



Monitoring and Maintaining the Digital Media Player

Series 2 DMPs: DMP-2K and SV-4K

Series 3 DMPs: CV-HD and CV-UHD

Series 4 DMPs: CV-HD2 and CV-UHD2

This module describes the workflow and tasks to monitor and maintain the working operation of the digital media player. It is intended for Cisco Vision Dynamic Signage Director administrators and installers.

For more information, see also the [Release 6.4: Cisco Vision Dynamic Signage Director Operations Guide](#).

This module includes the following topics:

- [Performing a Regular Reboot of the Digital Media Players, page 65](#)
- [Verifying Digital Media Player Compliance, page 65](#)
- [Management Information Base \(MIB\) Variables, page 67](#)
- [Clearing the Storage on the Digital Media Player, page 68](#)
- [Clearing Registries on the Digital Media Player by Restoring Factory Defaults, page 69](#)
- [USB and SD Card Restrictions on DMPs, page 69](#)

Performing a Regular Reboot of the Digital Media Players

Perform a regular reboot of the devices to maintain normal operation of the digital media players. We recommend a weekly reboot.

For information about how to configure the Reboot DMP system task, see the [Task Note: Configure Reboot DMPs](#).

Note: The reboot task applies globally to all media player devices. It is not enabled by default.

Verifying Digital Media Player Compliance

Cisco Vision Director allows you to compare values on the DMP device against required values configured in the Cisco Vision Dynamic Signage Director DMP settings.

[Figure 1 on page 66](#) shows how a DMP device should appear when it is fully compliant with the configured Cisco Vision Dynamic Signage Director settings:

- Required Value—Value configured in Cisco Vision Dynamic Signage Director, or automatically set by the system.

Verifying Digital Media Player Compliance

- Value on Device—Setting that the DMP device is running.

Figure 1 Normal Compliance for a DMP Device

Name	Required Value	Value on Device
✓ dwsEnabled	yes	yes
✓ init.DHCP	on	on
✓ init.startService_ntpc	yes	yes
✓ init.startService_snmp	yes	yes
✓ ntpc.hostname	1.ntp.esl.cisco.cor	1.ntp.esl.cisco.com
✓ ntpc.interval	3600	3600
✓ ntpc.timezone	PST	PST
msi.sw_vlan	\$svd_ignore	225
✓ use_igmp_v2	false	false
✓ init.version	8.0.72	8.0.72

Table 1 DMP Compliance Property Descriptions

Property Name	Description
dwsEnabled	Enables ability to access the DMPs Diagnostic Web Server. ¹
init.DHCP	Value is always “on.” Static IP addresses are not supported.
init.startService_ntpc	NTP client service on the DMP device. Value is always “yes.”
init.startService_snmp	(Release 4.1 and Later) SNMP agent service on the Series 2 and Series 3 device. Default value is no.
init.version	DMP firmware version.
ntpc.hostname	Name of the NTP server for the DMP. For PTP secondaries, setting the time via NTP is disabled on DMP.
ntpc.interval	Interval (in seconds) after which the PTP leader synchronizes its time with the NTP host.
ntpc.timezone	Timezone for the DMP.
msi.sw_vlan	Switch VLAN reported by LLDP for the DMP. “\$svd_ignore” setting in Dynamic Signage Director means that the value is not used for compliance verification.
use-igmp_v2	This corresponds to the global DMP setting “Force IGMPv2” (under Networking).

- The global DMP setting “Enable DWS” (under Networking) should match what the DMP reports. It is possible for a DMP to report a value different from the registry key. This can happen when DWS is enabled or disabled via DMP Command.

To verify digital media player compliance:

- Click **Device Management**.
- In the **Selected Devices** panel, select all DMPs about which you want an updated status. The lower **Status** pane appears.
- Click the **Compliance** tab.

Management Information Base (MIB) Variables

To get to Cisco MIB data:

1. Use an FTP client program to go to ftp.cisco.com.
2. Log in and use anonymous as the user name and your email address as the password.
3. Issue the **cd /pub/mibs** command to change directories to /pub/mibs/v2.

Note: If you encounter any problems, try to log in with a minus sign (-) as the first character of your password. This turns off a feature that might be confusing your FTP client program. To download files from Cisco.com, you must use a passive-mode-capable FTP client. Contact your systems administrator to obtain one.

Send any questions, comments, or problem reports about FTP-related issues to Cisco.com Feedback.

The following table lists the DMP MIBs currently supported.

Table 2 MIBs for the DMP

Source	Value
Disk	.1.3.6.1.4.1.2021.9.1.2 => disk identifier
	.1.3.6.1.4.1.2021.9.1.6.1 => Total size
	.1.3.6.1.4.1.2021.9.1.7.1 => Available space
	.1.3.6.1.4.1.2021.9.1.8.1 => Used space
	.1.3.6.1.4.1.2021.9.1.9.1 => Percentage of space
TV Status	.1.3.6.1.4.1.9.9.1051.3.1 => TV status
Memory	.1.3.6.1.4.1.2021.4.5.0 => Total RAM
	.1.3.6.1.4.1.2021.4.6.0 => RAM used
Network	.1.3.6.1.4.1.9.9.1051.3.4.1 => NIC names
	.1.3.6.1.4.1.9.9.1051.3.4.2 => Get Bytes IN
	.1.3.6.1.4.1.9.9.1051.3.4.3 => Get Bytes OUT
	.1.3.6.1.4.1.9.9.1051.3.4.4 => Packet counter
	.1.3.6.1.4.1.9.9.1051.3.4.5 => Packet error counter
CPU	.1.3.6.1.4.1.2021.11.9.0 => Percentage of user CPU time
	.1.3.6.1.4.1.9.9.1051.3.5.1 => Raw user CPU time
	.1.3.6.1.4.1.2021.11.11.0 => Percentages of idle CPU time
	.1.3.6.1.4.1.9.9.1051.3.5.2 => Raw idle CPU time
NTP Sync Status	.1.3.6.1.4.1.9.9.1051.3.2 => NTP sync status
PTP	.1.3.6.1.4.1.9.9.1051.3.3.1 => PTP sync status (freerun/master)
	.1.3.6.1.4.1.9.9.1051.3.3.2 => Master or slave
	.1.3.6.1.4.1.9.9.1051.3.3.3=> Deviation

Clearing the Storage on the Digital Media Player

The DMP devices have different sizes of local storage:

- The CV-HD2 DMPs have 128 GB of storage with approximately 100 GB available for content.
- The CV-UHD2 DMPs have 128 GB of solid-state storage with approximately 100 GB available for content.
- The SV-4K and Series 3 DMPs have 120 GB of solid-state storage with approximately 100 GB available for content.
- The DMP-2K DMPs have 64 GB of solid-state storage with approximately 53 GB available for content.

If you are running out of storage or need to recover the SSD, clear the storage on the media player.

To find information about available storage:

1. Select a DMP device in the **Device Dashboard** device list.
2. Click the **Settings** tab > **Storage** in the device details area of the dashboard.

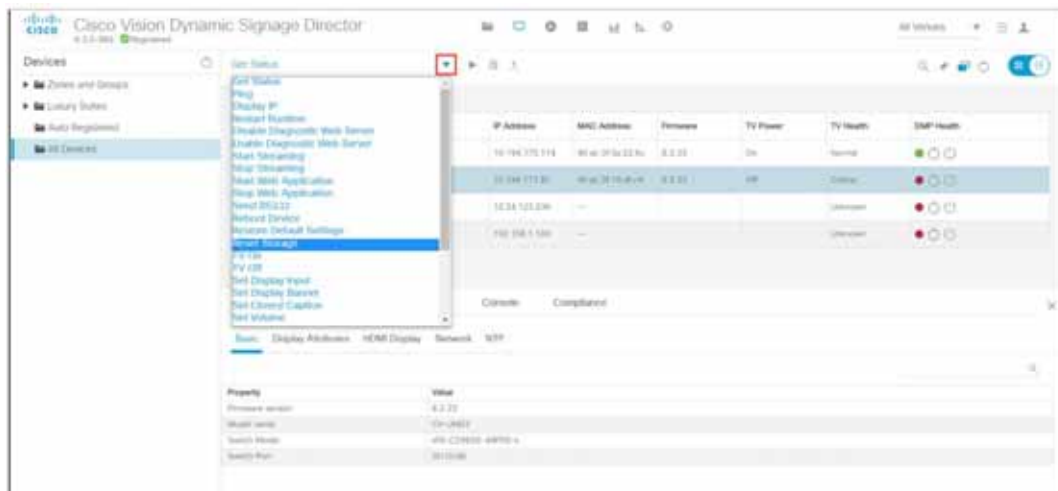
Note: The HTML runtime must be running on the digital media player to use this task.

You also can find information about available storage if you view device details from thumbnail view in **Device Management (CCM)**.

To clear the storage on the digital media player:

1. Click **Device Management**.
2. Select the DMP devices that you want to clear.
3. Use the drop-down arrow to select **Reset Storage** (Figure 2 on page 68).

Figure 2 Reset Storage Command



4. Click **Send Command**.

The contents of the SSD storage is removed (including the Cisco Vision Dynamic Signage Director runtime software and script contents) on the devices. The devices will not automatically reboot after this command.

5. Use the drop-down arrow to select **Reboot Device** (Figure 2 on page 68).

6. Click **Send Command**.

The selected devices reboot and re-provision firmware and settings.

Clearing Registries on the Digital Media Player by Restoring Factory Defaults

To clear the registries on the digital media player:

1. Click **Device Management**.
2. Select the devices that you want to clear.
3. Use the drop-down arrow to select **Restore Default Settings** (Figure 2 on page 68).
4. Click **Send Command**.
5. Any persistent device settings on the DMPs are erased and the box will be in factory default state. The DMP automatically reboots and re-provisions its firmware and settings.

USB and SD Card Restrictions on DMPs

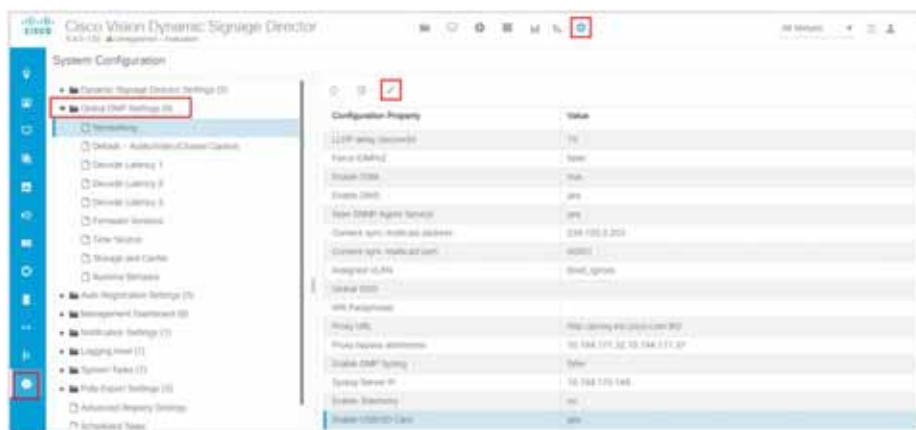
Release 6.4 introduces the ability to enable or disable the USB or SD card on groups or a single DMP using a new command in **Device Management**. For the command to work, we added a new registry to set in the **System Configuration** interface. The default is USB/SD card enabled.

Note: The CV-HD2 DMP has a micro SD card and this command is not supported.

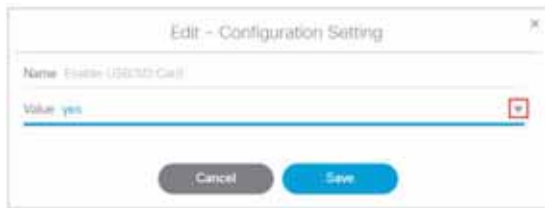
To set the Compliance Value to Enable USB/SD card registry:

1. Click **Configuration > System Configuration > Global DMP Settings > Networking** (Figure 3 on page 69).

Figure 3 Enable USB/SD Card Registry



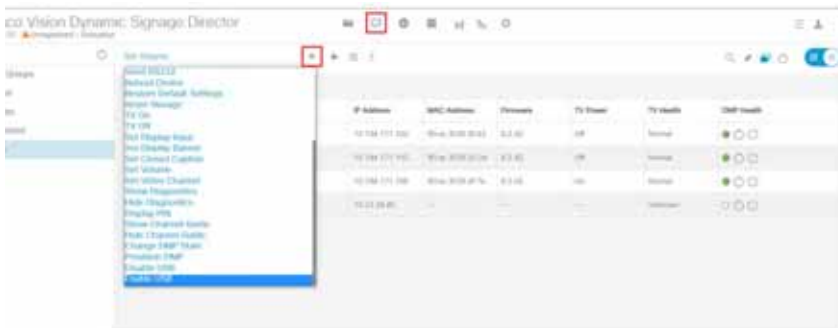
2. Click the **Enable USB/SD Card** property.
3. Click **Edit**. The Edit - Configuration Setting dialog box appears (Figure 4 on page 70).
4. Set the **Value** to **Yes**.
5. Click **Save**.

Figure 4 Enable USB/SD Card on the DMPs

This sets the compliance value to enable the USB/SD cards on all the DMPs, making them able to accept a Command from **Device Management**.

To enable the USB/SD Cards on specific DMPs:

1. Click **Device Management** and navigate to a DMP in the folders such as **Zones and Groups**.
2. Select the DMPs on which you want to act.
3. Click the down arrow in the Action Box. Scroll to the bottom of the list ([Figure 5 on page 70](#)).

Figure 5 Device Management Interface

4. Click **Enable USB** or **Disable USB**.
5. Click **Play (Send Command)**. The Send Command dialog box appears telling you how many DMPs are selected and that action will execute.

Note: When you run the **Enable** or **Disable the USB/SD Card** command, the selected DMPs reboot.

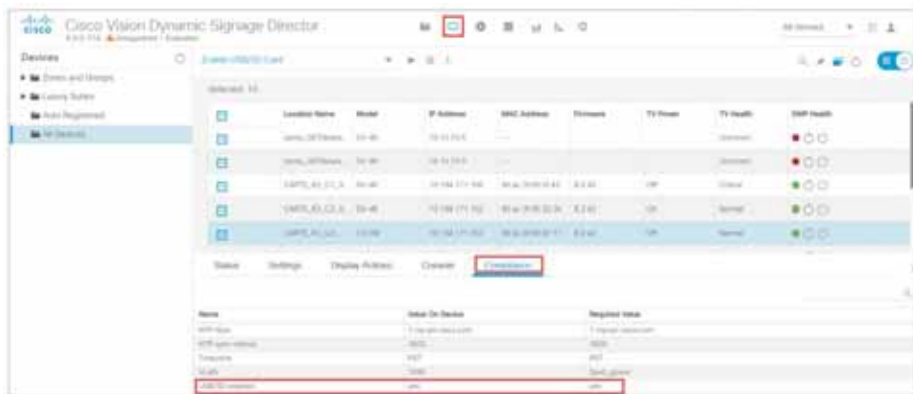
6. Click **OK** to execute command.

Check the enable/disable status of your command in the **Compliance** tab.

7. With a DMP selected in the list above, click **Compliance**. Verify the setting and values match ([Figure 6 on page 71](#)).

If the values do not match, Director notifies you that you are non-compliant for that DMP.

Figure 6 Check Compliance Values



Note: The **Value on the Device** field is the individual DMP value. The **Required Value** field comes from the global setting. If they don't match, a pale red highlighted region shows in the **Compliance** tab. The global setting only takes effect if you provision the DMPs. So if you set the global DMP value to Enable USB/SD Card, but change an individual DMP USB setting here to Disable USB/SD Card in **Device Management**, even though the DMP reboots, it will revert back to the global DMP setting *until* you reprovise the DMP.

