### · I | I · I | I · CISCO .

## Verifying the Upgrade

#### First Published: 2018-07-10

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 31 (required)
- Logging Into Cisco Vision Dynamic Signage Director, page 32 (required)
- Verifying the Control Panel and Other Menus, page 32 (required)
- Verifying that Services are Running, page 32 (required)
- Configuring the Media Player for VLAN Compliance Checking, page 33 (required)
- Upgrading the DMP Firmware, page 34 (required)
- Rebooting the DMPs, page 35 (required)
- Verifying Media Players, Groups, and Zones in the Management Dashboard, page 35 (required)
- Verifying the Multicast Configuration, page 36 (required)
- Completing the Post-Upgrade Checklist and Testing, page 36 (required)

### Clearing the Browser Cache

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

#### To clear the browser cache in Mozilla FireFox:

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

The Clear Recent History dialog box appears.

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

- 2. In the "Time range to clear:" box, select Everything.
- 3. Open the Details drop-down list and select the Cache checkbox if it does not have a checkmark.
- 4. Click Clear Now.

Clearing Expired Flash SWZ Files From Browser

### 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:

- 1. Go to Control Panel > Flash Player.
- 2. In the Flash Player Manager Settings dialog box (Storage tab), click Delete All.
- 3. Select Delete All Site Data and Settings (Figure 1 on page 30).

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

Delete All Site Data in Flash Player
Delete the following items in all browsers:
Delete All Site Data and Settings
Deletes local storage, camera and microphone settings, and peer- assisted network settings.
Local Storage may be used by websites to save data about this computer's use of Flash Player, such as viewing history, game progress, saved work, preferences, or data that identifies this computer.
To preserve important data, you can remove local storage on a site-by- site basis in the Storage tab.
Learn more about privacy controls
Delete All Audio and Video License Files
Deletes all license files to prevent Flash Player from playing protected content, such as movies and music you may have rented or purchased. Close all browsers before deleting these files.
To clear all browsing history, also clear history data in your browsers.
Cancel Delete Data

4. Click Delete Data.

Importing the Security Certificate

### Deleting Other Cached Files From Flash

#### To delete other cached files from Flash:

- 1. Close the browser window.
- 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

**Note:** 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 Vision Dynamic Signage Director server for the first time using Mozilla Firefox, a security certificate warning appears. Some Cisco Vision Dynamic Signage Director functionality requires that the certificate is imported.

### Adding a Security Exception for Mozilla Firefox

#### To add the security exception for Mozilla Firefox:

- 1. When you see the warning page with the title "This Connection is Untrusted," click the "I Understand the Risks" option.
- 2. Click Add Exception....
- 3. In the Add Security Exception dialog box, click Confirm Security Exception.
- 4. Close all Mozilla Firefox windows.

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

### Logging Into Cisco Vision Dynamic Signage Director

#### To verify that the upgrade was successful and that Cisco Vision Dynamic Signage Director is up and operating:

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

https://x.x.x.x/CiscoVision/login.html

or alternatively,

http://x.x.x.x

The Cisco Vision Dynamic Signage Director login screen appears.

2. Type your Cisco Vision Dynamic Signage Director administrator login credentials and click Log In.

**Note:** When you first log into Cisco Vision Dynamic Signage Director, the default administrator username and password is *admin*.

The Cisco Vision Dynamic Signage Director Asset Library screen appears.

3. Verify that the correct version displays in the upper left of the screen.

**Note:** If your window does not display the correct version, clear the browser cache as described in Clearing the Browser Cache, page 29.

### Verifying the Control Panel and Other Menus

#### To verify the control panel:

- From the Cisco Vision Dynamic Signage Director Main Menu, go to Tools > Control Panel. After a few moments of loading resources, the Cisco Vision Dynamic Signage Director Control Panel Setup screen opens in a new window.
- 2. Confirm the version and build number of your Cisco Vision Dynamic Signage Director software in the upper left of the Library (Main Menu) screen.

**Note:** If your window does not display the appropriate version and build that you loaded, clear the browser cache as describe in Clearing the Browser Cache, page 29.

3. Verify that you can open the other Cisco Vision Dynamic Signage Director screens and menus.

### Verifying that Services are Running

After you upgrade, go to **Tools > Management Dashboard** to verify that all of the primary Cisco Vision Dynamic Signage Director services are running.

#### To verify that services are running:

- 1. Go to Tools > Management Dashboard > Monitor and Status drawer > Services folder.
- 2. Expand the Service Alerts pane.
- 3. Verify that all of the primary services—in particular the Content Management CMS Server—are in "Normal" (green) state without any service alerts.

Configuring the Media Player for VLAN Compliance Checking



 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. See

### Configuring the Media Player for VLAN Compliance Checking

After you upgrade, 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:** We recommend setting the assigned VLAN property for the media players 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, configure **\$svd\_ignore**, which is the default.

#### To configure the Assigned VLAN property

- 1. Go to Tools > Management Dashboard > Dynamic Signage Director Configuration > System Configuration > Global DMP Settings.
- 2. Do the following, depending on your media player model:

Upgrading the DMP Firmware

🛃 Honitor and Status	Dynamic Signage Director Configuration	Q	
B DMP and TV Controls	Configuration Property	Value	10
V Event Viewer	LLOP enabled	true	*
A MANDON A STATUT	LLOP delay (seconds)	15	
Dynamic Signage Director Config	Start SNMP Agent Service	no	
🕈 🛅 System Configuration (12)	Content sync multicast address	239.193.0.253	
🕨 🧰 Dynamic Signage Director Setting	Content sync multicast port	50218	1
Y 🛅 Global DMP Settings (6)	Assigned VLAN	Bavd_ignore	
Networking	Global SSID		1
Audio/Video/Closed Caption	wifi Passphrase		
Firmware Versions	Proxy URL		E
Time Source	Proxy bypass addresses		•

### Figure 3 Assigned VLAN Property Configuration for the CV-UHD and SV-HD DMPs

Go to SV-DMP Common Settings (Figure 4 on page 34).

#### Figure 4 Assigned VLAN Property Configuration for the SV-4K and DMP-2K

8 DMP and TV Controls	Dynamic Signage Director Configuration	<u>8</u>	
DMP and TV Controls	Configuration Property	Value	
J Event Viewer	LLDP enabled	true	
Dynamic Signage Director Configu	LLDP delay (seconds)	15	
System Configuration (12)	Start SIMP Agent Service	ns	
Dynamic Signage Director Setting	Content sync multicast address	239,190.0.253	
v 🔁 Global DMP Settings (6)	Content sync multicast port	50001	
Networking	Assigned VLAN	\$evd_lanare	
Audie/Video/Closed Caption	Global SSID		
C Firmiuare Versions	Wifi Passphrase		
Time Source	Proxy URL		
Storage and Cache	Proxy bypass addresses		
C) Runtime Behavior			
Auto Registration Settings (2)	1.00		
Management Dashboard (10)	100 CO.		

- 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."
- 4. Click the Save icon.

### Upgrading the DMP Firmware

Verify whether your DMPs require a firmware upgrade and follow the steps in the corresponding modules of this guide to upload and install the required version(s) for your Cisco Vision Dynamic Signage Director release.

**Note:** If this is the initial upgrade of your system to Cisco Vision Dynamic Signage Director Release 6.1 software, a new firmware upgrade and configuration for the firmware is required. Follow the steps in Upgrading the DMP Firmware, page 37.

### Rebooting the DMPs

After an upgrade of the Cisco Vision Dynamic Signage Director software, restart the DMP to get the latest version of the runtime software.

- If this is the initial upgrade of your system to Release 6.1 and you performed a DMP firmware upgrade, then the DMPs already rebooted. Do not reboot the DMPs.
- If this an upgrade from Release 6.0 to Release 6.1 without a DMP firmware upgrade, then reboot the DMP to update the DMP's runtime software.

To verify the system runtime on the DMP, see Verifying Media Players, Groups, and Zones in the Management Dashboard, page 35.

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

**Note:** Before you verify media player status, set the Assigned VLAN property so that the VLAN compliance check can be performed. For more information, see Configuring the Media Player for VLAN Compliance Checking, page 33.

To check media players, groups, and zones after you upgrade your software:

- Go to Tools > Management Dashboard and verify that all of your groups, zones and media players are present and in the green state.
- From the DMP and TV Controls drawer, run the Get Status command on all devices to update Cisco Vision Dynamic Signage Director's record of MAC addresses:

#### DMP and TV Controls > Monitoring > Get Status.

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

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

- 4. Verify that the correct Cisco Vision Dynamic Signage Director runtime version is loaded on the DMP:
  - a. Select the DMP(s) that you want to verify. Click the Play icon.
  - b. Go to Status > Status Details.
  - c. In the DMP Status panel, expand the Runtime status and verify the Version reported.

#### Verifying the Multicast Configuration

-	Select Devices				92	_			2.
EMP and TV Centrols					Location		1P Address	NAC Address	Made
Maniformg .	Dense and Ontuge Dense and Ontuge Dense (4) Dense (4)		1	and the second sec	Despis 12 41		10.134.109.242	Minuted Children	De-la
Led Status			× 80°		Concernance of the second		10.194.169.241	9014-131-04-00-44	BU-65
- One				Inergia 42 42(64)		10.154.168.179	M-4-31-07-91-04	249-2	
Calif Commands				and the second second	Draipha 176A	A STREET AND A STREET AND A STREET A	10.294.169.247		000
Canada Strategia			-		trading to be		11.134.011.041	summer prive de las.	
C3 To Commanda									
Auto Registration			<b>`</b>						
2 Suchth Commands									
Command: Get Status									
The Gel Blatas command retrieves detail	1		•	1.1.1		-			-
-		* 0				24	iner a being	el el 🖌 🗴	-
	Ra Status	Sattinga 📷 Dia	ijla	Admin	- 10 mar	di	T. Consule	to System 24	Carright .
	Status Details	DHP Status		43	10 0	TV SI	lature .	E (1	. 1
		100000					etch.		
÷	Militation	P Plaatin			1.1				
6	Events	P Peaks			1.1				
S V Count Viewer	Events Uptone	T Rationa			1				
🕏 🌶 Event Verser 🔁 Dynamik Rignage Director Cavitys	Events		_	rial J build 528	-	1 + 10			

- 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.
- 6. Run Get Status to check the device state after the change.
- 7. Investigate any devices that are not in "Normal" state.

### Verifying the Multicast Configuration

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

The multicast group address for Cisco Vision Dynamic Signage Director is configured in the "MulticastHostPort" registry.

For more information about multicast configuration, see the "Configuring Multicast Ports for Cisco Vision Director" topic in the "Configuring the Cisco Vision Director Server System Settings" module of the Cisco Vision Server Administration Guide: Dynamic Signage Director.

To verify or configure the multicast addressing for Cisco Vision Dynamic Signage Director:

- 1. Go to Tools > Management Dashboard. Select Tools drawer > Advanced > Registry.
- 2. Scroll to the "MulticastHostPort" registry key in the Parameters list and confirm the entry for the registry.
- 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**.

4. Click Apply.

### Completing the Post-Upgrade Checklist and Testing

Use Appendix A: Post-Upgrade Checklist, page 43 to verify you completed the required steps.