



Verifying the Upgrade

First Published: March 20, 2015

Revised: August 31, 2015

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

To verify the upgrade, complete the following tasks:

- [Clearing the Browser Cache, page 29](#) (mandatory)
- [Clearing Expired Flash SWZ Files From Browser, page 30](#) (required)
- [Importing the Security Certificate, page 32](#) (required)
- [Logging Into Cisco StadiumVision Director, page 32](#) (required)
- [Verifying the Control Panel and Other Menus, page 33](#) (required)
- [Verifying that Services are Running, page 33](#) (required)
- [Configuring the Media Player for VLAN Compliance Checking, page 34](#) (required)
- [Verifying Media Players, Groups, and Zones in the Management Dashboard, page 36](#) (required)
- [Verifying the Multicast Configuration, page 36](#) (required)
- [Setting Up the Quest Venue Manager to Send Updates to Cisco StadiumVision Director Server, page 37](#) (required if using Quest for commerce integration)
- [Completing the Post-Upgrade Checklist and Testing, page 39](#) (required)

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**.

Clearing Expired Flash SWZ Files From Browser

This section includes the following tasks:

- [Clearing the Flash Player Cache, page 30](#)
- [Deleting Other Cached Files From Flash, page 31](#)

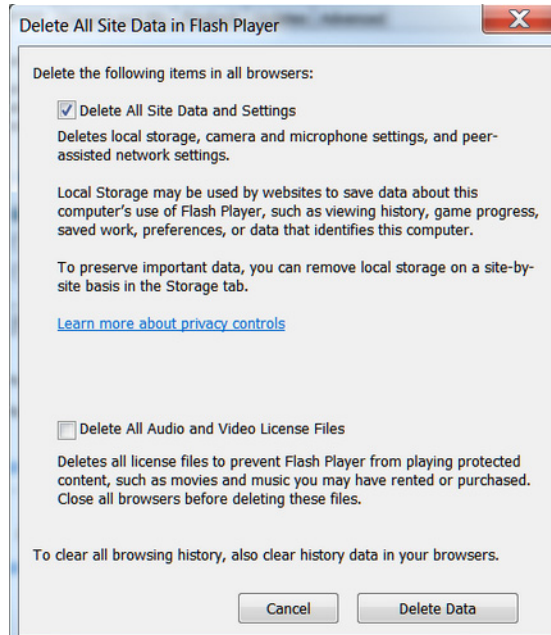
Clearing the Flash Player Cache

To clear the Flash player cache, complete the following steps:

Step 1 Go to **Control Panel > Flash Player**.

Step 2 In the Flash Player Manager Settings dialog box (Storage tab), click **Delete All**.

Step 3 Select Delete All Site Data and Settings ([Figure 1](#)).

Figure 1 Delete All Site Data in Flash Player Dialog Box—Windows Client Example

Step 4 Click **Delete Data**.

Deleting Other Cached Files From Flash

To delete other cached files from Flash, complete the following steps:

Step 1 Close the browser window.

Step 2 Delete cached files in the following paths for your browser application, and depending on your laptop client:

- From a Windows client:

- For Chrome

```
C:\Users\username\AppData\Local\Google\Chrome\User Data\Default\Pepper
Data\Shockwave Flash\CacheWritableAdobeRoot\AssetCache
```

- For Mozilla Firefox

```
C:\Users\username\AppData\Local\Mozilla\Firefox\Profiles
```



Tip

The AppData folder is a hidden folder in Microsoft Windows. If you cannot view it, go to **Control Panel > Folder Options** and verify the option is set to display hidden files and folders.

- From an Apple Mac OS X client:

- For Chrome

```
/Users/username/Library/Application Support/Google/Chrome/Default/Pepper
Data/Shockwave Flash/CacheWritableAdobeRoot/AssetCache/
```

- For Mozilla Firefox

`/Users/username/Library/Application Support/Firefox/Profiles/`

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 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 the correct version is displayed.



Tip If your window is not displaying the correct version, be sure that you have cleared the browser cache as describe in the [“Clearing the Browser Cache”](#) section on page 29.

- 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 29](#).

- 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 2 Verifying Normal Service States

Service Name	Status
Log Monitor	Normal
Cisco POS Server 3	Normal
Config Server	Normal
Director Server OS	Normal
Director Database	Normal
Local Control Server	Normal
Proof Of Play Database	Normal
Control Server	Normal
Monitor Server	Normal
Network Configuration	Normal
High Availability Hardware	Normal
Integration Broker	Normal
CUCM Server	Normal
Content Management CMS Server	Abnormal

- 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 Media Player for VLAN Compliance Checking

After you upgrade, you need to go to the Management Dashboard and change the Assigned VLAN property according to your VLAN configuration for the media players if you want to perform VLAN compliance checking.



Note

Setting the assigned VLAN property for the Cisco DMP 4310G or SV-4K media players is only recommended if all devices are located on the same VLAN. When a value is set, it is checked against what is being sent by the media player. Otherwise, you should configure `$svd_ignore`, which is the default.

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

- Step 1** From the Management Dashboard, go to **SV Director Configuration > System Configuration > Global DMP Settings**.
- Step 2** Do the following depending on your media player model:
- For the DMP 4310G—Go to **4310 v5.x.x Settings** (Figure 3).

Figure 3 Assigned VLAN Property Configuration for the Cisco DMP 4310G

Configuration Property	Value
Enable Syslog Service	on
Syslog Collector	10.194.172.154
Event Notification	no
ciscocraft.start_fl_alpha	0
ciscocraft.start_fl_fullscreen	true
ciscocraft.fl_fullscreen	true
ciscocraft.start_fl_input	true
init.STARTUP_URL	file:///tmp/ftproot/usb_1/SvFlashTemplate/S
ciscocraft.start_fl_url	file:///tmp/ftproot/usb_1/SvFlashTemplate/S
ciscocraft.fl_failover_url	http://10.194.172.154:8080/StadiumVision/f
Enable failover	false
Failover timeout	10000
init.version (DMP-4310)	5.4(1)RB(2P)
init.build	Mon Oct 6 07:03:30 PDT 2014 [b4652]
sigma.ptsTimer	60
sigma.ptsRange	3300220
ciscocraft.fl_colorkey_enable	0
Enable Medianet	yes
Assigned VLAN	\$svd_ignore

- For the SV-4K—Go to **SV-4K Settings** (Figure 4).

Figure 4 Assigned VLAN Property Configuration for the SV-4K

Configuration Property	Value
Standard Autorun Log Level	INFO
Standard Runtime Log Target	CONSOLE
Standard Runtime Default Log Level	INFO
Standard Runtime Override Log Levels	
Subset Logging Addresses	
Subset Autorun Log Level	INFO
Subset Runtime Log Target	CONSOLE
Subset Runtime Default Log Level	INFO
Subset Runtime Override Log Levels	
Maximum Pool Size (MB)	112640
Content sync multicast address	239.193.0.253
Content sync multicast port	50001
SV-4K sync content transition delay	200
init.version (SV-4K)	5.1.37.12
Runtime startup delay (seconds)	0
NTP Host	10.194.172.154
NTP sync interval	3600
Timezone	GMT
Closed caption standard.	NTSC_ATSC
Assigned VLAN	\$svd_ignore
Zone Based Synchronization	true

Step 3 Find the Assigned VLAN property, and do the following:

- If all of your DMPs are located on the same VLAN (recommended)—Type the number of the VLAN.
- If all of your DMPs are not located on the same VLAN, or you want to bypass any VLAN compliance checking—Type “\$svd_ignore.”

**Caution**

Cisco DMP 4310 auto-registration support requires that the VLAN value is correctly set or “\$svd_ignore” is used.

Step 4 Click the Save icon.

Verifying Media Players, Groups, and Zones in the Management Dashboard

**Note**

Before you verify media player status, be sure that you have set the Assigned VLAN property so that the VLAN compliance check can be performed. For more information, see the [“Configuring the Media Player for VLAN Compliance Checking”](#) section on page 34.

To check media players, 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 media players are present and in the green state.

Step 2 From the DMP and TV Controls dashboard drawer, run the Get Status command on all devices to update Cisco StadiumVision Director’s record of MAC addresses:

DMP and TV Controls > Monitoring > Get Status.

Step 3 Run Get Status to confirm that all devices have successfully rebooted and are in good health.

**Note**

This will also update the MAC address for the media players.

Step 4 (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 5 Run Get Status to check the device state after the change.

Step 6 Investigate any devices 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 4.0](#).

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.

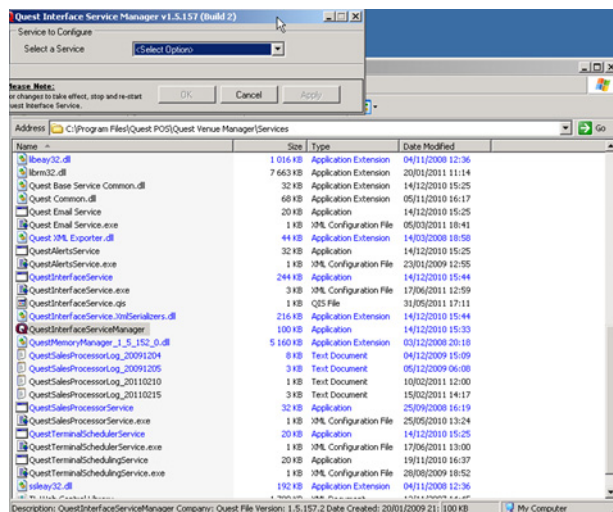
The steps described in this section assume that Quest has the notification service installed and enabled.

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 5).

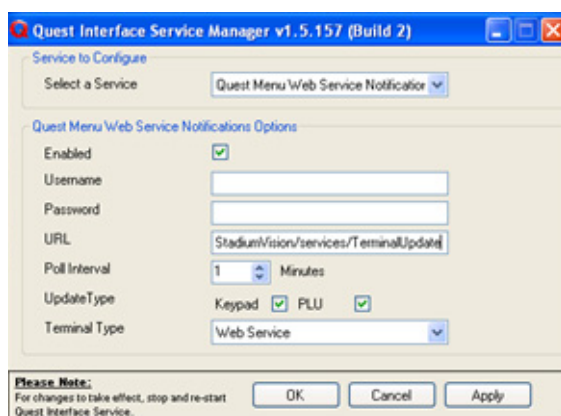
Figure 5 *QuestInterfaceServiceManager Application*



Step 4 When the Quest Interface Service Manager application window opens, specify the following options (Figure 6):

- 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 6 *Select a Service to Configure*



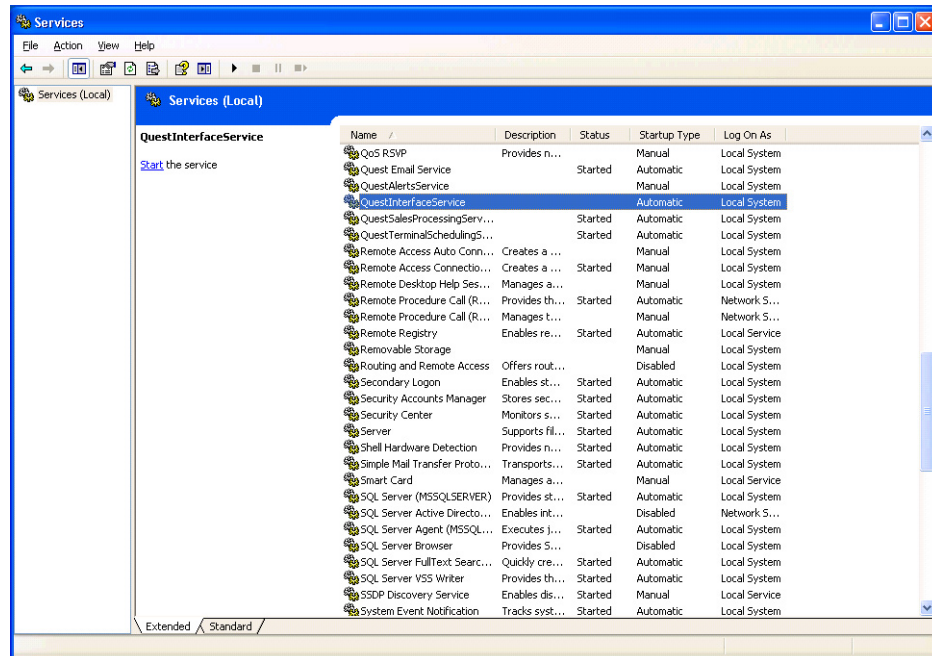
Step 5 Click **OK**.

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

- a. From the Quest Server, click **Start > Run...**
- b. When the Run dialog box opens, type “**services.msc**”.

- c. Find the Quest Interface Service and restart it (Figure 7).

Figure 7 Restart the Quest Interface Service



Completing the Post-Upgrade Checklist and Testing

Use the “[Appendix A: Post-Upgrade Checklist](#)” module on page 63 to be sure that you have completed the required verification steps.

