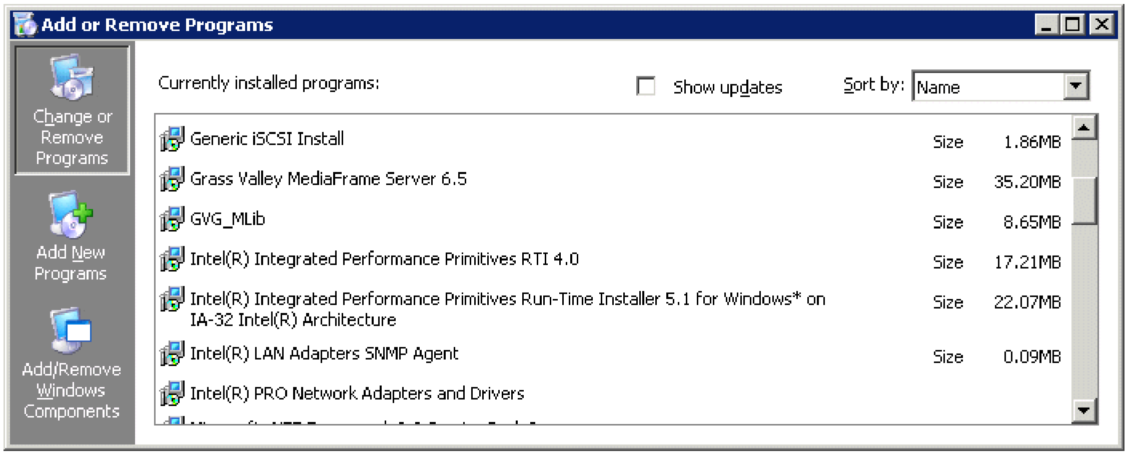
SiteConfig is pre-configured to use the following default credentials to access devices:

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

2. If necessary, change the device's credentials to match the credentials that SiteConifg uses to access the device.

Identify software installed on devices

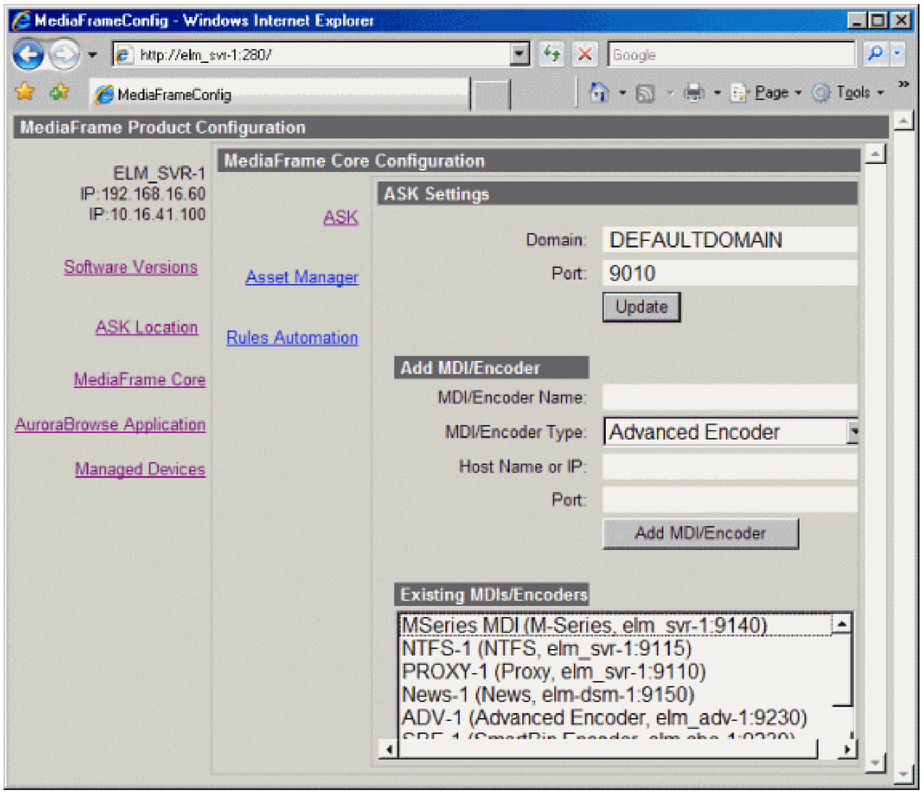
1. Open the Windows operating system **Add/Remove Programs** control panel.



Add or Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Currently installed programs:
□ Show updates
Sort by: Name

Generic iSCSI Install Size 1.86MB
Grass Valley MediaFrame Server 6.5 Size 35.20MB
GVG_MLib Size 8.65MB
Intel(R) Integrated Performance Primitives RTI 4.0 Size 17.21MB
Intel(R) Integrated Performance Primitives Run-Time Installer 5.1 for Windows* on IA-32 Intel(R) Architecture Size 22.07MB
Intel(R) LAN Adapters SNMP Agent Size 0.09MB
Intel(R) PRO Network Adapters and Drivers

2. Make a record of the Grass Valley and related software installed on the device.
3. To identify the devices on which MediaFrame MDI software is installed, do the following on the MediaFrame server:
   a) If a MediaFrame server at a software version lower than 6.5.0, view the server's configuration page at **MediaFrame Core | ASK**.



ELM_SVR-1
IP:192.168.16.60
IP:10.16.41.100

Domain: DEFAULTDOMAIN

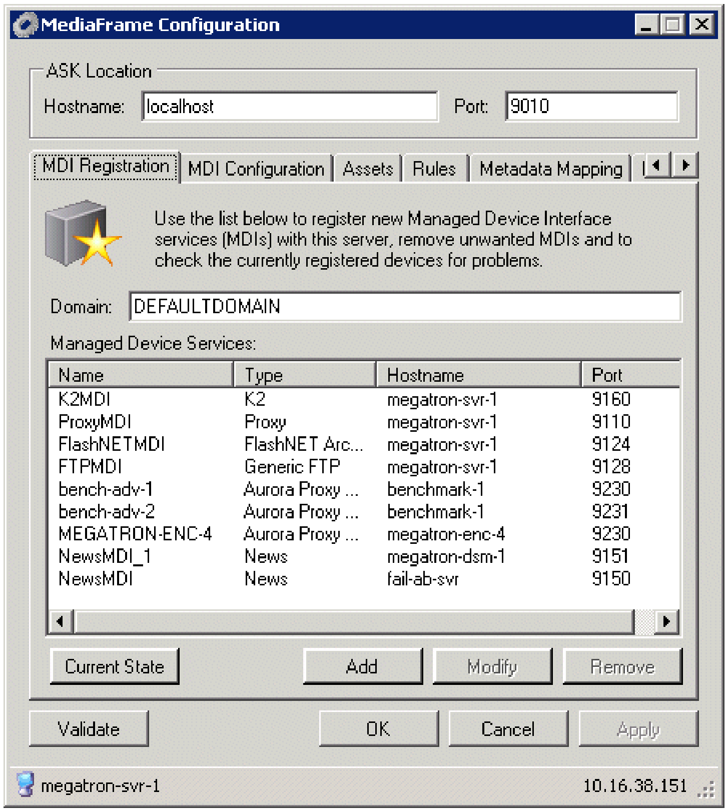
Port: 9010

MDI/Encoder Type: Advanced Encoder

MSeries MDI (M-Series, elm_svr-1:9140)
NTFS-1 (NTFS, elm_svr-1:9115)
PROXY-1 (Proxy, elm_svr-1:9110)
News-1 (News, elm-dsm-1:9150)
ADV-1 (Advanced Encoder, elm_adv-1:9230)

Existing MDIs/Encoders lists software components, the devices on which they are installed, and the configuration of the devices they control.

b) If a MediaFrame server at software version 6.5.0 or higher, view the MediaFrame Configuration MDI Registration tab.



Hostname: localhost Port: 9010

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

Domain: DEFAULTDOMAIN

Managed Device Services:

Name	Type	Hostname	Port
K2MDI	K2	megatron-svr-1	9160
ProxyMDI	Proxy	megatron-svr-1	9110
FlashNETMDI	FlashNET Arc...	megatron-svr-1	9124
FTPMDI	Generic FTP	megatron-svr-1	9128
bench-adv-1	Aurora Proxy ...	benchmark-1	9230
bench-adv-2	Aurora Proxy ...	benchmark-1	9231
MEGATRON-ENC-4	Aurora Proxy ...	megatron-enc-4	9230
NewsMDI_1	News	megatron-dsm-1	9151
NewsMDI	News	fail-ab-svr	9150

megatron-svr-1 10.16.38.151

MDIs and the devices on which they are installed are listed.

4. For each device listed, make a record of the MDIs installed.

Related Links

Identify components to upgrade on page 73

About device models and actual devices

SiteConfig is pre-loaded with standard placeholder device models for devices in managed systems. Device models primarily define the network interfaces and software roles. These models are based on known product configurations as shipped from Grass Valley. When SiteConfig adds a device, it creates a placeholder device with the network interfaces and software roles as defined by the device model. When you manually add a device, you can choose to include the network interfaces and software roles as defined by the device model, or you can choose a custom device with no network interfaces and software roles. For the custom device, you must than add network interfaces and software roles.

Network interfaces

When SiteConfig discovers a device, it attempts to map the actual device's network interfaces to the placeholder device's network interfaces. If the actual device's network interfaces are connected or configured differently than those in the placeholder device, SiteConfig frequently maps the interfaces incorrectly. This is especially true of the control network interface. If this problems occurs, the typical solution requires removing and adding interfaces to the placeholder device. Therefore, if your actual device's network interfaces do not match its device model's network interfaces, when you develop your system description you should customize that placeholder device's network interfaces, rather than use the network interfaces as provided by the device model. This allows you to define each placeholder network interface exactly as it is connected and configured on the actual device. This requires more steps and a longer process before you begin device discovery, but results in fewer problems, less troubleshooting, and less rework as you discover and assign devices.

For example, your device might have its network connections reversed compared to the device model. An example of reversed connections is the control connection connected to port 2 (2nd port on the motherboard) and the streaming connection connected to port 1. To solve this problem, remove both interfaces from the placeholder. Then add the first interface and select the streaming network from the list of networks. This tells SiteConfig which network that interface connects to. Then add the second interface and choose the control network from the network list. Your placeholder interfaces now match the actual devices interfaces.

Software roles

When SiteConfig checks software to prepare for software deployment, it provides software deployment tasks based on the software roles assigned to the device in the system description. If the actual device's software roles are different than those assigned to the device in the system description, SiteConfig can not provide the appropriate software deployment tasks and you can not deploy the software. Therefore, if your actual device's software roles do not match its device model's software roles, when you develop your system description you should customize that device's software roles, rather than use the roles as provided by the device model. This allows you to define each role exactly as it is on the actual device. This requires more steps and a longer process before you begin software deployment, but results in fewer problems, less troubleshooting, and less rework as you deploy software.

Qualifying network interfaces

Check network connections on your actual system devices and make sure that what SiteConfig expects, as configured in the placeholder device, matches what is on the actual device. Network interfaces as identified by SiteConfig typically correspond to rear panel connectors on devices as follows:

SiteConfig network interface	Rear panel connector on device
Ethernet 0	Port 1
Ethernet 1	Port 2
Ethernet 2	Port 3
Ethernet 3	Port 4

1. For each device, do the following:
    a) Refer to qualifications for managed devices and identify the network interface configurations that have the most potential to cause problems.

       For example, a common qualification for all device types is that Ethernet port 1 (the first port on the motherboard) is the control network. If this is not true on the actual device, it causes discovery problems. Some device types have other configurations, such as teaming, that can also cause problems if not configured as SiteConfig expects.

    b) In SiteConfig **Network Configuration | Device** tree view, select the placeholder device and then in the Interfaces list view identify the interfaces that SiteConfig expects to find when it discovers the actual device.
    c) At the managed device, check the connection and configuration of each network port and match it to the network interface on the placeholder device in SiteConfig.
2. If you identify a network interface on the actual device that is not configured as SiteConfig expects, when you develop your system description, do the following:
    a) For the placeholder device to which you intend to assign that actual device, remove the problematic network interfaces.
    b) Add network interfaces to the placeholder device and configure them as necessary to match the interfaces on the actual device.

Related Links

Qualifications for managed devices on page 59

About roles

A role is a grouping of software functionality. A device can have one or more software roles. A software role is typically provided by one or more programs or services running on the device. For some products, a single device type can be configured to have several different combinations of software roles, depending on the functionality that device provides to the system or systems to which it belongs.

Depending on a device's family, type, and model, SiteConfig automatically assigns the appropriate software roles to a device when the device is added to the system description. You can also manually modify a device's software roles.

SiteConfig knows what software should be installed for each software role, and deploys the software from a software package accordingly. SiteConfig matches managed package roles with device roles in order to generate appropriate deployment tasks for the actual software deployment activities.

Qualifying software roles

Check software as installed and configured on your actual system devices and make sure that what SiteConfig expects, as defined by software roles on the placeholder device, matches what is on the actual device.

1. For each device, do the following:
   a) Refer to qualifications for managed devices and identify the software roles, if any, that need special attention.
   b) In SiteConfig **Software Deployment | Devices** tree view, expand the placeholder device and identify the roles that SiteConfig expects to find on the actual device.
   c) At the managed device, check the software currently installed and match it to the software roles on the placeholder device in SiteConfig.
2. If you identify software on the actual device that is not installed or not configured as SiteConfig expects, when you develop your system description, do the following:
   a) For the placeholder device to which you intend to assign that actual device, remove the roles that do not match the software on the actual device.
   b) Add software roles to the placeholder device as necessary to match the software on the actual device.

Related Links

Qualifications for managed devices on page 59

Develop system description

NOTE: There might be a newer version of this document available. Check your product's release notes and the Grass Valley website at www.grassvalley.com/docs for references to an updated version that contains additional important information.

Use the topics in this section as appropriate to further modify your SiteConfig system description so that it accurately represents your actual system.

NOTE: Refer to the migration checklist for your system type to determine the appropriate topics and other system-specific information.

Related Links

Type I migration checklist on page 8

Type II migration checklist on page 9

Type III migration checklist on page 11

About planned and current IP configuration

If you add a device to the system description before discovering the actual device, you are working with the placeholder device. If you chose a device model, SiteConfig displays a list of the network interfaces that the model defines in the interfaces view.

You can edit all the network interfaces for the placeholder. You can select a network from which to assign an IP address and also a specific IP address from that network, if the interface connects to a managed network. You can also set a hostname for the device. Since you have not matched the placeholder to a discovered device, all settings are called "planned" settings and are saved in the system description only.

When you discover a device and match it to a placeholder, SiteConfig retrieves all the current network configuration from the device. For each network interface defined in the plan, SiteConfig matches it to the corresponding network interface retrieved and display. SiteConfig displays a planned tab that indicates the settings that do not match with the current settings.

You can now either choose to do one of the following:

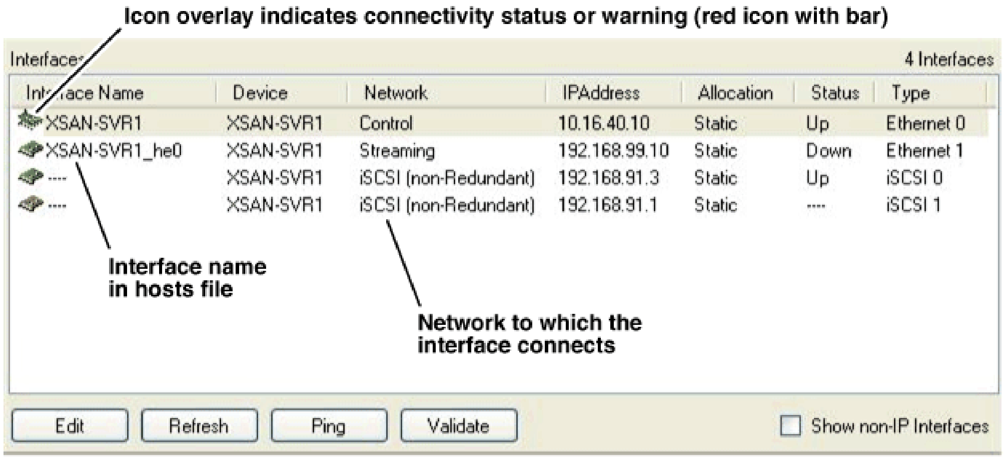
- Keep the current settings. To do this you remove planned settings, which allows SiteConfig to accept the current settings.
- Have SiteConfig apply the planned settings to the device. When this occurs, the settings currently configured on the actual network interface are overwritten, so you should compare planned settings and current settings and verify that the planned settings are correct.

Always set your control interface IP address before your other network interfaces.

SiteConfig also generates a planned tab if settings were modified outside of SiteConfig. A red icon overlay with tooltip provides contextual information.

Viewing device interfaces

1. In the **Network Configuration | Networks** tree view, select any node.


Icon overlay indicates connectivity status or warning (red icon with bar)
Interfaces
4 Interfaces
Interface name in hosts file
Network to which the interface connects
Edit
Refresh
Ping
Validate
□ Show non-IP Interfaces

Interface Name	Device	Network	IPAddress	Allocation	Status	Type
XSAN-SVR1	XSAN-SVR1	Control	10.16.40.10	Static	Up	Ethernet 0
XSAN-SVR1_he0	XSAN-SVR1	Streaming	192.168.99.10	Static	Down	Ethernet 1
----	XSAN-SVR1	iSCSI (non-Redundant)	192.168.91.3	Static	Up	iSCSI 0
----	XSAN-SVR1	iSCSI (non-Redundant)	192.168.91.1	Static	----	iSCSI 1

   The devices under that node are displayed in the device list view and the interfaces on the devices are displayed in the interface list view.

2. To view interfaces that do not use Internet Protocol (IP), such as Fibre Channel interfaces, as well as interfaces that do use IP, select **Show non-IP Interfaces**.
3. To view only interfaces that use IP, deselect **Show non-IP Interfaces**.
4. To view only the interfaces on a single device, select the device in the tree view or in the device list view.

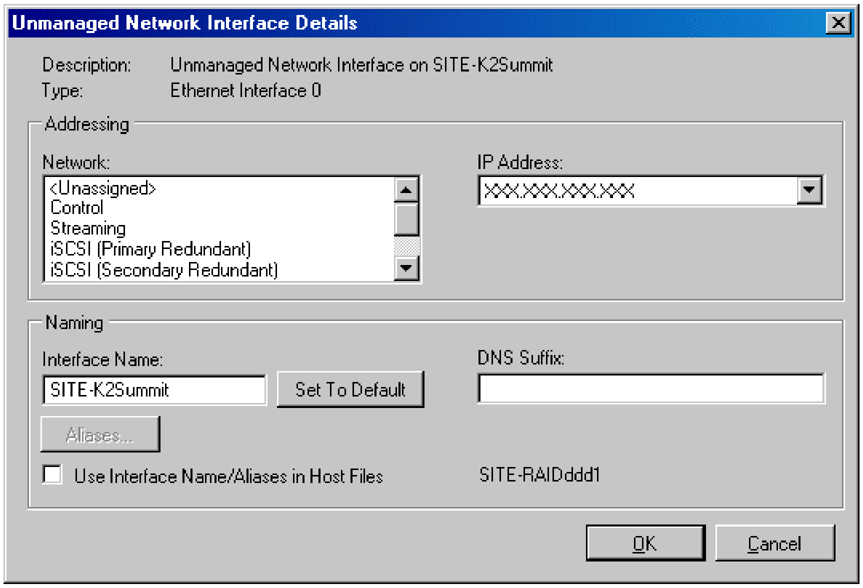
About IP configuration of network interfaces on devices

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

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

Placeholder device IP configuration

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



Unmanaged Network Interface Details

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

Addressing

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

IP Address: XXX.XXX.XXX.XXX

Naming

Interface Name: SITE-K2Summit

DNS Suffix:

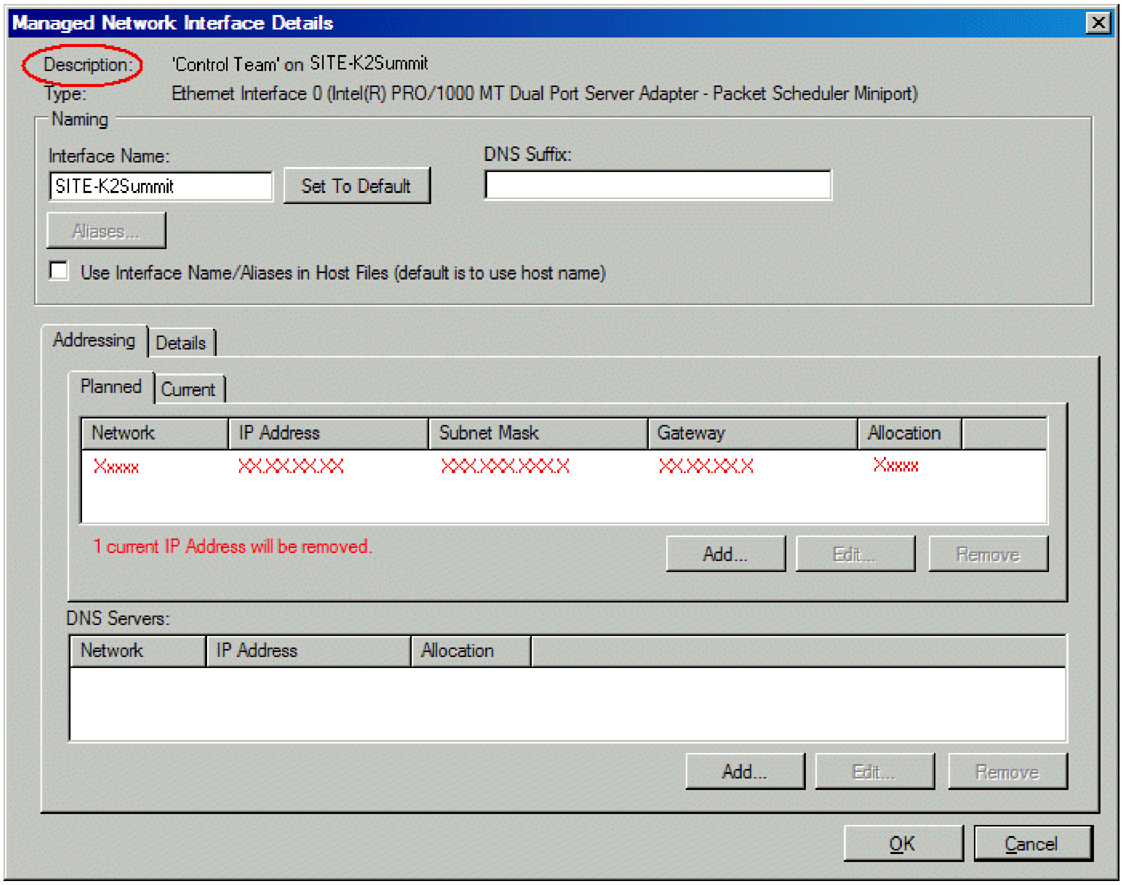
□ Use Interface Name/Aliases in Host Files

SITE-RAIDddd1

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

Discovered device IP configuration

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



Description: 'Control Team' on SITE-K2Summit
Type: Ethernet Interface 0 (Intel(R) PRO/1000 MT Dual Port Server Adapter - Packet Scheduler Miniport)

Interface Name: SITE-K2Summit

DNS Suffix:

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

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

1 current IP Address will be removed.

DNS Servers:

Network	IP Address	Allocation

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

Modifying an unassigned (unmanaged) interface

Prerequisites for this task are as follows:

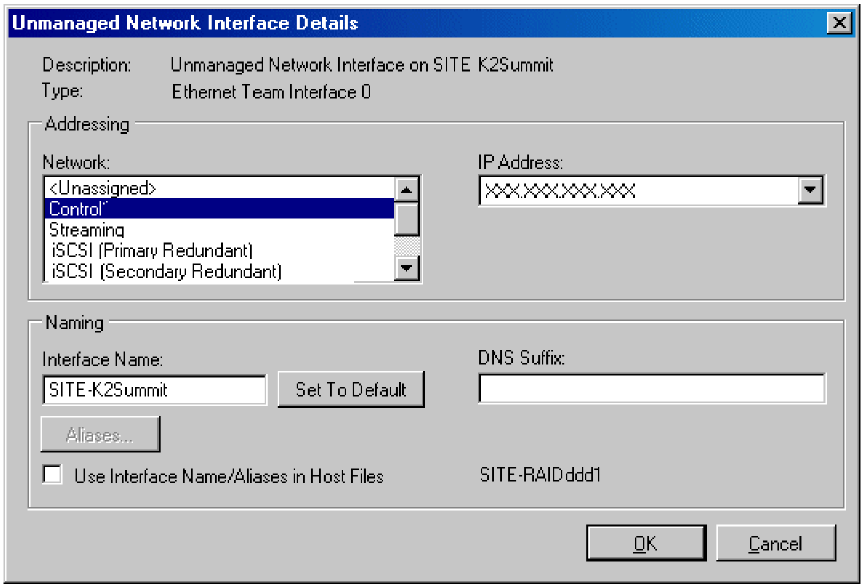
- The system description has one or more placeholder devices.
- The placeholder device has a one or more unmanaged network interfaces.

1. In the **Network Configuration | Devices** tree view, select a placeholder device.

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

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

   The Unmanaged Network Interface Details dialog box opens.



Unmanaged Network Interface Details

Description: Unmanaged Network Interface on SITE K2Summit

Type: Ethernet Team Interface 0

Addressing

Network:

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

IP Address: XXX.XXX.XXX.XXX

Naming

Interface Name: SITE-K2Summit

DNS Suffix:

□ Use Interface Name/Aliases in Host Files

SITE-RAIDddd1

3. Configure the settings for the interface as follows:

   - Network – This list includes the networks in the system description, as well as an <Unassigned> network. Select the network for the interface. If you select <Unassigned>, the interface can be on a network that is not included in the system description and therefore not managed by SiteConfig.
   - IP Address – A list of the available IP addresses for the selected network. Select the IP address for the interface.
   - Interface Name – The network name of the interface, as follows:
     - On the Control network, the network name of the interface must be the host name of the device.
     - On other networks (not the Control network) the network name of the interface shall not be the host name of the device. Some networks, such as the iSCSI network, do not allow interface names, and so naming controls are disabled.

     NOTE: In the networks view, you can specify that a particular network be excluded from the hosts file. This means that any network interfaces you assign to such a network are automatically excluded from the hosts file even if you checked the Use Interface Name/Aliases in Host Files checkbox. If you uncheck this box, it will default to using the host name as the interface name. Be careful that you do not specify two interfaces with the same host name.

   - Set to Default – Sets the name of the interface to SiteConfig’s default convention, based on the current host name of the device.
   - Use Interface Name/Aliases in Host Files – Enables the Aliases button. Tells SiteConfig to use this interface name in the hosts file. See note above.

- Aliases – Allows you to assign multiple network names to the adapter, such that they are managed by SiteConfig’s host file management features.
- DNS Suffix – For communication on some networks, a suffix, such as `mycorp.com`, must be added to host names.

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

Removing an interface

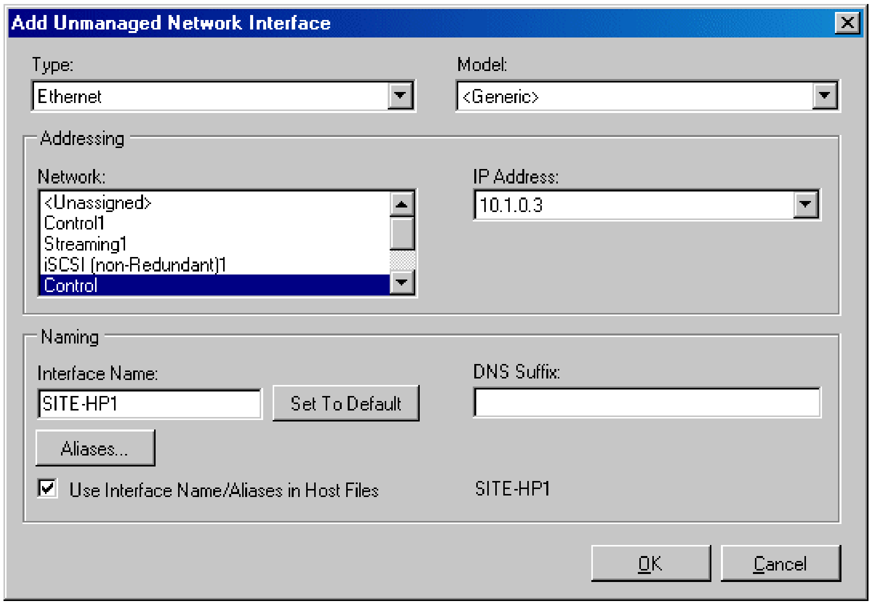
1. In the tree view, select the placeholder device from which you are removing the interface.
   The device's interfaces are displayed in the Interfaces list view.
2. In the Interfaces list view, right-click the interface you are removing.
3. Select **Remove**.

   The interface is removed from the device in the system description.

Adding an interface

1. In the **Network Configuration | Devices | Device** list view, right-click a device and select **Add Interface**.

   The Add Unmanaged Network Interface dialog box opens.



Add Unmanaged Network Interface

Type: Ethernet

Model: <Generic>

Addressing

Network:
<Unassigned>
Control1
Streaming1
iSCSI (non-Redundant)1
Control

IP Address: 10.1.0.3

Naming

Interface Name: SITE-HP1

DNS Suffix:

☑ Use Interface Name/Aliases in Host Files

SITE-HP1

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

   - Type – Select the type of interface you are adding.

     The interface types listed, such as Ethernet or Fibre Channel, are those currently defined in the system description.

   - Model – Select the model for the interface. Select <Generic> if the model of the interface you are adding is not listed.

     The models listed can include specific manufacturer product models for the interface, as defined in the system description, as well as a <Generic> model.

   - Network – Select the network for the interface.

     The networks listed include those in the system description, as well as an <Unassigned> network. If you select <Unassigned>, the interface can be on a network that is not included in the system description and therefore not managed by SiteConfig.

   - IP Address – Select the IP address for the interface.

     The list of IP addresses is available only for networks that support IP addresses. It is a list of the available IP addresses for the selected network.

   - Interface Name – Accept the default name or enter a different name.

     This is the network name of the interface. For example, on the Control network, the network name of the interface is the host name of the device. Some networks, such as the iSCSI network, do not allow interface names, and so naming controls are disabled.

   - Set to Default – Click to set the name of the interface to SiteConfig's default convention.

   - Use Interface Name/Aliases in Host Files – Click to enable the Aliases button.

     This checkbox is available only for networks that use host files.

   - Aliases – Click to assign multiple network names to the adapter.

     This button is available only for networks that use host files. Names entered as aliases are managed by SiteConfig's host file management features.

   - DNS Suffix – Enter a DNS suffix, if required by the selected network.

     For communication on some networks, a DNS suffix, such as *`mycorp.com`*, must be added to host names. The DNS Suffix field is available only for networks that can use DNS.

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

Removing a software role from a device

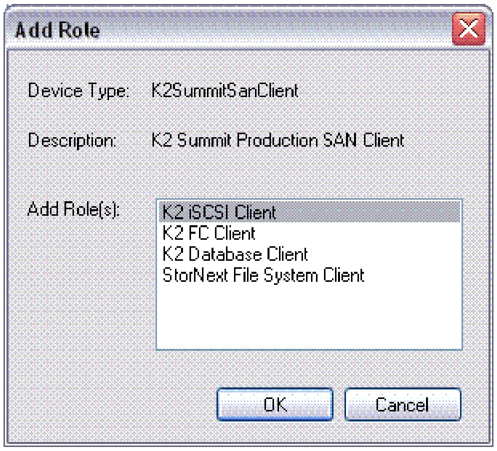
1. In the **Software Deployment | Devices** tree view, expand a device’s node to expose the roles currently assigned to the device.
2. Right-click the role you want to remove and select **Remove**.

   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.



Add Role

Device Type: K2SummitSanClient

Description: K2 Summit Production SAN Client

Add Role(s):
K2 iSCSI Client
K2 FC Client
K2 Database Client
StorNext File System Client

   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.

Discover and assign devices

NOTE: There might be a newer version of this document available. Check your product's release notes and the Grass Valley website at www.grassvalley.com/docs for references to an updated version that contains additional important information.

Use the topics in this section as appropriate for your system to establish communication between SiteConfig and your devices.

NOTE: Refer to the migration checklist for your system type to determine the appropriate topics and other system-specific information.

Related Links

Type I migration checklist on page 8

Type II migration checklist on page 9

Type III migration checklist on page 11

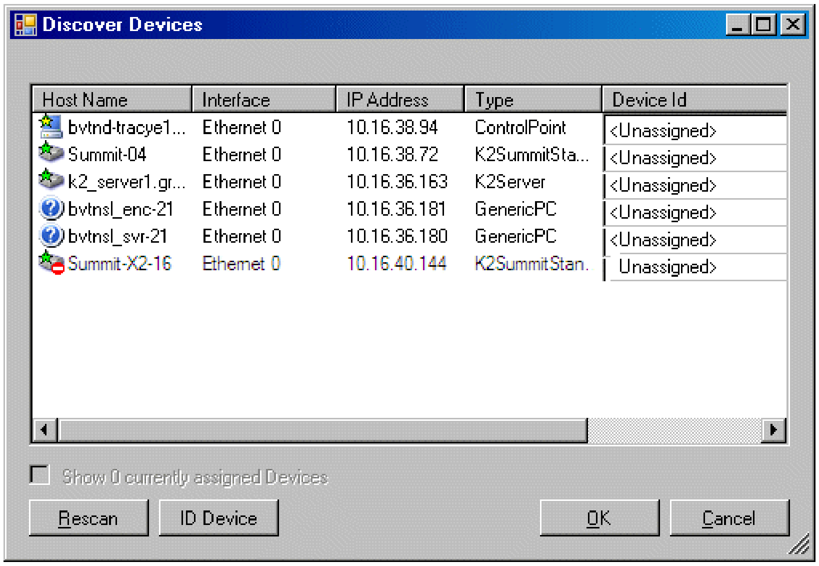
Discovering devices with SiteConfig

Prerequisites for this task are as follows:

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

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

   The Discover Devices dialog box opens.



Host Name	Interface	IP Address	Type	Device Id
bvtnd-tracye1...	Ethernet 0	10.16.38.94	ControlPoint	<Unassigned>
Summit-04	Ethernet 0	10.16.38.72	K2SummitSta...	<Unassigned>
k2_server1.gr...	Ethernet 0	10.16.36.163	K2Server	<Unassigned>
bvtnsl_enc-21	Ethernet 0	10.16.36.181	GenericPC	<Unassigned>
bvtnsl_svr-21	Ethernet 0	10.16.36.180	GenericPC	<Unassigned>
Summit-X2-16	Ethernet 0	10.16.40.144	K2Summit Stan.	Unassigned>

□ Show 0 currently assigned Devices

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.

Related Links

About installing SiteConfig on page 14

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.

Removing planned settings from a managed network interface

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 procedure to remove planned settings, if present, from network interfaces on each discovered and assigned device in the SiteConfig system description. This allows SiteConfig to use the current settings, as read from the actual device. Do this first for the control network interface, and then for each remaining network interface on the device.

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.

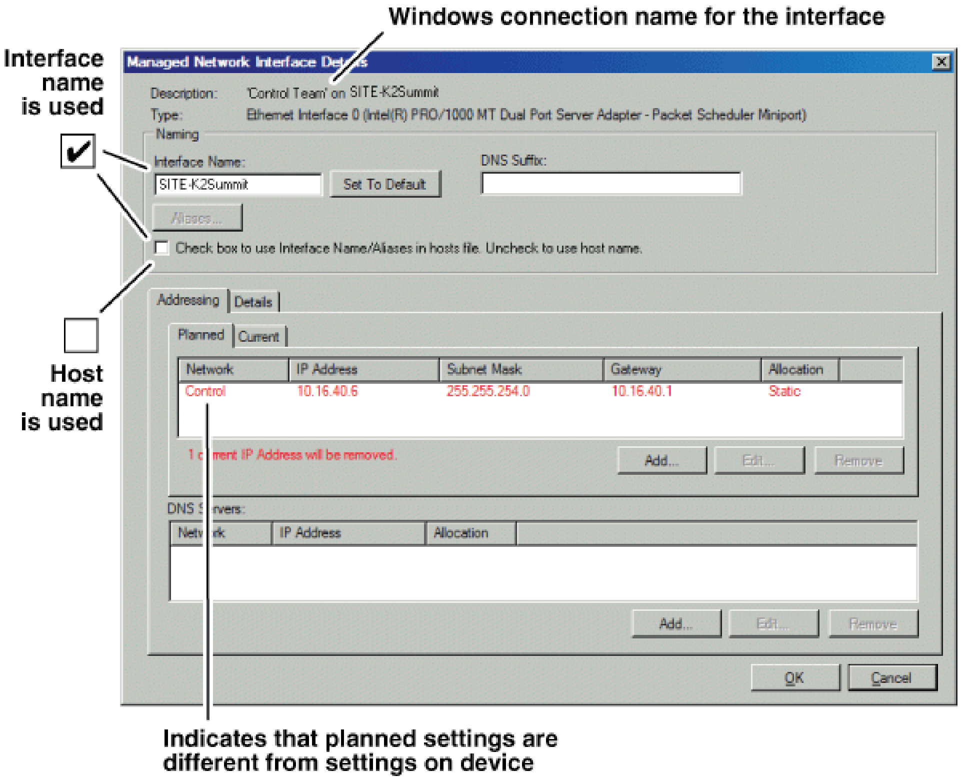
- Configure the control network interface first before configuring any of the other interfaces.
- After you have successfully configured the control network interface, return to this step to configure each remaining interface.

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

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

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

   The Managed Network Interface Details dialog box opens.



Description: 'Control Team' on SITE-K2Summit

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

Interface Name: SITE-K2Summit

DNS Suffix:

□ Check box to use Interface Name/Aliases in hosts file. Uncheck to use host name.

Network	IP Address	Subnet Mask	Gateway	Allocation
Control	10.16.40.6	255.255.254.0	10.16.40.1	Static

1 current IP Address will be removed.

DNS Servers:

Network	IP Address	Allocation

NOTE: Do not click OK if planned settings (red text) are displayed.

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.

- Identify iSCSI adapters by their "Type".

5. Configure **Use Interface/Aliases in Host Files** as follows:

   - If you want SiteConfig to use the current device hostname in the hosts file that it can create, leave the checkbox unchecked.
   - If you want SiteConfig to use the interface name in the hosts file that it can create, check the checkbox.

6. Evaluate IP settings as follows:

   - If only Current settings are displayed (the Planned tab is not displayed), it means the planned settings you configured on the placeholder device are identical to those on the actual device. If this is the case, no further configuration is required.
   - If both a Current tab and a Planned tab are displayed, it means the planned settings you configured on the placeholder device are not identical to those on the actual device. If this is the case, do not apply planned settings. Doing so overwrites IP settings on the actual device, which stops network communication. Instead, select the **Planned** tab and click **Remove**.

   NOTE: Do not click OK if planned settings (red text) are displayed.

7. When you are sure that only Current settings are displayed and that those are the current valid settings for the device, click **Apply**, then **OK** to save settings and close.
8. After configuring control network settings, do the following

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

   The Ping Host dialog box opens.

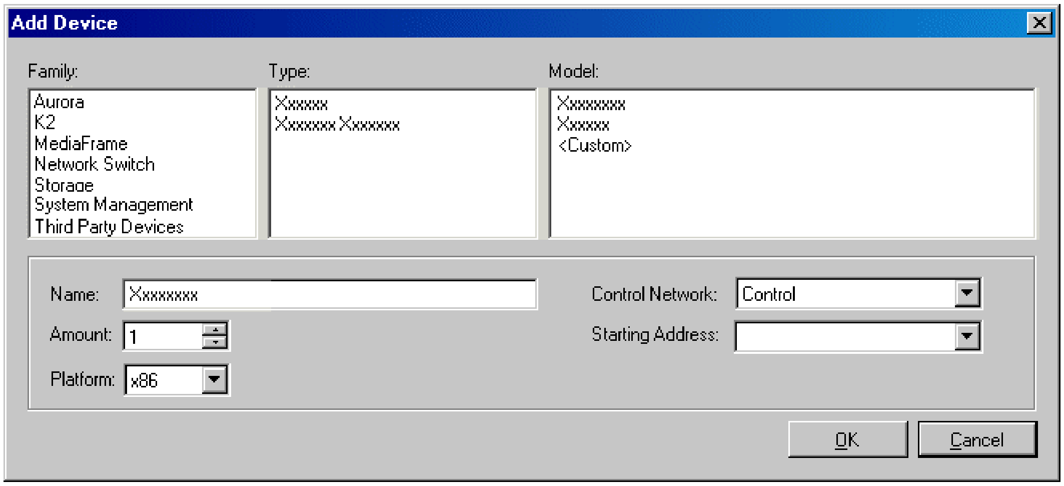
   If ping status reports success, the interface is communicating on the control network.

Adding a control point PC placeholder device to the system description

Prerequisites for this task are as follows:

- The system description contains a group.

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



Name: Xxxxxxxx

Amount: 1

Platform: x86

Control Network: Control

Starting Address:

The Add Device dialog box opens.

2. Configure settings for the device you are adding as follows:
   - Family – Select **System Management**.
   - Type – Select **ControlPoint PC**.
   - Model – Select **Control Point PC**.
   - Name - This is the device name, as displayed in the SiteConfig device tree view and device list view. You must configure this name to be the same as the host name on the actual control point PC.
   - Amount – Leave this setting at **1**. Do not attempt to configure multiple control point PC simultaneously.
   - Control Network – Select the control network.
   - Starting Address – Select the IP address that is the address currently configured on the actual control point PC.

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

Verify that IP settings for the placeholder device's control network interface are identical to those on the actual control point PC before using SiteConfig to discover the control point PC on the control network.

Assigning the control point PC

Prerequisites for this task are as follows:

- The SiteConfig control point PC has the "SiteConfig Network Configuration Connect Kit" installed.
- The system description contains a control point PC placeholder device.
- The placeholder's control network interface is configured with the control network IP address that is currently on the actual control point PC.

- The device name of the control point PC placeholder is same as the host name of the actual control point PC.

In this procedure you discover the physical control point PC and assign it to the placeholder control point PC in the system description.

1. Open SiteConfig on the control point PC.
2. Discover devices and identify the control point PC discovered device.
3. Assign the discovered device to the control point PC placeholder.
4. In the **Network Configuration | Devices** tree view, select the control point PC.
5. In the Interfaces list view, right-click the control network interface and select **Edit**.

   The Managed Network Interface Details dialog box opens.
6. Evaluate IP settings as follows:

   - If only Current settings are displayed (the Planned tab is not displayed), it means the planned settings you configured on the placeholder device are identical to those on the actual control point PC If this is the case, no further configuration is required.
   - If both a Current tab and a Planned tab are displayed, it means the planned settings you configured on the placeholder device are not identical to those on the actual control point PC. If this is the case, do not apply planned settings. Doing so overwrites IP settings on the actual control point PC, which stops network communication. Instead, select the **Planned** tab and click **Remove**.

   NOTE: Do not click OK if planned settings (red text) are displayed.
7. When you are sure that only Current settings are displayed and that those are the current valid settings for the control point PC, click **Apply**, then **OK** to save settings and close.

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**.

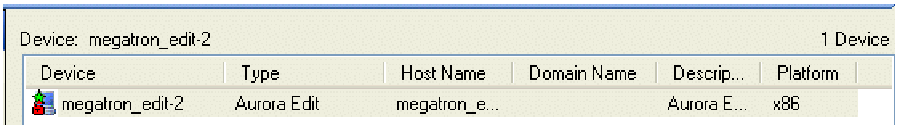
   The Ping Devices dialog box opens and lists the selected device or devices.

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

Verifying Discovery Agent installation

You should make sure that the Discovery Agent is installed on each device before proceeding.

1. In the Network Configuration tree view, select a node.
2. In the Devices list view, check for the green star overlay icon.



Device: megatron_edit-2 1 Device

Device	Type	Host Name	Domain Name	Descrip...	Platform
megatron_edit-2	Aurora Edit	megatron_e...		Aurora E...	x86

- If the green star overlay icon is present, the Discovery Agent is installed and no further steps are required to verify the Discovery Agent.
- If the green star overlay icon is not present, the Discovery Agent is not installed. Install the Discovery Agent on the device before proceeding.

Related Links

Installing SiteConfig support on page 30

About hosts files and SiteConfig

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

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

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

name resolution through the hosts file be configured accordingly in the SiteConfig system description.

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

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

Generating host tables for devices with SiteConfig

Prerequisites for this task are as follows:

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

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

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

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

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

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

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

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

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

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

Configure deployment groups and prepare for deployment

NOTE: There might be a newer version of this document available. Check your product's release notes and the Grass Valley website at www.grassvalley.com/docs for references to an updated version that contains additional important information.

Use the topics in this section as appropriate for your system to prepare devices for software deployment.

NOTE: Refer to the migration checklist for your system type to determine the appropriate topics and other system-specific information.

Related Links

Type I migration checklist on page 8

Type II migration checklist on page 9

Type III migration checklist on page 11

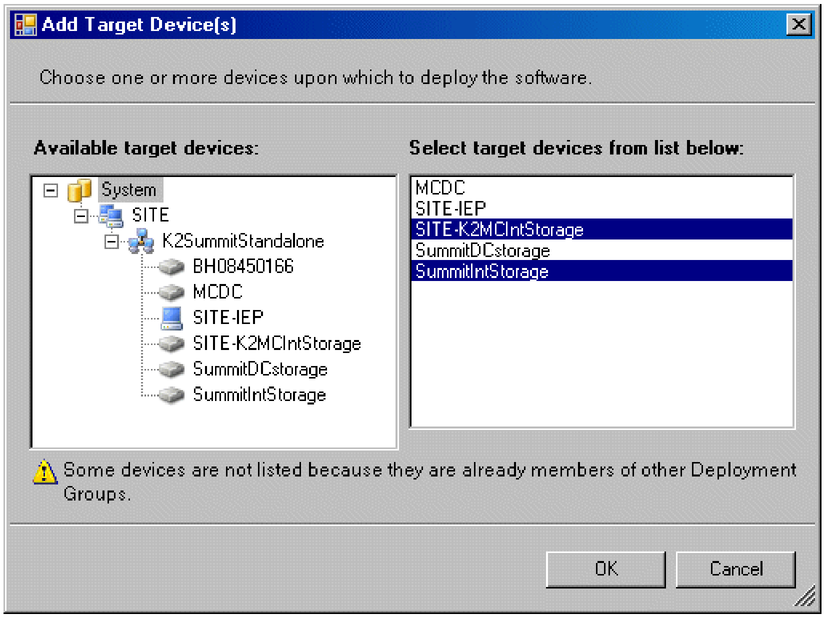
Configuring deployment groups

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.



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

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

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

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

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

Uninstall software

For some devices, software that you installed manually—before your first use of SiteConfig to deploy software to the device—can be problematic. If the software installation program doesn't communicate with SiteConfig or if the installation program embeds dependencies that SiteConfig does not expect, unexpected results can occur when you first deploy software using SiteConfig.

To avoid problems uninstall the following software from your devices:

- Aurora Suite
- NewsShare
- SmartBins
- AuroraFTP

- Conform Server

1. Identify the devices in your system on which the software is installed.
2. On each device, open the Windows operating system Add/Remove Programs control panel and locate the software to be uninstalled.
3. Uninstall the software using Add/Remove Programs.
4. Restart the device.

About deploying software

The tasks that you follow in this *SiteConfig Migration Instructions* document prepare your devices to support software deployment using SiteConfig, but do not provide specific instructions for actually deploying the software. Your product's release notes provide the software deployment instructions. This is because you must control the sequence of software deployment tasks and device restarts as you upgrade software. The exact steps can vary from software version to version, so only the product release notes for the version of software to which you are upgrading can provide you with verified correct steps.

Qualifications for managed devices

The following tables list the items on an actual device that need special attention. You should check these items to make sure that the actual device matches its corresponding placeholder device in SiteConfig. If the actual device is not connected/configured as specified, change the placeholder device. When the placeholder device and the actual device match, the device is qualified to be discovered and managed by SiteConfig.

Typically on an actual device, the rear panel Ethernet port numbering starts with the number one, while in SiteConfig network interface numbering is zero-based, as follows:

SiteConfig network interface	Rear panel connector on device
Ethernet 0	Port 1
Ethernet 1	Port 2
Ethernet 2	Port 3
Ethernet 3	Port 4

Keep this in mind as you compare network connections.

K2 Media Client stand-alone internal or direct-connect storage

Network interfaces	Qualifications
Control connection	No ports teamed. Rear panel GigE port 1 is the control network connection.
Software	**Qualifications**
MPIO	If direct-connect storage, verify that MPIO has been upgraded as specified in K2 Release Notes.

K2 Media Client shared (SAN) storage

Network interfaces	Qualifications
Control connection	Rear panel GigE ports 1 and 3 teamed. If basic SAN, port 1 is control network. If redundant SAN, port 1 is control A, port 3 is control B.
Software	**Qualifications**
MPIO	If redundant SAN, verify that MPIO has been upgraded as specified in K2 Release Notes.

K2 Summit Production Client stand-alone internal or direct-connect storage

Network interfaces	Qualifications
Control connection	Rear panel GigE ports 1 and 4 teamed. Port 1 is control network.

Software	Qualifications
MPIO	If direct-connect storage, verify that MPIO has been upgraded as specified in K2 Release Notes.

K2 Summit Production Client shared (SAN) storage

Network interfaces	Qualifications
Control connection	Rear panel GigE ports 1 and 4 teamed. If basic SAN, port 1 is control network. If redundant SAN, port 1 is control A, port 4 is control B.

Software	Qualifications
MPIO	If redundant SAN, verify that MPIO has been upgraded as specified in K2 Release Notes.

K2 Media Server

Network interfaces	Qualifications
Control connection	Rear panel GigE port 1 is control network.

Aurora Edit workstation with local or NAS storage

Network interfaces	Qualifications
Control connection	Rear panel GigE port 1 is control network.

Software	Qualifications
AuroraEdit	Must be installed. Software role **Aurora Edit Application** required.

Aurora Edit workstation with K2 SAN storage

Network interfaces	Qualifications
Control connection	Rear panel GigE port 1 is control network.

Software	Qualifications
AuroraEdit	Must be installed. Software role **Aurora Edit Application** required.

Software	Qualifications
GVG MLib, Generic iSCSI Client (non K2 only), and StorNext File System Client (non K2 only)	Must be installed. Software roles **GVG MLib**, **Generic iSCSI Client (non K2 only)**, and **StorNext File System Client (non K2 only)** are required. Dependencies.

Aurora Edit LD workstation

Network interfaces	Qualifications
Control connection	Rear panel GigE port 1 is control network.
Other	Configure for software deployment only, if on the corporate network and not available to SiteConfig for device discovery and network configuration. Do not install ProductFrame Discovery Agent and other SiteConfig support software on the Edit LD computer.
Software	**Qualifications**
AuroraEditLD	Must be installed. Software role **Aurora Edit LD (browse)** required.

Aurora Browse/MediaFrame Server

Network interfaces	Qualifications
Control connection	Rear panel GigE port 1 is control network.
Software	**Qualifications**
MediaFrame Core Components	Must be installed. Software role **MediaFrame Core Services** required.
Avalon Network Archive MDI	Might be installed. Add/remove software role **MediaFrame Avalon MDI** as appropriate.
DIVA Archive MDI	Might be installed. Add/remove software role **MediaFrame DIVA MDI** as appropriate.
FlashNet Archive MDI	Might be installed. Add/remove software role **MediaFrame FlashNet MDI** as appropriate.
M Series MDI	Might be installed. Add/remove software role **MediaFrame MSeries MDI** as appropriate.
NTFS MDI	If Aurora Edit LD connects, must be installed and software role **MediaFrame NTFS MDI** required.

Software	Qualifications
Profile MDI	Might be installed. Add/remove software role **MediaFrame Profile MDI** as appropriate. Must not be on same device with GV MLib.
Proxy MDI	Must be installed. Software role **MediaFrame Proxy MDI** required.
K2 MDI	Might be installed. Add/remove software role **MediaFrame K2 MDI** as appropriate.
(Generic) FTP MDI	Might be installed. Add/remove software role **MediaFrame FTP MDI** as appropriate.
NewsShare MDI	Might be installed. Add/remove software role **MediaFrame News MDI** as appropriate. Dependency on GVG MLib.
GVG MLib	If hosting the NewsShare MDI, must be installed and software role **GVG MLib** required.
Generic iSCSI client	If hosting the NewsShare MDI with V drive iSCSI mounted, must be installed and software role **Generic iSCSI Client (non K2 only)** required.
SNFS client	If hosting the NewsShare MDI with V drive iSCSI mounted, must be installed and software role **StorNext File System Client (non K2 only)** required.
Aurora Browse	Must be installed. Software role **Aurora Browse Application** required.

Aurora Browse/MediaFrame MDI Server

Network interfaces	Qualifications
Control connection	Rear panel GigE port 1 is control network.
Software	**Qualifications**
Avalon Network Archive MDI	Might be installed. Add/remove software role **MediaFrame Avalon MDI** as appropriate.
DIVA Archive MDI	Might be installed. Add/remove software role **MediaFrame DIVA MDI** as appropriate.
FlashNet Archive MDI	Might be installed. Add/remove software role **MediaFrame FlashNet MDI** as appropriate.

Software	**Qualifications**
M Series MDI	Might be installed. Add/remove software role **MediaFrame MSeries MDI** as appropriate.
Profile MDI	Might be installed. Add/remove software role **MediaFrame Profile MDI** as appropriate. Must not be on same device with GV MLib.
K2 MDI	Might be installed. Add/remove software role **MediaFrame K2 MDI** as appropriate.
(Generic) FTP MDI	Might be installed. Add/remove software role **MediaFrame FTP MDI** as appropriate.
NewsShare MDI	Might be installed. Add/remove software role **MediaFrame News MDI** as appropriate. Dependency on GV MLib.
GVG MLib	If hosting the NewsShare MDI, must be installed and software role **GVG MLib** required.
Generic iSCSI client	If hosting the NewsShare MDI with V drive iSCSI mounted, must be installed and software role **Generic iSCSI Client (non K2 only)** required.
SNFS client	If hosting the NewsShare MDI with V drive iSCSI mounted, must be installed and software role **StorNext File System Client (non K2 only)** required.

K2 Basecamp Express

Network interfaces	**Qualifications**
Control connection	Rear panel GigE port 1 is control network.
Software	**Qualifications**
MediaFrame Core Components	Must be installed. Software role **MediaFrame Core Services** required.
M Series MDI	Might be installed. Add/remove software role **MediaFrame MSeries MDI** as appropriate.
Profile MDI	Might be installed. Add/remove software role **MediaFrame Profile MDI** as appropriate. Must not be on same device with GV MLib.
Proxy MDI	Must be installed. Software role **MediaFrame Proxy MDI** required.

Software	Qualifications
K2 MDI	Might be installed. Add/remove software role **MediaFrame K2 MDI** as appropriate.
(Generic) FTP MDI	Might be installed. Add/remove software role **MediaFrame FTP MDI** as appropriate.
NewsShare MDI	Might be installed. Add/remove software role **MediaFrame News MDI** as appropriate. Dependency on GVG MLib.
GVG MLib	If hosting the NewsShare MDI, must be installed and software role **GVG MLib** required.
Generic iSCSI client	If hosting the NewsShare MDI with V drive iSCSI mounted, must be installed and software role **Generic iSCSI Client (non K2 only)** required.
SNFS client	If hosting the NewsShare MDI with V drive iSCSI mounted, must be installed and software role **StorNext File System Client (non K2 only)** required.
Aurora Browse	Must be installed. Software role **Aurora Browse Application** required.
Aurora Proxy Encoder	Must be installed. Software role **MediaFrame Proxy Encoder** required.

Aurora IEP HA and Aurora IEP CIFS

Network interfaces	Qualifications
Control connection	Rear panel GigE port 1 is control network.
Software	**Qualifications**
SmartBins	Might be installed. Add/remove software role **Smart Bins** as appropriate.
NewsShare	Must be installed. Software role **NewsShare** required.

Aurora IEP iSCSI

Network interfaces	Qualifications
Control connection	Rear panel GigE port 1 is control network.
Software	**Qualifications**
SmartBins	Might be installed. Add/remove software role **Smart Bins** as appropriate.

Software	Qualifications
NewsShare	Must be installed. Software role **NewsShare** required.
GVG MLib, Generic iSCSI Client (non K2 only), and StorNext File System Client (non K2 only)	Must be installed. Software roles **GVG MLib**, **Generic iSCSI Client (non K2 only)**, and **StorNext File System Client (non K2 only)** are required. Dependencies.

Aurora DSM HA and Aurora DSM Non-Redundant CIFS

Network interfaces	Qualifications
Control connection	Rear panel GigE port 1 is control network.
Software	**Qualifications**
SmartBins	Might be installed. Add/remove software role **Smart Bins** as appropriate.
NewsShare	Must be installed. Software role **NewsShare** required.

Aurora DSM Non-Redundant iSCSI

Network interfaces	Qualifications
Control connection	Rear panel GigE port 1 is control network.
Software	**Qualifications**
SmartBins	Might be installed. Add/remove software role **Smart Bins** as appropriate.
NewsShare	Must be installed. Software role **NewsShare** required.
GVG MLib, Generic iSCSI Client (non K2 only), and StorNext File System Client (non K2 only)	Must be installed. Software roles **GVG MLib**, **Generic iSCSI Client (non K2 only)**, and **StorNext File System Client (non K2 only)** are required. Dependencies.

Aurora Proxy Encoder

Network interfaces	Qualifications
Control connection	Rear panel GigE port 1 is control network.
Software	**Qualifications**
Aurora Proxy Encoder	Must be installed. Software role **MediaFrame Proxy Encoder** required.
AuroraFTP	Must be installed. Software role **Aurora FTP Server** required.

Software	Qualifications
GVG MLib, Generic iSCSI Client (non K2 only), and StorNext File System Client (non K2 only)	Must be installed. Software roles **GVG MLib**, **Generic iSCSI Client (non K2 only)**, and **StorNext File System Client (non K2 only)** are required. Dependencies.

Aurora SmartBin Proxy Encoder

Network interfaces	Qualifications
Control connection	Rear panel GigE port 1 is control network.

Software	Qualifications
Aurora Proxy Encoder	Must be installed. Software role **MediaFrame Proxy Encoder** required.
SmartBins	Must be installed. Software role **Smart Bins** required.
SmartBins Encoder	Must be installed. Software role **Smart Bin Encoder** required.
GVG MLib, Generic iSCSI Client (non K2 only), and StorNext File System Client (non K2 only)	Must be installed. Software roles **GVG MLib**, **Generic iSCSI Client (non K2 only)**, and **StorNext File System Client (non K2 only)** are required. Dependencies.

Aurora SmartBin Server CIFS

Network interfaces	Qualifications
Control connection	Rear panel GigE port 1 is control network.

Software	Qualifications
SmartBins	Must be installed. Software role **Smart Bins** required.

Aurora SmartBin Server iSCSI

Network interfaces	Qualifications
Control connection	Rear panel GigE port 1 is control network.

Software	Qualifications
SmartBins	Must be installed. Software role **Smart Bins** required.
GVG MLib, Generic iSCSI Client (non K2 only), and StorNext File System Client (non K2 only)	Must be installed. Software roles **GVG MLib**, **Generic iSCSI Client (non K2 only)**, and **StorNext File System Client (non K2 only)** are required. Dependencies.

AuroraFTP CIFS

Network interfaces	Qualifications
Control connection	Rear panel GigE port 1 is control network.
Software	**Qualifications**
AuroraFTP	Must be installed. Software role **Aurora FTP Server** required.

AuroraFTP iSCSI

Network interfaces	Qualifications
Control connection	Rear panel GigE port 1 is control network.
Software	**Qualifications**
AuroraFTP	Must be installed. Software role **Aurora FTP Server** required.
GVG MLib, Generic iSCSI Client (non K2 only), and StorNext File System Client (non K2 only)	Must be installed. Software roles **GVG MLib**, **Generic iSCSI Client (non K2 only)**, and **StorNext File System Client (non K2 only)** are required. Dependencies.

Aurora Conform Server CIFS

Network interfaces	Qualifications
Control connection	Rear panel GigE port 1 is control network.
Software	**Qualifications**
ConformServer	Must be installed. Software role **ConformServer** required.

Aurora Conform Server iSCSI

Network interfaces	Qualifications
Control connection	Rear panel GigE port 1 is control network.
Software	**Qualifications**
ConformServer	Must be installed. Software role **ConformServer** required.
GVG MLib, Generic iSCSI Client (non K2 only), and StorNext File System Client (non K2 only)	Must be installed. Software roles **GVG MLib**, **Generic iSCSI Client (non K2 only)**, and **StorNext File System Client (non K2 only)** are required. Dependencies.

Aurora Ingest Server

Network interfaces	Qualifications
Control connection	Rear panel GigE port 1 is control network.

Software	Qualifications
Server	Must be installed. Software role **Aurora Ingest Server** required.
Hot Standby Database Server	Might be installed. Add/remove software role **Aurora Playout Hot Standby SDB** as appropriate.

Aurora Ingest Client RMI

Network interfaces	Qualifications
Control connection	Rear panel GigE port 1 is control network.

Software	Qualifications
RMICore	Must be installed. Software role **Aurora Suite RMI Core Components** required. Dependency on Aurora Ingest Removable Media Ingest.
RMI	Must be installed. Software role **Aurora Ingest Removable Media Ingest** required. Dependency on Aurora Suite RMI Core Components.

Aurora Ingest Client Scheduler

Network interfaces	Qualifications
Control connection	Rear panel GigE port 1 is control network.

Software	Qualifications
Scheduler	Must be installed. Software role **Aurora Ingest Scheduler** required.

Aurora Ingest Client RS422 Control of VTRs

Network interfaces	Qualifications
Control connection	Rear panel GigE port 1 is control network.

Software	Qualifications
VTR Ingest	Must be installed. Software role **Aurora VTR Ingest** required.

Software	Qualifications
VTR Controller	Must be installed. Software role **Aurora VTR Controller** required.

Aurora Ingest Client VTR Ingest

Network interfaces	Qualifications
Control connection	Rear panel GigE port 1 is control network.
Software	**Qualifications**
VTR Ingest	Must be installed. Software role **Aurora VTR Ingest** required.

Aurora Playout Server

Network interfaces	Qualifications
Control connection	Rear panel GigE port 1 is control network.
Software	**Qualifications**
Hot Standby Database Server	Might be installed. Add/remove software role **Aurora Playout Hot Standby SDB** as appropriate.
Aurora Playout Application	Must be installed. Software role **Aurora Playout Application** required.
Housekeeper	Must be installed. Software role **Aurora Housekeeper** required.

Aurora Playout Client

Network interfaces	Qualifications
Control connection	Rear panel GigE port 1 is control network.
Software	**Qualifications**
Aurora Playout Application	Must be installed. Software role **Aurora Playout Application** required.

Aurora Playout Client Assignment List Plug-in

Network interfaces	Qualifications
Control connection	Rear panel GigE port 1 is control network.
Software	**Qualifications**
Aurora Playout Application	Must be installed. Software role **Aurora Playout Application** required.

Software	Qualifications
Assignment List Manager	Must be installed. Software role **Aurora Assignment List Plugin** required.

Upgrading Browse and MediaFrame devices to support 6.5.0 and higher

NOTE: There might be a newer version of this document available. Check your product's release notes and the Grass Valley website at www.grassvalley.com/docs for references to an updated version that contains additional important information.

If you have an Aurora Browse/MediaFrame system at a version lower than 6.5.0, you must upgrade the system to support version 6.5.0 and higher before using SiteConfig to deploy 6.5.0 or higher software.

Browse system upgrade considerations

Browse systems that were built with versions of Browse software lower than 6.5.0 have special considerations for upgrading to support versions 6.5.0 or higher, as follows:

- **Upgrade for all systems with less than 4GB RAM** — The MediaFrame server at version 6.5.0 or higher requires 4GB of RAM. The Dell documentation describes how to install memory for your Dell-based server (either 2850 or 2950).
- **Upgrade considerations for systems built with software version 2.7a or 3.1** — Most of the Browse system devices originally built with version 3.1 or lower are not qualified with version 6.5.0 or higher. If your system is currently running with version 2.7a or 3.1, or is using one or more devices originally used with version 2.7a or 3.1, you need to upgrade to version 6.0b and then upgrade to version 6.5.0 or higher.
- **Upgrade considerations for systems built with software version 6.0b** — If you have a Browse system originally built with version 6.0b, you will need to upgrade to version 6.5.0 or higher. If you have version 6.0b, depending on the design of your system, you might have some devices that are not supported by version 6.5.0 or higher and so can not be upgraded.

  The following devices can not be upgraded version 6.5.0 or higher:

  - Single-channel Encoder
  - Sequential Encoder
  - Image Support Server
  - Router Gateway

  If your system uses one or more devices that are not supported by version 6.50 or higher, your system must be reconfigured before it can be upgraded. For example, a system with Browse controlled ingest to Profile XP/Open SAN using Single-channel Encoders must be reconfigured to use Aurora Proxy Encoders instead of Single-channel Encoders, and a Profile XP standalone or else a K2 or M-Series system.

Systems built only with supported devices may by upgraded to version 6.5.0 or higher using the upgrade procedure in this section.

If NetBIOS has been disabled in the network properties, make sure it is enabled before performing an upgrade.

In addition, if you are upgrading from a Browse system that has version 6.0b, you will need to back up the database and config files, and save them to the NAS or some central server. MDIs no longer have transfer targets on archives.

You cannot use the old configuration file, except as a reference. The data is the same, but you need to go into the MediaFrame Config tool and specify the transfer target in the News, K2, M-Series or Profile MDI.

If the MediaFrame server does not have the Windows operating system Server 2003 SP2 and SQL database version 2005 SP2, you will need to backup the database and re-import it after you have upgraded the system.

The Aurora Browse Client now runs on a user's PC rather than through a website. User licenses are now handled through Active Directory. Administrators need to create licenses for Aurora Browse Client users. Roles need to be specified. For more information, refer to the *Aurora Browse Installation & Configuration Guide*.

- **Upgrade considerations for systems built with software version 6.3** — If you have a Browse system originally built with version 6.3, you will need to back up the database and config files, and save them to the NAS or some central server. MDI devices no longer have transfer targets on archives.

  You cannot use the old configuration file, except as a reference. The data is the same, but you need to go into the MediaFrame Config tool and specify the transfer target in the News or K2 MDI.

  The Aurora Browse Client now runs on a user's PC rather than through a website. User licenses are now handled through Active Directory. Administrators need to create licenses for Aurora Browse Client users. Roles need to be specified. For more information, refer to the *Aurora Browse Installation & Configuration Guide*.

  If the MediaFrame server does not have the Windows operating system Server 2003 SP2 and SQL database version 2005 SP2, you will need to backup the database and re-import it after you have upgraded the system.

Upgrading Aurora Browse systems

NOTE: These upgrade instructions assume that current Browse software is at version 6.0b or higher. If you have a lower version of software, you will need to upgrade to version 6.0b before upgrading using these instructions.

The following installation steps provide information specifically for upgrading an Aurora Browse system to version 6.5.0 or higher software. Read the information in these sections carefully before attempting the upgrade.

To upgrade software on the system, work through the following procedures sequentially.

Prepare for system upgrade

Do the following to gather information and put the system in the state required for the upgrade:

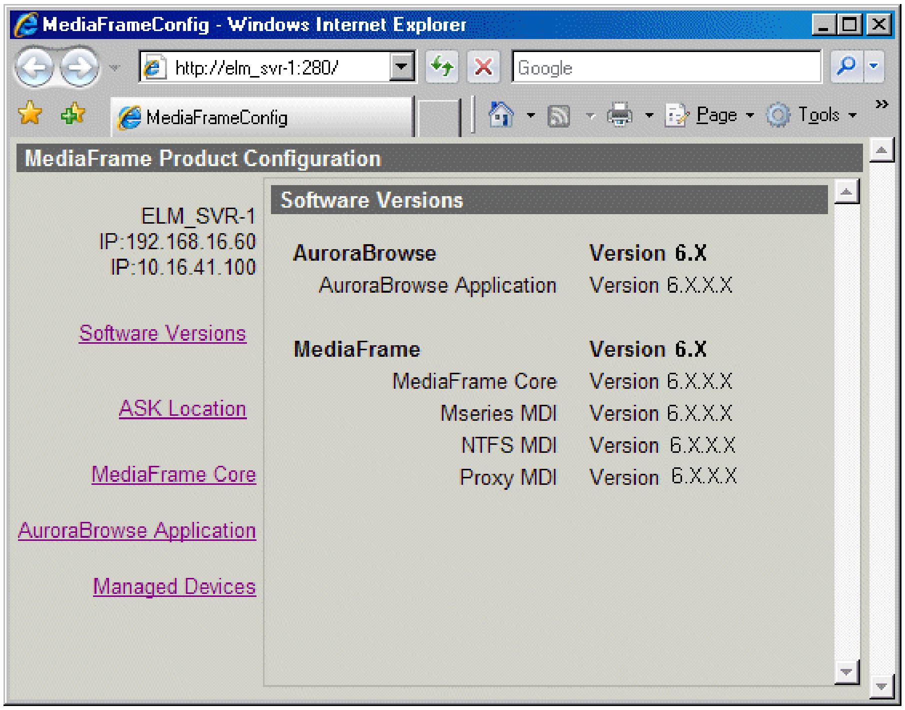
Identify components to upgrade

For your particular system, you must know what software components are in use, their current versions, on what devices those software components are installed, and their configuration.

NOTE: You must fully back up the SQL database and configuration files before upgrading the system.

If you have not yet clearly identified software components in this way, do so as follows:

1. View the MediaFrame server's configuration page at **Software Versions**.



MediaFrame Product Configuration

ELM_SVR-1
IP:192.168.16.60
IP:10.16.41.100

Software Versions

ASK Location

MediaFrame Core

AuroraBrowse Application

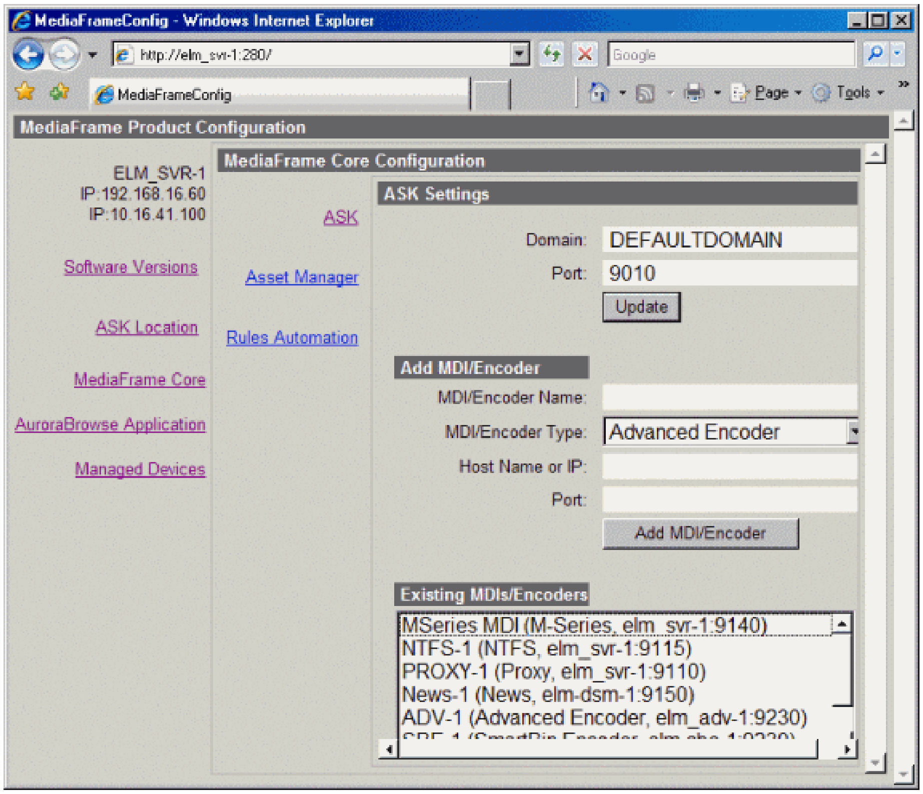
Managed Devices

Software Versions

AuroraBrowse	**Version 6.X**
AuroraBrowse Application	Version 6.X.X.X
MediaFrame	**Version 6.X**
MediaFrame Core	Version 6.X.X.X
Mseries MDI	Version 6.X.X.X
NTFS MDI	Version 6.X.X.X
Proxy MDI	Version 6.X.X.X

This page lists the components installed on the server and their versions.

2. View the server's configuration page at **MediaFrame Core | ASK**.



MediaFrame Product Configuration

ELM_SVR-1
IP:192.168.16.60
IP:10.16.41.100

MediaFrame Core Configuration

ASK Settings

Domain: DEFAULTDOMAIN
Port: 9010

Add MDI/Encoder

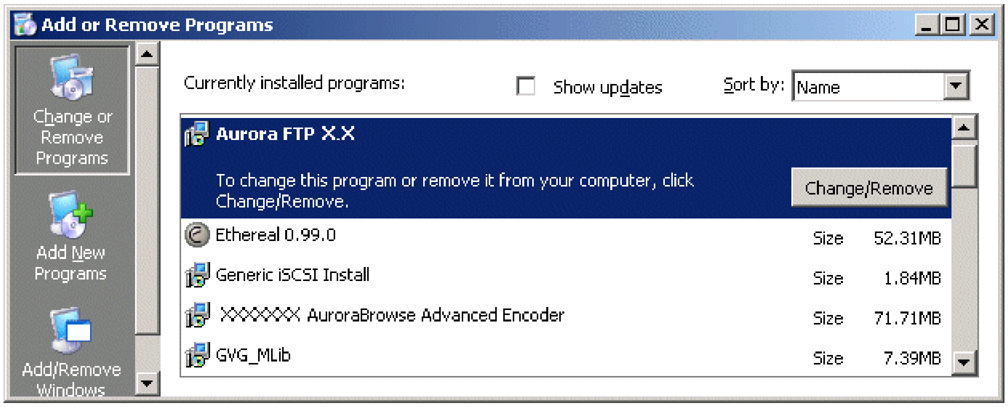
MDI/Encoder Name:
MDI/Encoder Type: Advanced Encoder
Host Name or IP:
Port:

Existing MDIs/Encoders

MSeries MDI (M-Series, elm_svr-1:9140)
NTFS-1 (NTFS, elm_svr-1:9115)
PROXY-1 (Proxy, elm_svr-1:9110)
News-1 (News, elm-dsm-1:9150)
ADV-1 (Advanced Encoder, elm_adv-1:9230)

Existing MDIs/Encoders lists software components, the devices on which they are installed, and the configuration of the devices they control.

3. At each device in the Browse system, view the Windows **Add/Remove Programs** control panel.



Aurora FTP X.X
To change this program or remove it from your computer, click Change/Remove.

Ethereal 0.99.0	Size	52.31MB
Generic iSCSI Install	Size	1.84MB
XXXXXX AuroraBrowse Advanced Encoder	Size	71.71MB
GVG_MLib	Size	7.39MB

Identify the software installed on the device and determine what components must be compatible. Depending on your system design, there can be software related to K2 products, MediaFrame/Browse products, and other Aurora products all installed on a single device.

4. When you have the complete list of all the components that need to be at compatible versions on your system, proceed with the next task.

Related Links

Identify software installed on devices on page 32

Verify versions of supporting systems

Depending on the system design, the MediaFrame/Browse system requires that components from other systems be upgraded.

- If your system does not have the following software versions, you will need get the software upgraded in this order:
  - a) Windows 2003
  - b) Windows 2003 Service pack 2
  - c) Microsoft Web Services Enhancements (WSE) 3.0
  - d) IIS
  - e) SQL 2005
  - f) SQL Service pack 2

  NOTE: After you have upgraded your system, you will need to import a fully backed up database. (Do not use an incremental backup.)
- K2 systems, M-Series, or standalone Profiles must be running a compatible version.
- K2 systems must have a version of K2 software that has the SetRTIO service running. (If not, SetRTIO.exe can be downloaded from the FTP site. Start the service after installing it.)
- Aurora Edit, Aurora Ingest, or Aurora Playout systems must be running a compatible version.
- The Aurora FTP version must be compatible.
- Encoders must have software components upgraded as necessary to access shared storage. For example, if accessing K2 shared storage, Encoders must have SNFS, Generic iSCSI, and GVG_MLib software upgraded to compatible versions and be able to successfully access the shared storage.
- Before upgrading an encoder, SmartBins (SmartBin encoder) or Aurora FTP (Aurora Proxy encoder) must be installed on the machine. Before upgrading an encoder on K2 BaseCamp Express, the Intel IPP files must be installed.

When you have verified that other systems are already running compatible versions or can be upgraded to compatible versions along with this Browse system upgrade, proceed with the next task.

Stop all system use

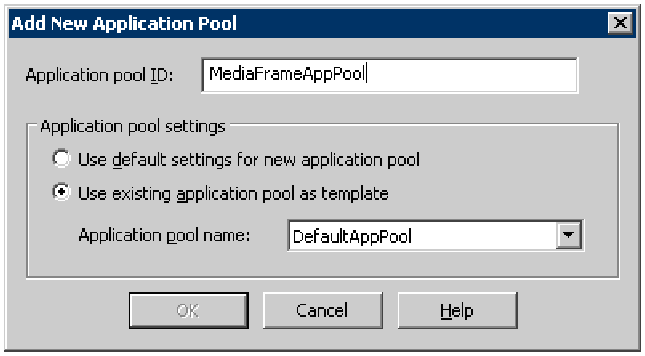
1. Stop all media access on the Browse system and on connected systems. This includes all ingest, playout, record, play, and transfer operations.
2. If it is not already on the system, install QuickTime.

Configure IIS Application Pool and Authentication

After you have installed the MediaFrame software, you need to configure the IIS application pool and authentication.

The MediaFrameWebAPI web site must run with administrative privileges because it makes event log entries. There are two ways to accomplish this; either configure the default application pool to run as an account with administrative privileges, or create a new application pool with administrative privileges and set the MediaFrameWebAPI web site to run with this application pool. The instructions provided are for the second method.

1. Open **Internet Information Services Manager**.
2. Navigate to the **Application Pools** tab.
3. Right-click on the **Application Pools** and select **New | Application Pool**.
4. Provide a name for the application pool, and check the radio button which reads **Use existing application pool as template**; ensure the application pool in the drop down box is **DefaultAppPool**.



Add New Application Pool

Application pool ID: MediaFrameAppPool

Application pool settings

○ Use default settings for new application pool

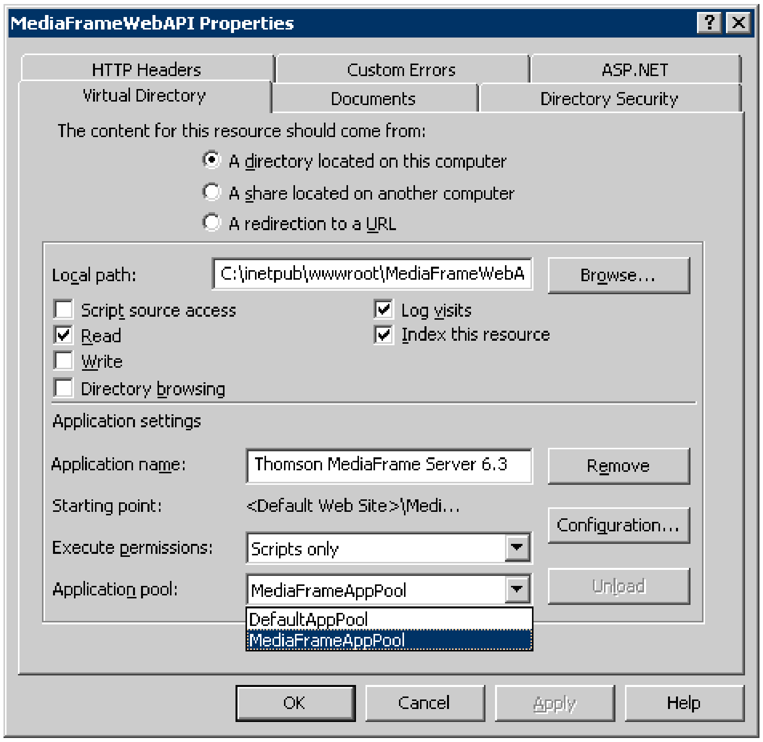
● Use existing application pool as template

Application pool name: DefaultAppPool

5. Right-click on the new application pool and select **Properties**.
6. Click on the **Identity** tab.
7. Select the **Configurable** radio button and enter credentials for an account with administrative privileges and click **OK**.

   NOTE: This account must also be a member of the IIS_WPG group. For more information on adding users to groups, see the Aurora Browse Installation and Configuration Guide.

8. Navigate to **Web Sites | Default Web Site | MediaFrameWebAPI**. Right-click on **MediaFrameWebAPI** and click **Properties**.
9. Select the **Virtual Directory** tab; use the **Application pool** drop-down list to select the new application pool you have created.



The content for this resource should come from:

● A directory located on this computer
○ A share located on another computer
○ A redirection to a URL

Local path: C:\inetpub\wwwroot\MediaFrameWebA

☐ Script source access
☑ Read
☐ Write
☐ Directory browsing
☑ Log visits
☑ Index this resource

Application settings

Application name: Thomson MediaFrame Server 6.3

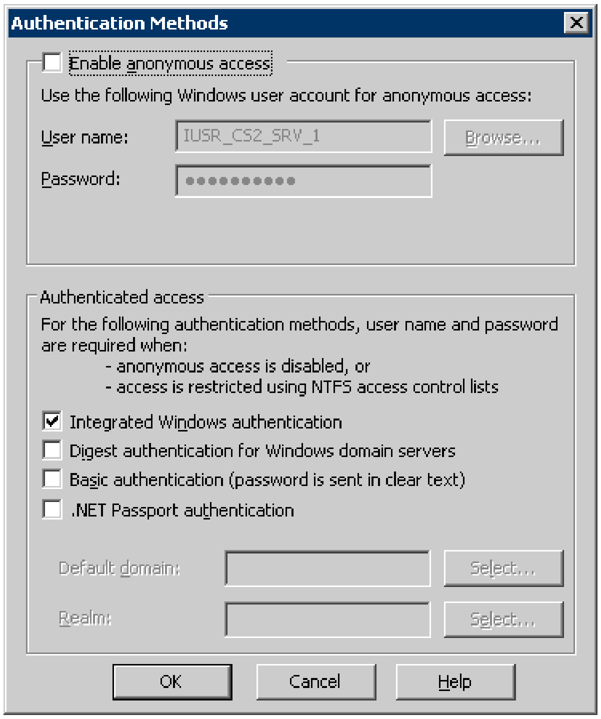
Starting point: <Default Web Site>\Medi...

Execute permissions: Scripts only

Application pool: MediaFrameAppPool

DefaultAppPool
MediaFrameAppPool

10. Select the **Directory Security** tab and click the **Edit** button under **Authentication and access control**.
11. Ensure the **Enable anonymous access** checkbox is unchecked.
12. Check the **Integrated Windows authentication** checkbox; the dialog box should look similar to the following illustration:



□ Enable anonymous access

Use the following Windows user account for anonymous access:

User name: IUSR_CS2_SRV_1

Password: ••••••••••

Authenticated access

For the following authentication methods, user name and password are required when:
- anonymous access is disabled, or
- access is restricted using NTFS access control lists

☑ Integrated Windows authentication

□ Digest authentication for Windows domain servers

□ Basic authentication (password is sent in clear text)

□ .NET Passport authentication

Default domain:

Realm:

13. Click **OK** and exit the Internet Information Services Manager.
14. Repeat steps 8 through 13 for the following:
    a) Settings manager
    b) License manager

Upgrade the MediaFrame server

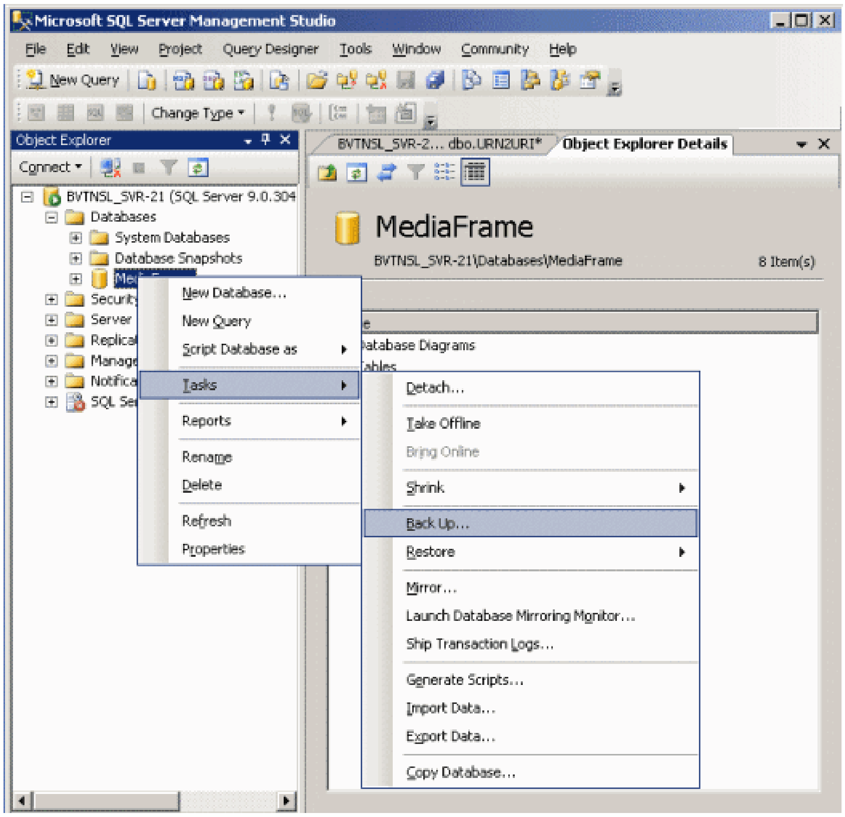
Do the following to upgrade software on the MediaFrame server:

Back up database and configuration

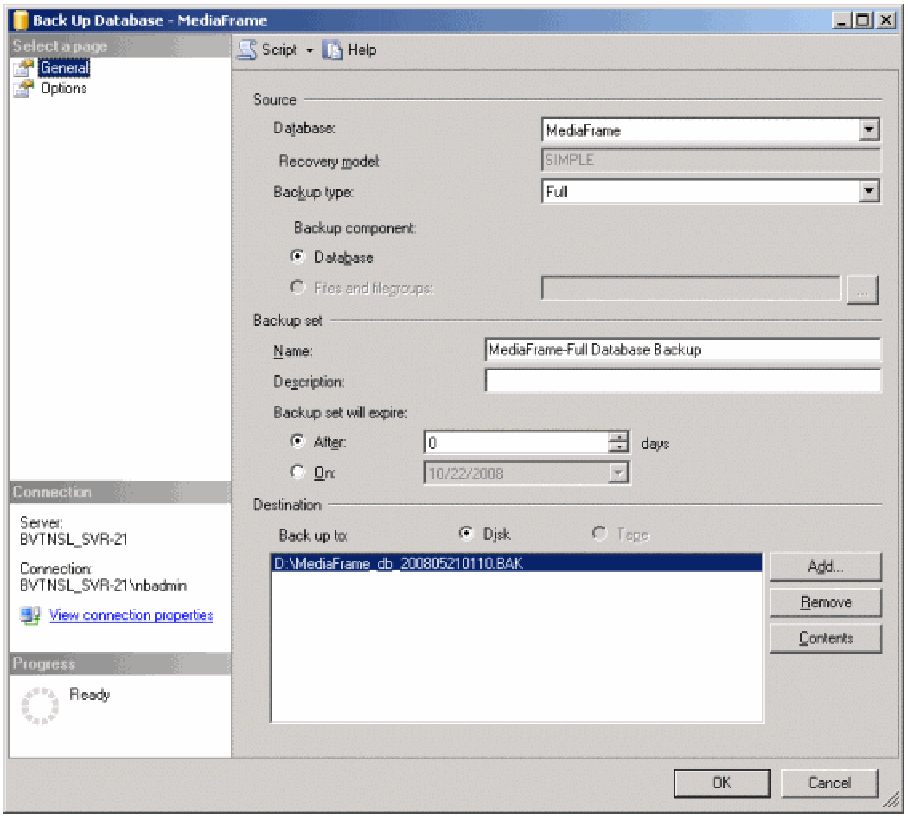
You should make sure that you have recent backups of the MediaFrame database and the Browse configuration file before upgrading software.

To back up the database and configuration files, perform the following steps:

1. Verify that the database maintenance plan on the MediaFrame server is running correctly. Refer to the *Aurora Browse Installation and Configuration Guide* for a complete description and procedures for the database maintenance plan.
2. Back up the database
    a) Open Microsoft SQL Server Management Studio.
    b) Right-click on MediaFrame database.
    c) Select **Tasks | Backup**.



d) Select **Full** as the Backup type; click **Add** and select a destination location.



Database: MediaFrame

Recovery model: SIMPLE

Backup type: Full

Backup component:

● Database

○ Files and filegroups:

Name: MediaFrame-Full Database Backup

Description:

Backup set will expire:

● After: 0 days

○ On: 10/22/2008

Back up to: ● Disk ○ Tape

D:\MediaFrame_db_200805210110.BAK

Server:
BVTNSL_SVR-21

Connection:
BVTNSL_SVR-21\nbadmin

e) Click **OK** .

3. Copy the `C:\Thomson` directory to a different location. This directory contains the configuration files for the locally installed software components.
4. After copying the C:\Thomson directory, delete the configuration files in the C:\Thomson\MediaFrame folder except for `MediaFrameCore.Config` file.

Install Web Services Enhancements 3.0

1. Double-click on the Microsoft WSE3.msi installation file.
2. On the Welcome page, click **Next** .
3. On the License Agreement page, select the **I accept the terms in the license** agreement radio button and click **Next** .
4. Select the **Administrator** radio button on the Setup Type page and click **Next** .
5. On the Ready to Install the Program page, click **Install** .

Install IIS version 6

Internet Information Services (IIS) is a component of the Windows 2003 Server software.

If IIS is already installed, skip ahead and install Microsoft .NET 2.0.

Install IIS, version 6.

a) Open **Add/Remove programs** .

b) Select **Add/Remove Windows Components** .

c) Open **Application Server | Internet Information Services (IIS)** .

d) Select **Common files** .

e) Open the **World Wide Web Service Internet Information Services Manager** .

f) Select **World Wide WebService** .

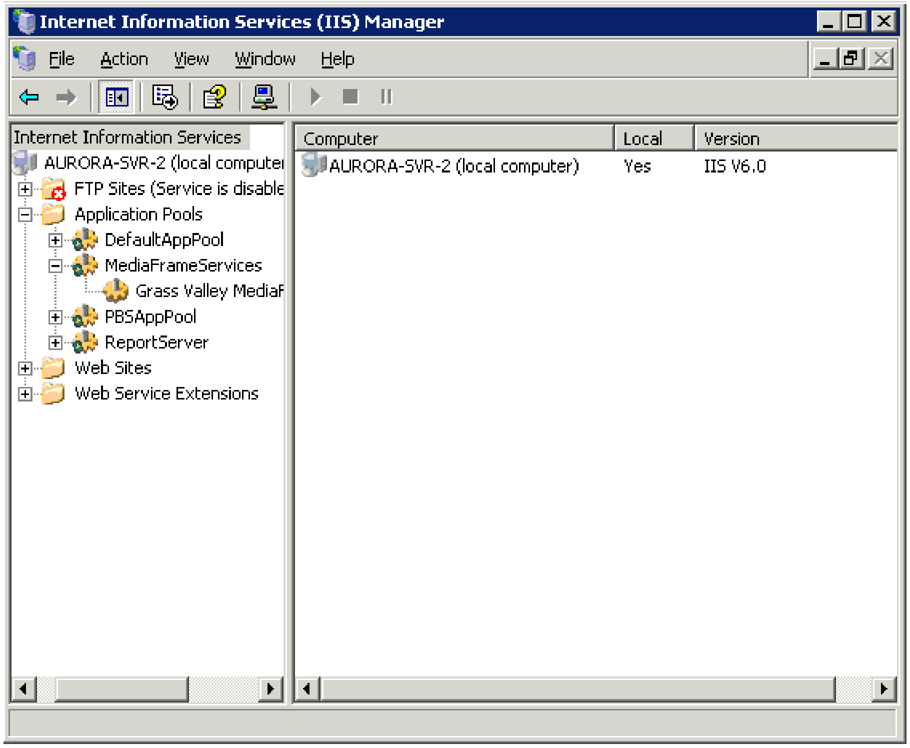
Install Microsoft .Net 2.0

NOTE: Install Microsoft .Net 2.0 after IIS has been installed. This avoids performing extra steps to make the ASP.Net 2.0 extensions register properly with IIS. Microsoft .Net needs to be installed before configuring IIS.

Install Microsoft .Net 2.0 SP2. (This is shipped with the MediaFrame servers and Encoders.)

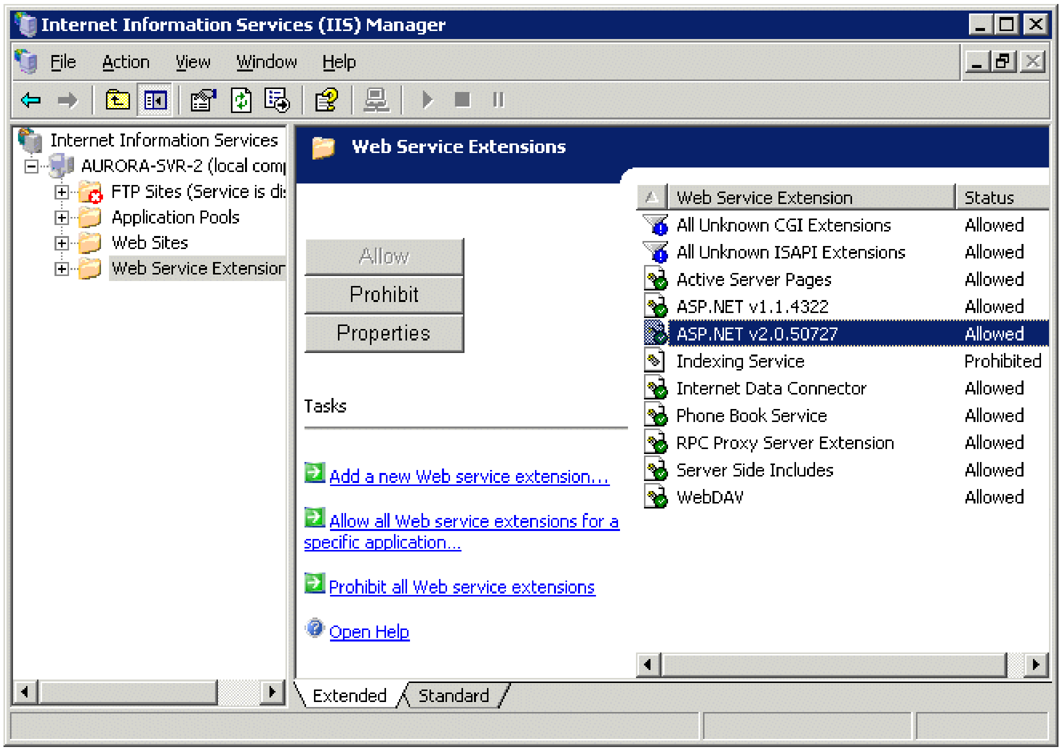
Configure IIS version 6

1. Open the **Windows Control Panel | Administrative Tools | Internet Information Services** (which may also be named Internet Services Manager).
2. Verify that the version running is IIS V6.0.



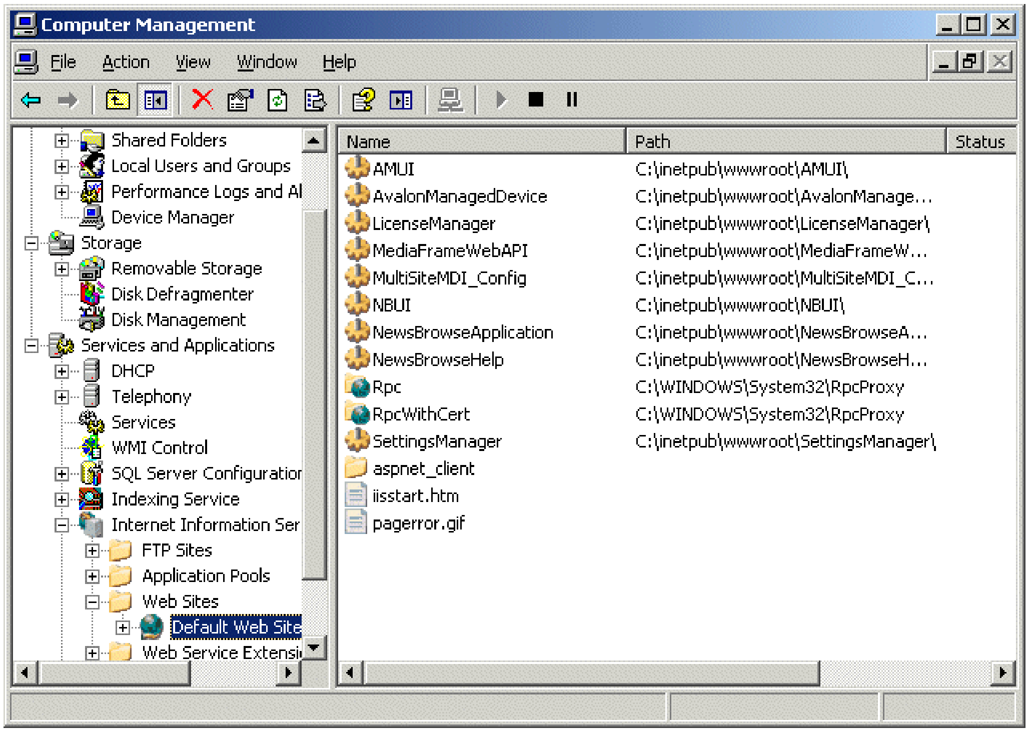
Computer	Local	Version
AURORA-SVR-2 (local computer)	Yes	IIS V6.0

3. Under Web Service Extensions, enable **ASP.NET** (by default, it is prohibited).


Internet Information Services (IIS) Manager
File Action View Window Help
Internet Information Services
AURORA-SVR-2 (local com
FTP Sites (Service is di
Application Pools
Web Sites
Web Service Extension
Web Service Extensions
Allow
Prohibit
Properties
Tasks
Add a new Web service extension...
Allow all Web service extensions for a specific application...
Prohibit all Web service extensions
Open Help
Extended
Standard

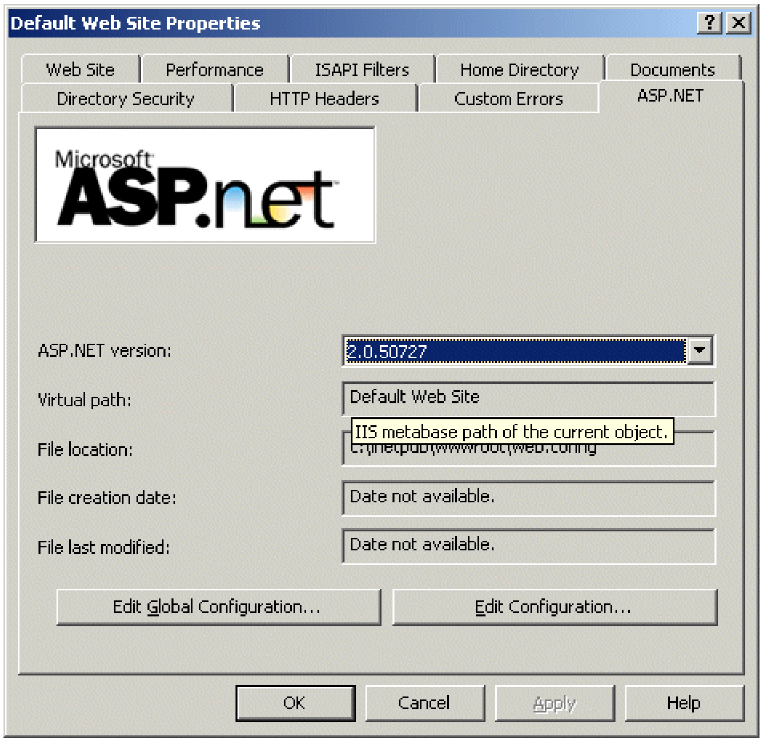
Web Service Extension	Status
All Unknown CGI Extensions	Allowed
All Unknown ISAPI Extensions	Allowed
Active Server Pages	Allowed
ASP.NET v1.1.4322	Allowed
ASP.NET v2.0.50727	Allowed
Indexing Service	Prohibited
Internet Data Connector	Allowed
Phone Book Service	Allowed
RPC Proxy Server Extension	Allowed
Server Side Includes	Allowed
WebDAV	Allowed

4. Under Web Sites, select the **Default Web Site** .



Name	Path	Status
AMUI	C:\inetpub\wwwroot\AMUI\	
AvalonManagedDevice	C:\inetpub\wwwroot\AvalonManage...	
LicenseManager	C:\inetpub\wwwroot\LicenseManager\	
MediaFrameWebAPI	C:\inetpub\wwwroot\MediaFrameW...	
MultiSiteMDI_Config	C:\inetpub\wwwroot\MultiSiteMDI_C...	
NBUI	C:\inetpub\wwwroot\NBUI\	
NewsBrowseApplication	C:\inetpub\wwwroot\NewsBrowseA...	
NewsBrowseHelp	C:\inetpub\wwwroot\NewsBrowseH...	
Rpc	C:\WINDOWS\System32\RpcProxy	
RpcWithCert	C:\WINDOWS\System32\RpcProxy	
SettingsManager	C:\inetpub\wwwroot\SettingsManager\	
aspnet_client		
iisstart.htm		
pagerror.gif		

5. Right click and select **Properties** . Set the ASP.net version as shown in the following illustration.



ASP.NET version: 2.0.50727

Virtual path: Default Web Site

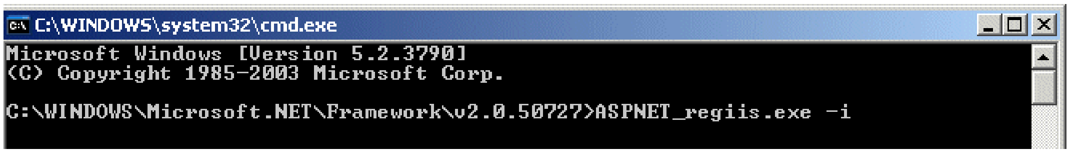
IIS metabase path of the current object.

File location: c:\inetpub\wwwroot\web.config

File creation date: Date not available.

File last modified: Date not available.

6. Click on the Web Site tab and verify that Enable Logging is unchecked. (Otherwise, IIS log files will accumulate and not get deleted.)
7. From the command line, navigate to the following path:
   C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727
8. Enter the following command:
   ASPNET_regiis.exe -i



```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727>ASPNET_regiis.exe -i
```

9. From the command line (or the Run command on the Windows Start menu) enter the following command:
   iisreset
10. Exit out of IIS.

Close all programs

On the MediaFrame server, do the following:

Close all applications, windows, and any other program. Check the Windows taskbar and make sure that it is empty.

Uninstall software

NOTE: At this step, do not delete the database from the system if prompted to do so.

On the MediaFrame server, do the following:

1. Open Windows **Add/Remove Programs** .
2. Locate the server software. Depending on your version of Browse software, it is named one of the following:
   - Thomson NewsBrowse Server
   - Thomson Aurora Browse Server
3. Select the server software and click **Remove** .
4. When prompted "You must restart...", click **Yes** . The MediaFrame server restarts.
5. When startup processes complete, log on to Windows and then proceed to the next task.

Install SQL Server 2005

NOTE: SQL Server 2005 must be running on the same server as the MediaFrame services.

Skip this step if:

Your system is currently running Microsoft SQL Server 2005.

- If you need to install SP2, skip title and install SQL 2005 Service Pack 2.
- If your system is currently running Microsoft SQL 2005 with SP2, skip title and upgrade the database.

If you are currently running SQL Server 2000 on this machine, you need to uninstall 2000 and back up the MediaFrame database before installing 2005.

Install SQL Server 2005 using a default instance and default administrator username and password. The following instructions guide you through the installation.

1. Under the Install heading, click on **Server components, Books Online and samples**.
2. On the licensing agreement page, check the box to agree with the terms and conditions and click **Next** .
3. In the Microsoft SQL Server 2005 installation window, click **Install**.
4. When the prerequisites complete installation, click the **Next** button.
5. On the Welcome to the Microsoft SQL Server Installation Wizard, click **Next**.
6. At the System Configuration Check window, ensure there are no errors and click **Next**.
7. On the Registration Information window, enter the product key in the fields provided, and click **Next** .

8. On the Components to Install window, check the **SQL Server Database Services and Workstation components, Books Online and development tools** checkboxes; then click **Next**.
9. On the Instance Name window, select the **Default instance** radio button, and press **Next** .
10. On the Service Account page, make sure the **Use a domain user account radio button** is checked, and input a set of credentials with administrative privileges in the appropriate boxes; then click Next.
11. On the Authentication Mode page, if it is needed for your system select the Mixed Mode radio button. For the administrator username, you can enter **SA** , and for the password, you can enter a strong password such as *P@55w0rd*. Click **Next**.
12. On the Collation Settings page click **Next**.
13. On the Error and Usage Report Settings page click **Next**.
14. On the Ready to Install page, click **Install**.

Install SQL 2005 Service Pack 2

Skip this step if:

- Your MediaFrame server has SQL 2005 with Service Pack 2.

Do this step if:

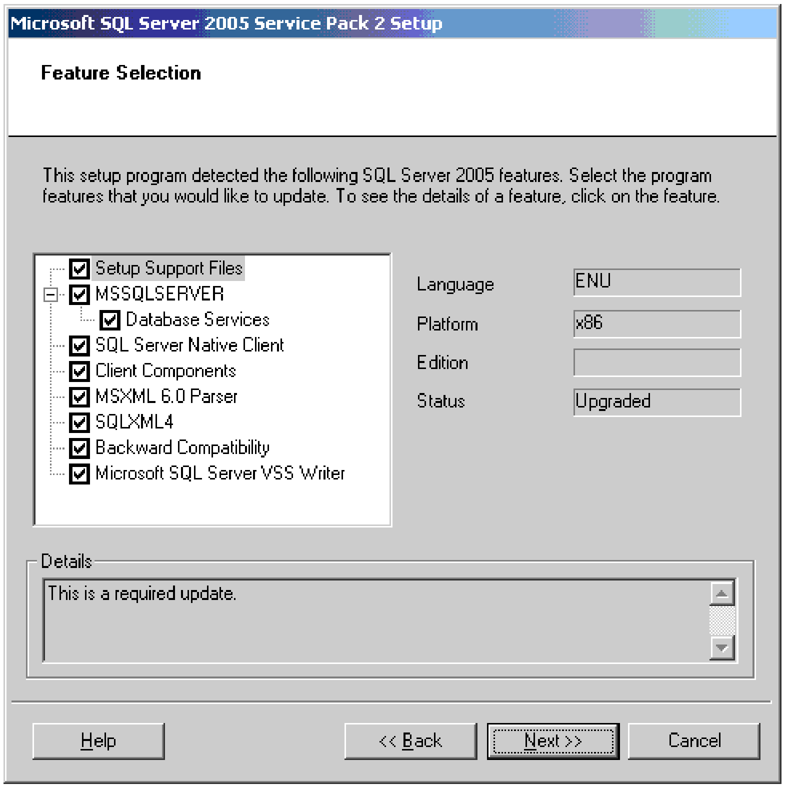
- Your MediaFrame server has SQL 2005.

To install SQL 2005 SP 2, do the following:

1. If you are currently running SQL 2000, uninstall this version.
2. Procure the SP 2 installation file. Find information at the following:

   http://support.microsoft.com/kb/913089

   Follow links to obtain SQL Server 2005 SP2 (not Express) and download SQLServer2005SP2-KB921896-x86-ENU.exe
3. On the MediaFrame server, close all applications, windows, and any other program. Check the Windows taskbar and make sure that it is empty.
4. Open the SP 2 installation file and work through the installation wizard.
5. If a Feature Selection window displays, check all features.



Microsoft SQL Server 2005 Service Pack 2 Setup

Feature Selection

This setup program detected the following SQL Server 2005 features. Select the program features that you would like to update. To see the details of a feature, click on the feature.

- ☑ Setup Support Files
- ☑ MSSQLSERVER
  - ☑ Database Services
- ☑ SQL Server Native Client
- ☑ Client Components
- ☑ MSXML 6.0 Parser
- ☑ SQLXML4
- ☑ Backward Compatibility
- ☑ Microsoft SQL Server VSS Writer

Language	ENU
Platform	x86
Edition	
Status	Upgraded

Details

This is a required update.

6. In the Authentication pane, select **Windows Authentication** .
7. Restart the MediaFrame server

Upgrade the database

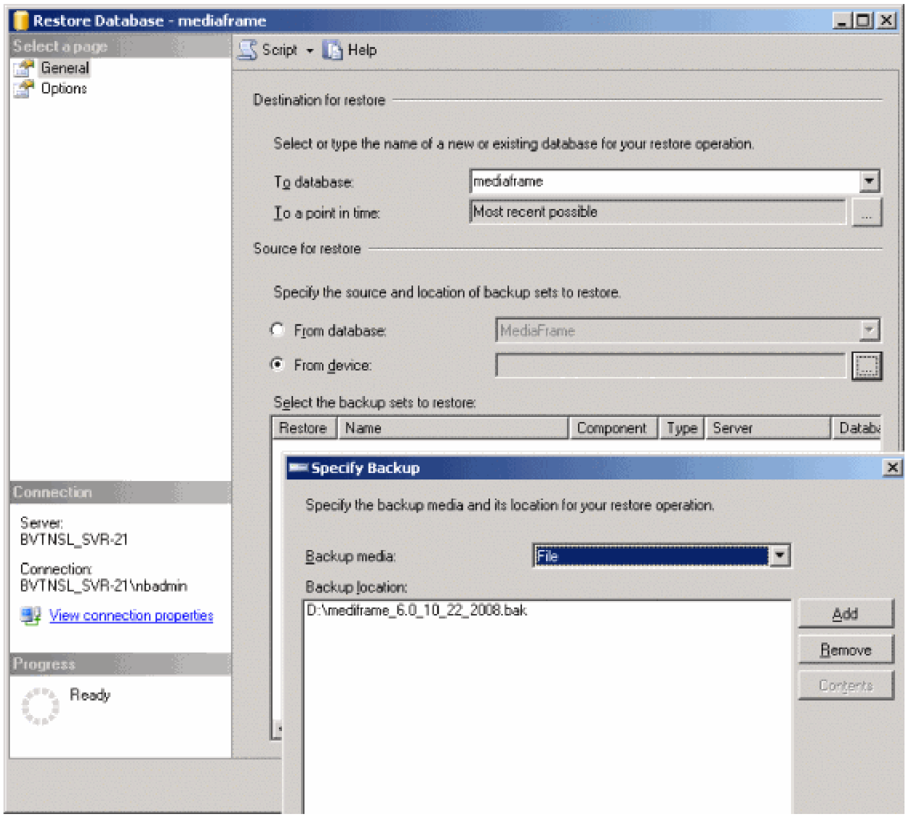
Make sure you have backed up the database and configuration before upgrading the database.

NOTE: Upgrade the database before installing the MediaFrame software on this system. If the MediaFrame software is already installed on this machine, uninstall before proceeding.

The upgradeDatabase utility automatically backs up and upgrades the database. A database install log provides information about the upgrade as it progresses.

1. Back up the database.
2. Perform the necessary upgrade(s):
   - If your system has Windows 2003, but you need to upgrade to SQL 2005, upgrade SQL now
   - If you need to upgrade to Windows 2003 and SQL 2005, upgrade Windows and SQL now
3. Restore the database.
   a) Open SQL Server Management Studio.
   b) Right-click on **System Database**.

c) Select **Restore Database**.



Select or type the name of a new or existing database for your restore operation.

To database: mediaframe

To a point in time: Most recent possible

Specify the source and location of backup sets to restore.

○ From database: MediaFrame

● From device:

Server: BVTNSL_SVR-21

Connection: BVTNSL_SVR-21\nbadmin

Specify the backup media and its location for your restore operation.

Backup media: File

Backup location: D:\mediframe_6.0_10_22_2008.bak

d) Click the **From Device** radio button.

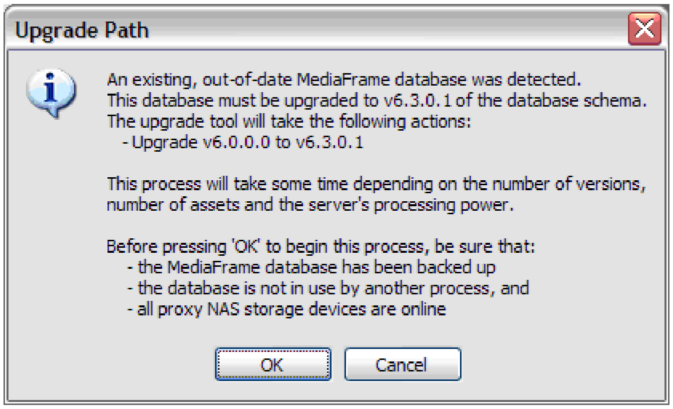
e) Use the **...** icon to specify the backup media and location.

f) Click **Add**, and then click **OK**.

Running the database utility upgrade

NOTE: You cannot run the upgradeDatabase.exe file from a remote location.

1. Run the upgradeDatabase.exe file. A dialog box displays.



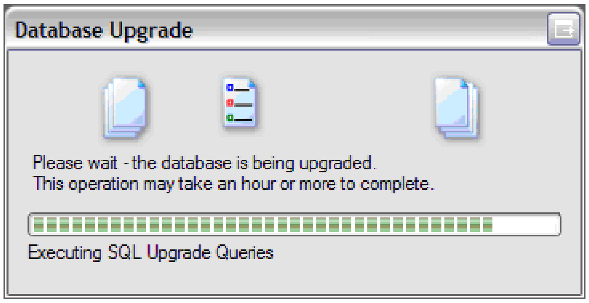
An existing, out-of-date MediaFrame database was detected.
This database must be upgraded to v6.3.0.1 of the database schema.
The upgrade tool will take the following actions:
- Upgrade v6.0.0.0 to v6.3.0.1

This process will take some time depending on the number of versions, number of assets and the server's processing power.

Before pressing 'OK' to begin this process, be sure that:
- the MediaFrame database has been backed up
- the database is not in use by another process, and
- all proxy NAS storage devices are online

NOTE: The dialog box describes version 6.3. However, the utility upgrades to version 6.5.x.

2. After verifying that the MediaFrame database has been backed up, click **OK**. The upgrade displays its progress.



Please wait - the database is being upgraded.
This operation may take an hour or more to complete.

Executing SQL Upgrade Queries

3. When the database upgrade has completed successfully, click **OK**.

License Sabretooth

Refer to release notes for more information about licensing.

1. On the encoder or MediaFrame server, install Sabretooth from the software CD:

   `C:\Software\Software installs\Sabretooth\Setup.exe`

2. Generate a unique ID of the device where you will install software, as follows:
   a) Click on the License Manager icon on the Windows Desktop.

      The SabreTooth License Manager opens.

   b) Choose **File | Generate Unique Id** the License Manager.
   c) Click **Copy to clipboard** to copy the generated ID, and **OK** to exit.

3. Prepare an email that includes the following information:

   - Customer Name
   - Customer Email
   - Sales Order Number
   - Unique ID of the device where you will install software.

4. In the email, also include the number of licenses, as follows:
   a) Encoder —1 license needed for each encoder (licensed locally) as well as licenses for the following:

      - For SmartBin Encoder—Aurora-XRE-SBIN-GXF and Aurora-XRE-SBIN-FTP
      - For Aurora Proxy Encoder—Aurora-XRE-SBIN-FTP

   b) MediaFrame Server — need 1 license for each role per user.

5. Send the email to AuroraLicenses@grassvalley.com.

The SabreTooth license number will be emailed to the email address you specified.

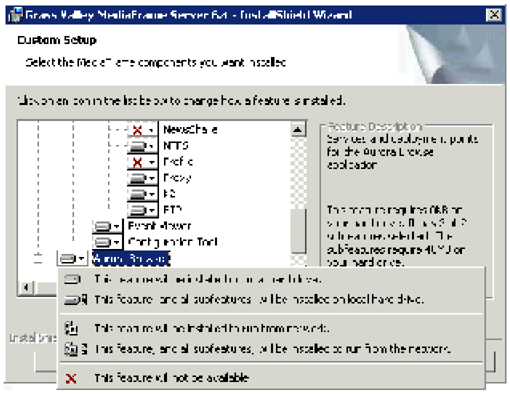
Your software license, Licenses_<SalesNumber>.txt, is provided as a text file. You will receive one text file per machine; it will have all the licenses requested for that MAC address

Install software

NOTE: If Sabretooth has not been installed, you will get an error message when you attempt to install the software.

On the MediaFrame server, do the following:

1. Insert the Aurora Browse software CD or otherwise gain access to the Aurora Browse software installation files.
2. Open `C:\Software\MediaFrame Server 6.5.x\Setup.exe.` The MediaFrame server installation wizard opens.
3. Click **Next** to progress through the wizard. When you arrive at the Custom Setup screen, select the components that were previously installed on the MediaFrame server, as follows:


Grass Valley MediaFrame Server 6.x - InstallShield Wizard
Custom Setup
Select the MediaFrame components you want installed
Click on an icon in the list below to change how a feature is installed.
NewsShare
NTFS
Profile
Proxy
K2
FTP
Event Viewer
Configuration Tool
Aurora Browse
Feature Description
Services and deployment points for the Aurora Browse application
This feature requires 0KB on your hard drive. It has 2 of 2 subfeatures selected. The subfeatures require 40MB on your hard drive.
This feature will be installed on local hard drive.
This feature, and all subfeatures, will be installed on local hard drive.
This feature will be installed to run from network.
This feature, and all subfeatures, will be installed to run from the network.
This feature will not be available.
Install to:

- If a component that you want to install displays a red X, click the component and select **This feature will be installed on local hard drive**.
- If a component that you do not want to install does not display a red X, click the component and select **This feature will not be available**.

4. When components to install are selected, click **OK** .
5. Specify the administrator name and password, click **Next** , and work through the remainder of the installation wizard accepting the default values.

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. This account is critical for most Aurora Browse proxy access. For more information, see "About the Administrator Account" in the Aurora Browse Installation and Configuration Guide.