StadiumVision

Cisco StadiumVision Director Software Installation and Upgrade Guide

Release 2.4

August 2, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Cisco StadiumVision Director Software Installation and Upgrade Guide

CISCO

StadiumVision

CONTENTS

Preface

This document describes the requirements and tasks to install and upgrade the software for Cisco StadiumVision Director Release 2.4.

The content is intended for Cisco StadiumVision system administrators and technical field engineers who are responsible for designing and deploying Cisco StadiumVision solutions. It is expected that readers of this document are familiar with basic IP networking and UNIX, have a general understanding of the sports and entertainment business, and understand the objectives and operations of live events.

Document Revision History

Table 1 lists the technical changes made to this document since it was first published.

Table 1 Document Revision History

Date	Change Summary
August 2, 2012	The following changes were made: • Revised the procedure for CIMC firmware upgrade to use the TFTP server method in the "Upgrading the CIMC and BIOS Firmware on a Cisco StadiumVision Director Platform 2 Server" module. • Revised the "Migrating the Cisco StadiumVision Director Server Environment to Platform 2 from the Cisco ADE 2140 Series Appliance" module to add a step for replacing the backup.cgi file, and to add a step for using the **sudo system-configure-network** command when changing the IP address on the server.
June 12, 2012	The following changes were made: • Revised the "Upgrading the DMP Firmware" task in the "Upgrading a Cisco StadiumVision Director Server From Release 2.3 to Release 2.4" module for information about installing the required firmware Version SE 2.2.2 Build 2744 for the Cisco DMP 4310G. • Added optional task for "Disabling the AIM Software" in the "Using the TUI Upgrade Utility to Update an Existing Release 2.4 Server" module. • Revised the tasks in the "Migrating the Cisco StadiumVision Director Server Environment to Platform 2 from the Cisco ADE 2140 Series Appliance" module.

Table 1 Document Revision History

Date	Change Summary
March 22, 2012	The following changes were made: • Added the "Migrating the Cisco StadiumVision Director Server Environment to Platform 2 from the Cisco ADE 2140 Series Appliance" module. • Documented "svd-server-aim" as additional AIM service to be removed when disabling AIM support in the "Upgrading a Cisco StadiumVision Director Server From Release 2.3 to Release 2.4" module.
February 16, 2012	An additional step was added to the "Appendix A: Post-Upgrade Checklist" to reconfigure the backup and restore environment after failback.
January 20, 2012	This document was updated for Cisco StadiumVision Director Release 2.4.0-147 Service Pack 1. The following changes were made: • Modified the "Using the TUI Upgrade Utility to Update an Existing Release 2.4 Server" module to include installation of service packs. • Added the "Upgrading the CIMC and BIOS Firmware on a Cisco StadiumVision Director Platform 2 Server" module. • Modified the "Appendix B: Port Reference" content to remove information about single server environment which is no longer applicable in Cisco StadiumVision Director Release 2.4. • Added step to "Verifying a New Installation" section of the "Installing Cisco StadiumVision Director Software From a DVD" to document changing the default admin password after the initial login.
November 4, 2011	This document was updated for Cisco StadiumVision Director Release 2.4.0-147. The following changes were made: • The following modules were added: – "Installing Cisco StadiumVision Director Software From a DVD" – "Using the TUI Upgrade Utility to Update an Existing Release 2.4 Server" – "Appendix A: Post-Upgrade Checklist" – "Appendix B: Port Reference" • Verification for the VLAN compliance check was added to the "Upgrading a Cisco StadiumVision Director Server From Release 2.3 to Release 2.4" module.
August 8, 2011	First release of this document for Cisco StadiumVision Director Release 2.4.0-118.

Document Organization

Chapter	Description
"Getting Started Installing or Upgrading Cisco StadiumVision Director"	Provides information that you should read before you perform an initial installation or upgrade of the Cisco StadiumVision Director Release 2.4 software.
"Upgrading a Cisco StadiumVision Director Server From Release 2.3 to Release 2.4"	Describes how to upgrade a Cisco StadiumVision Director server previously installed with Release 2.3-78 to Cisco StadiumVision Director Release 2.4.
"Installing Cisco StadiumVision Director Software From a DVD"	Describes how to install the Cisco StadiumVision Director Release 2.4 software from an installation DVD that ships with your newly-purchased server hardware. The process applies to a brand new server that has never been installed with any version of Cisco StadiumVision Director software.
"Using the TUI Upgrade Utility to Update an Existing Release 2.4 Server"	Describes how to upgrade an existing server already running Cisco StadiumVision Director Release 2.4 to a more recent 2.4 version, including installation of service packs. This procedure is also referred to generally as an ISO upgrade to refer to both the service pack and upgrade ISO process.
"Upgrading the CIMC and BIOS Firmware on a Cisco StadiumVision Director Platform 2 Server"	Describes how to verify and upgrade a Cisco StadiumVision Director Platform 2 server to the recommended version 1.4(2) (or later) of the UCS Cisco Integrated Management Interface (CIMC) and BIOS firmware.
"Appendix A: Post-Upgrade Checklist"	Provides a checklist that is useful after you upgrade your software on a Cisco StadiumVision Director server.
"Appendix B: Port Reference"	Identifies the ports used by Cisco StadiumVision Director.

Getting Started Installing or Upgrading Cisco StadiumVision Director

First Published: August 8, 2011
Revised: January 20, 2012

Read this module before you perform an initial installation or upgrade of the Cisco StadiumVision Director Release 2.4 software. It includes the following topics:

Before You Begin

Be sure that you understand and have met the following prerequisites before you begin to install or upgrade the Cisco StadiumVision Director software:

- Refer to the *Release Notes for Cisco StadiumVision Director Release 2.4* for the latest information about hardware and software requirements, changes, important notes, and caveats for your software release.
- Determine if you have compatible Cisco Digital Media Player (DMP) models and firmware versions installed.
- Determine if your Cisco StadiumVision Director server is being installed for the first time, if it is an existing server being upgraded from a software release before release 2.4, or if you are upgrading an existing server that already has a 2.4 version of software installed.

  The requirements and tasks for installation and upgrade vary by the initial state of your Cisco StadiumVision Director server.
- Determine if your server hardware is a 32-bit (Cisco 2140 ADE Server) or 64-bit system (SV-DIRECTOR-K9 or SV-PLATFORM2=) so that you can download the appropriate software packages from the Cisco.com download site.
- If you are installing a Platform 2 server, be sure that you are running a minimum of CIMC and BIOS firmware version 1.4(2) to avoid server power off problems. For more information, see the "Cisco StadiumVision Director Server Support" section and "CIMC and BIOS Firmware Installation for Cisco StadiumVision Director Platform 2 Servers" section in the *Release Notes for Cisco StadiumVision Director Release 2.4*.

- Be sure that you have a supported browser (Microsoft Internet Explorer Version 8 or Mozilla FireFox Version 4.x) and Adobe Flash Player (Version 10.3) installed for access to Cisco StadiumVision Director.
- Be sure that you have a secure FTP application to transfer your downloaded software files to the Cisco StadiumVision Director server.
- Verify that the Cisco StadiumVision Director server is connected to the network using the Ethernet port eth0 on the rear panel.

If you are installing Cisco StadiumVision Director for the first time on a new server:

- Verify that a monitor and keyboard are connected to the Cisco StadiumVision Director server.
- Be sure to have the network information required to configure the Ethernet connection on the Cisco StadiumVision Director server, such as:
  - IP address (IPv4 only) and mask
  - Default gateway address
  - DNS server address
  - Hostname

If you are upgrading an existing Cisco StadiumVision Director server:

- Be sure that an SNE TAC account and login credential have been obtained for each server by your Cisco representative, or otherwise contact the Cisco Technical Assistance Center (TAC). This account will be needed to authenticate and obtain an access token for the Cisco StadiumVision server and to create a user with privileges to perform the upgrade and other system tasks.
- Verify that a monitor and keyboard are connected to the Cisco StadiumVision Director server, or that you have a laptop computer connected to the same network as the Cisco StadiumVision Director server with an SSH client (such as PuTTY) to upgrade an existing server.
- Be sure that you do not have any duplicate luxury suite names when you perform an upgrade to Cisco StadiumVision Director Release 2.4 or the upgrade process will fail. Luxury suite names are not case-sensitive, so a duplicate can occur when the only difference in the character string is by case. Unnamed suites are not considered as duplicate.

Overview of the Installation and Upgrade Process

This document describes three different processes to install or upgrade your Cisco StadiumVision Director server for software Release 2.4, depending on your existing server environment:

- Upgrading a server from Release 2.3 to Release 2.4—Upgrade process involves a manual installation of a set of .rpm files from a .zip file available from Cisco.com. For detailed information, see the "Upgrading a Cisco StadiumVision Director Server From Release 2.3 to Release 2.4" module.
- Installing a server with Release 2.4 for the first time—Installation process involves installation from a DVD using a full ISO image file that runs an installation program with configuration prompts for your network information. For detailed information, see the "Installing Cisco StadiumVision Director Software From a DVD".
- Upgrading an existing Release 2.4 server—Upgrade process involves upload of an upgrade ISO image file available from Cisco.com that is used to do an automated upgrade using the Text Utility Interface (TUI) in the Cisco StadiumVision Director software. For detailed information, see the "Using the TUI Upgrade Utility to Update an Existing Release 2.4 Server".

Important Notes About Installation and Upgrade

Caution Duplicate luxury suite names will cause an upgrade to Cisco StadiumVision Director Release 2.4 to fail.

The following changes to the installation process and support have been implemented in Cisco StadiumVision Director Release 2.4:

- Installation integration with Cisco Unified Applications Environment (CUAE) is removed. CUAE is no longer required for Cisco IP Phone Luxury Suite control.
- The DMP firmware image is no longer bundled with the Cisco StadiumVision Director software. You must download the firmware image separately from the software download center site for the Cisco Digital Media Player model. For more information about supported firmware versions, see the *Release Notes for Cisco StadiumVision Director Release 2.4*.
- Addition of an upgrade utility available from the TUI main menu to simplify the upload of ISO image files to perform future upgrades of the Cisco StadiumVision Director Release 2.4 software without requiring shell access.

Note The TUI upgrade utility cannot be used to upgrade from Cisco StadiumVision Director Release 2.3 to Cisco StadiumVision Director Release 2.4.

Upgrading a Cisco StadiumVision Director Server From Release 2.3 to Release 2.4

First Published: August 8, 2011
Revised: June 12, 2012

This module describes how to upgrade a Cisco StadiumVision Director server previously installed with Release 2.3-78 to Cisco StadiumVision Director Release 2.4.

It includes the following topics:

Best Practices

Before you begin upgrading a Cisco StadiumVision Director server from Release 2.3-78 to Release 2.4 software, consider the following best practices:

- Choose an appropriate down time to perform the upgrade on the Cisco StadiumVision Director server when there is adequate time to complete and verify the upgrade before any scheduled events and to allow time to resolve any unexpected issues that might occur.
- Refer to the *Release Notes for Cisco StadiumVision Director Release 2.4* for the latest information about hardware and software requirements, changes, important notes, and caveats for your software release.
- Pay particular attention to the required hardware and software versions for other devices supporting your Cisco StadiumVision solution and be sure that you upgrade those devices as needed. For example, generally only certain firmware versions are supported for the DMP hardware, or a new firmware version is needed to provide additional functionality supported by the Cisco StadiumVision Director software.
- Perform a backup and restore of the primary and secondary servers:
  - Perform a backup of the currently active primary server.
  - Restore the backup data onto the standby secondary server.

- Promote the secondary server to active.
- Access the promoted secondary server to perform the upgrade.

For more information about performing a backup and restore on a Cisco StadiumVision Server running release 2.3, see the *Backing Up and Restoring StadiumVision Director, Release 2.3* guide.

Note In Cisco StadiumVision Director Release 2.4, a backup and restore automated configuration utility has been added to the Text Utility Interface (TUI), which runs based on the backup schedule that is configured from the Cisco StadiumVision Director dashboard.

For more information about promoting a secondary server to active, see the *Cisco StadiumVision Director Server Redundancy, Release 2.3* guide.

Prerequisites

Be sure that the following requirements are met before you upgrade your server:

- Be sure that you have compatible Cisco Digital Media Player (DMP) models and firmware versions installed.
  - The latest firmware recommended for Cisco StadiumVision Director Release 2.4 on the Cisco DMP 4310G is DMP-Vision Version SE 2.2.2 Build 2744.
  - In Cisco StadiumVision Director Release 2.4, once you create a device and specify that it's a 4310 DMP, the Dashboard retrieves the firmware version running on the DMP and updates the DMP device in the Cisco StadiumVision Director database.

  For more information about DMP hardware and software requirements, and a description of changes to DMP settings on the Management Dashboard, see the *Release Notes for Cisco StadiumVision Director Release 2.4*.

  For information about performing the firmware upgrade, see the "Upgrading the DMP Firmware" section on page 7.
- Be sure that your existing Cisco StadiumVision server software is at the minimum release level of Release 2.3 (78).

Note It is not a requirement to have the release 2.3 service packs installed to upgrade to release 2.4. The minimum upgrade requirement is to have installed the base image for Cisco StadiumVision Director Release 2.3 (78). If your system is not running Cisco StadiumVision Director Release 2.3 (78), perform the appropriate upgrade process(es) from your version to Release 2.3 (78) before you run an upgrade to Cisco StadiumVision Director Release 2.4. For more information about upgrades for release 2.3, see the *Cisco StadiumVision Director Installation and Upgrade Guide, Release 2.3*.

- Be sure that an SNE TAC account and login credential have been obtained for each server by your Cisco representative, or otherwise contact the Cisco Technical Assistance Center (TAC). This account will be needed to authenticate and obtain an access token for the Cisco StadiumVision server and to create a user with privileges to perform the upgrade and other system tasks.
- Be sure that you have a sudo root user account.

- Verify that a monitor and keyboard are connected to the Cisco StadiumVision Director server, or that you have a laptop computer connected to the same network as the Cisco StadiumVision Director server with an SSH client (such as PuTTY) to upgrade an existing server.
- Be sure that you have a secure FTP application to transfer your downloaded software files to the Cisco StadiumVision Director server.

Caution Be sure that you do not have any duplicate luxury suite names when you perform an upgrade to Cisco StadiumVision Director Release 2.4 or the upgrade process will fail. Luxury suite names are not case sensitive, so a duplicate can occur when the only difference in the character string is upper- or lowercase. For example, a luxury suite named "SuiteA" and a suite named "suitea" are duplicates. Unnamed suites are not considered duplicates.

- Process any outstanding Proof of Play reports. For more information, see the *Cisco StadiumVision Director Proof of Play* module.

Upgrade Tasks

To upgrade your Cisco StadiumVision Director server from Release 2.3 to 2.4, complete the following tasks:

- Upgrading the DMP Firmware, page 7 (as required)
- Running Proof of Play Reports, page 9 (as required)
- Downloading the Upgrade Files, page 10 (required)
- Logging in to the Server Using an Authenticated Account, page 10 (required)
- Upgrading the Software From Release 2.3 to Release 2.4, page 11 (required)
- Disabling the AIM Software, page 13 (as required)
- Verifying the Upgrade, page 13 (required)

Upgrading the DMP Firmware

This section provides a summary of the steps to perform to upgrade your DMP firmware. For more detailed information, see the related documentation.

Note The Cisco DMP 4310G only supports DMP-Vision Version SE 2.2.2 Build 2744 in Cisco StadiumVision Director Release 2.4.

To upgrade your DMP firmware, complete the following steps on each DMP as needed:

Step 1 To download the DMP-Vision Version SE 2.2.2 Build 2744 (filename DMP4310_b2744.fwimg), go to the Software Download Center for Cisco StadiumVision Director, click **2.4.0 SP1** and select the SE 2.2.2 build 2744 link, and click **Download**:

http://www.cisco.com/cisco/software/release.html?mdfid=283489263&flowid=31962&softwareid=283866237&release=3.0.0&relind=AVAILABLE&rellifecycle=&reltype=latest

Step 2 Click **2.4.0 SP1** and select the SE 2.2.2 build 2744 link, and click **Download**.

Step 3 Go to the **Management Dashboard > DMP and TV Controls > DMP Install > Firmware Upgrade**.

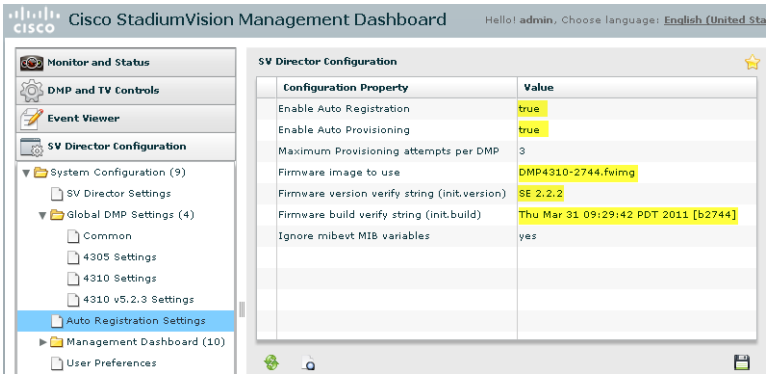
Step 4 Upload the firmware file to the server and upgrade the firmware for the DMP 4310Gs.

For more information, see the "Upgrading the Firmware Image" section of the *Cisco StadiumVision Management Dashboard Device Configuration Commands* guide.

Step 5 Go to the **Management Dashboard > SV Director Configuration > System Configuration > Auto Registration Settings**. Confirm or set the following values as shown in Figure 1 as required:

- Enable_Auto_Registration = true
- Enable_Auto_Provisioning = true
- Firmware image to use = DMP4310- 2744.fwimg (select from the dropdown box)
- Firmware version verify string (init.version) = SE 2.2.2
- Firmware build verify string (init.build) = Thu Mar 31 09:29:42 PDT 2011 [b2744]

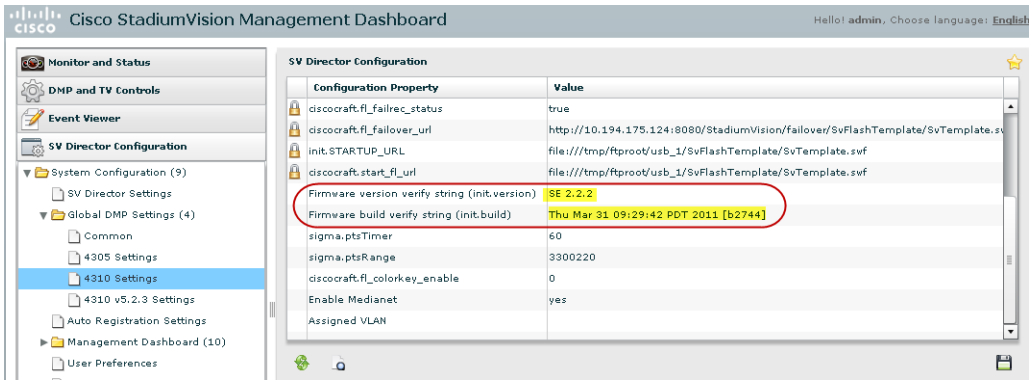
Figure 1 Auto Registration Settings in Management Dashboard



Step 6 Go to the **Management Dashboard > SV Director Configuration > Global DMP Settings** and confirm the firmware version and build date in the 4310 v5.2.3 and 4310 Settings as shown in Figure 2.

Note Be sure that both the 4310 Settings section *and* the 4310 v5.2.3 Settings have the same values for init.build and init.version.

Figure 2 Global DMP Settings in Management Dashboard



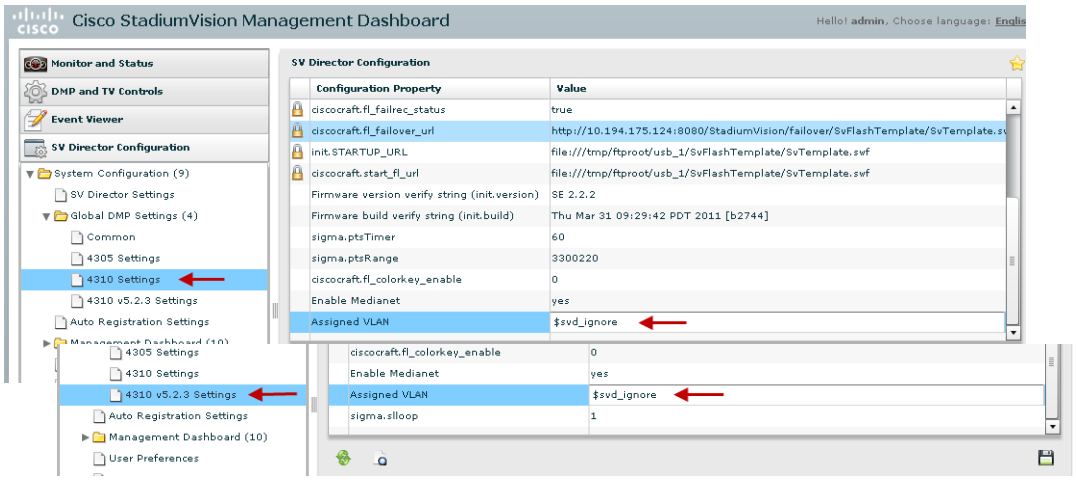
Step 7 Configure the Assigned VLAN property under both the 4310 v5.2.3 and 4310 Settings as $svd_ignore or the actual VLAN number on which your DMPs reside. Do *not* leave blank.

Note DMP auto-registration support requires that the VLAN value is correctly set or "**$svd_ignore**" is used.

Figure 3 shows how to configure the Assigned VLAN property under the 4310 Settings for DMPs that are *not located on the same VLAN* using the "$svd_ignore" string.

Note You will also need to set this Assigned VLAN property value for the 4310 v5.2.3 Settings.

Figure 3 Assigned VLAN Property Configuration for DMPs



Step 8 Go to **Management Dashboard > DMP and TV Controls > DMP Install > Firmware Upgrade**.

Select **All Devices** and click the Play (**>**) icon to run the command.

Step 9 Go to **Management Dashboard > DMP and TV Controls > Global Settings > Global DMP Settings**.

Select **All Devices** and click the Play (**>**) icon to run the command.

Step 10 Go to **Management Dashboard > DMP and TV Controls > Monitoring > Get Status**.

Select **All Devices** and click the Play (**>**) icon to run the command.

Running Proof of Play Reports

Before you perform the upgrade from Release 2.3 to 2.4, be sure that you have processed any outstanding Proof of Play reports. If you do not run these reports before the upgrade, the data will be lost.

For more information, see the *Cisco StadiumVision Proof of Play* module.

Downloading the Upgrade Files

Be sure to download the upgrade files to a location, such as a laptop computer, where you can access them for installation onto the Cisco StadiumVision Director server.

To download the upgrade files, complete the following steps:

Step 1 Go to the Cisco StadiumVision Director software download site at:

http://www.cisco.com/cisco/software/release.html?mdfid=283489263&flowid=25361&softwareid=283866237&release=2.4.0-147&relind=AVAILABLE&rellifecycle=&reltype=latest

Note This site page is also available from the Cisco StadiumVision Director product support page by clicking **Download Software** > **Cisco StadiumVision Director**.

Step 2 Select the upgrade .zip file and companion MD5 checksum file for your server model (32- or 64-bit) and download them. Table 1 shows the filename conventions used for each server model.

Table 1 Filename Conventions by Server Hardware

Hardware Product ID	Filename Convention[1]
64-bit Model SV-DIRECTOR-K9 or SV-PLATFORM2=	• SV-DIRECTOR-UPGRADE-2.4.0-*nnn*.x86_64.zip • SV-DIRECTOR-UPGRADE-2.4.0-*nnn*.x86_64.zip.md5sum
32-bit Model CADE-2140-K9	• SV-DIRECTOR-UPGRADE-2.4.0-*nnn*.i386.zip • SV-DIRECTOR-UPGRADE-2.4.0-*nnn*.i386.zip.md5sum

1. "*nnn*" represents the build number of the image in the file.

You can download the files using one of the following methods:

- Download both files at one time—Select each file and click **Add to Cart**. Then at the top of the download page, click the "Download Cart (2 items)" link.
- Download each file independently—Click the **Download Now** button in the file selection box for each file.

Logging in to the Server Using an Authenticated Account

Prerequisites

Be sure that the following requirements are met before you can login to the server with an authenticated account:

- A Cisco representative has obtained a secure token from an internal credential server for the Cisco StadiumVision Director server to be upgraded.

Caution If the token is being copied and saved for later use in authenticating with the Cisco StadiumVision Server, it must be saved exactly as given in plain text. Anything that adds invisible characters, such as RTF format, will make the copied token invalid for use.

- The authentication token must be pasted into Cisco StadiumVision Director when the Cisco representative logs in with the SNE TAC account and establishes a new temporary user account with privileges to perform system tasks. The account will be usable for 90 days.

Caution After you change the password for creation of the authenticated temporary user account, you *must* log out and log back in to the server to perform an upgrade. If you do not, the upgrade might fail.

To log in to the Cisco StadiumVision Director server, complete the following steps:

Step 1 Use a directly connected console, or use an SSH client from a laptop computer that is connected to the Cisco StadiumVision Server network to run a secure login to the Cisco StadiumVision Director server using the IP address for your server.

Step 2 Enter the userid and password for the authenticated system account set up by your Cisco representative.

Upgrading the Software From Release 2.3 to Release 2.4

To upgrade the software on the Cisco StadiumVision Director server, complete the following steps:

Step 1 Create a folder in your Linux home directory on the Cisco StadiumVision Director server where the .rpm installation files can be placed. The following example shows how to create a directory called “sv-2.4”:

```
mkdir ~/sv-2.4
```

Step 2 Go to the directory on your laptop where the .zip and .md5sum files were downloaded and copy the files to your Linux home directory. For example:

```
scp SV-DIRECTOR-2.4.0-118.i386.zip <your_username>@<ip address of SV Director
server>:sv-2.4/

scp SV-DIRECTOR-2.4.0-118.i386.zip.md5sum <your_username>@<ip address of SV Director
server>:sv-2.4/
```

Step 3 Verify the integrity of the zip file by calculating the MD5 checksum on the .zip file, and compare that value to the value in the MD5 checksum file. The following example shows how to run this for a 32-bit version of a .zip file and its corresponding checksum file:

```
md5sum SV-DIRECTOR-2.4.0-118.i386.zip
cat SV-DIRECTOR-2.4.0-118.i386.zip.md5sum
```

The output values should match, If they do not, you need to retry downloading the software files.

Step 4 Unzip the .zip file that contains the .rpm installation files using the following command, where <filename> is the name of your .zip file:

```
unzip <filename>.zip
```

Step 5 Stop the Cisco StadiumVision Director applicaton processes that are currently running:

Note If this is the first time that you are running a sudo command, you will be prompted for the sudo root user password.

```
sudo service svd stop
sudo service liferay stop
```

Step 6 Display the running Java instances using the following command and confirm that none are running:

```
ps -ef | grep java
```

Step 7 Run the upgrade on the .rpm files using Linux rpm and yum commands as shown in the following example:

```
cd sv-2.4/
sudo rpm -Uvh --noscripts svd-server-hornetq*.rpm
sudo chkconfig --del svd-hornetq
sudo rpm -Uvh --noscripts liferay-portal*.rpm
sudo yum --nogpgcheck install *.rpm
```

Step 8 After you receive the Transaction Summary and confirmation of the total download size, enter "y" when the prompt "Is this ok [y/N]" appears as shown in the following example:

```
Transaction Summary
================================================================================
Install      5 Package(s)
Update      17 Package(s)
Remove       0 Package(s)

Total download size: 395 M
Is this ok [y/N]: y
```

Step 9 Ignore the following error:

```
Feb 9, 2011 10:11:12 AM org.apache.catalina.startup.Catalina stopServer
SEVERE: Catalina.stop:
java.net.ConnectException: Connection refused
        at java.net.PlainSocketImpl.socketConnect(Native Method)
        at java.net.PlainSocketImpl.doConnect(Unknown Source)
        at java.net.PlainSocketImpl.connectToAddress(Unknown Source)
        at java.net.PlainSocketImpl.connect(Unknown Source)
        at java.net.SocksSocketImpl.connect(Unknown Source)
        at java.net.Socket.connect(Unknown Source)
        at java.net.Socket.connect(Unknown Source)
        at java.net.Socket.<init>(Unknown Source)
        at java.net.Socket.<init>(Unknown Source)
        at org.apache.catalina.startup.Catalina.stopServer(Catalina.java:421)
        at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
        at sun.reflect.NativeMethodAccessorImpl.invoke(Unknown Source)
        at sun.reflect.DelegatingMethodAccessorImpl.invoke(Unknown Source)
        at java.lang.reflect.Method.invoke(Unknown Source)
        at org.apache.catalina.startup.Bootstrap.stopServer(Bootstrap.java:337)
        at org.apache.catalina.startup.Bootstrap.main(Bootstrap.java:415)
```

Note There is no need to reboot the Cisco StadiumVision Director server. The server is restarted automatically after the upgrade is complete.

Disabling the AIM Software

If your site does not use the Ad Insertion Manager (AIM), you can remove it from the Cisco StadiumVision Director software and main menu by commenting out the menu code lines.

To disable the AIM software if it is not being used, complete the following steps:

Step 1 Exit the Cisco StadiumVision Director home page using the following command:

```
sudo vi /opt/sv/servers/config/webapps/StadiumVision/index.jsp
```

Step 2 Comment out lines 141-146. Go to line 141 in the vi editor and insert comment mark <!-- at the beginning of the line 141, and --> at the end as shown in the following example:

```
vi:141
<!--<tr align="left">
    <td><img src="cues_images/new-window_link_icon.gif" alt=""></td>
    <td class="textStyle">
    <a href="/AIMWeb/home.html" target="_blank">Ad Insertion Manager</a>
    </td>
</tr>-->
```

Step 3 Write the change using the following command:

```
:w
```

Step 4 Exit the vi editor using the following command:

```
:x
```

Step 5 Remove the AIM package using the following command:

```
sudo rpm -e sv-aim svd-server-aim --nodeps
```

Note When Cisco StadiumVision Director starts, it will show a process named svd-aim running. You can ignore this process as it does not run the AIM web application.

Verifying the Upgrade

To verify the upgrade, complete the following tasks:

- Clearing the Browser Cache, page 14 (required)
- Importing the Security Certificate, page 14 (required)
- Logging Into Cisco StadiumVision Director, page 15 (required)
- Verifying the Control Panel and Other Menus, page 17 (required)
- Checking for Duplicate MAC Address Entries, page 18 (required)
- Configuring the DMP 4310 Assigned VLAN Property for VLAN Compliance Check, page 19 (required)
- Verifying DMPs, Groups, and Zones in the Management Dashboard, page 20 (required)
- Verifying the Multicast Configuration, page 21 (required)

- Setting Up the Quest Venue Manager to Send Updates to Cisco StadiumVision Director Server, page 21 (required if using Quest for commerce integration)

Clearing the Browser Cache

After you perform the Cisco StadiumVision Director Release 2.4 software upgrade, you must clear the browser cache to be sure that you are viewing the latest version of Cisco StadiumVision Director.

To clear the browser cache in Mozilla FireFox, complete the following steps:

Step 1 From the menu bar, go to **Tools > Clear Recent History**.

The Clear Recent History dialog box appears.

Step 2 In the "Time range to clear:" box, select **Everything**.

Step 3 Open the Details drop-down list and select the **Cache** checkbox if it does not have a checkmark.

Step 4 Click **Clear Now**.

To clear the browser cache in Microsoft Internet Explorer, complete the following steps:

Step 1 From the menu bar, go to **Tools > Delete Browsing History**.

Step 2 Select the Temporary Internet Files checkbox if it does not have a checkmark.

Step 3 Click **Delete**.

Importing the Security Certificate

When you access a Cisco StadiumVision Director 2.4 server for the first time using Microsoft Internet Explorer or Mozilla Firefox, a security certificate warning will appear. Some Cisco StadiumVision Director functionality requires that the certificate is imported.

Importing the Security Certificate for Microsoft IE

To import the security certificate in Microsoft Internet Explorer, complete the following steps:

Step 1 When you see the warning page with the title "There is a problem with this website's security certificate," click the "**Continue to this website...**" option.

Step 2 Next to the URL bar on the top of the browser window, click **Certificate Error** and then click the "**View certificates**" link.

Step 3 In the Certificate dialog box, click **Install Certificate...** .

Step 4 In the Certificate Import Wizard dialog box, click **Next>**.

Step 5 In the next step of the wizard, select "Place all certificates in the following store" radio button and then click **Browse...** .

Step 6 In the Select Certificate Store dialog box, select the "Trusted Root Certification Authorities" store and click **Ok**.

Step 7 Click **Next>** in the Certificate Import Wizard dialog.

Step 8 Click **Finish**.

Step 9 In the Security Warning dialog box, click **Yes**.

Confirm that a dialog stating "The import was successful." appears.

Step 10 Close all Microsoft IE windows.

You should now be able to access the Cisco StadiumVision Director server using Microsoft IE without any security certificate warnings.

Adding a Security Exception for Mozilla Firefox

To add the security exception for Mozilla Firefox, complete the following steps:

Step 1 When you see the warning page with the title "This Connection is Untrusted," click the "**I Understand the Risks**" option.

Step 2 Click **Add Exception...**.

Step 3 In the Add Security Exception dialog box, click **Confirm Security Exception**.

Step 4 Close all Mozilla Firefox windows.

You should now be able to access the Cisco StadiumVision Director server using Mozilla Firefox without any security certificate warnings.

Logging Into Cisco StadiumVision Director

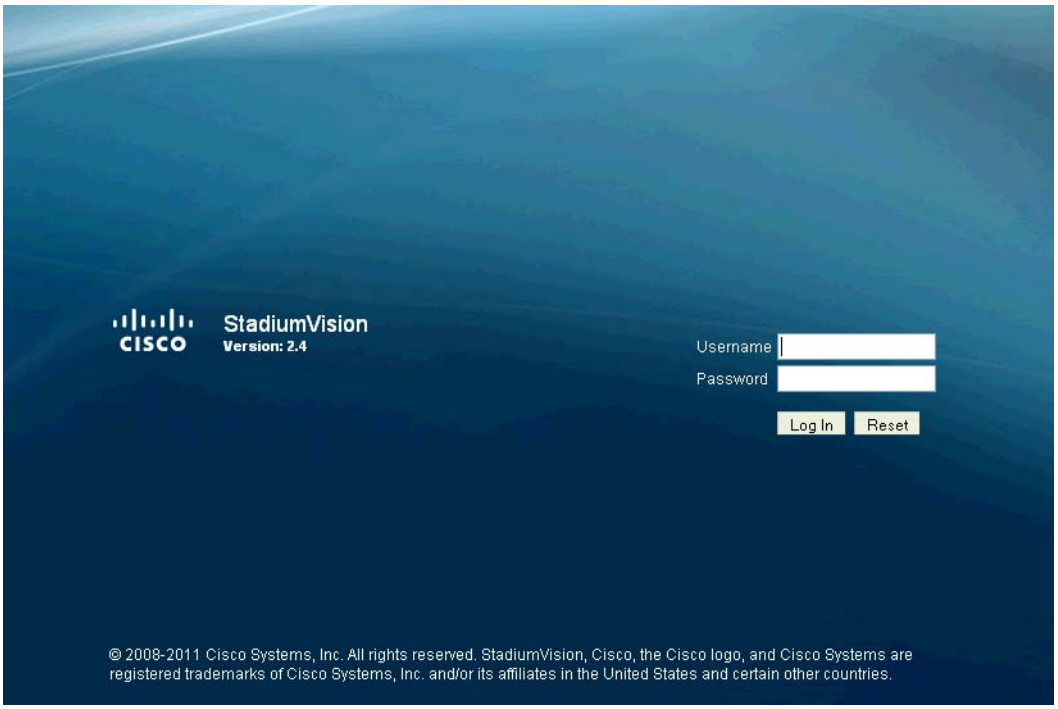
To verify that the upgrade to Cisco StadiumVision Director Release 2.4 was successful, and that Cisco StadiumVision Director is up and operating, complete the following steps:

Step 1 Open a browser window and type the URL for the Cisco StadiumVision Director server, in the following sample format, where *x.x.x.x* is the IPv4 address of the Cisco StadiumVision Director server:

```
http://x.x.x.x
```

The Cisco StadiumVision Director login screen appears (Figure 4).

Figure 4 Cisco StadiumVision Director Login Screen



Step 2 Verify that the Version 2.4 is displayed.

Tip If your window is not displaying Version 2.4, be sure that you have cleared the browser cache as describe in the "Clearing the Browser Cache" section on page 14.

Step 3 Type your Cisco StadiumVision Director administrator login credentials and click **Log In**.

Note When you first log into Cisco StadiumVision Director, the default administrator username and password is *admin*.

The Cisco StadiumVision Director Main Menu screen appears (Figure 5).

Figure 5 Cisco StadiumVision Director Main Menu

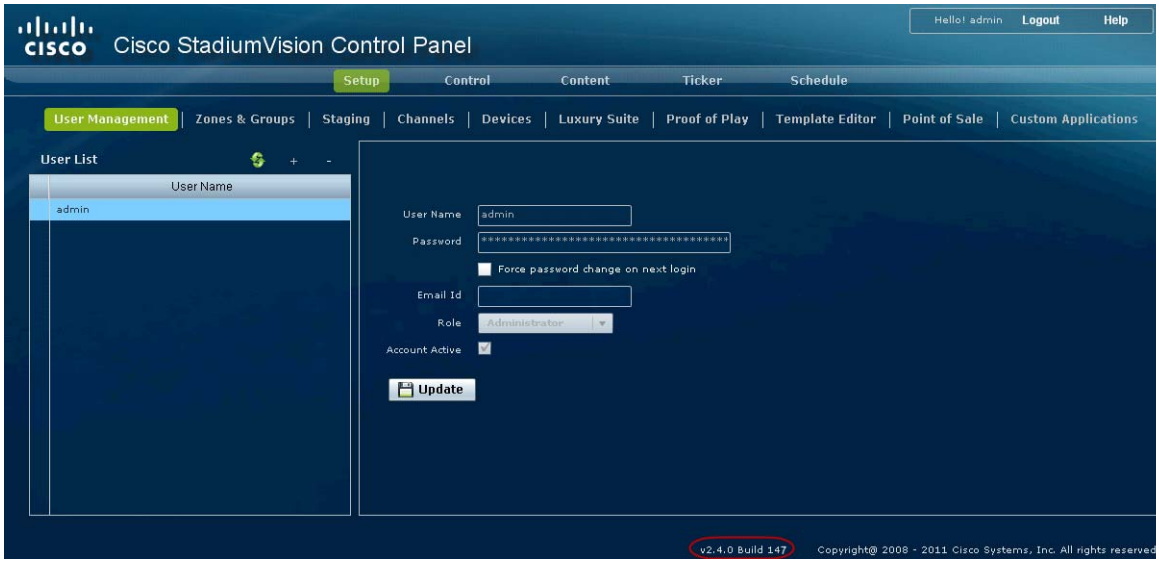
Verifying the Control Panel and Other Menus

To verify the control panel, complete the following steps:

Step 1 From the Cisco StadiumVision Director Main Menu, click **Control Panel**.

After a few moments of loading resources, the Cisco StadiumVision Control Panel Setup screen will open in a new window (Figure 6).

Figure 6 Cisco StadiumVision Control Panel



Step 2 Confirm the version and build number of your Cisco StadiumVision Director software in the lower right corner of the Control Panel window.

Tip If your window is not displaying the appropriate version and build that you loaded, be sure that you have cleared the browser cache as describe in the "Clearing the Browser Cache" section on page 14.

Step 3 Verify that you can open the other Cisco StadiumVision Director screens and menus.

Checking for Duplicate MAC Address Entries

Cisco StadiumVision Director does not support duplicate MAC addresses for the DMPs. After you have upgraded your software, check the following file for any duplicates:

/var/sv/db/mysql/upgrade-invalidmac.csv

Tip You can also run the GetStatus operation on selected DMPs in the Management Dashboard to update the MAC address for the selected DMPs in the Cisco StadiumVision Director database.

Configuring the DMP 4310 Assigned VLAN Property for VLAN Compliance Check

A new VLAN compliance check for DMPs has been added to Cisco StadiumVision Director Release 2.4. Therefore, after you upgrade to release 2.4, you need to go to the Management Dashboard and change the Assigned VLAN property under Global DMP Settings for both the 4310 and 4310 v5.2.3 settings according to your DMP VLAN configuration.

Configuring this property in the Management Dashboard settings for the DMP 4310s will ensure that the Dashboard value can be checked for compliance with the value being sent by the DMP:

- If all of your DMPs are located on the same VLAN (recommended)—Type the number of the VLAN and save the configuration.
- If all of your DMPs are not located on the same VLAN, or you want to bypass any VLAN compliance checking—Type "**$svd_ignore**" and save the configuration.

The value in the Assigned VLAN property in the Management Dashboard settings for the DMP 4310s is checked against what is being sent by the DMP, unless you have configured $svd_ignore.

Caution DMP auto-registration support requires that the VLAN value is correctly set or "$svd_ignore" is used.

Figure 7 shows how to configure the Assigned VLAN property under the 4310 Settings for DMPs that are not located on the same VLAN using the "$svd_ignore" string.

Note You need to set a value for the Assigned VLAN property for both the 4310 Settings and the 4310 v5.2.3 Settings under Global DMP Settings in the Management Dashboard..

To configure the Assigned VLAN Property, complete the following steps:

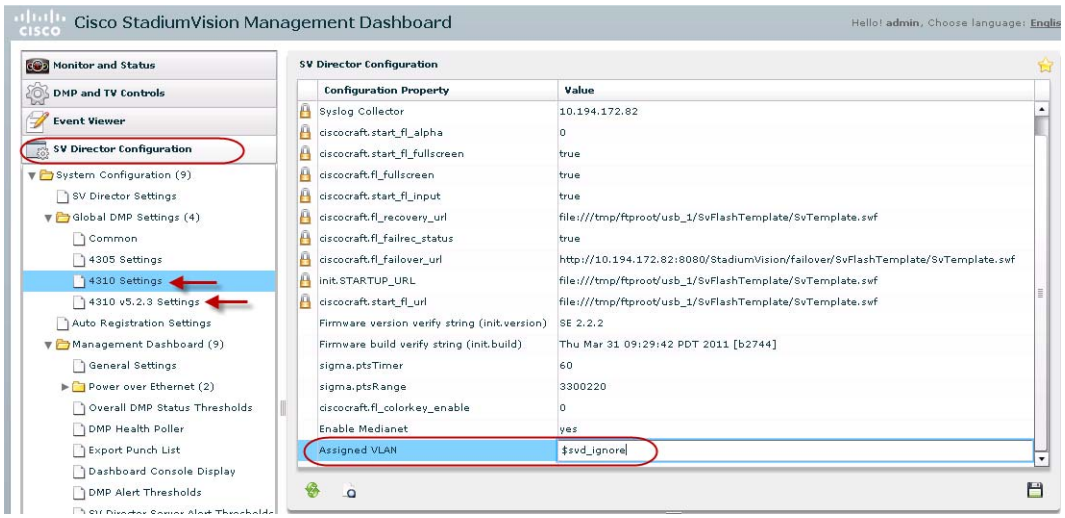
Step 1 Go to the Management Dashboard, and click **SV Director Configuration > System Configuration > Global DMP Settings**.

Step 2 Complete both of the following steps, as shown in Figure 7:

a. Click **4310 Settings**. Find the Assigned VLAN property. In the box, type either the VLAN number where the DMP resides, or $svd_ignore.

b. Click **4310 v5.2.3 Settings**. Find the Assigned VLAN property. In the box, type either the VLAN number where the DMP resides, or $svd_ignore

Figure 7 Assigned VLAN Property Configuration for DMPs



Step 3 Click the Save icon.

Verifying DMPs, Groups, and Zones in the Management Dashboard

Note Before you verify DMP status, be sure that you have set the Assigned VLAN property for your DMP 4310s so that the VLAN compliance check can be performed. For more information, see the "Configuring the DMP 4310 Assigned VLAN Property for VLAN Compliance Check" section on page 19.

To check DMPs, groups, and zones after you upgrade your software, complete the following steps:

Step 1 Go to the Management Dashboard and verify that all of your groups, zones and DMPs are present and in the green state.

Step 2 From the DMP and TV Controls dashboard drawer, run a Get Status on all DMPs to update Cisco StadiumVision Director's record of DMP MAC addresses using the following dashboard command path: **DMP and TV Controls > Monitoring > Get Status**.

Step 3 Run an Initial Config to enable the Video Distribution Manager (VDM) configuration using the following dashboard command path:
DMP and TV Controls > DMP Install > Initial Config.

Step 4 Run Get Status to confirm that all DMPs have successfully rebooted.

Step 5 Stage the Flash template using the following dashboard command path:
DMP and TV Controls > DMP Install > Stage Template.

Step 6 Send Global DMP Settings to the DMPs using the following dashboard command path:
DMP and TV Controls > Global > Global DMP Settings.

Note You must send the Global DMP Settings command twice to reboot the DMPs due to an issue with enabling Medianet services for the first time.

Step 7 Run Get Status to confirm that the DMPs are in good health.

Note This will also update the MAC address for the DMPs.

Step 8 (Optional) Change the DMP State of healthy DMPs to "Production" using the following dashboard command path:
DMP and TV Controls > Auto Registration > Change DMP State.

Step 9 Run Get Status to check the DMP state after the change.

Step 10 Investigate any DMPs that are not in "Normal" state.

Verifying the Multicast Configuration

Cisco StadiumVision Director Release 2.4 uses both unicast and multicast communications for DMP control-plane operation. The Cisco Connected Stadium design requires that Cisco StadiumVision Director uses the 239.193.0.0 multicast group address range.

The multicast group address for Cisco StadiumVision Director is configured in the "MulticastHostPort" registry.

To verify or configure the multicast addressing for Cisco StadiumVision Director, complete the following steps:

Step 1 From the Management Dashboard, select **Tools > Advanced > Registry**.

Step 2 Scroll to the "MulticastHostPort" registry key in the Parameters list and confirm the entry for the registry.

Step 3 To change the value, click on the value field and specify a multicast address in the range 239.193.0.0/24.

Step 4 Click **Apply**.

Setting Up the Quest Venue Manager to Send Updates to Cisco StadiumVision Director Server

After you upgrade, you need to set up the Quest Venue Manager to support sending updates to the Cisco StadiumVision server when menu items change.

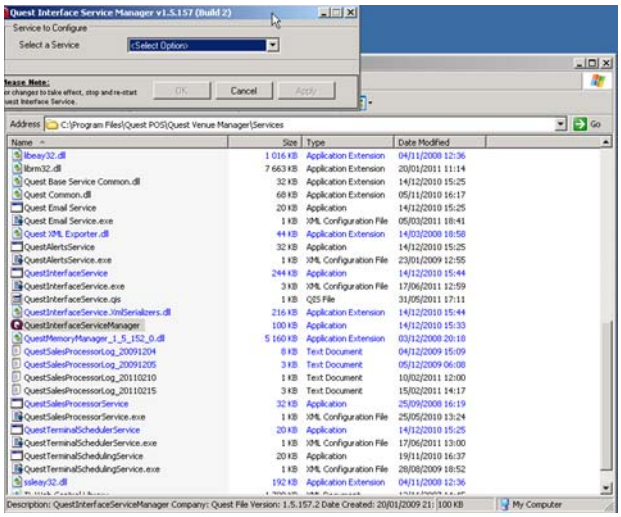
To set up the Quest Venue Manager to send updates to the Cisco StadiumVision Director server, complete the following steps:

Step 1 Access the Quest server.

Step 2 Go to the C:\Program Files\Quest POS\Quest Venue Manager\Services directory.

Step 3 Start the executable application program named "QuestInterfaceServiceManager" (Figure 8).

Figure 8 QuestInterfaceServiceManager Application



Step 4 When the Quest Interface Service Manager application window opens, specify the following options (Figure 9):

a. In the Select a Service box, choose the **Quest Menu Web Service Notification**.

b. Select the **Enabled** checkbox so a checkmark appears.

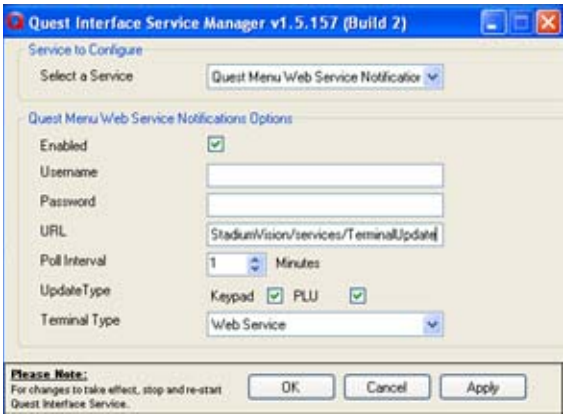
c. In the URL box, enter "**http://svd:8080/StadiumVision/services/TerminalUpdate**."

d. In the Poll Interval box, select **1** minute.

e. Select the **Keypad** and **PLU** update checkboxes so a checkmark appears.

f. In the Terminal Type box, select **Web Service**.

Figure 9 Select a Service to Configure



Step 5 Click **OK**.

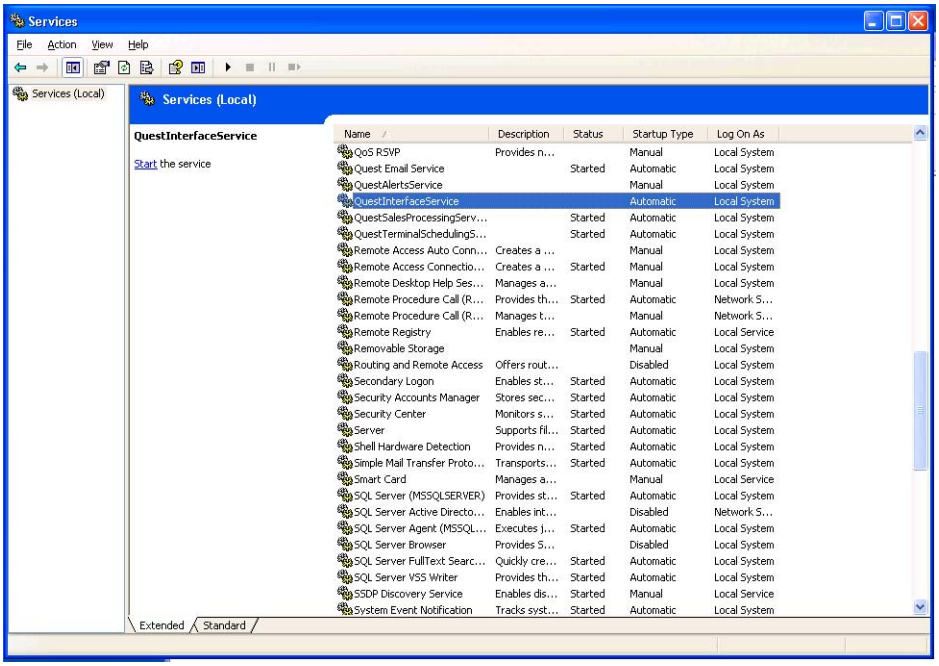
Step 6 Restart the windows service to implement the configuration by completing the following steps:

a. From your laptop, click **Start > Run. . .**

b. When the Run dialog box opens, type "**services.msc**".

c. Find the Quest Interface Service and restart it (Figure 10).

Figure 10 Restart the Quest Interface Service



What to Do Next

Use the "Appendix A: Post-Upgrade Checklist" to be sure that you have completed the required verification steps.

Installing Cisco StadiumVision Director Software From a DVD

First Published: November 4, 2011
Revised: January 20, 2012

This module describes how to install the Cisco StadiumVision Director Release 2.4 software from an installation DVD that ships with your newly-purchased server hardware. The process applies to a brand new server that has *never* been installed with any version of Cisco StadiumVision Director software.

This module includes the following topics:

Prerequisites

Be sure that the following requirements are met before you upgrade your server:

- Your new server is installed in its production location and does not currently have any version of the Cisco StadiumVision Director software installed. For more information about installing your hardware, go to: http://www.cisco.com/en/US/products/ps11274/prod_installation_guides_list.html
- Verify that a monitor and keyboard are connected to the Cisco StadiumVision Director server.
- Be sure to have the network information required to configure the Ethernet connection on the Cisco StadiumVision Director server, such as:
  - IP address (IPv4 only) and mask
  - Default gateway address
  - DNS server address
  - Hostname
- You have a supported browser version for Cisco StadiumVision Director. For more information about the latest supported browsers, see the *Cisco StadiumVision Release Notes for Release 2.4*.
- The Cisco StadiumVision Director server is connected to the network and has power.

- To access the Text Utility Interface (TUI) to verify the installation, you can use a directly connected console or be sure that you have a laptop computer connected to the same network as the Cisco StadiumVision Director server with an SSH client (such as PuTTY).

Information About Installing Cisco StadiumVision Director Software From a DVD

The installation program automatically begins when you install the DVD into the server drive and boot the server by either powering the server off or using the reset switch.

The installation DVD program will present you with screens asking you to confirm or provide information before moving to the next installation screen.

Navigating the Installation Screens

Note The installation program only supports keyboard controls and not any mouse selection. Each screen also provides information about how to navigate through the options and screens.

To provide input to the prompts on the installation screens, use the following keys:

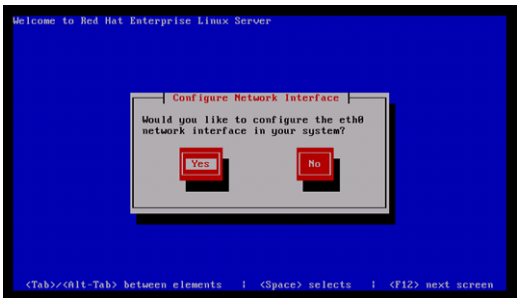
- To move between selection options on the screen—Press **Tab** or **Alt**-**Tab**.
- To confirm selection of an option on the screen—Press the **spacebar**.
- To accept your selection and move to the next installation screen—Press **F12**.

Installing the Software

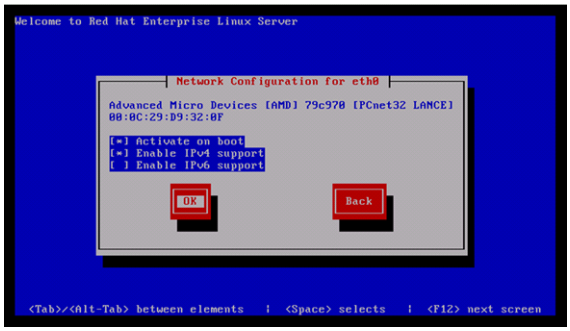
To install Cisco StadiumVision Director Release 2.4 software for the first time on a new server, complete the following steps:

Step 1 Insert the installation disk into the DVD drive, power on or reset the server, and follow the prompts. The server will boot from the installation disk.

Step 2 At the Configure Network Interface screen, press the **spacebar** to select **Yes**:



Step 3 In the Network Configuration for eth0 screen, select **Activate on boot** and **Enable IPv4 support** and select **OK**:



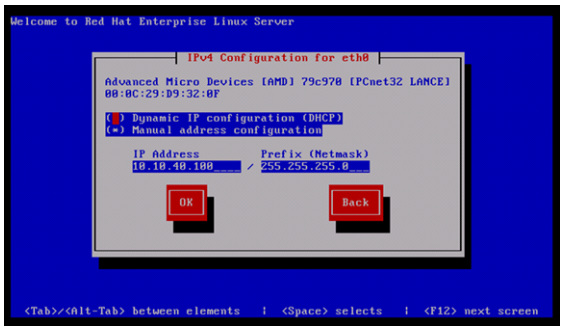
Step 4 In the IPv4 Configuration for eth0 screen, do the following:

a. Select **Manual address configuration**.

b. Type the **IPv4 address** for the server.

c. Type the **Prefix** (network mask) for the IP address.

d. Select **OK**.

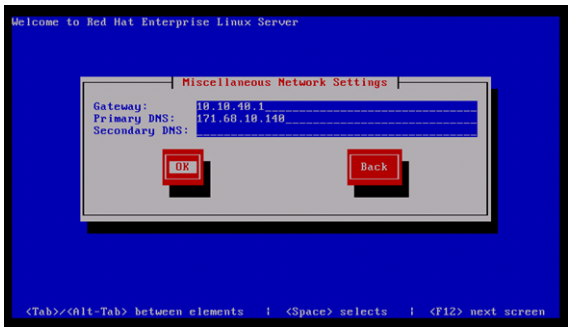


Step 5 In the Miscellaneous Network Settings screen, do the following:

a. Type the IPv4 address of the default gateway.

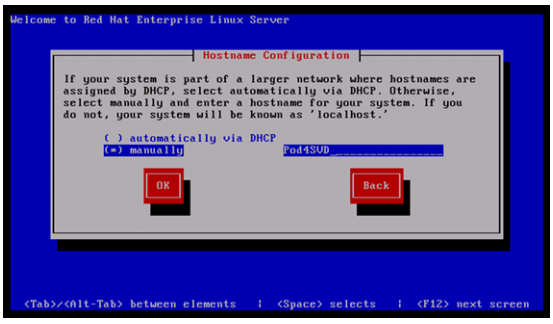
b. Type the IPv4 address(es) of the primary and secondary (if used) Doman Name Server (DNS).

c. Select **OK**.

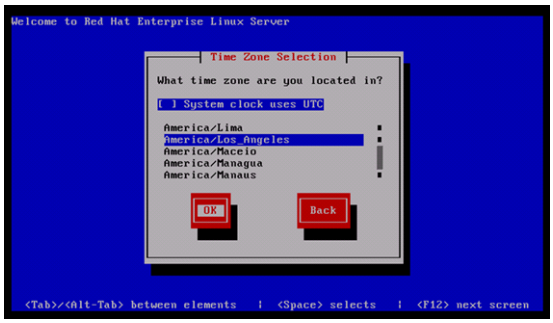


Step 6 In the Hostname Configuration screen, select **manually** and type a host name for your system. Select **OK**.

Tip When specifying a hostname for the server, use a descriptive name that identifies the location or customer and the server number. For example: svd-mylocation-1.

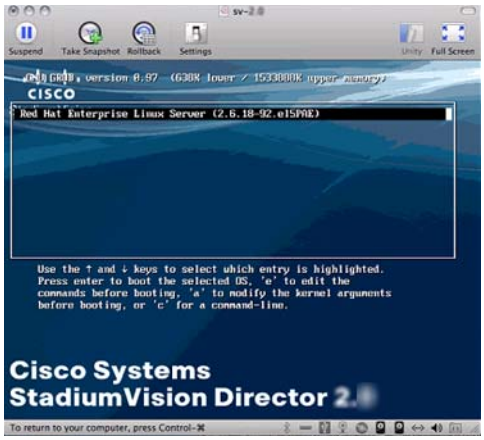


Step 7 In the Time Zone Selection screen, select the time zone and select **OK**.



The Cisco StadiumVision Director software installs, the DVD is ejected, and the system reboots. This process takes about 30 minutes.

When the reboot is complete, the following screen is displayed:



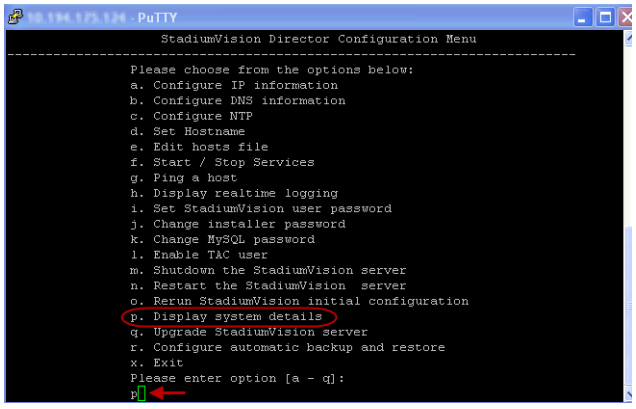
Verifying a New Installation

To verify a new installation of Cisco StadiumVision Director Release 2.4, complete the following steps:

Step 1 Use a directly connected console, or use an SSH client from a laptop computer that is connected to the Cisco StadiumVision Server network to run a secure login to the Cisco StadiumVision Director server using the IP address for your server.

Step 2 When the login prompt appears, enter the **installer** userid followed by the installer password **cisco!123** at the password prompt.

Step 3 When the StadiumVision Director Configuration menu appears, type **p** and press **Enter**:

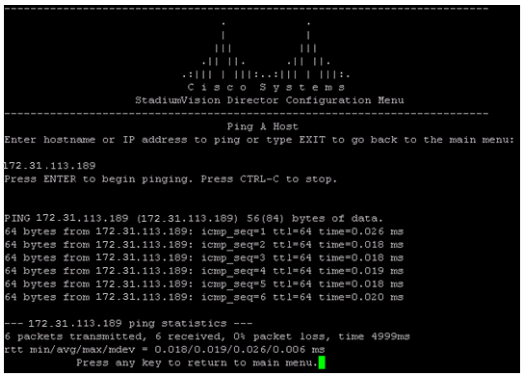


Step 4 When the system details are displayed, verify the server IP address and other system information has been properly configured.

Step 5 Type **r** and press **Enter** to return to the TUI main menu.

Step 6 If there are any system configuration settings that you want to change, access the appropriate TUI menu option to modify your configuration.

Step 7 To verify connectivity to another host connected on the network, type **g** to ping a host and press **Enter**. Type the IP address of the host that you want to test and press **Enter**.



Step 8 To stop the ping, press **Ctl-C** and then press any key to return to the TUI main menu.

Step 9 Type **x** and press **Enter** to exit the TUI.

Step 10 From your browser, open the Cisco StadiumVision Director software using the following secure HTTPS URL, where *x.x.x.x* is the IP address of your server:

`https://x.x.x.x`

Step 11 At the Cisco StadiumVision Director login screen, verify that the window displays the appropriate version. Then type the default username **admin** with password **admin**, and click **Login**.

Step 12 After you log in with the default admin credential for the first time, enter a new password when prompted to change it at the next screen.

What to Do Next

This section describes some of the initial things you can do to begin configuring your Cisco StadiumVision Director server:

- Open the Management Dashboard to begin the process of provisioning DMPs for auto-registration.

Note Beginning in Cisco StadiumVision Director Release 2.4, the default global DHCP setting for auto-registration is set to enabled.

For more information about DMP configuration, see the *Cisco StadiumVision Video Endpoint (DMP) Design and Implementation Guide*.

- If your site does not use the Ad Insertion Manager, it can be removed from the Cisco StadiumVision Director main menu by somebody with sudo root access to the server. For more information, see the "Disabling the AIM Software" section of the "Upgrading a Cisco StadiumVision Director Server From Release 2.3 to Release 2.4" module.
- Change the default password for the admin user account.
- Add additional user accounts.
- Refer to the other design, configuration, and operation guides on Cisco.com to continue setting up your Cisco StadiumVision Director server at:

  http://www.cisco.com/en/US/products/ps11274/tsd_products_support_series_home.html

Using the TUI Upgrade Utility to Update an Existing Release 2.4 Server

First Published: November 4, 2011
Revised: June 12, 2012

Note Do *not* use the information in this module to perform an upgrade from Cisco StadiumVision Director Release 2.3 to Release 2.4. For more information about how to perform that upgrade, see the "Upgrading a Cisco StadiumVision Director Server From Release 2.3 to Release 2.4" module.

This module describes how to upgrade an existing server already running Cisco StadiumVision Director Release 2.4 to a more recent 2.4 version, including installation of service packs. This procedure is also referred to generally as an *ISO upgrade* to refer to both the service pack and upgrade ISO process.

This module includes the following topics:

Best Practices

Before you begin upgrading a Cisco StadiumVision Director server from an existing Release 2.4 version to a more recent 2.4 version, consider the following best practices:

- Choose an appropriate down time to perform the upgrade on the Cisco StadiumVision Director server when there is adequate time to complete and verify the upgrade before any scheduled events and to allow time to resolve any unexpected issues that might occur.
- Refer to the *Release Notes for Cisco StadiumVision Director Release 2.4* for the latest information about hardware and software requirements, changes, important notes, and caveats for your software release.

- Pay particular attention to the required hardware and software versions for other devices supporting your Cisco StadiumVision solution and be sure that you upgrade those devices as needed. For example, generally only certain firmware versions are supported for the DMP hardware, or a new firmware version is needed to provide additional functionality supported by the Cisco StadiumVision Director software.
- Perform a backup and restore of the primary and secondary servers:
  - Perform a backup of the currently active primary server.
  - Restore the backup data onto the standby secondary server.
  - Promote the secondary server to primary.
  - Access the promoted secondary server to perform the upgrade.

  For more information about performing a backup and restore on a Cisco StadiumVision Server running release 2.4, see the *Backing Up and Restoring Cisco StadiumVision Director Servers, Release 2.4* guide.

Prerequisites

Note If you are upgrading from Cisco StadiumVision Director Release 2.4.0-118, be sure that you login to the Cisco StadiumVision Director server as a sudo root user and run the following command before you upgrade to a later version of Release 2.4:

```
$ sudo yum clean all
```

Be sure that the following requirements are met before you upgrade your server:

- Your server is running a minimum of Cisco StadiumVision Director Release 2.4.0-118 or higher.

Note If you are installing a service pack for release 2.4, you must be running a minimum of Cisco StadiumVision Director Release 2.4.0-147.

- You have the IP address for the Cisco StadiumVision Director server where you want to upload the ISO upgrade image. You will need to use this information as part of the URL to access the ISO upload utility.
- You have a supported browser version for Cisco StadiumVision Director. For more information about the latest supported browsers, see the *Cisco StadiumVision Release Notes for Release 2.4*.
- You have an installer account on the Cisco StadiumVision Director server.

Information About Using the TUI Upgrade Utility to Update an Existing Release 2.4 Server

The ISO upgrade procedure for Cisco StadiumVision Director Release 2.4 includes the following tasks:

1. Downloading an ISO service pack or upgrade file from the software download site on Cisco.com.
2. Uploading the ISO file from your laptop to the Cisco StadiumVision Director server using the upload utility through your browser.
3. Installing the ISO image using the upgrade utility in the Text Utility Interface (TUI).

ISO Upgrade Files

The ISO upgrade files are stored in the following location:

/var/www/cgi-bin/ISOupload

You can store multiple ISO upgrade files on a Cisco StadiumVision Director server. The files will be displayed with a sequence number and the ISO filename in the TUI upgrade utility for you to select which file to install.

Disk Maintenance

There is no automatic aging of ISO upgrade files or any utility to remove files from the Cisco StadiumVision Director server.

You should periodically maintain your disk storage by manually removing any ISO upgrade files that you no longer need.

Upgrade Tasks

To upgrade your Cisco StadiumVision Director server from Release 2.4 to a newer version of Release 2.4, or a service pack, complete the following tasks:

- Downloading ISO Upgrade Files From Cisco.com, page 35 (required)
- Uploading an ISO Upgrade File to the Cisco StadiumVision Director Server, page 37 (required)
- Installing the ISO Upgrade Image on the Cisco StadiumVision Director Server, page 39 (required)
- Disabling the AIM Software, page 42 (optional)
- Verifying the Upgrade, page 42 (required)

Downloading ISO Upgrade Files From Cisco.com

Be sure to download the upgrade files to a location, such as a laptop computer, where you can access them for installation onto the Cisco StadiumVision Director server.

To download an ISO upgrade file, complete the following steps:

Step 1 Go to the Cisco StadiumVision Director software download site at:

http://www.cisco.com/cisco/software/release.html?mdfid=283489263&flowid=25361&softwareid=283866237&release=2.4.0-147

Note This site page is also available from the Cisco StadiumVision Director product support page by clicking **Download Software > Cisco StadiumVision Director**.

Step 2 Select the ISO service pack or upgrade file for your server model (32- or 64-bit) and optionally, ther companion MD5 checksum file, and download them.

Table 1 shows the filename conventions used for service pack (SP) upgrades for each server model.

Table 1 SP Filename Conventions by Server Hardware [1]

Hardware Product ID	Filename Convention
64-bit Model SV-DIRECTOR-K9 or SV-PLATFORM2=	• SV-DIRECTOR-SPx-2.4.0.x86_64.iso • SV-DIRECTOR-SPx-2.4.0.x86_64.iso.md5sum
32-bit Model CADE-2140-K9	• SV-DIRECTOR-SPx-2.4.0.i386.iso • SV-DIRECTOR-SPx-2.4.0.i386.iso.md5sum

1. "x' represents the ordered number of the service pack file. The first service pack is SP1.

Table 2 shows the filename conventions used for upgrades for each server model.

Table 2 Upgrade Filename Conventions by Server Hardware

Hardware Product ID	Filename Convention[1]
64-bit Model SV-DIRECTOR-K9 or SV-PLATFORM2=	• SV-DIRECTOR-UPGRADE-2.4.0-*nnn*.x86_64.iso • SV-DIRECTOR-UPGRADE-2.4.0-*nnn*.x86_64.iso.md5sum
32-bit Model CADE-2140-K9	• SV-DIRECTOR-UPGRADE-2.4.0-*nnn*.i386.iso • SV-DIRECTOR-UPGRADE-2.4.0-*nnn*.i386.iso.md5sum

1. "*nnn*" represents the build number of the image in the file.

You can download the files using one of the following methods:

- Download both files at one time—Select each file and click **Add to Cart**. Then at the top of the download page, click the "Download Cart (2 items)" link.
- Download each file independently—Click the **Download Now** button in the file selection box for each file.

Step 3 (Optional) To verify the integrity of your upgrade file from the download, you can use a command-line or GUI utility on your laptop to calculate the checksum on the .iso file. Open the .md5sum file to compare the value that you calculated with the expected value provided in the .md5sum file.

The values should match. If they do not, retry the download.

Uploading an ISO Upgrade File to the Cisco StadiumVision Director Server

After you have downloaded the ISO upgrade file from Cisco.com, you need to upload the file to the Cisco StadiumVision Director server using a URL from a browser to access the ISO uploader utility. Once you have uploaded the software to the server, then you will use the TUI to install the upgrade image.

Prerequisites

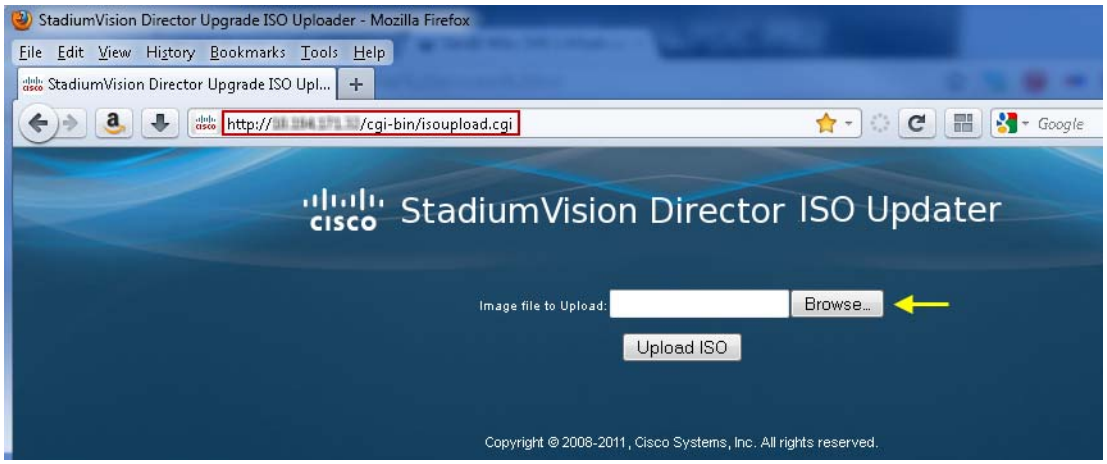
Be sure that you know the IP address of the Cisco StadiumVision Director server where you want to upload the file, and you have a supported browser version for Cisco StadiumVision Director.

To upload an ISO upgrade file to the Cisco StadiumVision Director server, complete the following steps:

Step 1 Open your browser, and to go the following URL, where *x.x.x.x* is replaced by the IP address of the server where you want to upload the upgrade software (Figure 1):

`http://x.x.x.x/cgi-bin/isoupload.cgi`

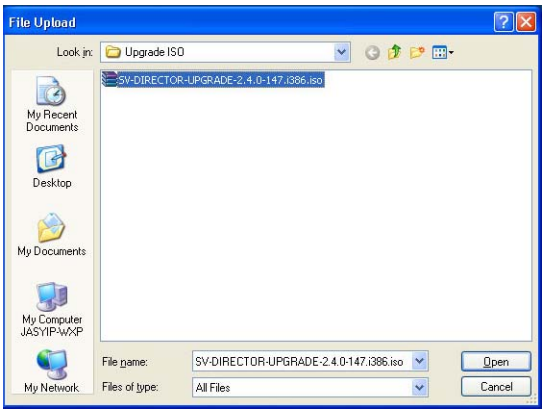
Figure 1 ISO Updater Utility



Step 2 Click **Browse** (Figure 1).

Step 3 From the File Upload dialog box, navigate to the location of the ISO upgrade file that you downloaded from Cisco.com. Select the file that you want to upload and click **Open**. Figure 2 shows an example of selection of a 32-bit ISO upgrade file, but you need to upload the appropriate image for your server.

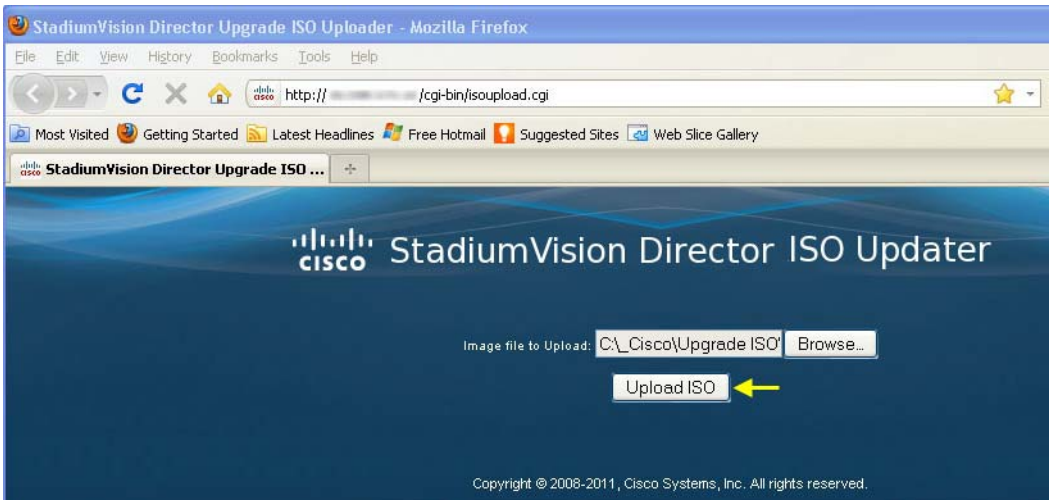
Figure 2 File Upload Dialog Box



Step 4 Click the **Upload ISO** button (Figure 3). The file is sent to the server.

Caution The upload might take several minutes. Do *not* refresh or reload the ISO Updater page while the upload process is running. Any interruption will corrupt the ISO image being uploaded.

Figure 3 ISO File Selection and Upload



When the ISO upload is complete, one of the following occurs:

- Image integrity is verified before an image is stored on the server. When the image is validated and uploaded successfully, a message is displayed stating that the ISO image has been uploaded.
- The image upload failed for some reason and you will need to retry the upload again.

Installing the ISO Upgrade Image on the Cisco StadiumVision Director Server

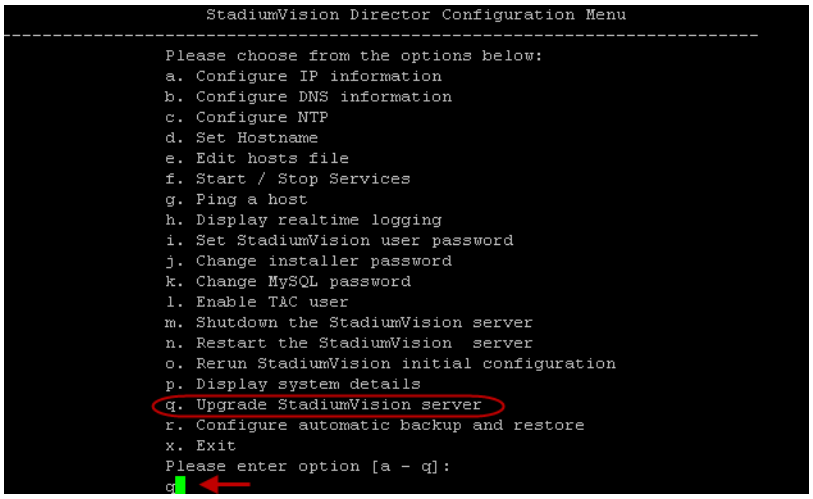
To install the ISO upgrade image on the Cisco StadiumVision Director server, complete the following steps:

Step 1 Use a directly connected console, or use an SSH client from a laptop computer that is connected to the Cisco StadiumVision Server network to run a secure login to the Cisco StadiumVision Director server using the IP address for your server.

Step 2 When the login prompt appears, enter the **installer** userid followed by the installer password at the password prompt.

Step 3 When the StadiumVision Director Configuration menu appears, type **q** and press Enter (Figure 4):

Figure 4 TUI Main Menu Option for Upgrade of Cisco StadiumVision Server

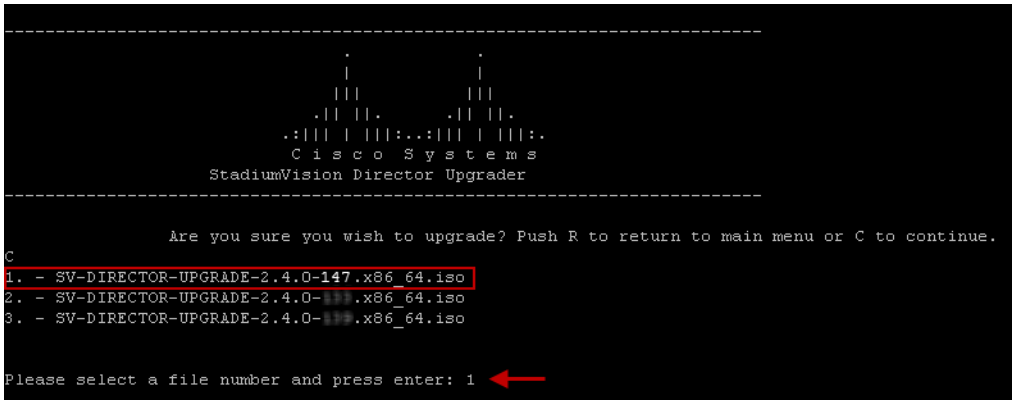


Step 4 When the upgrade configuration confirmation prompt appears, type **c** to continue (Figure 5):

Figure 5 TUI Upgrade Configuration Confirmation

Step 5 All of the ISO upgrade files that you have uploaded are displayed with a sequence number and the image name. Type the sequence number that corresponds to the image that you want to install, and press **Enter**. Figure 6 shows an example of selection of a 64-bit ISO upgrade file for installation.

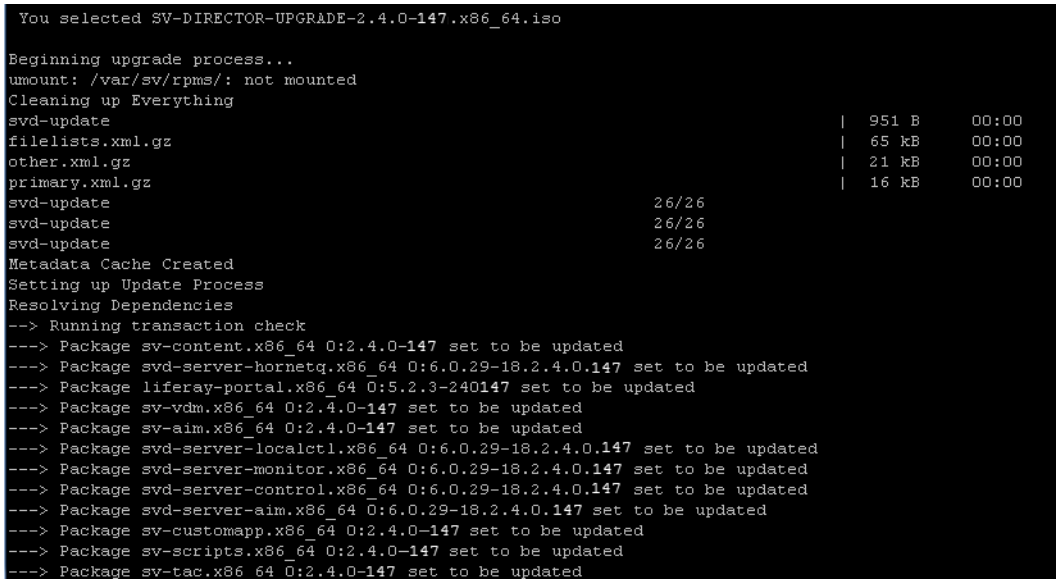
Figure 6 ISO Upgrade Image File List



The upgrade process begins (Figure 7).

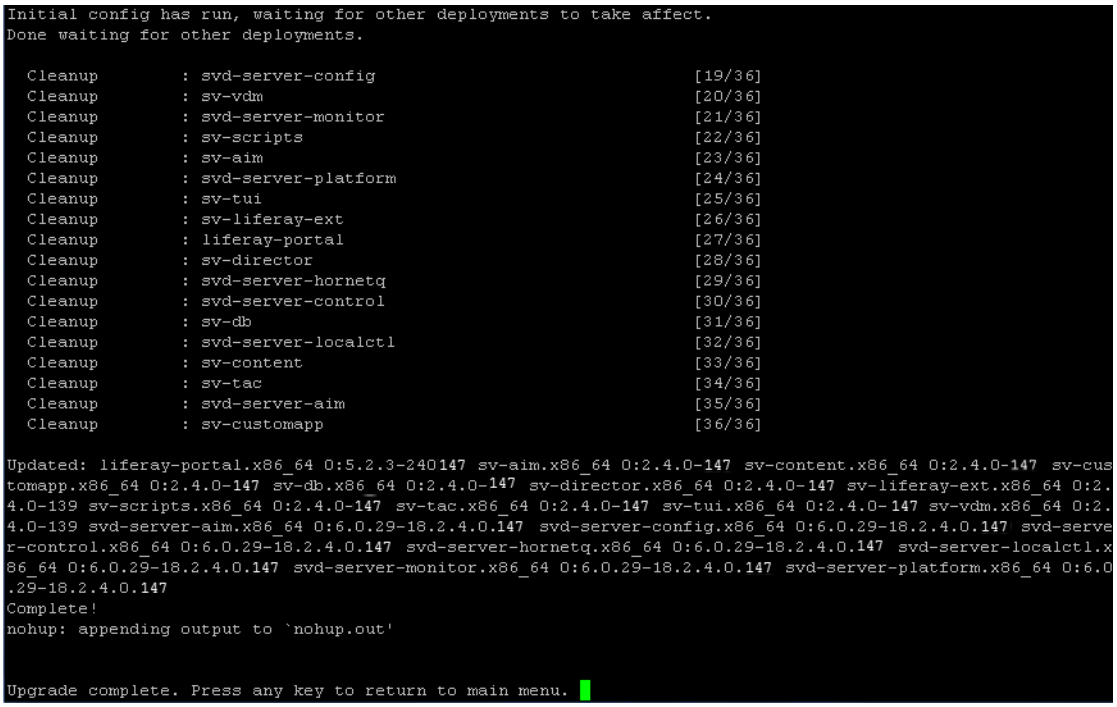
Caution Wait until the upgrade process completes. *Do not* close the terminal while the upgrade is in progress. You will get notification once the installation is complete.

Figure 7 Start of ISO Upgrade Process



Step 6 When the "Upgrade complete" message appears, press any key. (Figure 8):

Figure 8 End of ISO Upgrade Process



Note There is no need to reboot the Cisco StadiumVision Director server. The server is restarted automatically after the upgrade is complete.

Step 7 Exit the TUI, and do one of the following:

- If you are upgrading from a 2.4 image later than 2.4.0-118, go on to the "Verifying the Upgrade" section on page 42.
- If you are upgrading from 2.4.0-118, go on to Step 8.

Only if you are upgrading from Cisco StadiumVision Director Release 2.4.0-118, complete the following steps:

Step 8 Login to the Cisco StadiumVision Director server as a sudo root user.

Step 9 Stop and start the processes using the following commands:

```
sudo service svd stop
sudo service liferay restart
sudo service svd start
```

Step 10 Log out and go on to the "Verifying the Upgrade" section on page 42.

Disabling the AIM Software

If your site does not use the Ad Insertion Manager (AIM), you can remove it from the Cisco StadiumVision Director software and main menu by commenting out the menu code lines.

To disable the AIM software if it is not being used, complete the following steps:

Step 1 Exit the Cisco StadiumVision Director home page using the following command:

```
sudo vi /opt/sv/servers/config/webapps/StadiumVision/index.jsp
```

Step 2 Comment out lines 141-146. Go to line 141 in the vi editor and insert comment mark <!-- at the beginning of the line 141, and --> at the end as shown in the following example:

```
vi:141
<!--<tr align="left">
    <td><img src="cues_images/new-window_link_icon.gif" alt=""></td>
    <td class="textStyle">
    <a href="/AIMWeb/home.html" target="_blank">Ad Insertion Manager</a>
    </td>
</tr>-->
```

Step 3 Write the change using the following command:

```
:w
```

Step 4 Exit the vi editor using the following command:

```
:x
```

Step 5 Remove the AIM package using the following command:

```
sudo rpm -e sv-aim svd-server-aim --nodeps
```

Note When Cisco StadiumVision Director starts, it will show a process named svd-aim running. You can ignore this process as it does not run the AIM web application.

Verifying the Upgrade

To verify the upgrade, complete the following tasks:

- Clearing the Browser Cache, page 43 (required)
- Importing the Security Certificate in Microsoft IE, page 43 (required)
- Logging Into Cisco StadiumVision Director, page 44 (required)
- Verifying the Control Panel and Other Menus, page 45 (required)
- Checking for Duplicate MAC Address Entries, page 46 (required)
- Configuring the DMP 4310 Assigned VLAN Property for VLAN Compliance Check, page 46 (required)
- Verifying DMPs, Groups, and Zones in the Management Dashboard, page 48 (required)
- Verifying the Multicast Configuration, page 48 (required)

Clearing the Browser Cache

After you perform the Cisco StadiumVision Director Release 2.4 software upgrade, you must clear the browser cache to be sure that you are viewing the latest version of Cisco StadiumVision Director.

To clear the browser cache in Mozilla FireFox, complete the following steps:

Step 1 From the menu bar, go to **Tools > Clear Recent History**.

The Clear Recent History dialog box appears.

Step 2 In the "Time range to clear:" box, select **Everything**.

Step 3 Open the Details drop-down list and select the **Cache** checkbox if it does not have a checkmark.

Step 4 Click **Clear Now**.

To clear the browser cache in Microsoft Internet Explorer, complete the following steps:

Step 1 From the menu bar, go to **Tools > Delete Browsing History**.

Step 2 Select the Temporary Internet Files checkbox if it does not have a checkmark.

Step 3 Click **Delete**.

Importing the Security Certificate in Microsoft IE

When you access a Cisco StadiumVision Director 2.4 server for the first time using Microsoft Internet Explorer, a security certificate warning will appear. Some Cisco StadiumVision Director functionality requires that the certificate is imported in IE.

To import the security certificate in Microsoft Internet Explorer, complete the following steps:

Step 1 When you see the warning page with the title "There is a problem with this website's security certificate," click the "**Continue to this website...**" option.

Step 2 Next to the URL bar on the top of the browser window, click **Certificate Error** and then click the "**View certificates**" link.

Step 3 In the Certificate dialog box, click **Install Certificate...** .

Step 4 In the Certificate Import Wizard dialog box, click **Next>**.

Step 5 In the next step of the wizard, select "Place all certificates in the following store" radio button and then click **Browse...** .

Step 6 In the Select Certificate Store dialog box, select the "Trusted Root Certification Authorities" store and click **Ok**.

Step 7 Click **Next>** in the Certificate Import Wizard dialog.

Step 8 Click **Finish**.

Step 9 In the Security Warning dialog box, click **Yes**.

Confirm that a dialog stating “The import was successful.” appears.

Step 10 Close all Microsoft IE windows.

You should now be able to access the Cisco StadiumVision Director server using Microsoft IE without any security certificate warnings.

Logging Into Cisco StadiumVision Director

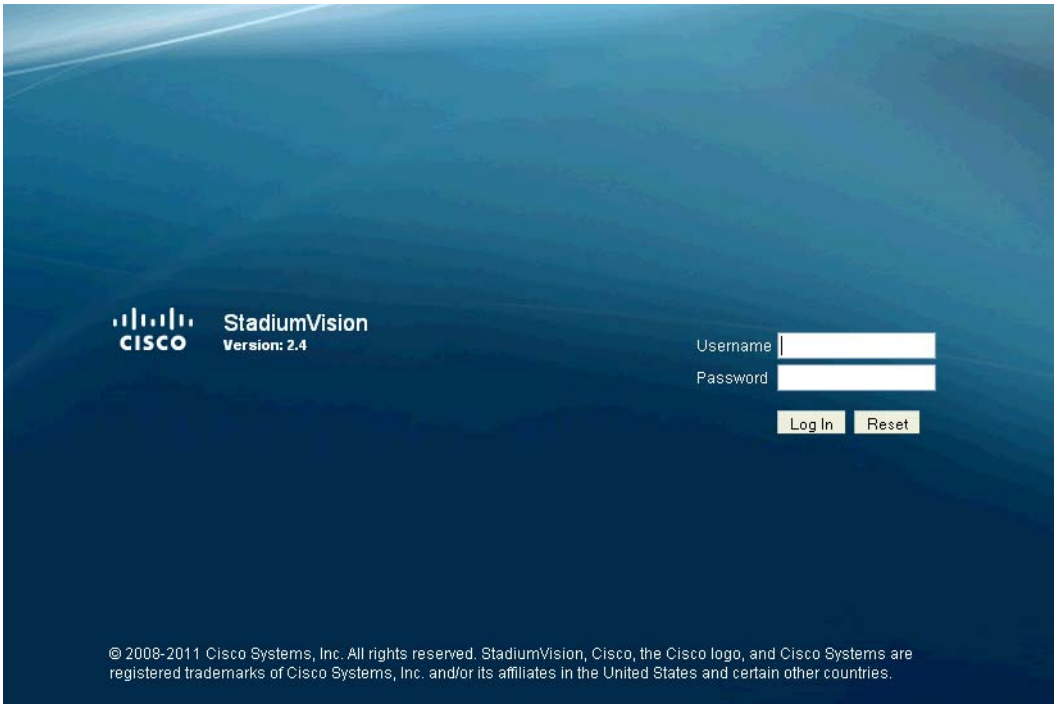
To verify that the upgrade was successful, and that Cisco StadiumVision Director is up and operating, complete the following steps:

Step 1 Open a browser window and type the URL for the Cisco StadiumVision Director server, in the following sample format, where *ipaddress* is the IPv4 address of the Cisco StadiumVision Director server:

`http://ipaddress:8080/StadiumVision/`

The Cisco StadiumVision Director login screen appears (Figure 9).

Figure 9 Cisco StadiumVision Director Login Screen



Step 2 Verify that the Version 2.4 is displayed.

Tip If your window is not displaying Version 2.4, be sure that you have cleared the browser cache as describe in the “Clearing the Browser Cache” section on page 43.

Step 3 Type your Cisco StadiumVision Director administrator login credentials and click **Log In**.

Note When you first log into Cisco StadiumVision Director, the default administrator username and password is *admin*.

The Cisco StadiumVision Director Main Menu screen appears (Figure 10).

Figure 10 Cisco StadiumVision Director Main Menu

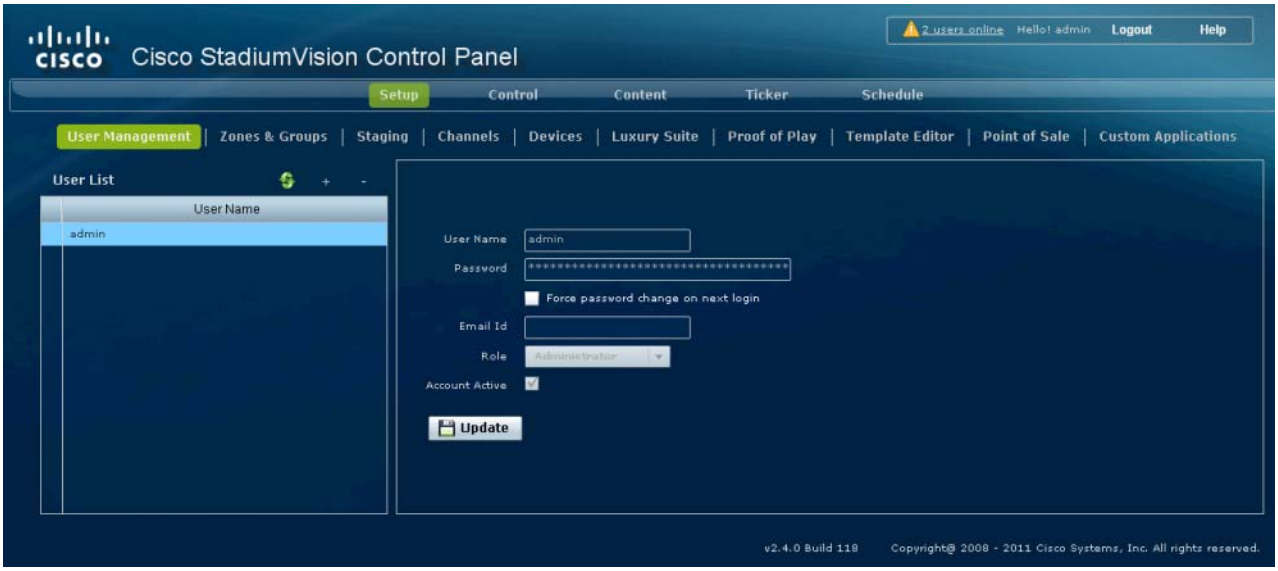
Verifying the Control Panel and Other Menus

To verify the control panel, complete the following steps:

Step 1 From the Cisco StadiumVision Director Main Menu, click **Control Panel**.

After a few moments of loading resources, the Cisco StadiumVision Control Panel Setup screen will open in a new window (Figure 11).

Figure 11 Cisco StadiumVision Control Panel



Step 2 Confirm the version and build number of your Cisco StadiumVision Director software in the lower right corner of the Control Panel window.

Tip If your window is not displaying the appropriate version and build that you loaded, be sure that you have cleared the browser cache as describe in the "Clearing the Browser Cache" section on page 43.

Step 3 Verify that you can open the other Cisco StadiumVision Director screens and menus.

Checking for Duplicate MAC Address Entries

Cisco StadiumVision Director does not support duplicate MAC addresses for the DMPs. After you have upgraded your software, check the following file for any duplicates:

/var/sv/db/mysql/upgrade-invalidmac.csv

Configuring the DMP 4310 Assigned VLAN Property for VLAN Compliance Check

A new VLAN compliance check for DMPs has been added to Cisco StadiumVision Director Release 2.4. Therefore, after you upgrade to release 2.4, you need to go to the Management Dashboard and change the Assigned VLAN property under Global DMP Settings for both the 4310 and 4310 v5.2.3 settings according to your DMP VLAN configuration.

Configuring this property in the Management Dashboard settings for the DMP 4310s will ensure that the Dashboard value can be checked for compliance with the value being sent by the DMP:

- If all of your DMPs are located on the same VLAN (recommended)—Type the number of the VLAN and save the configuration.

- If all of your DMPs are not located on the same VLAN, or you want to bypass any VLAN compliance checking—Type "**$svd_ignore**" and save the configuration.

The value in the Assigned VLAN property in the Management Dashboard settings for the DMP 4310s is checked against what is being sent by the DMP, unless you have configured $svd_ignore.

Caution DMP auto-registration support requires that the VLAN value is correctly set or "$svd_ignore" is used.

Figure 12 shows how to configure the Assigned VLAN property under the 4310 Settings for DMPs that are not located on the same VLAN using the "$svd_ignore" string.

Note You need to set a value for the Assigned VLAN property for both the 4310 Settings and the 4310 v5.2.3 Settings under Global DMP Settings in the Management Dashboard..

To configure the Assigned VLAN Property, complete the following steps:

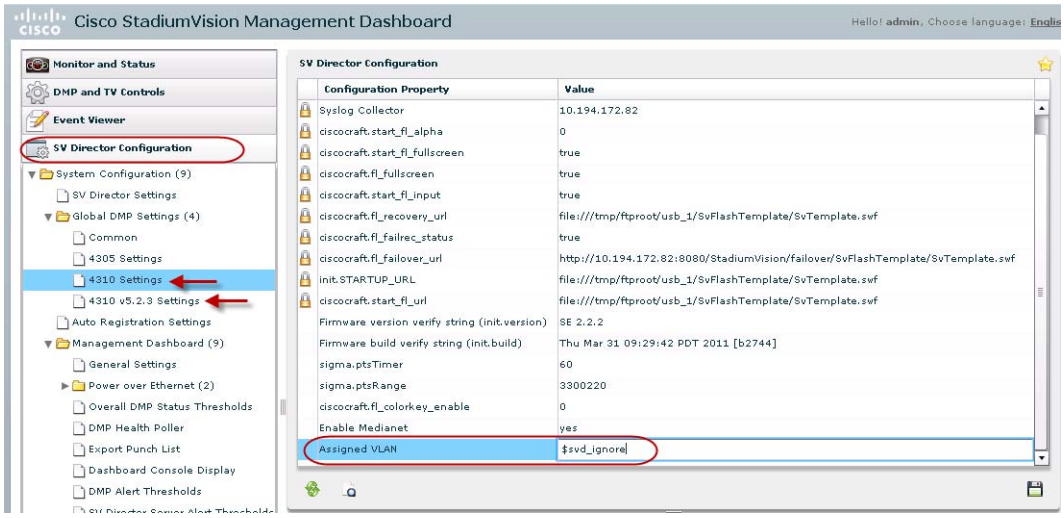
Step 1 Go to the Management Dashboard, and click **SV Director Configuration > System Configuration > Global DMP Settings**.

Step 2 Complete both of the following steps, as shown in Figure 12:

a. Click **4310 Settings**. Find the Assigned VLAN property. In the box, type either the VLAN number where the DMP resides, or $svd_ignore.

b. Click **4310 v5.2.3 Settings**. Find the Assigned VLAN property. In the box, type either the VLAN number where the DMP resides, or $svd_ignore

Figure 12 Assigned VLAN Property Configuration for DMPs



Step 3 Click the Save icon.

Verifying DMPs, Groups, and Zones in the Management Dashboard

Note Before you verify DMP status, be sure that you have set the Assigned VLAN property for your DMP 4310s so that the VLAN compliance check can be performed. For more information, see the "Configuring the DMP 4310 Assigned VLAN Property for VLAN Compliance Check" section on page 46.

To check DMPs, groups, and zones after you upgrade your software, complete the following steps:

Step 1 Go to the Management Dashboard and verify that all of your groups, zones and DMPs are present and in the green state.

Step 2 From the DMP and TV Controls dashboard drawer, run a Get Status on all DMPs to update Cisco StadiumVision Director's record of DMP MAC addresses using the following dashboard command path:
DMP and TV Controls > Monitoring > Get Status.

Step 3 Run an Initial Config to enable the Video Distribution Manager (VDM) configuration using the following dashboard command path:
DMP and TV Controls > DMP Install > Initial Config.

Step 4 Run Get Status to confirm that all DMPs have successfully rebooted.

Step 5 Stage the Flash template using the following dashboard command path:
DMP and TV Controls > DMP Install > Stage Template.

Step 6 Send Global DMP Settings to the DMPs using the following dashboard command path:
DMP and TV Controls > Global > Global DMP Settings.

Note You must send the Global DMP Settings command twice to reboot the DMPs due to an issue with enabling Medianet services for the first time.

Step 7 Run Get Status to confirm that the DMPs are in good health.

Note This will also update the MAC address for the DMPs.

Step 8 (Optional) Change the DMP State of healthy DMPs to "Production" using the following dashboard command path:
DMP and TV Controls > Auto Registration > Change DMP State.

Step 9 Run Get Status to check the DMP state after the change.

Step 10 Investigate any DMPs that are not in "Normal" state.

Verifying the Multicast Configuration

Cisco StadiumVision Director Release 2.4 uses both unicast and multicast communications for DMP control-plane operation. The Cisco Connected Stadium design requires that Cisco StadiumVision Director uses the 239.193.0.0 multicast group address range.

The multicast group address for Cisco StadiumVision Director is configured in the "MulticastHostPort" registry.

To verify or configure the multicast addressing for Cisco StadiumVision Director, complete the following steps:

Step 1 From the Management Dashboard, select **Tools** > **Advanced** > **Registry**.

Step 2 Scroll to the "MulticastHostPort" registry key in the Parameters list and confirm the entry for the registry.

Step 3 To change the value, click on the value field and specify a multicast address in the range 239.193.0.0/24.

Step 4 Click **Apply**.

What to Do Next

Use the "Appendix A: Post-Upgrade Checklist" to be sure that you have completed the required verification steps.

Upgrading the CIMC and BIOS Firmware on a Cisco StadiumVision Director Platform 2 Server

First Published: January 20, 2012
Revised: August 2, 2012

Platform 2 of the Cisco StadiumVision Director Server requires installation of the Unified Computing System (UCS) Server Firmware Version 1.4(2) to avoid problems powering off the server hardware.

This module describes how to verify and upgrade a Cisco StadiumVision Director Platform 2 server to the recommended version 1.4(2) of the UCS Cisco Integrated Management Interface (CIMC) firmware and version 1.4.1 of the BIOS firmware.

Caution Do *not* perform this upgrade on a Cisco ADE 2140 Series server. Be sure that you can confirm your server model before continuing. Figure 1 shows an example of a Platform 2 server.

This module includes the following topics:

Best Practices

Before you begin upgrading the CIMC and BIOS firmware, consider the following best practices:

- Choose an appropriate down time to perform the upgrade on the Cisco StadiumVision Director server when there is adequate time to complete and verify the upgrade before any scheduled events and to allow time to resolve any unexpected issues that might occur.
- Refer to the *Release Notes for Cisco StadiumVision Director Release 2.4* for the latest information about hardware and software requirements, changes, important notes, and caveats for your software release.

Prerequisites

Before you upgrade the Cisco StadiumVision Director server firmware for Platform 2, be sure that the following requirements are met:

- You have installed a Platform 2 server. Figure 1 shows an example of a Platform 2 server applicable for this upgrade.

Figure 1 Front Panel of a Cisco StadiumVision Director Platform 2 Server

- You have configured the CIMC interface on your server. You will need another available IP address for the server and should be prepared to change the default login and password. For more information, see the "Initial Server Setup" section of the "Installing the Server" chapter in the *Cisco UCS C200 Installation and Service Guide*.
- Your current CIMC firmware version is any version earlier than 1.4(2), and your BIOS firmware version is earlier than 1.4.1.
- You have access to Cisco.com to download the firmware.
- You have access to a TFTP server from which you can install the downloaded firmware, and the Platform 2 server has read permission for the destination folder on the TFTP server.
- You are performing the firmware installation with local access to the Cisco StadiumVision Director Platform 2 server.
- You have a monitor and keyboard that you can connect to the server.
- You have a blank DVD that you can use to burn the BIOS ISO software.
- You have a tool (such as "7-zip") to extract the contents of the ZIP file to obtain the CIMC installation BIN file contained within the ISO software file that you will download.

Upgrade Tasks

To upgrade your CIMC and BIOS firmware, complete the following tasks:

- Verifying the BIOS Firmware Version, page 53 (required)
- Downloading the ISO Firmware Upgrade Files From Cisco.com, page 54 (required)
- Installing the CIMC Firmware from a TFTP Server, page 55 (required)
- Burn the BIOS ISO File, page 55 (required)
- Upgrading the BIOS Firmware, page 55 (required)

Verifying the BIOS Firmware Version

You can verify the firmware version installed on Platform 2 of the Cisco StadiumVision Director server by running a Basic System State Report. Once you have installed the Cisco StadiumVision Director server software and have logged in, you can run a System State Report from the Cisco StadiumVision Director main menu.

To verify the BIOS firmware version, complete the following tasks:

Step 1 Log into the Cisco StadiumVision Director server.

Step 2 From the main menu, click System State Reports:

Step 3 From the Cisco StadiumVision Director Status Report screen, select one or both report destination options, and be sure that the "Basic first level" option (default) is selected:

Step 4 Click **Get System Status**.

Step 5 Click the link to download the ZIP report file, or to view the report from the browser.

Step 6 Do one of the following:

- If you downloaded a ZIP report, extract the osinfo.html file and open it.
- From your browser, click the **OS information** link in the report window.

Step 7 Look for "BIOS Information" and "Version" below "Handle 0x00005, DMI type 0, 24 bytes" line, as shown in the following example. If your version number is less than "1.4.1," then an upgrade is needed:

```
Handle 0x0005, DMI type 0, 24 bytes.
BIOS Information
Vendor: Cisco Systems, Inc.
Version: C200.1.1.1a.0.032920100525
Release Date: 03/29/2010
```

Tip If the vendor information in this section is Intel Corporation, and the version begins with "S5000," then this is not a Platform 2 server, but rather a Cisco ADE 2140 Series server. This BIOS upgrade process does *not* apply to the Cisco ADE 2140 Series server.

Downloading the ISO Firmware Upgrade Files From Cisco.com

Be sure to download the upgrade files to a location, such as a laptop computer, where you can access them for installation onto the Cisco StadiumVision Director server.

To download the BIOS ISO upgrade file, complete the following steps:

Step 1 Go to the Cisco UCS C200 M2 Rack-Mount Server Software software download site at:

http://www.cisco.com/cisco/software/release.html?mdfid=283860950&flowid=25801&softwareid=283850974&release=1.4(2)

Note This site page is also available from the Download Software for Cisco products site page by clicking **Products > Unified Computing and Servers > Cisco UCS C-Series Rack-Mount Standalone Server Software > Cisco UCS C200 M2 Rack-Mount Server Software > Unified Computing System (UCS) Server Firmware**. Be sure that the 1.4 release is selected.

Step 2 Click **Download Now** beside the **ucs-c200-huu-1.4.2.iso** file.

The Download Cart dialog box appears.

Step 3 Review the information in the Download Cart dialog box, and then click **Proceed with Download**.

The Software Download Rules page appears.

Step 4 Review the download rules, and click **Agree**.

A dialog box listing your download appears. The Select Location dialog box also appears. This dialog box has the focus.

Step 5 Select a location in the Select Location dialog box, and then click **Open**.

The download begins.

Note The ISO file contains a ZIP file named C200M1_1.4.2.zip.

Step 6 Extract the contents of the C200M1_1.4.2.zip file to your computer, which includes the following ZIP file location: **1.4.2\cimc\c200-m1-cimc.1.4.2.zip**.

Step 7 From the c200-m1-cimc.1.4.2.zip file, extract the 1.4.2 CIMC BIN file (**c200-m1-cimc.1.4.2\upd-pkg-c200-m1-cimc.full.1.4.2.bin**) to be used in updating the CIMC firmware.

Installing the CIMC Firmware from a TFTP Server

Before you install the CIMC firmware, be sure that the following requirements are met:

- The CIMC interface has been configured. See the "Prerequisites" section on page 52.
- You have extracted the upd-pkg-c200-m1-cimc.full.1.4.2.bin file from the downloaded ISO package.

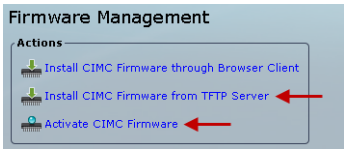
To install the CIMC firmware, follow the procedures to both *install and activate* the CIMC firmware using a TFTP server in the "CIMC Firmware Management" chapter of the *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide, Release 1.4* in the following sections:

- "Installing CIMC Firmware from a TFTP Server"
- "Activating Installed CIMC Firmware"

Note Certain Platform 2 servers cannot support a CIMC firmware upgrade using a web browser. For best results, be sure to install the CIMC firmware using the TFTP server method.

Figure 2 shows an example of the actions available from the Firmware Management screen, and identifies the two required actions for the Cisco StadiumVision Director Platform 2 Server.

Figure 2 Firmware Management Actions



Burn the BIOS ISO File

Note Only a local upgrade of the BIOS firmware is recommended. Do not perform a remote upgrade.

To prepare the BIOS ISO file for a local upgrade, create a bootable disk by burning the **ucs-c200-huu-1.4.2.iso** file to a writable CD or DVD.

Upgrading the BIOS Firmware

Caution Before you upgrade the BIOS firmware, be sure that you have completed installing the CIMC firmware.

To upgrade the BIOS firmware, complete the following steps:

Step 1 Insert the disk with the BIOS ISO file into the DVD drive of the server.

Step 2 Follow the instructions in the *Cisco Host Upgrade Utility Release 1.4(x) Quick Start Guide:*

- Begin at Step 4 of the "Using the Utility" section, to boot from the disk.
- At the Host Upgrade Menu, choose the option to **Update BIOS** and proceed with the installation instructions.
- After the BIOS upgrade is successful, choose the **Reboot (Retains current settings of CIMC)** option.

Verifying the Upgrade

Note The ucs-c200-huu-1.4.2.iso ISO package contains two different, but compatible firmware versions:

CIMC firmware version 1.4.2 and C200 BIOS version 1.4.1.

To verify the upgrade, run the Basic System State report again from Cisco StadiumVision Director and confirm that the BIOS version information shows "1.4.1."

Migrating the Cisco StadiumVision Director Server Environment to Platform 2 from the Cisco ADE 2140 Series Appliance

First Published: March 22, 2012
Revised: August 2, 2012

This module describes how to migrate your Cisco StadiumVision Director data from the Cisco ADE 2140 (32-bit) server environment, to the Platform 2 (64-bit) server environment.

It includes the following topics:

Prerequisites for Server Migration

Before you begin the migration, be sure that the following requirements are met:

- You are migrating from a redundant Cisco ADE 2140 Series Appliance server environment to a redundant Cisco StadiumVision Platform 2 server environment.
- The existing primary and secondary Cisco ADE 2140 Series appliances are both running the same version of Cisco StadiumVision Director Release 2.4 software.
- The new primary and secondary Platform 2 servers are both running the same version of Cisco StadiumVision Director Release 2.4 software.

Tip The software version on the Cisco ADE 2140 Series appliances can start off being different than what you will be running on the new Platform 2 servers. However, ideally, both sets of redundant servers would all be running the same version that you want to run in production for simplicity of the migration.

- All servers are installed on the same local network and have unique IP addresses.
- You have chosen an appropriate down time to perform the migration when there is adequate time to complete and verify the migration before any scheduled events and to allow time to resolve any unexpected issues that might occur.

- Verify that a monitor and keyboard are connected to the Cisco StadiumVision Director server, or that you have a laptop computer connected to the same network as the Cisco StadiumVision Director server with an SSH client (such as PuTTY) to log in as installer and upgrade an existing server.
- Be sure that you have a secure FTP (SFTP) application to transfer any necessary software files to the Cisco StadiumVision Director server, such as backup files when doing server migration.

How to Perform the Server Migration

To perform the server migration, complete the following tasks:

- Running a Backup and Restore on the Cisco ADE 2140 Servers, page 58 (required)
- Promoting the Secondary Cisco ADE 2140 Server, page 59 (required)
- Upgrading the Active Secondary Cisco ADE 2140 Server to Production Version, page 59 (as needed)
- Upgrading the Primary and Secondary Platform 2 Servers to Production Version, page 59 (as needed)
- Replacing the Backup Script and Modifying the Timeout Value on the Primary and Secondary Platform 2 Servers, page 59 (required)
- Verifying the Cisco ADE 2140 and Platform 2 Server Software Versions, page 60 (required)
- Copying Backup Files From the Cisco ADE 2140 Server to the Primary Platform 2 Server, page 60 (required)
- Stopping Services and Shutting Down the Cisco ADE 2140 Servers, page 61 (required)
- Changing the IP Address on the Primary Platform 2 Server, page 61 (required)
- Running a Restore on the Primary Platform 2 Server, page 62 (required)
- Staging the Flash Template to All DMPs on the Primary Platform 2 Server, page 62 (required)
- Running a Backup and Restore on the Platform 2 Servers, page 63 (required)

Running a Backup and Restore on the Cisco ADE 2140 Servers

For more information about running backup and restore on a Cisco StadiumVision Director server, see the *Backing Up and Restoring Cisco StadiumVision Director Servers, Release 2.4* guide.

To run a backup and restore on the Cisco ADE 2140 servers, complete the following steps:

Step 1 Perform a backup of the currently active (primary) Cisco ADE 2140 server.

Step 2 Verify that the backup was successful.

Step 3 Perform a restore of system data from backup on the secondary Cisco ADE 2140 server.

Promoting the Secondary Cisco ADE 2140 Server

Follow the steps in the "Promoting a Standby Secondary Server to the Active Server" section of the *Cisco StadiumVision Director Server Redundancy, Release 2.4* guide.

Upgrading the Active Secondary Cisco ADE 2140 Server to Production Version

Note This task is only required if you did not upgrade the primary and secondary Cisco ADE 2140 servers to the latest Cisco StadiumVision Director Release 2.4 software that you want to run in production on the new Platform 2 server.

Follow the steps in the "Using the TUI Upgrade Utility to Update an Existing Release 2.4 Server" module.

Upgrading the Primary and Secondary Platform 2 Servers to Production Version

Note This task is only required if you did not upgrade the primary and secondary Platform 2 servers to the latest Cisco StadiumVision Director Release 2.4 software that you want to run in production.

Follow the steps in the "Using the TUI Upgrade Utility to Update an Existing Release 2.4 Server" module.

Replacing the Backup Script and Modifying the Timeout Value on the Primary and Secondary Platform 2 Servers

Note This task requires that you have obtained the "backup.cgi" file from your Cisco Systems representative.

To replace the backup script and modify the timeout value, complete the following steps:

Step 1 Log into the Cisco StadiumVision Director primary server using a SNE TAC account login credential.

Step 2 Go to the folder where the current backup script file is stored using the following command:

```
cd /var/www/cgi-bin/
```

Step 3 Rename the original backup.cgi file in this folder to another name using the following command:

```
sudo mv backup.cgi old_backup.cgi
```

Step 4 Using an SFTP client on the PC or laptop where you downloaded the new backup.cgi file, transfer the file to the "/tmp" folder.

Step 5 Move the backup.cgi file to the "/var/www/cgi-bin" folder on the primary Cisco StadiumVision Director server using the following command:

```
sudo mv /tmp/backup.cgi /var/www/cgi-bin
```

Step 6 After transferring the script, verify that the permissions and ownership of the backup.cgi script matches the rest of the scripts in the folder. To change the permissions, use the following commands:

```
sudo chown apache:apache backup.cgi
sudo chmod 755 backup.cgi
```

Step 7 Change the HTTPD timeout value from 120 to 5400 using the following commands:

```
cd /etc/httpd/conf/
sudo vi httpd.conf
```

Search for "Timeout" and increase the value from 120 to 5400.

Step 8 Restart HTTPD using the following command:

```
sudo service httpd restart
```

Step 9 Repeat this task on the secondary server.

Verifying the Cisco ADE 2140 and Platform 2 Server Software Versions

Before you proceed with the next task, verify that the active Cisco ADE 2140 server and both of the primary and secondary Platform 2 servers are running the latest version of Cisco StadiumVision Director Release 2.4 software that you plan to upgrade to in production.

Copying Backup Files From the Cisco ADE 2140 Server to the Primary Platform 2 Server

To move the data from your Cisco ADE 2140 server environment to the new primary Platform 2 server, you need to manually copy the backup files to the new primary Platform 2 server.

To copy backup files from the Cisco ADE 2140 server to the primary Platform 2 server, complete the following steps:

Step 1 On the active Cisco ADE 2140 server, go to the /var/sv/BACKUP directory.

Step 2 Find the following files and copy them:

- File ending in .chksum, which contains an MD5 checksum for the .tar file.
- File ending in .tar.

Note Both files must be copied because the restore process automatically uses both files to verify the MD5 signature.

Step 3 On the primary Platform 2 server, go to the /var/sv/BACKUP directory.

Step 4 Put the .chksum and .tar files that you copied from the Cisco ADE 2140 server into the Platform 2 server backup directory.

Stopping Services and Shutting Down the Cisco ADE 2140 Servers

Note The primary Cisco ADE 2140 server should already be shut down during the promotion of the secondary Cisco ADE 2140 server, but if it is not for some reason, repeat this procedure to shut it down.

To stop services and shut down the Cisco ADE 2140 servers, complete the following steps:

Step 1 Log into the active secondary server as a root user using an SSH client.

Step 2 Shut down the Cisco StadiumVision Director services using the following commands:

```
sudo service httpd stop
sudo service svd stop
sudo service liferay stop
sudo service mysql stop
```

Step 3 When the services are stopped, shut down the secondary server using the following command:

```
sudo shutdown -h now
```

Both Cisco ADE 2140 servers should now be shut down.

Changing the IP Address on the Primary Platform 2 Server

Note Before you begin this task, be sure that you know the IP address of the primary Cisco ADE 2140 server.

To change the IP address on the primary Platform 2 server, complete the following steps:

Step 1 Log into the primary Platform 2 server as a root user using an SSH client.

Step 2 Shut down the Cisco StadiumVision Director services using the following commands:

```
sudo service httpd stop
sudo service svd stop
sudo service liferay stop
sudo service mysql stop
sudo service svd-hornetq stop
```

Step 3 Enter the following command to open a text editor for the /etc/hosts file:

```
sudo vi /etc/hosts
```

Step 4 Change the IP address of the primary Platform 2 server to match the address of the primary CADE server as shown in the sample entry below:

primary-cade-ipaddress primary-platform2-hostname

Step 5 Change the IP address of the actual interface using the following command:

```
sudo system-configure-network
```

Step 6 Restart the network daemon to put the IP address change into effect on the server using the following command:

```
sudo service network restart
```

Step 7 Verify connectivity to the primary Platform 2 server using the ping command, as shown in the following example:

```
ping ip-address
```

Step 8 Restart Cisco StadiumVision Director services using the following commands:

```
sudo service mysql start
sudo service liferay start
sudo service svd start
sudo service httpd start
```

Running a Restore on the Primary Platform 2 Server

Follow the steps in the "Starting a Restore Manually for Immediate Execution" in the *Backing Up and Restoring Cisco StadiumVision Director Servers, Release 2.4* guide.

Staging the Flash Template to All DMPs on the Primary Platform 2 Server

To stage the flash template to all DMPs on the primary Platform 2 server, complete the following steps:

Step 1 Log into Cisco StadiumVision Director as an administrator.

Step 2 From the main menu, click **Control Panel**.

The Control Panel is opened in a new window.

Step 3 Select **Setup** > **Staging**.

Step 4 In the icon bar, click the Plus (+) icon to start manual staging.

The Start manual staging dialog box opens.

Step 5 In the Start manual staging dialog box, do the following:

- For Type, select **Flash template**.
- For Target, select **All configured DMPs**.

Step 6 Click **Start Staging**.

Running a Backup and Restore on the Platform 2 Servers

For detailed information about configuring the backup and restore environment and running a backup and restore, see the *Backing Up and Restoring Cisco StadiumVision Director Servers, Release 2.4* guide.

To run a backup and restore on the Platform 2 servers, complete the following steps:

Step 1 Using the Text Utility Interface (TUI), configure your backup and restore environment.

Step 2 Run a backup on the primary server.

Verify that the backup was successful.

Step 3 Run a manual restore from backup on the secondary server.

How to Roll Back the Server Migration

If for some reason you need to roll back your server environment to the original Cisco ADE 2140 servers, complete the following tasks:

- Stopping Services and Shutting Down the Primary and Secondary Platform 2 Servers, page 63 (required)
- Staging the Flash Template to All DMPs on the Secondary Cisco ADE 2140 Server, page 64 (required)
- Changing the IP Address on the Secondary Cisco ADE 2140 Server, page 64 (required)
- Downgrading the Secondary Cisco ADE 2140 Server Software, page 65 (as required)
- Powering on the Primary Cisco ADE 2140 Server, page 65 (required)
- Running a Backup and Restore on the Cisco ADE 2140 Servers, page 66 (required)
- Verifying the Migration Failback, page 66 (required)

Stopping Services and Shutting Down the Primary and Secondary Platform 2 Servers

Note Be sure to shut down the primary Platform 2 server first.

To stop services and shut down the Platform 2 servers, complete the following steps:

Step 1 Log into the primary Platform 2 server as a root user using an SSH client.

Step 2 Enter the following commands on the server:

```
sudo service httpd stop
sudo service svd stop
sudo service liferay stop
sudo service mysql stop
```

Step 3 When the services are stopped, shut down the server using the following command:

```
sudo shutdown -h now
```

Step 4 Log into the secondary Platform 2 server as a root user using an SSH client.

Step 5 Repeat Step 2 and Step 3 for the secondary server.

Both Platform 2 servers should now be shut down.

Staging the Flash Template to All DMPs on the Secondary Cisco ADE 2140 Server

This task should be performed on the original secondary Cisco ADE 2140 server.

To stage the flash template to all DMPs on the secondary Cisco ADE 2140 server, complete the following steps:

Step 1 Power on the original secondary Cisco ADE 2140 server.

Step 2 Log into Cisco StadiumVision Director as an administrator.

Step 3 From the main menu, click **Control Panel**.

The Control Panel is opened in a new window.

Step 4 Select **Setup > Staging**.

Step 5 In the icon bar, click the plus (+) icon to start manual staging.

The Start manual staging dialog box opens.

Step 6 In the Start manual staging dialog box, do the following:

- For Type, select **Flash template**.
- For Target, select **All configured DMPs**.

Step 7 Click **Start Staging**.

Changing the IP Address on the Secondary Cisco ADE 2140 Server

You need to know the original IP address of the secondary server to complete this task.

To change the IP address on the secondary Cisco ADE 2140 server, complete the following steps:

Step 1 Log into the secondary server as a root user using an SSH client.

Step 2 Display the contents of the /etc/hosts file using the following command:

```
cat /etc/hosts
```

Look for the localhost and secondary server hostname entries in the display from the /etc/hosts file, and confirm the IP address of the secondary server.

Note The system will run if only the localhost entry exists and the hostname entry is missing. The IP address of the secondary server must be changed back to its original IP address.

Step 3 Enter the following command to open a text editor for the /etc/hosts file:

```
sudo system-config-network
```

Step 4 Change the IP address of the secondary server to reflect its original address as a standby server:

```
ipaddress secondary-hostname
```

Step 5 Change the IP address of the actual interface using the following command:

```
sudo system-configure-network
```

Step 6 Restart the network daemon to put the IP address change into effect on the secondary server using the following command:

```
sudo service network restart
```

Step 7 Verify connectivity to the secondary server using the ping command, as shown in the following example:

```
ping ipaddress
```

Note If you cannot reach the secondary server, see the "Clearing the ARP Cache on the Switch" section in the of the *Cisco StadiumVision Director Server Redundancy, Release 2.4* guide and clear the ARP cache entry for the secondary IP address.

Downgrading the Secondary Cisco ADE 2140 Server Software

Note This task is only required if the secondary Cisco ADE 2140 server does not match the software version of the primary Cisco ADE 2140 server. This could happen if you upgraded the secondary server to the latest Cisco StadiumVision Director Release 2.4 software for compatibility with the new Platform 2 servers to which you were migrating.

To downgrade the secondary Cisco ADE 2140 server software, obtain the appropriate ISO upgrade image and follow the steps in the "Using the TUI Upgrade Utility to Update an Existing Release 2.4 Server" module of the *Cisco StadiumVision Director Software Installation and Upgrade Guide, Release 2.4* guide.

Powering on the Primary Cisco ADE 2140 Server

Before you power on the primary Cisco ADE 2140 server, be sure that you have completed the following tasks:

- You have changed the IP address on the secondary Cisco ADE 2140 server to remove any conflict with the primary server.

- You have confirmed that the primary and secondary Cisco ADE 2140 servers are running the same software version.

Running a Backup and Restore on the Cisco ADE 2140 Servers

For detailed information about configuring the backup and restore environment and running a backup and restore, see the *Backing Up and Restoring Cisco StadiumVision Director Servers, Release 2.4* guide.

To run a backup and restore on the Cisco ADE 2140 servers, complete the following steps:

Step 1 Log into the primary server as an installer.

Step 2 Using the TUI, configure your backup and restore environment to set up the directories.

Step 3 Run a backup on the primary server.

Verify that the backup was successful.

Step 4 Run a manual restore from backup on the secondary server.

Verifying the Migration Failback

Complete the steps documented in the "Migration Failback Checklist" section on page 67.

Migration Failback Checklist

Use the following checklist after you failback from an attempted migration to be sure that your Cisco StadiumVision Director software is running normally.

.

List Item	Checkoff
1. Complete any specific verification steps documented for the installation of your particular software version as documented in the *Cisco StadiumVision Director Software Installation Guide*.	❑
2. Clear the browser cache.	❑
3. Verify that the Control Panel shows the Cisco StadiumVision Director version and build number that you installed.	❑
4. If you are using phone control, verify that the phones work.	❑
5. If using IP phones for local TV control, verify that channels can be successfully changed.	❑
6. Verify that channel names and favorites are properly set.	❑
7. If using suite commerce integration, verify that an order can be successfully placed using the IP phone.	❑
8. Verify that all devices are properly in the nonevent_group.	❑
9. Go to the Services Alert window in the Management Dashboard and make sure that all relevant services are green. **Tip** You might need to click the refresh button to be sure that all services are re-polled for status. If needed, you can Disable services that are not part of your installation	❑
10. Verify that all DMPs and TVs in the Management Dashboard are green.	❑
11. Start an existing event script and validate that screens display the expected content.	❑
12. Stop the event script and validate that screens are powered off.	❑
13. Make a minor edit to the event script and make sure it can be saved.	❑
14. Verify that VDM can push a new video file to the DMPs.	❑
15. If using dynamic menu boards, make a change to a menu item and verify that the change is reflected on the menu board.	❑

Appendix A: Post-Upgrade Checklist

First Published: November 4, 2011
Revised: February 16, 2012

The following checklist is useful after you upgrade your software on a Cisco StadiumVision Director server.

.

List Item		Checkoff
1.	Complete any specific verification steps documented for your particular upgrade. For example, some additional verification is required when upgrading from Release 2.3-78 to Release 2.4.	❑
2.	Clear the browser cache.	❑
3.	Verify that the Control Panel shows the Cisco StadiumVision Director version and build number that you installed.	❑
4.	If you are using phone control, verify that the phones work.	❑
5.	If using IP phones for local TV control, verify that channels can be successfully changed.	❑
6.	Verify that channel names and favorites are properly set.	❑
7.	If using suite commerce integration, verify that an order can be successfully placed using the IP phone.	❑
8.	Verify that all devices are properly in the nonevent_group.	❑
9.	Go to the Services Alert window in the Management Dashboard and make sure that all relevant services are green. **Tip** You might need to click the refresh button to be sure that all services are re-polled for status. If needed, you can Disable services that are not part of your installation	❑
10.	Verify that all DMPs and TVs in the Management Dashboard are green.	❑
11.	Start an existing event script and validate that screens display the expected content.	❑
12.	Stop the event script and validate that screens are powered off.	❑

List Item	Checkoff
13. Make a minor edit to the event script and make sure it can be saved.	❑
14. Verify that VDM can push a new video file to the DMPs.	❑
15. If using dynamic menu boards, make a change to a menu item and verify that the change is reflected on the menu board.	❑
16. Perform a server backup for the upgrade configuration.	❑
17. After satisfying your site's testing and event requirements, failback to the primary server and upgrade it to the same version of software that you validated on your secondary server.	❑
18. After you perform failback, be sure that you reconfigure your backup and restore environment using the Text Utility Interface (TUI).	❑

Appendix B: Port Reference

First Published: November 4, 2011
Revised: January 20, 2012

The following tables identify the ports used by Cisco StadiumVision Director.

Cisco StadiumVision Director Input Ports

Table 1 lists the input ports used by all Cisco StadiumVision Director servers.

Table 1 Cisco StadiumVision Director Input Ports

Originator	Protocol	Port	Target Application	Usage
Laptop	TCP	22	SSH	Remote login
Laptop / DMP	TCP	80	Apache	Redirect to port 8080
DMP	TCP	8080	Tomcat / Apache	Fetch config/data
Laptop	TCP	8080	Tomcat / Apache	Main web UI
Laptop	TCP	9090	Tomcat for Liferay	Liferay web UI, i.e. Dynamic Menu Board application
DMP	UDP	514	Syslog	Proof of play, Alerts

Table 2 lists the additional input ports used by Cisco StadiumVision Director server instances.

Table 2 Cisco StadiumVision Director Input Ports

Originator	Protocol	Port	Target Application	Usage
Laptop	TCP	7041	Java	Jmx management interface for control server instance
Laptop	TCP	7042	Java	Jmx management interface for config server instance
Laptop	TCP	7043	Java	Jmx management interface for monitor server instance

Table 2 Cisco StadiumVision Director Input Ports (continued)

Originator	Protocol	Port	Target Application	Usage
Laptop	TCP	7044	Java	Jmx management interface for aim server instance
Laptop	TCP	7050	Java	Jmx management interface for local control server instance

Cisco StadiumVision Director Output Ports

Table 3 Cisco StadiumVision Director Output Ports

Originator	Protocol	Port	Target Application	Usage
StadiumVision Director	TCP	22	ssh	DMP troubleshooting
StadiumVision Director	TCP	80	httpd	4305 web UI
StadiumVision Director	TCP	443	httpd	4310 web UI
StadiumVision Director	TCP	873	rsyncd	Content distribution to 4305
StadiumVision Director	TCP	7777	httpd	DMP control commands
StadiumVision Director	TCP	10000	SV daemon	SVD v1.5 binary commands
StadiumVision Director	TCP	10001	httpd	SVD v2.0 http commands
StadiumVision Director	UDP	Default=50001	DMP flash template	Multicast commands (default is 239.192.0.254:50001)

DMP Input Ports

Table 4 DMP Input Ports

Originator	Protocol	Port	Target Application	Usage
Laptop	TCP	80	httpd	4305 web UI
Laptop	TCP	443	httpd	4310 web UI
StadiumVision Director	TCP	873	rsyncd	Content distribution to 4305
StadiumVision Director	TCP	7777	httpd	DMP control commands

Table 4 DMP Input Ports

Originator	Protocol	Port	Target Application	Usage
StadiumVision Director	TCP	10000	SV daemon	SVD v1.5 binary commands
StadiumVision Director	TCP	10001	httpd	SVD v2.0 http commands
StadiumVision Director	UDP	varies	DMP flash template	Multicast commands (default is 239.192.0.254:50001)
Headend	UDP	varies	Sigma chipset	Multicast video