Verifying the Upgrade

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)
- Importing the Security Certificate, page 30 (required)
- Logging Into Cisco Vision Dynamic Signage Director, page 31 (required)
- Verifying the Menus, page 31 (required)
- Verifying that Services are Running, page 31 (required)
- Configuring the Media Player for VLAN Compliance Checking, page 32 (required)
- Upgrading the DMP Firmware, page 33 (required)
- Rebooting the DMPs, page 33 (required)
- Verifying Media Players, Groups, and Zones in the Device Management, page 33 (required)
- Verifying the Multicast Configuration, page 34 (required)
- Completing the Post-Upgrade Checklist and Testing, page 34 (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. 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: Or 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**.

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.

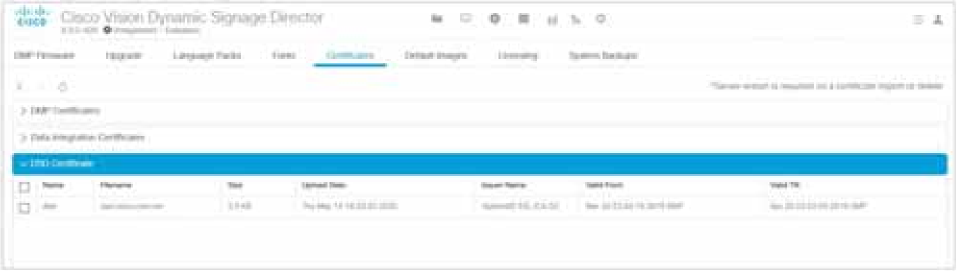
DSD Certificate Import

Manage certificates for Cisco Vision Dynamic Signage Director (DSD) with the Software Manager interface. It eliminates untrusted browser warnings from popping up. This features allows you to import your own DSD certificate so that the annoying security warning goes away. These certificates types .cer, .crt and .pem are supported.

To import DSD certificates:

1. Click **More > Manage Software > DSD Certificate** (Figure 1 on page 30).
2. Click the **Upload** icon. The Certificate Upload dialog box appears.

Figure 1 Import DSD Certificate



3. Choose a Certificate Name file.
4. Choose a Private Key file.
5. Click **Upload**. If successful, a success message displays.

   For details on using this new feature, refer to Release 6.3: Cisco Vision Dynamic Signage Director System Administration Guide.

Note: After uploading the certificate, restart the DSD web server for the new certificate to take effect. Use a TUI.

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 is *admin* and password is *C-V1$i0n*.

   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 Menus

To verify menus:

1. From the Cisco Vision Dynamic Signage Director **Main Menu**, click the new icon for **System Configuration**. After a few moments of loading resources, the Cisco Vision Dynamic Signage Director 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 described 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 installing or upgrading to Release 6.3, verify and confirm the update and virtual machine profile of the Dynamic Signage Director configuration from TUI.

After you upgrade, verify that all of the primary Cisco Vision Dynamic Signage Director services are running.

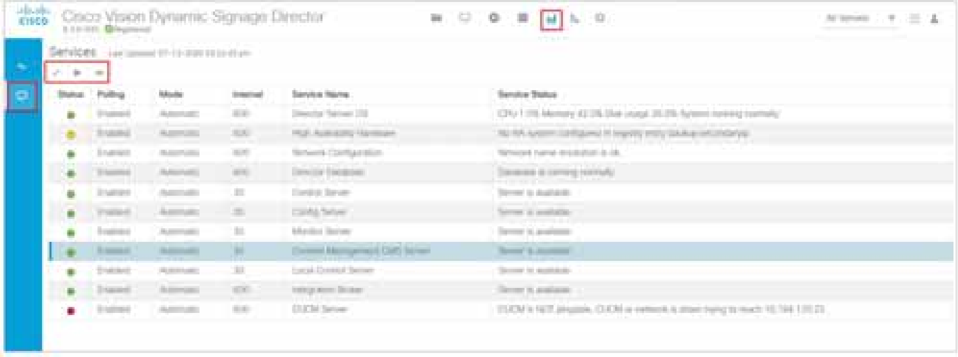
To verify that services are running:

1. Click to **System Status > Monitor and Status**.

2. The **Services** panel appears (Figure 2 on page 32).

3. 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



Cisco Vision Dynamic Signage Director

Services

Status	Polling	Mode	Interval	Service Name	Service Status
●	Enabled	Automatic	[illegible]	Director Server (3)	CPU 1.1% Memory 42.3% Disk usage 35.0% System running normally
●	Enabled	Automatic	[illegible]	High Availability Hardware	No HA system configured in registry entry [illegible]
●	Enabled	Automatic	[illegible]	Network Configuration	Network name resolution is ok.
●	Enabled	Automatic	[illegible]	Director Database	Database is running normally
●	Enabled	Automatic	[illegible]	Control Server	Server is available
●	Enabled	Automatic	[illegible]	Config Server	Server is available
●	Enabled	Automatic	[illegible]	Monitor Server	Server is available
●	Enabled	Automatic	[illegible]	Content Management (CMS) Server	Server is available
●	Enabled	Automatic	[illegible]	Local Control Server	Server is available
●	Enabled	Automatic	[illegible]	Integration Broker	Server is available
●	Enabled	Automatic	[illegible]	CUCM Server	CUCM is NOT pingable. CUCM or network is down trying to reach [illegible]

4. 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. Go to **Main Menu > Services Control > Content Management System (cms)**.

Configuring the Media Player for VLAN Compliance Checking

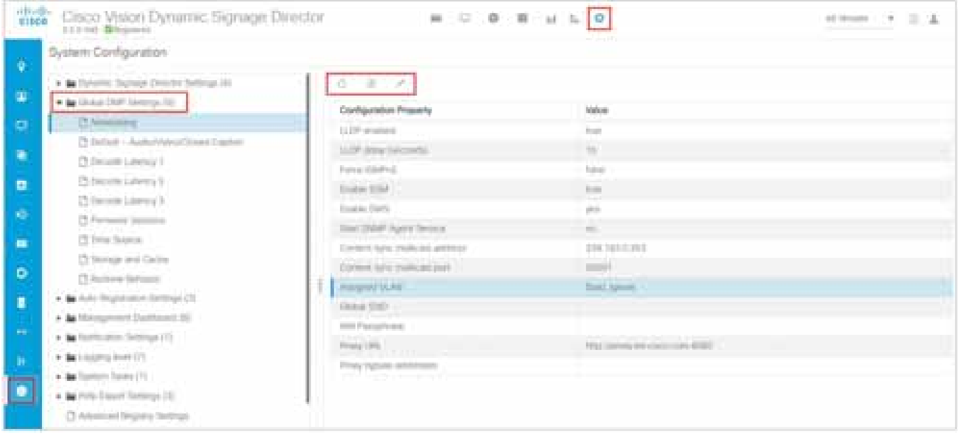
After you upgrade, change the Assigned VLAN property according to your VLAN configuration for the media players if you want to perform VLAN compliance checking.

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. Click **Configuration > System Configuration > Global DMP Settings > Networking.**

Figure 3 Assigned VLAN Property Configuration for the DMPs



Cisco Vision Dynamic Signage Director

System Configuration

- Dynamic Signage Director Settings (4)
- Global DMP Settings (9)
  - Networking
  - Default - Audio/Video/Closed Caption
  - Decode Latency 1
  - Decode Latency 5
  - Decode Latency 3
  - Firmware Versions
  - Time Source
  - Storage and Cache
  - Reclaim Behavior
- Auto Registration Settings (3)
- Management Dashboard (6)
- Notification Settings (1)
- Logging level (7)
- System Tasks (1)
- PoPs Export Settings (3)
- Advanced Registry Settings

Configuration Property	Value
LLDP enabled	true
LLDP delay (seconds)	15
Force IGMPv2	false
Enable SSM	true
Enable DAPS	yes
Start DNMP Agent Service	no
Content Sync multicast address	239.193.0.253
Content Sync multicast port	50001
Assigned VLAN	$svd_ignore
Global SSID	
Wifi Passphrase	
Proxy URL	http://proxy-wsa.esl.cisco.com:80
Proxy bypass addresses	

2. Find the Assigned VLAN property.

3. Click **Edit**. The Edit Configuration Setting dialog box appears. Do one the following:

- If all of your DMPs are located on the same VLAN (recommended)—Type the number of the VLAN in the **Value** field.

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

4. Click **Save**.

Upgrading the DMP Firmware

IMPORTANT: All DMPs require a firmware upgrade for Release 6.3.

If this is the initial upgrade of your system to Cisco Vision Dynamic Signage Director Release 6.3 software, a new firmware upgrade and configuration for the firmware is required. Go to the chapter Upgrading the DMP Firmware, page 35.

Rebooting the DMPs

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

- If this is the initial upgrade of your system to Release 6.3 and you performed a DMP firmware upgrade, then the DMPs already rebooted. Do not reboot the DMPs.
- If this is an upgrade from Release 6.2 to Release 6.3, 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 Device Management, page 33.

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

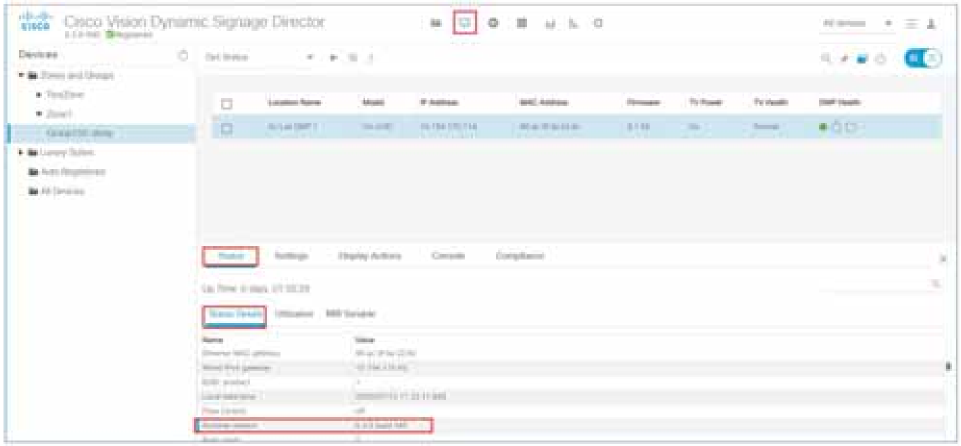
Note: Before you verify media player status, set the Assigned VLAN property so that the VLAN compliance check can be performed. For more information, see Configuring the Media Player for VLAN Compliance Checking, page 32.

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

1. Click **Device Management** and verify that all of your groups, zones and media players are present and in the green state.
2. Run the **Get Status** command on all devices to update and confirm that all devices successfully reboot and are in good health.

   Note: This will also update the MAC address for the media players.
3. 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. Scroll to the Runtime version and verify the Version reported (Figure 4 on page 34).

Figure 4 Device Status Details in Device Management



4. (Optional) Change the DMP State of healthy DMPs to “Production” using the Command pull-down menu: **Change DMP State**.
5. Run **Get Status** to check the device state after the change.
6. 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. Click **Configuration > System Configuration > Advanced Registry Settings**.
2. Scroll to the “MulticastHostPort” registry key in the list and confirm the entry for the registry.
3. To change the value, click **Edit**. The Edit Configuration Settings dialog box appears.
4. In the **Value** field, 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**.
5. Click **Save**.

Completing the Post-Upgrade Checklist and Testing

Use Appendix A: Post-Upgrade Checklist, page 49 to verify you completed the required steps.