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**.

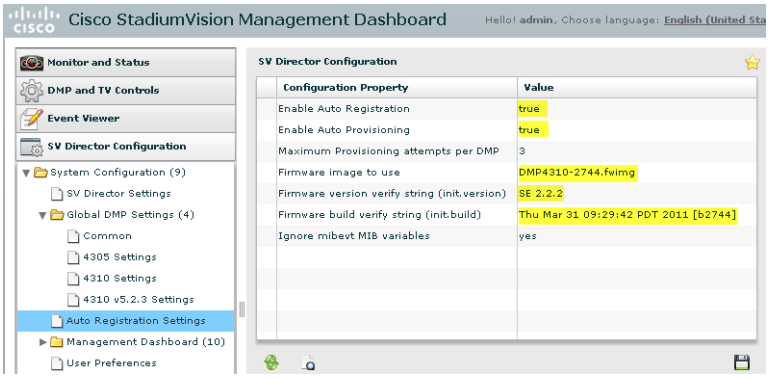
Step 4 Upload the firmware file to the server and upgrade the firmware for the DMP 4310Gs.

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]

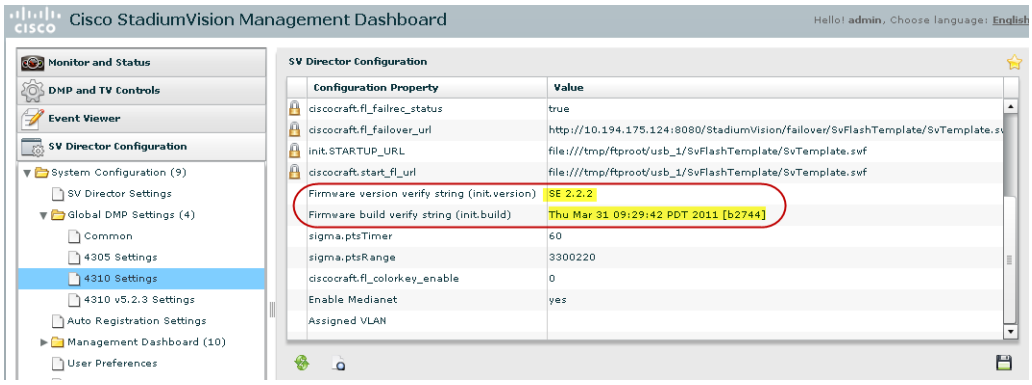
Figure 1 Auto Registration Settings in Management Dashboard



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



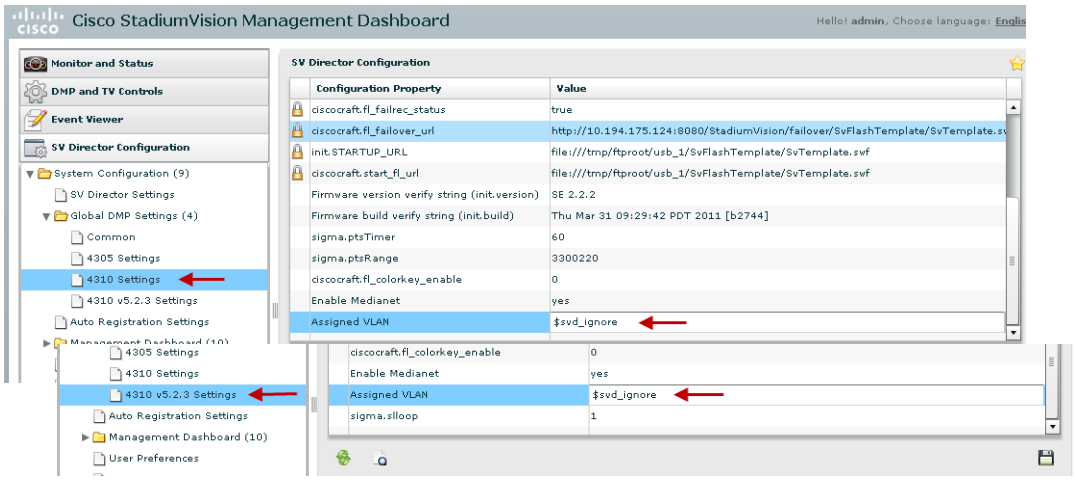
Step 7 Configure the Assigned VLAN property under both the 4310 v5.2.3 and 4310 Settings as $svd_ignore or the actual VLAN number on which your DMPs reside. Do *not* leave blank.

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

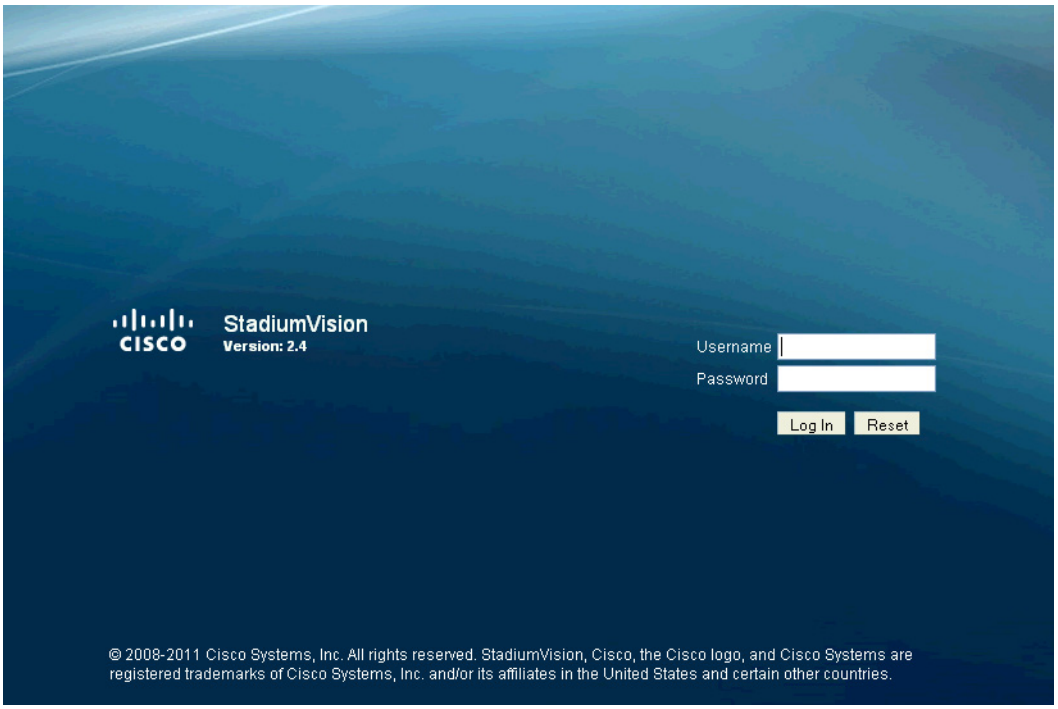
To verify that the upgrade to Cisco StadiumVision Director Release 2.4 was successful, and that Cisco StadiumVision Director is up and operating, complete the following steps:

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

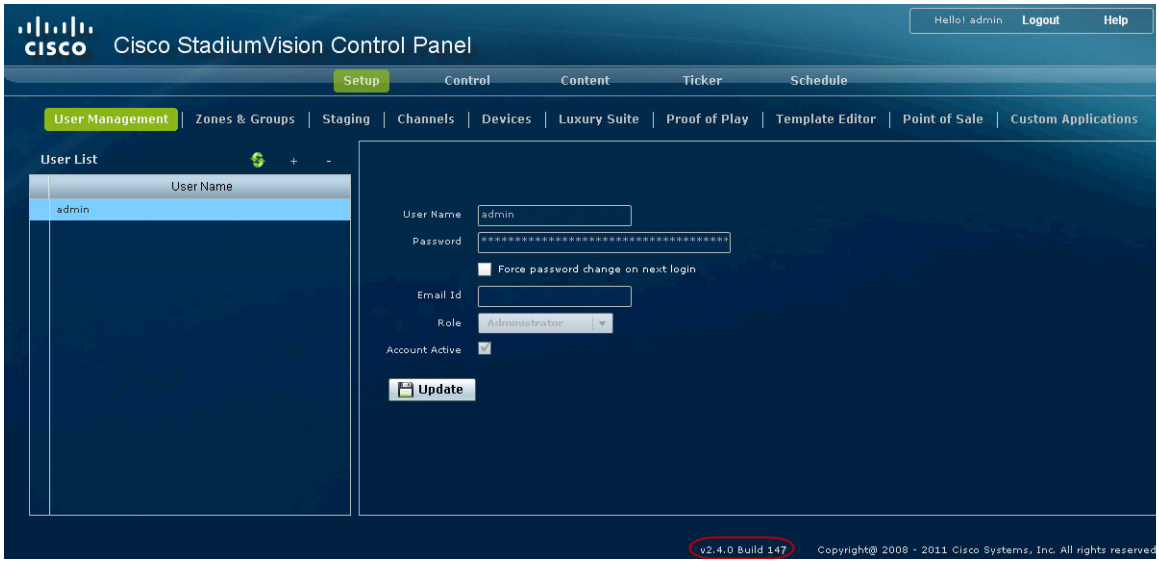
Verifying the Control Panel and Other Menus

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:

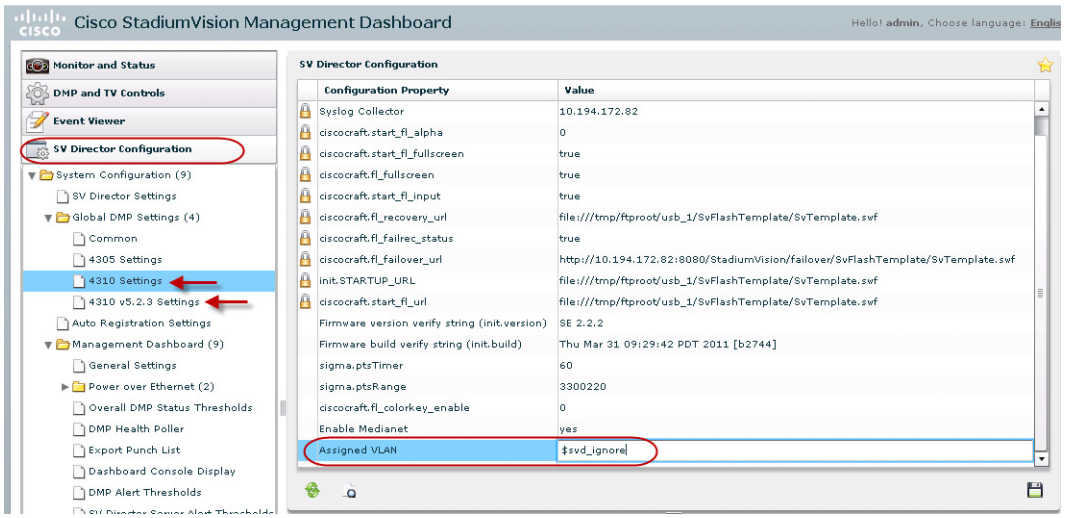
Step 1 Go to the Management Dashboard, and click **SV Director Configuration > System Configuration > Global DMP Settings**.

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.

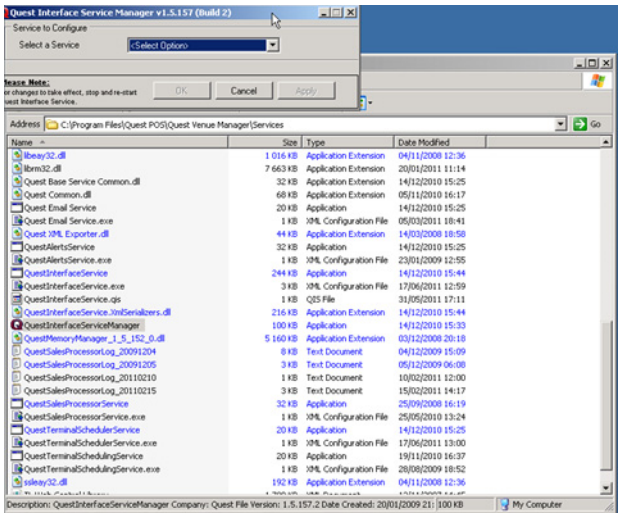
To set up the Quest Venue Manager to send updates to the Cisco StadiumVision Director server, complete the following steps:

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.

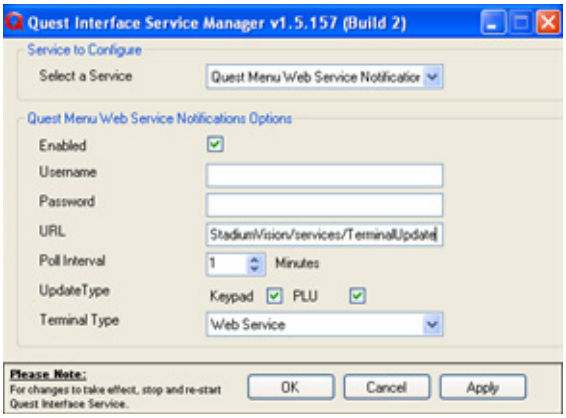
c. In the URL box, enter "**http://svd:8080/StadiumVision/services/TerminalUpdate**."

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**.

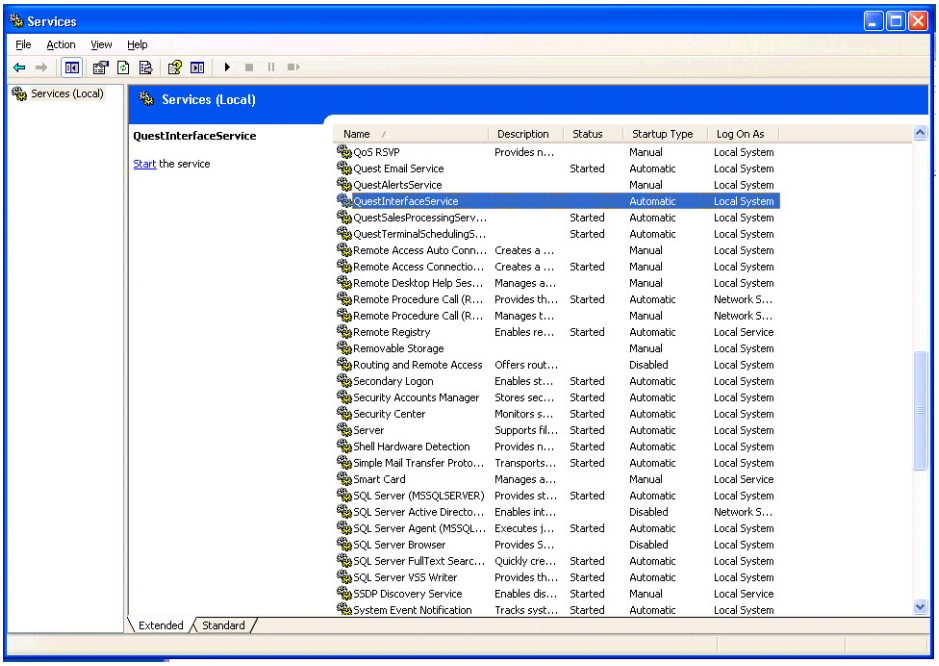
Step 6 Restart the windows service to implement the configuration by completing the following steps:

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.