Verifying the Upgrade

First Published: April 21, 2014
Revised: June 4, 2014

This module describes how to verify that the upgrade process was successful.

To verify the upgrade, complete the following tasks:

Clearing the Browser Cache

Caution It is critical that *all* Cisco StadiumVision Director users clear their browser cache to prevent permanent database corruption and to be sure that you are running the latest version of Cisco StadiumVision Director. Be sure to notify all users of the Cisco StadiumVision Director system to clear their browser cache before using the system after an upgrade.

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.

Tip You can also press Ctrl + Shift + Delete to open the Clear Recent History dialog box.

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**.

Importing the Security Certificate

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

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 3.2 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:

`https://`*`x.x.x.x`***`/StadiumVision/login.jsp`**

or alternatively,

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

The Cisco StadiumVision Director login screen appears .

Step 2 Verify that Version 3.2 is displayed.

Tip If your window is not displaying Version 3.2, be sure that you have cleared the browser cache as describe in the "Clearing the Browser Cache" section on page 25.

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.

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.

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 25.

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

Verifying that Services are Running

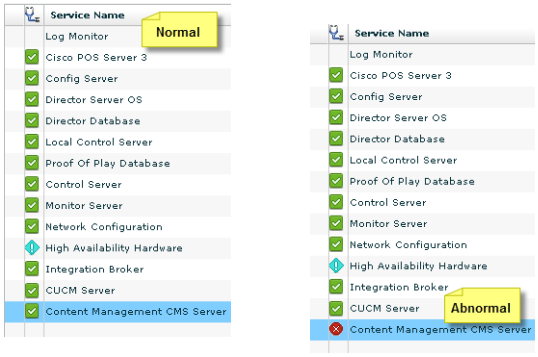
After you upgrade, go to the Management Dashboard to verify that all of the primary Cisco StadiumVision Director services are running.

To verify that services are running, complete the following steps:

Step 1 From the Management Dashboard, expand the Service Alerts pane.

Step 2 Verify that all of the primary services—in particular the Content Management CMS Server—are in "Normal" (green) state without any service alerts.

Figure 1 Verifying Normal Service States



Step 3 If the CMS server or another service in the above list is not in Normal state but should be, use the TUI services menu to restart it.

Configuring the DMP 4310 Assigned VLAN Property for VLAN Compliance Check

After you upgrade, 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.x.x 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.

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

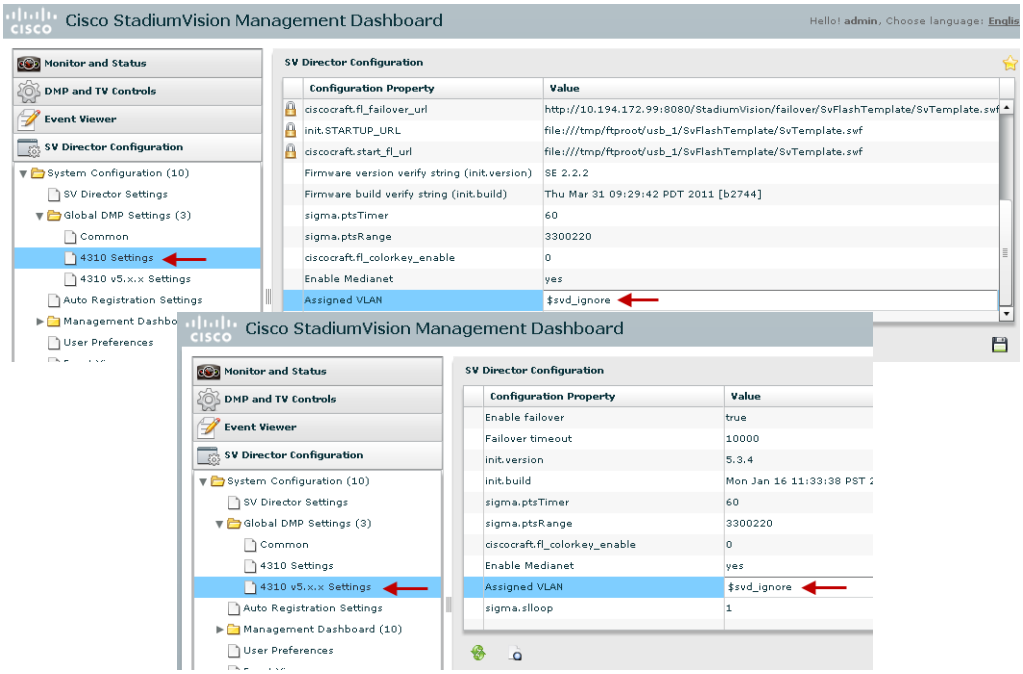
To configure the Assigned VLAN Property, complete the following steps:

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 2:

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

Figure 2 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 28.

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 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 and are in good health.

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

Step 5 (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 6 Run Get Status to check the DMP state after the change.

Step 7 Investigate any DMPs that are not in "Normal" state.

Verifying the Multicast Configuration

Cisco StadiumVision Director 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.

For more information about multicast configuration, see the "Configuring Multicast Ports for Cisco StadiumVision Director" topic in the "Configuring the Cisco StadiumVision Director Server System Settings" module of the *Cisco StadiumVision Director Server Administration Guide, Release 3.2*.

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.

Note Be sure to use the value that is configured in your Cisco Connected Stadium network and include the **:***port*. The recommended default is **:50001**.

Step 4 Click **Apply**.

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

Note This task is only required if you are using the Quest Point of Sale system.

The steps described in this section assume that Quest has the notification service installed and enabled.

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.

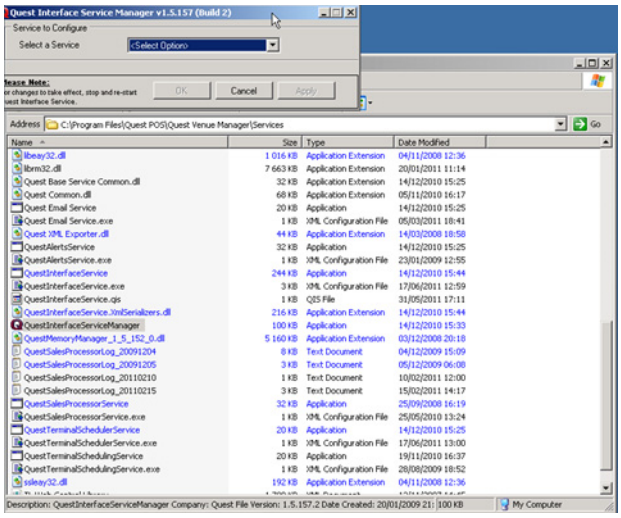
To set up the Quest Venue Manager to send updates to the Cisco StadiumVision Director server, complete the following steps:

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 3).

Figure 3 QuestInterfaceServiceManager Application



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

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

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

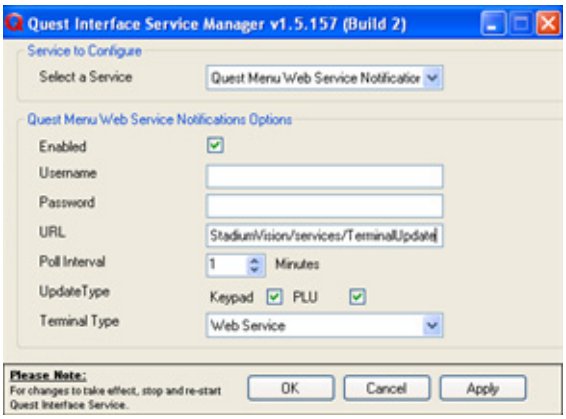
c. In the URL box, enter "**http://svd:8080/StadiumVision/services/TerminalUpdate**."

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 4 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 5).

Figure 5 Restart the Quest Interface Service