Configuring the Cisco Vision Director Server System Settings

This document is intended for System Administrators and describes how to configure the initial setup of the Cisco Vision Director server.

New Deployment Options

New in Release 6.3: two more options of Cisco Vision Director server deployment–the Mini Deployment and the Large Deployment.

Table 1   Cisco Vision Director Server Deployments Available

| Configuration	RAM	CPU Clock Speed	vCPU Count
Mini	8 GB	1.9 GHz	6
Small	8 GB	2.5 GHz	6
Standard	32 GB	2.5 GHz	24
Large	60 GB	3.6 GHz	32

The Mini and Small differ in clock speed. During a full installation, the installer will detect and select a server size, based on resources available to the VM: RAM, CPU clock speed, and vCPU count. During an upgrade, the current configuration is unchanged. Use TUI to verify server is within these specifications.

IMPORTANT: TUI will not show all options if virtual machine does not meet those specifications.

To select a Cisco Vision Director deployment:

1. Log in using TUI.

2. Select **Cisco Vision Server Administration.**

3. Select **Setup Server Profile** (Figure 1 on page 16).

Figure 1   Setup Server Profile for Cisco Vision Director
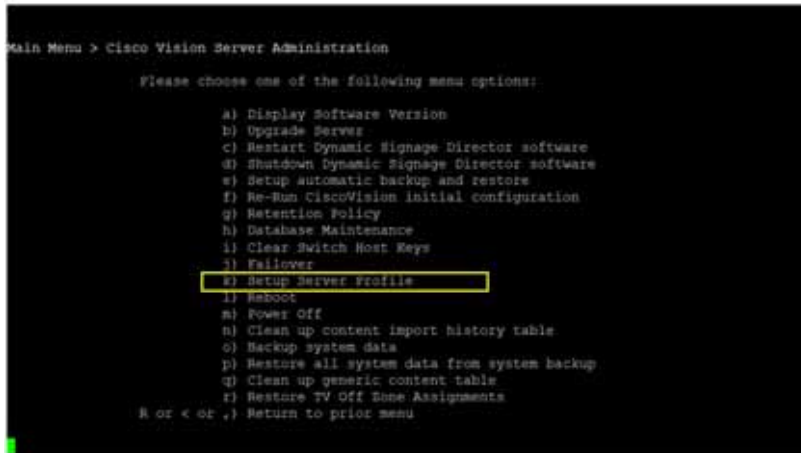
If the VM resources are insufficient to deployment particular configuration, the menu options may display NA (Figure 2 on page 16).

Figure 2   Select System Size
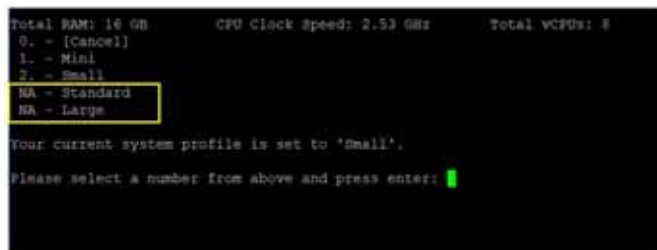
4. Reboot the server to have changes take effect.

Here are the new limitations for the available deployment configurations.

Table 2

Number of:	Mini/Small	Standard	Large
Groups	125	5,000	5,000
Zones	25	250	250
Running Scripts	5	100	250
Venues	0	25	250
Data Sources	50	100	250
Devices	1250	5000	5000

Contents

- What To Do Next, page 45

Prerequisites for Configuring Cisco Vision Director Server System Settings

Before you configure Cisco Vision Director servers, meet the following requirements:

- The Cisco Vision Director server hardware and software is installed. For more information, see Cisco Vision Software Installation and Upgrade Guide: Dynamic Signage Director Release 6.3.

- The Cisco Vision Director server is installed and you know the IP address.

- You have a supported browser version for Cisco Vision Director. For more information about the latest supported browsers, see Cisco Vision Software Installation and Upgrade Guide: Dynamic Signage Director Release 6.3.

- You have either physical console access or an SSH client such as PuTTY to log into the Cisco Vision Director server.

- The installer account credentials of cisco!123 on the Cisco Vision Director server. We strongly recommend you change this account password after the full installation is complete.

- You understand how to use the Text Utility Interface (TUI). For more information, see Cisco Vision Dynamic Signage Director Server Text-Based User Interface, page 103. For simplicity in these tasks, the instruction to "select" a particular menu item implies that you type the character that corresponds to the menu option and press **Enter**.

- For NTP configuration requirements, see Prerequisites for Configuring NTP on Cisco Vision Director Servers and DMPs, page 27.

- For multicast configuration requirements, see Unicast Registry Key in Cisco Vision Director, page 40.

How to Configure Cisco Vision Director Server System Settings

This section includes the following tasks:

- New DSD Full ISO Installation—Mandatory, page 17 (required)

- Editing the Hosts File, page 23 (as required)

- Editing the Hosts File, page 23 (as required)

- Restarting the Network Service on the Server, page 24 (as required)

- Generating the SSL Certificate, page 24 (required)

- Configuring NTP on Cisco Vision Director Servers and DMPs, page 26 (required)

- Configuring Multicast Ports for Cisco Vision Director, page 36 (required)

New DSD Full ISO Installation—Mandatory

To perform a full ISO installation:

1. Download the full install. See the Release Notes 6.3 for Cisco Vision Dynamic Signage Director.

2. Mount and boot off of full install ISO from step above.

3. When prompted, press "ENTER" to proceed with network configuration. Figure 3 on page 18 displays.
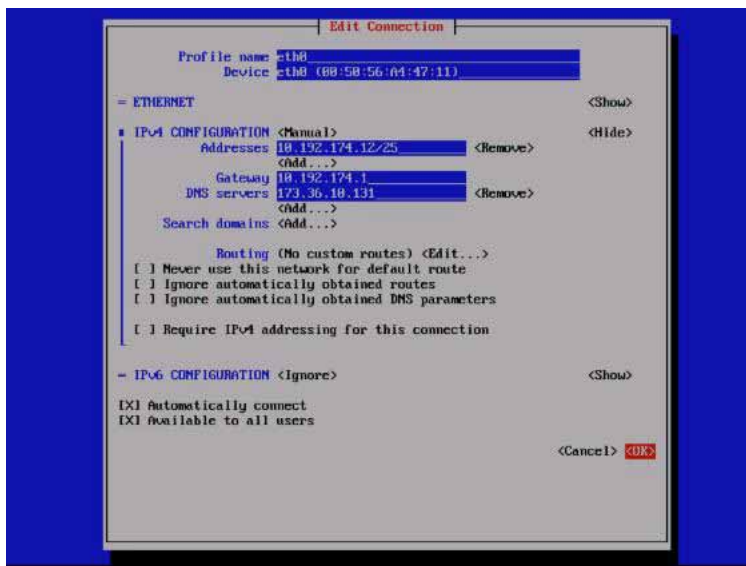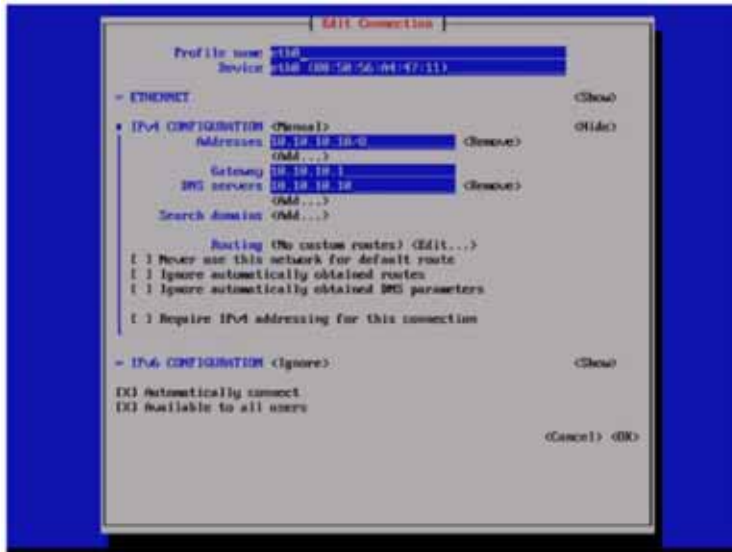
Figure 3   Network Configuration
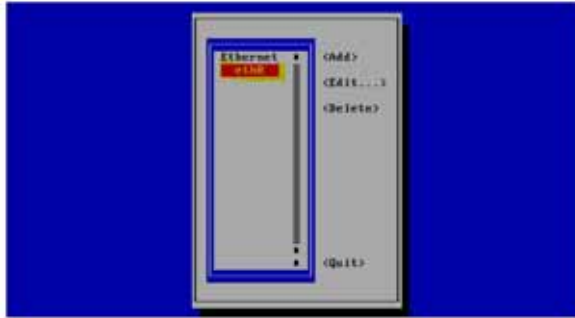
Note: Use left and right arrow keys to move the cursor to the previous or next fields. Use Space to make a selection (shown highlighted in red).

   4. Move cursor to **Edit**, press space bar.

Note: IPv4 address should be in xxx.xxx.xxx.xxx/CIDR format. Refer to CIDR conversion table for more information.

Figure 4   Edit Connection Address Update

5. Select "Quit" to exit out of network configuration TUI (Figure 5 on page 20).

Figure 5   Exit Network Configuration TUI

6. Assign a "Hostname" in the next TUI window (Figure 6 on page 20).

Figure 6   Set Hostname

Note: We recommend that the hostname be set to a fully-qualified domain name (FQDN). An FQDN is one with a domain name, rather than just a single name, like "sv-director" in the above graphic.

7. Click **OK** (Figure 7 on page 20). DSD components should begin installing.

Figure 7   Set Hostname using FQDN

8. When the DSD component installation completes, login to DSD from a browser.

9. Activate the eth0 interface (Figure 8 on page 21).

Note: There is a known issue related to SSL certification generation during the full install. If the browser does not load, regenerate the certificate and restart apache from TUI.

Figure 8   Activate Connection
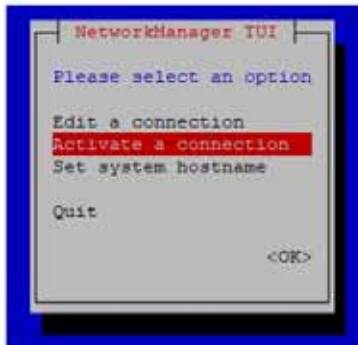
Completing Initial Configuration of System Settings After a Full ISO Installation

If the network configuration is successfully completed as part of the installation, then generate the SSL certificate, set the date and time options on the server (NTP and PTP), and restart the Cisco Vision Director software.
Security Alert: re-set the installer password.

For detailed information about how to configure the date and time options, see Configuring NTP on Cisco Vision Director Servers and DMPs, page 26.

Setting Up the Network Information

Tip: If you need to back out of the TUI menus for any reason, type `:q` or a comma.

To setup the Cisco Vision Director server network information:

1. Log into the TUI as installer using a directly-connected console or SSH client. The TUI Main Menu displays.

2. From the Main Menu, go to **System Settings** > **Network Settings** > **Setup Network Information**.

   Tip: To navigate through the TUI menus, type the character that corresponds to the menu area (a, b, c, and so on) and press **Enter**. To return to other menus, use one of the indicated keys to return to prior menus.
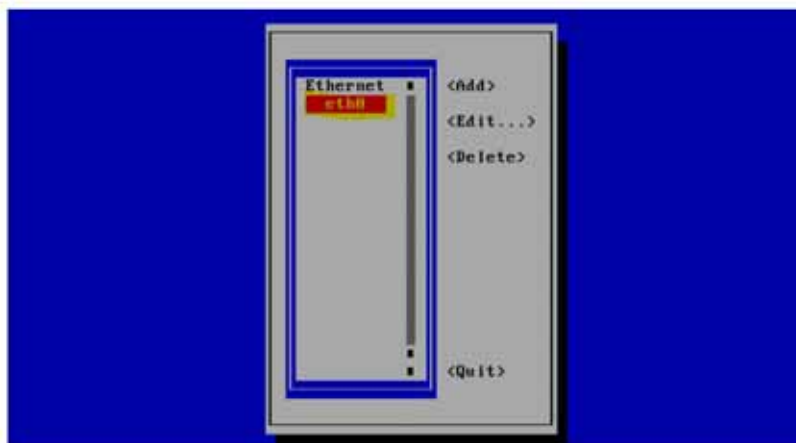
3. At the Network Manager TUI screen, select **Edit a Connection** (Figure 9 on page 21).

Figure 9   Edit a Connection

4. Select "eth0"

5. Select "Edit..."(Figure 10 on page 22).

Figure 10   Editing the Network

6. Set IPv4 CONFIGURATION to "Manual" (Figure 11 on page 22).

7. Select "Show" to provide details.

8. Enter the Cisco Vision Director IP address followed by the network prefix.

Format is: *ip address/prefix*

9. Supply the IPv4 settings for:

– Gateway

– DNS servers

– Search domains

Figure 11   Network Setup
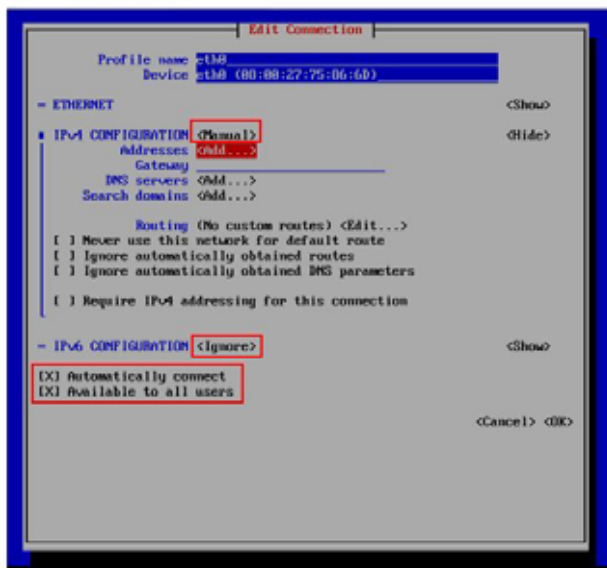
IMPORTANT: Verify the default values boxed above and listed below are checked or selected.

- – Keep the name of "eth0".

- – Keep the IPv6 CONFIGURATION to "Ignore".

- – Keep the boxes for "Automatically connect" and "Available to all users" checked.

10. Navigate to **OK** and hit **Enter**.

11. Go back to Network Manager TUI main menu.

12. Select **Set system hostname** (Figure 12 on page 23).

Figure 12   Set System Hostname

13. Provide the Cisco Vision Director server name and hit OK.

Note: Use a fully-qualified domain name (FQDN) for the hostname.
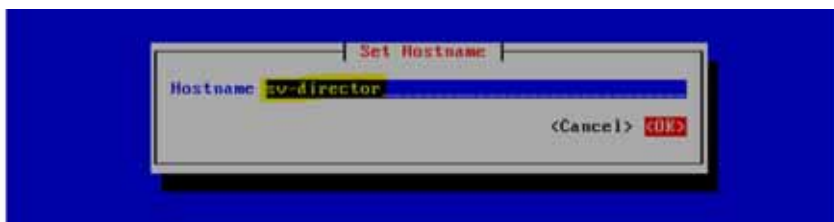
Editing the Hosts File

Note: If you were unable to complete the network configuration as part of the full ISO installation, then complete this task.

Before you begin, be sure that you know how to use the vi editor. For more information, see Cisco Vision Dynamic Signage Director Server Text-Based User Interface, page 103.

To edit the hosts file:

1. Log on to the TUI interface.

2. Type a for **System Settings**.

3. Type a for **Network Settings**.

4. Type c for **Edit hosts file** option.

IMPORTANT: Changing the host name in etc/hosts will require a server reboot to take effect.

5. At the confirmation prompt, press any key to open the /etc/hosts file for editing.

6. Change the line with IP address "10.10.10.10" to a comment (insert a # character at the beginning of the line) as shown in the following example:

   #10.10.10.10

7. Change the line for the IPv6 localhost entry "::1" to a comment as shown in the following example:

   #::1

8. Add a line for the server IP address and hostname as shown in the following example, where *x.x.x.x* is the IPv4 address of the Cisco Vision Director server, and *hostname* is the name to identify the server:

   x.x.x.x hostname

   Note: Use a fully qualified domain name (FQDN) with the domain information included.

9. Press **Esc** to enter vi command mode.

10. Save the changes to the file by typing the following command:

   :wq

11. Press any key to return to the Network Settings menu.

Restarting the Network Service on the Server

Note: If you were unable to complete the network configuration as part of the full ISO installation, then complete this task.

After you complete the network configuration on the Cisco Vision Director server, restart the network service to apply the network configuration.

1. Log into the TUI as System Status on the server using a directly-connected console or SSH client. The TUI Main Menu displays.

2. From the Main Menu, go to **Services Control** > **Networking** > **Restart networking**. The network interface eth0 restarts.

3. Confirm that the command completed successfully.

4. Press any key to return to the Networking menu.

5. Return to the Main Menu.

Generating the SSL Certificate

Note: Generate a new SSL certificate after initial upgrade to Release 6.3.

To generate the SSL certificate:
1. From the Main Menu, go to **System Settings** > **Network Settings**.

2. Select the **Generate certificate file** option.

3. When the confirmation warning prompt appears, type **Y** to continue and generate a new SSL certificate.

   To cancel without generating a new certificate, type **N**.

4. Press any key to return to the Network Settings menu.

Importing DMP Certificates

To support external URLs, the DMP may need to import certificates to render the website correctly. Upload new DMP certificates, change, and delete DMP certificates from the DSD server. Also, the list is fully sortable.

This feature provide a web-based UI to allow users to manage certificates used for Cisco Vision Director. It supports accessing Cisco Vision Director over a secure protocol without the security warnings associated with self signed certificates. These certificates types .cer, .crt and .pem are supported.

The UI will list the certificates that are imported. It will show the Name of the certificate, the File name, the Size of the file, the Upload Date, the Issuer Name, and when the certificate is Valid.

To import DMP Certificates:

1. Go to: **More > Manage Software**. The Software Manager window appears (Figure 13 on page 25).

2. Click the **Certificates** tab.

3. Click **Upload** (Figure 14 on page 25).
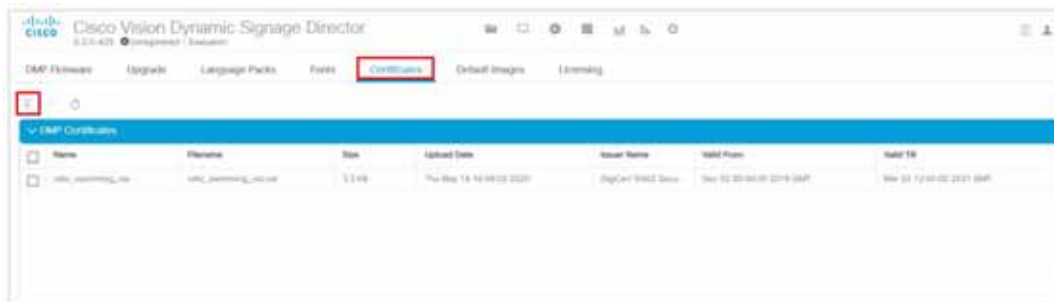
Figure 13   DMP Certificates

Figure 14   Certificates Upload Screen

4. Choose a file, click **OK**, it appears as uploaded.

When you delete a file, you get a warning dialog box making sure you know you are deleting a certificate. Click **Delete**. You can **Delete All** by clicking the check box near the **Name** column.

5. Import the certificate private key.

Imported certificates are backed up and subject to a restore operation. The UI certificate information shows the following:

■ common name of the issuer

■ period of validity (begin and expiry dates)

Note: After uploading a certificate, stage content so the DMP certificate gets pushed to the DMP. Reboot the DMP so the new certificate takes effect. Use **Script Management** to manually start content staging from the Cisco Vision Director UI.
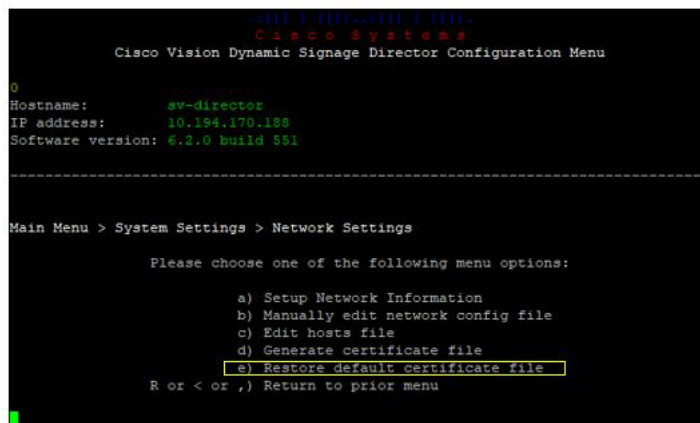
Importing Dynamic Signage Director (DSD) Certificates

In case a DSD certificate that is uploaded via **Software Manager** either expires or is invalid and you cannot access/login to Cisco Vision Director via web interface, you can restore a default certificate. Use this option to restore the default self-signed certificate that Cisco Vision Director will generate. Then restart the web server and access DSD via the primary server IP.

To restore a DSD default certificate file:

1. Log in to the Cisco Vision Director TUI. Use your user ID and password.

2. From the Main Menu, type **a** for **System Settings**.

3. Type **a** for **Network Settings**.

4. Type **e** for **Restore default certificate file** (Figure 15 on page 26).

Figure 15   Restore Default Certificate File

Configuring NTP on Cisco Vision Director Servers and DMPs

Cisco Vision Director requires Network Time Protocol (NTP) service on the following devices:

- Cisco Vision Director servers

- DMP Precision Time Protocol (PTP) lead device

NTP provides reliable clocking for your Cisco Vision network and helps ensure synchronicity between redundant servers.

Note: For optimized synchronization on the media players, use PTP. Only the PTP leads derive a clock using NTP.

Verify the NTP configuration for your Cisco Vision Director servers, since the default NTP source is a public pool and might not be the NTP server source that you want to use for your venue.

Configure the DMP NTP source within the Cisco Vision Director. Go to **Configuration > System Configuration > Global DMP Settings > Time Source**. As a best practice, the Cisco Vision Director server is already set as the NTP host by default for all media players. This does not need to be changed unless the venue requires a different NTP source.

Caution: The Cisco Vision Director server is itself enabled as an NTP host to provide timing to the media players only. Do not use Cisco Vision Director as an NTP host for other devices in your network.

This section includes the following tasks:

- Prerequisites for Configuring NTP on Cisco Vision Director Servers and DMPs, page 27 (required)

26

- Configuring System Date and Time Using NTP on Cisco Vision Director Servers, page 28 (required)

- Restarting the Cisco Vision Director Software, page 31

- Configuring the Date and Time Manually, page 32

- Configuring NTP and PTP on the Digital Media Players, page 32 (required)

Prerequisites for Configuring NTP on Cisco Vision Director Servers and DMPs

CAUTION: **Reference a reliable NTP server running on a dedicated device, rather than relying on a clock from a VM environment that can drift and is not accurate.**

Before configuring NTP on Cisco Vision Director servers and DMPs, be sure that the following requirements are met:

- You understand how to use vi editor commands.

- You understand the NTP host requirements for your Cisco Vision Director servers:

  – If you do not want to use the default public pool of NTP servers for the Cisco Vision Director servers, you have the IP address or DNS name of the NTP host for your network.

  – If you plan to use a public pool of NTP servers, be sure that the servers are reachable from the Cisco Vision Director network. By default, the ntp.conf file on Cisco Vision Director servers has configured the following Red Hat Linux public pool of servers:

    ```
    server 0.rhel.pool.ntp.org iburst
    server 1.rhel.pool.ntp.org iburst
    server 2.rhel.pool.ntp.org iburst
    server 3.rhel.pool.ntp.org iburst
    ```

    Tip: For more information about using NTP pool servers see the Network Time Protocol website.

- If you plan to change the default best practice of using the Cisco Vision Director server as the NTP source for DMPs, be sure that the following requirements are met:

  – You have configured the NTP host for the Cisco Vision Director server first.

  – You have upgraded the DMP firmware.

    For more information about how to upgrade the DMP firmware, see the Cisco Vision Software Installation and Upgrade Guide: Dynamic Signage Director, Release 6.3 for your release.

  – For optimal synchronization, use the same NTP server that is configured for the Cisco Vision Director server. However, it is not required.

  – The DMP must not reference an NTP server pool. If the Cisco Vision Director server references an NTP server pool (the default), then select a specific server from that same pool as the NTP server for the DMPs.

  – Only IPv4 is supported for the NTP server address on the DMPs.

  – The NTP server for the DMPs must not be a load-balanced server.

- The Cisco Vision Director network is configured to allow bidirectional transmission of UDP messages on port 123 for NTP messages.

  UDP port 123 is used for communication between the Cisco Vision Director servers and NTP hosts, and the DMPs and NTP host (by default, this is the Cisco Vision Director server).

  For a complete port reference for Cisco Vision Director servers, see the "Port Reference" module of the Cisco Vision Software Installation and Upgrade Guide: Dynamic Signage Director, Release 6.3 for your release.

Configuring System Date and Time Using NTP on Cisco Vision Director Servers

When you install or upgrade the Cisco Vision Director, you need to configure the system date and time in the TUI. You also need to configure the time zone.

Note: Although you can manually configure the system date and time on your servers when necessary, this should be avoided for your production network.

- Setting Up the NTP Source on Cisco Vision Director Servers, page 28 (required)

- Configuring the Time Zone, page 29 (required)

- Restarting the Cisco Vision Director Software, page 31 (required)

- Configuring the Date and Time Manually, page 32 (if necessary)

Setting Up the NTP Source on Cisco Vision Director Servers

Note: Complete this task only if you do not want to use the default public pool of servers.

Standard NTP server configuration uses the word "server" followed by the Domain Name System (DNS) name or IP address of an NTP server. By default, the ntp.conf file on Cisco Vision Director servers has configured the following Red Hat Linux public pool of servers:

```
server 0.rhel.pool.ntp.org iburst
server 1.rhel.pool.ntp.org iburst
server 2.rhel.pool.ntp.org iburst
server 3.rhel.pool.ntp.org iburst
```

For these servers to be used as a reference clock, they must be reachable from the Cisco Vision Director network.

If you want to use your own server, be sure to add it and comment out these default pool servers in the ntp.conf file. Otherwise, you do not need to do any further editing of the ntp.conf file in this task.

To set up the NTP host on Cisco Vision Director servers:

1. From the TUI Main Menu, go to **System Settings** > **Date and Time Settings** > **Setup NTP Source**.

   A confirmation screen to Configure NTP and edit the ntp.conf file displays.

2. To open the ntp.conf file for edit, press any key.

   The ntp.conf file opens in the vi editor and the cursor is positioned at the end of the last configured NTP server line. If this is not the case, navigate to the server configuration section.

3. To enter INSERT line editing mode, type **i**.

   The vi editor changes to INSERT mode.

4. If you have a server that you want to use as the reference clock source at your site, do the following:

   – Add a line and type "**server** *ip-address*" or "**server** *dns-name*," where *ip-address* or *dns-name* is replaced by the IP address or name of the NTP server that you want to configure.

   – Go to the lines where the pool servers are configured and add a "#" sign in front to comment them out of the configuration as shown below:

   ```
   #server 0.rhel.pool.ntp.org iburst
   #server 1.rhel.pool.ntp.org iburst
   #server 2.rhel.pool.ntp.org iburst
   #server 3.rhel.pool.ntp.org iburst
   ```

5. To exit INSERT mode and return to vi command mode, press **Esc**.

6. To save your changes, type **:wq**

   Press Return. The configuration is saved and the ntpd service is restarted. Verify that you see the "OK" confirmation that the ntpd has started.

7. To return to the Date and Time Settings menu, press any key.

Configuring NTP AUTH3

An NTP server somewhere on your network provides accurate time to the DSD server. For additional security, this NTP server can be configured to allow authentication. This uses the NTP AUTH 3 protocol. If you want to set up the communication to the NTP server to use authentication, first find out some information on how the NTP server is configured. Specifically, you need to know the ID for the key and the key value, as well as the IP address of the NTP server.

1. Using the TUI, go to **Main Menu > System Settings > Date and Time Settings > Setup NTP Symmetric Keys for NTP authentication**.

2. Your terminal session will start an editor in which you can add a line of configuration for the NTP client.

3. Provide the ID, type, and key information. In this example, we chose ID 15, type M, and key I_see!

4. Save the file and return to the TUI menu.

5. Go to the previous TUI menu option.

6. Select **a** for **Setup NTP Source**. In this file you need a line that lists your NTP server. Make a line in that file that in our example would look like this:

7. Save the file. After several minutes, the Cisco Vision Director server's time should match the correct time based on the NTP server.

Configuring the Time Zone

Configuring the time zone is required for the Cisco Vision Director server.

Note: Although there is an option to set the time zone in **Configuration > Venues** interface on the Cisco Vision Director server, this option is informational only and is also used for proof-of-play reporting.

This section includes the following tasks:

- Finding the Time Zone Code for System Configuration, page 29 (optional)

- Configuring the System Time Zone, page 31 (required)

Finding the Time Zone Code for System Configuration

Use this task if you need to find out the time zone code to configure the server's time zone information.

Note: This task provides information only and does not actually configure the time zone.

To find the time zone code for system configuration:

    a. From the TUI interface, go to **System Settings** > **Date and Time Settings** > **Change Timezone**.

    b. Type the number that corresponds to the applicable continent or ocean for the location of the server.

    c. Type the number that corresponds to the country.

    d. Type the number for the time zone (as applicable).

    e. When the confirmation of the time zone information that you configured is displayed, type **1** (for Yes) to accept your settings, or 2 (for No) to cancel (Figure 16 on page 30).

Figure 16 Time Zone Confirmation Prompt

```
The following information has been given:

        United States
        Pacific Time

Therefore TZ='America/Los_Angeles' will be used.
Local time is now:      Mon Feb 18 16:42:55 PST 2013.
Universal Time is now:  Tue Feb 19 00:42:55 UTC 2013.
Is the above information OK?
1) Yes
2) No
#?
```

    f. After confirming Yes at the prompt, note the time zone string that is provided.

        Figure 17 on page 30 shows a sample time zone code for America/Los_Angeles.

Figure 17 Sample Time Zone Code

```
The following information has been given:

        United States
        Pacific Time

Therefore TZ='America/Los_Angeles' will be used.
Local time is now:      Mon Feb 18 16:56:47 PST 2013.
Universal Time is now:  Tue Feb 19 00:56:47 UTC 2013.
Is the above information OK?
1) Yes
2) No
#? 1

You can make this change permanent for yourself by appending the line
        TZ='America/Los_Angeles'; export TZ
to the file '.profile' in your home directory; then log out and log in again.

Here is that TZ value again, this time on standard output so that you
can use the /usr/bin/tzselect command in shell scripts:
America/Los_Angeles
Press any key to return to the menu.
```

8. Press any key to return to the Date and Time Settings menu.

9. Configure the system time zone using the appropriate code for the server location. See Configuring the System Time Zone, page 31.

Configuring the System Time Zone

Prerequisites

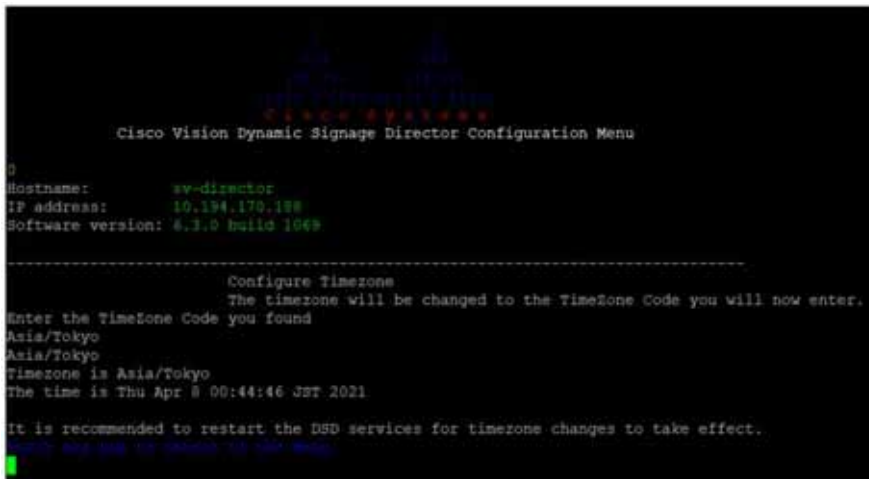Before you configure the system time zone, you should know the following information:

- How to use vi editor commands.

- The time zone code for the server location. If you need to look up the time zone code, see Finding the Time Zone Code for System Configuration, page 29.

Procedure

To configure the system time zone so that it persists after restart of the server:

1. From the TUI Main Menu on the server, go to **System Settings** > **Date and Time Settings** > **Change System Timezone**.

2. Enter the TimeZone Code. In this example, Asia/Tokyo (Figure 18 on page 31).

Figure 18   Editing the Time Zone

3. Return to the Main Menu.

4. Click **Cisco Vision Server Administration > Restart Dynamic Signage Director software**.

5. Restart the server to put the time zone changes into effect.

Restarting the Cisco Vision Director Software

After you configure an NTP server and time zone in the TUI on the server, you must restart the Cisco Vision Director software.

To restart the Cisco Vision Director software:

1. From the TUI Main Menu on the server, go to:

    Cisco Vision Server Administration > **Restart Cisco Vision Dynamic Signage Director software**.

2. When the prompt appears, press any key to return to the Server Administration menu.

3. Return to the Main Menu and exit the TUI.

Configuring the Date and Time Manually

Note: This task is provided as a precaution if you should find it necessary to manually set the system date and time. Manual date and time configuration should be avoided on a production system and NTP service used instead.

To configure the date and time manually:

1. From the TUI Main Menu on the server, go to **System Settings** > **Date and Time Settings** > **Change Date and Time**.

2. At the confirmation prompt, type **Y** to continue.

3. Type the new date and time in the format: MMDDhhmm[[CC] YY] [.ss], where:

   – MMDDhhmm is required (MM is month, DD is day, hh is hour, and mm is minutes).

   – CC is the century (first 2 digits of the year) and is optional for use with YY. For example "20" in the year 2013.

   – YY is the last 2 digits of the year and is optional. For example "13" in the year 2013.

   – .ss is seconds and is optional.

4. Press any key to return to the Date and Time Settings menu.

Configuring NTP and PTP on the Digital Media Players

By default, both NTP and PTP services are automatically enabled for digital media players. The digital media players use PTP to achieve optimal synchronization. However, an NTP source also must be used to provide initial clocking to the devices that are elected PTP leads in the network.

This section provides information about the default settings and how to modify them. It includes the following tasks:

- Restrictions for NTP and PTP on the Digital Media Players, page 32

- Guidelines for NTP and PTP on the Digital Media Players, page 33

- Modifying the Standard NTP and PTP Configuration on All DMPs in the System, page 34 (optional)

- Verifying PTP Operation for the Digital Media Player, page 36

Restrictions for NTP and PTP on the Digital Media Players

Before you configure PTP on the digital media players, consider the following restrictions:

- By default, PTP messages will not cross VLANs and PTP leader candidates need to be identified for each VLAN and configured in the **Configuration > System Configuration** page.

- The system supports a configurable Precision Time Protocol (PTP) Time To Live (TTL) setting in the **Configuration > System Configuration** page. The PTP TTL specifies the number of VLANs that can be crossed for selection of a PTP leader. The default value of 1 (recommended) means that each VLAN will elect its own PTP leader.

  Note: For ease of configuration for venues with multiple VLANs, the system is configured by default to list all digital media players as eligible PTP leader candidates. However, be aware that although this simplifies configuration, the time that it takes for the devices to arbitrate a leader device in each network will vary, and depends on the number of eligible devices in each network.

- Content synchronization for video playback on the digital media players relies on precise time across DMPs using PTP. If the DMPs are playing video and one of the devices reboots, the rebooting unit will restart video playback from the beginning and will only synchronize with the other players when the next item in the playlist is rendered.

- If digital media players are participating in zone-based content synchronization for video walls, with some enhanced synchronization capability, the rebooting unit will synchronize with the current item being played by the device leader in the video wall. For more information, see "Working with Video Walls" in Release 6.3: Cisco Vision Dynamic Signage Director Operations Guide.

Guidelines for NTP and PTP on the Digital Media Players

Before you configure NTP and PTP on the digital media players, consider the following guidelines:

- For new installations of Cisco Vision Director, PTP is the default time source for the digital media players, with NTP as the default time source for the elected PTP leader.

NTP Guidelines

- Each digital media player designated as PTP leader (per VLAN) will use NTP as its time source. The other devices in the network operate using a PTP reference clock from the elected PTP leader.

- When PTP is disabled (not recommended), all devices use NTP to set their local clock.

  Note: For synchronized video playback, NTP alone cannot be relied upon for devices and PTP must be used.

- The default NTP synchronization interval with the host time server is one hour and is configurable.

- An NTP source must be configured in Cisco Vision Director. By default, the Cisco Vision Director server is configured as the device NTP host.

PTP Guidelines

- PTP version 2 is supported only for the digital media players and applies globally to all devices in the Cisco Vision Director network when configured.

- PTP configuration includes a PTP domain and a set of leader candidates:

  - PTP domain—Default is 0.

    Be sure that this domain does not conflict with any other PTP domain (and multicast addressing) in use in your network, and revise as needed. See table "Global DMP Settings—PTP Property Values" for more information.

  - PTP leader candidates—Default is *.

    This specifies that all devices in the network are eligible as leader candidates and will go through arbitration to designate a leader for their respective subnets.

- If you revise the default PTP leader candidates configuration, you must configure one or more devices as leader candidates in a semicolon-separated list of IP addresses for each VLAN.

  A minimum of two leader candidates per network is recommended.

- If there is an in-house PTP leader for your network, leave the "PTP leader candidates" property value blank. However, this configuration is only supported for venues without multiple subnets.

Modifying the Standard NTP and PTP Configuration on All DMPs in the System

By default the NTP and PTP services are automatically enabled and configured for digital media players. Use this task if you need to modify the default settings described in and .

Table 3   Global DMP Settings—PTP Property Values

Property (Registry key)	Description	Values
PTP domain (Globaldmpsetting.common.init.ptp.domain)	Domain number for the PTP network, which defines the multicast address for PTP communication.	For IEEE-1588 PTP, possible values are: **0**–(Default) 224.0.1.129 **1**–224.0.1.130 **2**–224.0.1.131 **3**–224.0.1.132
PTP leader candidates (Globaldmpsetting.common.init.ptp.master.host)	Eligible devices for leader candidate selection.	Possible values are: ■ *****–(Default). Wildcard pattern that specifies all devices in the network as eligible PTP leader candidates. ■ Semicolon-separated IPv4 addresses of the devices for each subnet. **Example:** 10.0.0.3;10.0.0.4;192.168.0.5;192.168.0.6 ■ blank—Specifies that a PTP leader source external to Cisco Vision Director is used. This configuration is only valid for a venue without devices in multiple subnets.
PTP time-to-live (Globaldmpsetting.common.init.ptp.ttl)	Number of VLANs that can be crossed for selection of a PTP leader.	1 (Default) **Note:** Best practice is to retain the default value of 1 for election of a PTP leader per video wall. With a TTL > 1, degradation in local video synchronization can occur.

Note: If the domain setting gets blanked, it will disable PTP on all DMPs. The DMPs will revert to using NTP as the time source.

Table 4   Global DMP Settings–NTP Property Values

Property (Registry Key)	Description	Values
NTP Host (Globaldmpsetting.common.deploy.ntpc.hostname)	IPv4 address of the NTP server.	Default–IP address of the Cisco Vision Director server.
NTP sync interval (Globaldmpsetting.common.deploy.ntpc.interval)	Number of seconds that the device waits before trying to synchronize its time with the configured NTP host.	**3600** (Default)
Timezone (Globaldmpsetting.common.deploy.ntpc.timezone)	Code for the timezone to be used.	**GMT** (Default)

To modify the standard NTP and PTP configuration on all DMPs:

1. Log into the Cisco Vision Director server as an administrator.

2. Click **Configuration > System Configuration > Global DMP Settings > Time Source** (Figure 19 on page 35).

Figure 19   Global DMP Settings for NTP and PTP on the DMPs
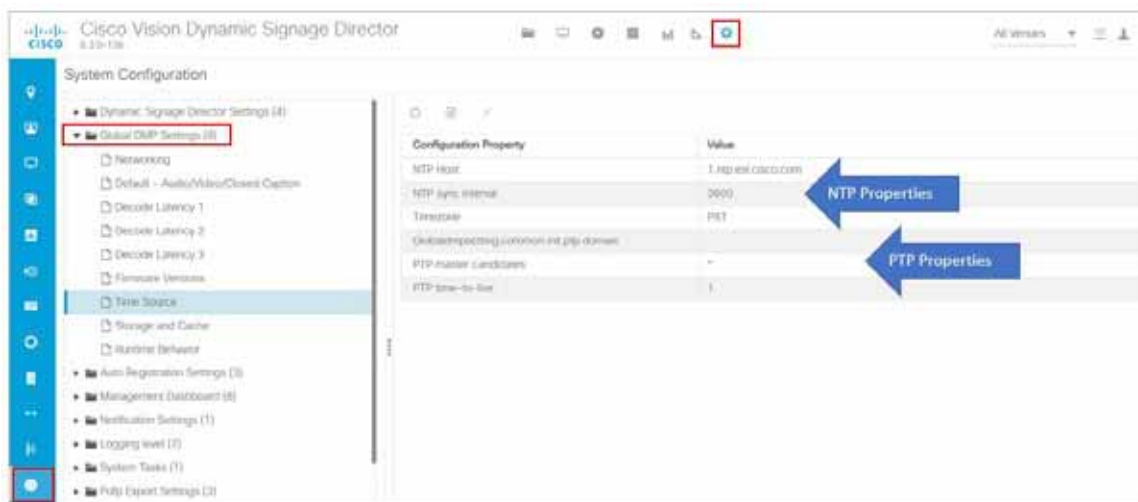
3. (Optional) Change the global PTP properties as required for your network. Click the **Edit** icon (pencil). Refer to Table 3 on page 34.

4. (Optional) Change the global NTP properties as required for your environment. Click the **Edit** icon (pencil). Refer to Table 4 on page 35.

5. Click **Save**.

6. Reboot the devices.

Verifying PTP Operation for the Digital Media Player

This section describes how to verify the PTP configuration and also the operation of PTP for your devices.

To verify the PTP operation for the digital media player:

1. Open your browser and navigate to one of the DMPs:

   http://_sv4k-ip-address_**/ptp.html**

2. Identify the PTP leader by finding the unit that has an "offsetFromMaster" value of 0.0.

highlights the PTP leader and shows a network where PTP is operating successfully with 12 members.

Figure 20   Successful PTP Clock Operation

Configuring Multicast Ports for Cisco Vision Director

This section includes the following topics:

- Information about Multicast Support in Cisco Vision Director, page 37

- Unicast Registry Key in Cisco Vision Director, page 40

- How to Configure Multicast Ports in Cisco Vision Director, page 40

Information about Multicast Support in Cisco Vision Director

This section includes the following topics:

- HDMI-In Encoding on the SV-4K, CV-UHD, and CV-UHD2 Media Players to Stream Video as a Channel, page 37

- Per-Script Multicast Optimization, page 37

- Multicast Registry Keys in Cisco Vision Director, page 38

HDMI-In Encoding on the SV-4K, CV-UHD, and CV-UHD2 Media Players to Stream Video as a Channel

Cisco Vision Director supports streaming video from a laptop or other supported device connected to the HDMI-In port on the SV-4K, CV-UHD, or CV-UHD2 digital media players to be played as a multicast-based channel in Cisco Vision Director.

We recommend you use the part of the Administratively Scoped Address range called the IPv4 Organization Local/Site Scope or the expansion of the IPv4 Org Local/Site Scope Range (239.0.0.0/8) for multicast range to use for this feature in the Connected Venue (Connected Stadium) network. For SSM, we recommend a specific block of the Administratively Scope range of 239.232.0.0/16.

Note: If you want to maintain privacy of channels, create a DMP-encoded channel per suite with a unique multicast address (from 239.193.20.0/24 range), and create a separate channel guide per suite. For example, if you have 10 suites—create 10 separate DMP-encoded channels with unique multicast addresses, create 10 different channel guides for each DMP-encoded channel, and assign each suite to a different channel guide.

For more information about configuring this feature, see the Cisco Vision Dynamic Signage Director Operations Guide, Release 6.3.

Per-Script Multicast Optimization

Currently, we use Per-Script Multicast Optimization (for up to 20 different scripts) to reduce the number of multicast messages that each DMP must process. Per-Script Multicast Optimization is designed to reduce the load on DMPs when the following conditions are present in Cisco Vision Director:

- More than one event script is run simultaneously in a venue.

  The scripts can be running across multiple venues or scripts running in a single venue.

- The External Content Integration feature is used, which sends multiple messages to the DMPs in a script.

Additional information about per-script multicast optimization:

- Per script, you can use 20 maximum

- If you are running more than 20 scripts, then the first 20 scripts operate using per-script multicast channels, and the additional scripts are run over the global multicast host port.

- No remote servers required

- Default: disabled

37

Benefits of Per-Script Multicast

You can configure multiple multicast channels, over which the server sends only the multicast messages needed for a particular event script for up to 20 scripts.

Figure 21 on page 38 shows the message separation: with or without per-script multicast. Each DMP goes from seeing four packets to seeing two. More importantly, each DMP now only has to process one XML payload, which is important when the XML payloads are sizeable.

Figure 21   Multicast Messaging With and Without Per-Script Multicast Optimization
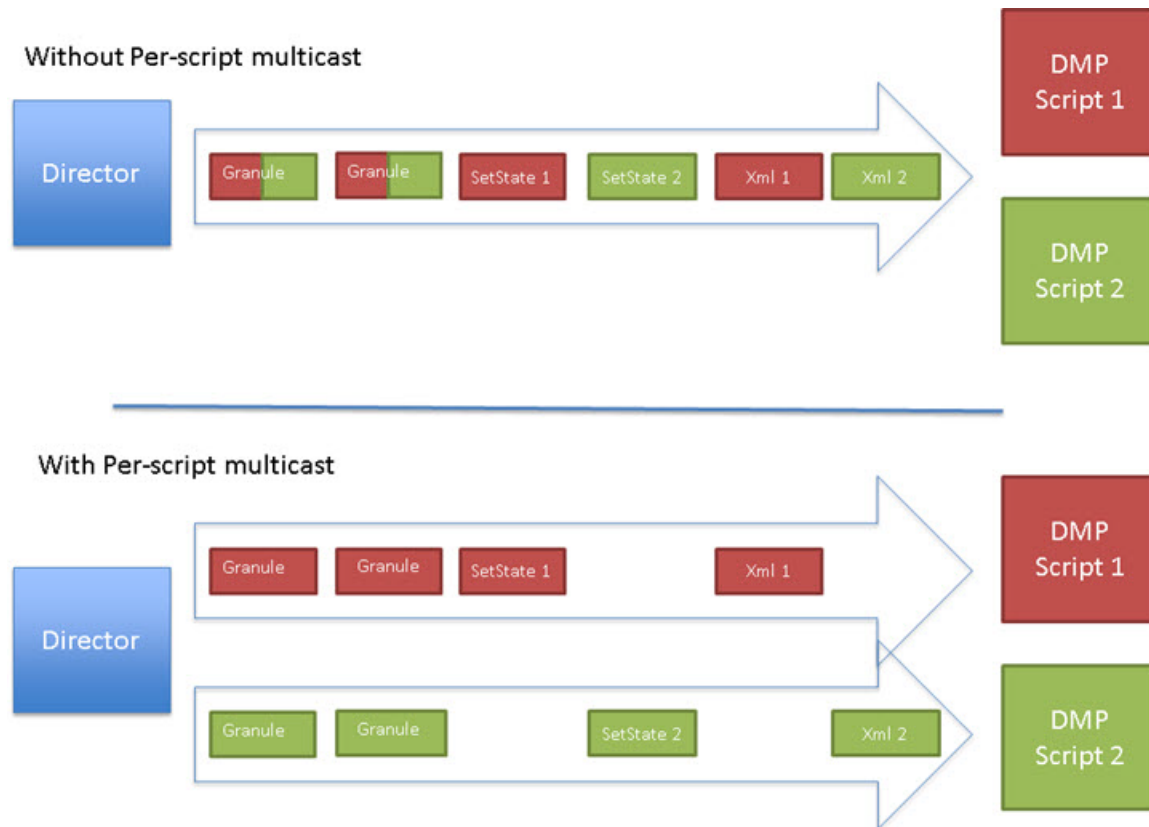
All DMPs, including those associated with a remote site, listen on these per-script multicast channels.

For messages that apply to multiple event scripts, the message is duplicated and sent to each multicast channel. Therefore, this feature can increase the load on Cisco Vision Director servers (increasing the number of messages sent and copying of messages) as a tradeoff for reducing the number of messages seen and processed by DMPs. However, this load is expected to be negligible.

For information on the new unicast feature in Release 6.3, see Configuring Per-Script Unicast in Cisco Vision Director, page 42.

Multicast Registry Keys in Cisco Vision Director

Cisco Vision Director uses multicast messages for DMP control-plane operation. Cisco Connected Venue (Connected Stadium) network design assigns the following multicast group addresses for use by Cisco Vision Director:

- 239.193.0.0/24—For control communication

- 239.192.0.0/24—For video communication (This network should be avoided for the multicast configuration described in this module.)

Multicast addressing is configured using registry keys from the Cisco Vision Director **Configuration > System Configuration > Advanced Registry Settings** page.

Table 5 on page 39 describes the registry keys in Cisco Vision Director that control the multicast configuration.

Note: The default PTP domain 0 uses multicast address 224.0.1.129. For more information, see Table 3 on page 34.

Table 5   Multicast Registry Keys in Cisco Vision Director

Registry Key	Default Value	Description
Globaldmpsetting.sv4k.init.dmpsync.multicast.address	239.193.0.253	Sets the global multicast address used for zone-based synchronization on the DMPs.
Globaldmpsetting.sv4k.init.dmpsync.multicast.port	50001 **Note:** The system automatically uses an additional port based on this default (default + 1) for secondary video. In the case of the 50001 default, 50002 is also reserved for secondary video use.	Sets the default port for the primary video for zone-based synchronization multicast address on the DMPs.
MulticastHostPort	239.192.0.254:50001 **Caution:** This default multicast address should be changed after installation to use the **239.193**.0.0/24 address range, or the network that is configured in your Cisco Connected Stadium network for Cisco Vision Director control.	Sets the global multicast address and port for Cisco Vision Director.
transport.dynamic.enable	■ False (for upgraded servers) Per-Script Multicast Optimization is disabled and the Cisco Vision Director server sends all communication over the MulticastHostPort address directly to all DMPs, including all remote DMPs. ■ True (for new installations)	Enables and disables Per-Script Multicast optimization.
transport.dynamic.send_range	50080-50099 If the MulticastHostPort registry key is 239.193.0.254:50001, then 239.193.0.254:50080–239.193.0.254:50099 is used as the range of Global hostports for the running scripts.	Specifies the range of ports for Per-Script Multicast Optimization. These ports are used with the network specified in the MulticastHostPort registry key, to define a range of additional global hostports to be assigned for running scripts.

Unicast Registry Key in Cisco Vision Director

Since Release 6.2, a unicast registry setting has been supported that allows DMPs to receive unicast state change messages via a unicast control message from Cisco Vision Director. The registry setting for unicast is: **script.stateChange.nextStateDelay**

Note: The following caveats apply to using unicast:

- Unicast does not remove **any other** need for multicast

  - When using widgets that rely on data from data integration, make sure that the widget pulls data versus relying on multicast.

  - For multicast video channels, do not use, or use a unicast video channel

  - There is no alternative for video wall synchronization

- Sync that relies on setState messages arriving at the same time may be out of sync

- This feature is an alternative to cover edge conditions **only**

IMPORTANT: If you want to synchronize the DMPs using setState, the registry value **script.stateChange.nextStateDelay** delays all state change messages (both multicast / unicast), to try to synchronize. Use it as "best effort." Tune it to the environment. If it is set to 5 seconds, **all state changes will be delayed 5 seconds**).

For details, see Configuring Per-Script Unicast in Cisco Vision Director, page 42.

Prerequisites for Configuring Multicast Ports in Cisco Vision Director

Before you configure multicast ports, be sure that the following requirements are met:

- Be sure that you understand the multicast addressing in use for all areas of your Cisco Vision Director network, including Cisco Connected Venue and Cisco Vision Mobile networks. Confirm that there are not any multicast address/port overlaps.

  Caution: Because of the large number of ports that per-script multicast configuration requires, and the possibility for hard-to-diagnose failures if video is routed to a DMP's control channel (which can occur when the port numbers are the same and even if the group/host portion is different), it is critical to verify that the port ranges you plan to use are not used by any other source of multicast in the network.

  - For more information about the recommended multicast addressing for the Cisco Connected Venue network, see the *Cisco Vision Network, Server, and Video Headend Requirements Guide* available to authorized partners and from your Cisco Systems representative.

- The network is properly configured to route the global multicast host port to be visible for all DMPs in the Cisco Vision Director network, including those at remote venues and associated to venues in a multi-venue environment.

How to Configure Multicast Ports in Cisco Vision Director

This section includes the following tasks:

- Configuring the Global Multicast Host Port in Cisco Vision Director, page 40 (required)

- Configuring Per-Script Multicast in Cisco Vision Director, page 41 (recommended)

- Configuring Multicast Support for Zone-Based Content Synchronization for the DMPs, page 44 (optional)

Configuring the Global Multicast Host Port in Cisco Vision Director

The global multicast host port is used by Cisco Vision Director to send messages to DMPs when they are not part of a script, when per-script multicast is disabled, or when the number of scripts running exceeds to configured maximum of per-script multicast ports.

It is configured in the "MulticastHostPort" registry key in the **Configuration > System Configuration > Advanced Registry Settings** interface.

Note: The default value currently uses the address 239.192.0.254:50001 and should be changed to a network address in the range 239.193.0.0/24.

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

1. Click **Configuration > System Configuration > Advanced Registry Settings**.

2. Scroll to the "MulticastHostPort" registry key in the Key list and confirm the entry for the registry.

3. Click on the Value field and click **Edit**. The **Edit – Configuration Setting** dialog box appears.

4. Specify a multicast address in the range 239.193.0.0/24 and port number.

   Note: Be sure to use the value that is configured in your Cisco Connected Venue network for Cisco Vision Director control messages and include the :port. The recommended default is :50001.

5. Click **Save**.

Configuring Per-Script Multicast in Cisco Vision Director

By default, Per-Script Multicast Optimization is disabled and the Cisco Vision Director server sends all communication over the MulticastHostPort address directly to all DMPs, including all remote DMPs.

To configure per-script multicast (increase/decrease number of ports):

1. Stop all running scripts.

2. Click **Configuration > System Configuration > Advanced Registry Settings**.

To enable per-script multicast, change the values of the following registry keys:

   – **transport.dynamic.enable**—Specify a value of **true**.

   – **transport.dynamic.send_range**—(As Required) Change the range of ports to comply with your network configuration. The default is 50080-50099.

      Note: Be sure that these ports do not overlap with other multicast ports in use on your network.

3. Click **Save**.

4. Reload the HTML runtime on all DMPs:

   a. Select all of the DMP devices where the command should be applied.

   b. Click **Play** to run the command on the selected devices.

5. To verify the configuration:

   a. Start and stop event scripts and change states.

   b. Verify that the multicast port that the DMP is listening on is one of the per-script ports (50080-50099 by default), rather than the global multicast hostport (50001).

If the scripts do not start and stop, see .

Configuring Per-Script Unicast in Cisco Vision Director

Since Release 6.2, unicast state change deployment ability has been supported. Unicast state change DMPs do not have the full feature set that multicast offers. Multicast state change deployments are the **recommended** best practice. Use unicast state changes in situations where there may be DMPs outside the main venue or DMPs located and configured in such a way that you cannot use multicast routing.
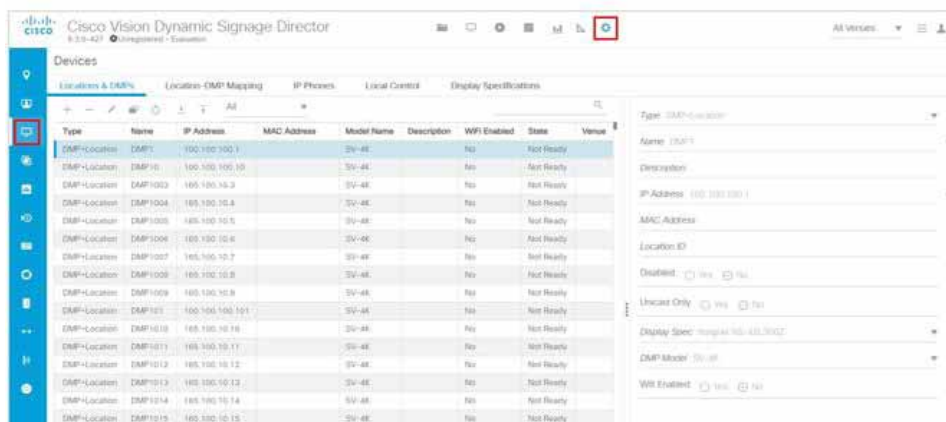
There are some limitations with unicast state change messages:

■ DMPs using unicast state change messages will not synchronize state changes, either with other unicast state change DMPs, or with DMPs using multicast state change messages. This lack of synchronization may affect all content types.

■ Unicast state change messages are sent to all DMPs, but due to network delays, DMP server processing load, and the state of the DMPs, the state change messages may be delayed. This is the cause of the lack of synchronization.

■ For 5000 DMPs using a large server deployment, the best case is that transmitting to all 5000 DMPs would take at least 3 seconds. However, this is a best case estimate. Under real-world conditions, timings greater than 3 seconds would occur as the difference in state starting from the first DMP to receive the setState message, to the last.

■ Unicast state change messages do not solve any other required use of multicast in the system, including the following:

  – Multicast video streams

  – Zone-based video wall synchronization communication between DMPs relies on multicast communication between the DMPs within a video wall.

  – PTP use of multicast communication

  – Multicast updates of external data sources through the data integration feature, in combination with a widget. As a workaround, configure a data binding component within widgets that use the data integration feature.

  – Unicast state change messages are not retransmitted. If the server is unable to reach the DMP with the state change message in time (due to network issues, DMP being down, etc.), the message will not be retransmitted. The DMP will show the prior state, until a state change message is successfully sent on a future state change.

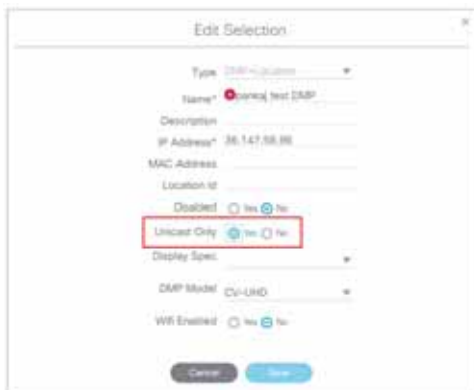**To select unicast on a device using the Cisco Vision Director UI:**

1. Click **Configuration > Devices > Locations & DMPs** tab (Figure 22 on page 42).

Figure 22   Choose the Device to Unicast

2. Select a specific device from your list and click the **Edit** icon. The Edit selection dialog box appears (Figure 23 on page 43).

Figure 23   Selecting Unicast Option for a Specific DMP

3. Click **Yes** for **Unicast Only** for your device.

4. Fill in the rest of your fields and click **Save**.

State Delay—A Better Solution

DMPs using unicast state change messages will not synchronize their state changes with other DMPs, either those using unicast state change DMPs, or with DMPs using multicast state changes.

One possible workaround is for the system to delay the implementation of state changes, to try to allow the system to communicate to all unicast DMPs.

Note: This procedure is intended solely as a workaround for those experiencing synchronization issues due to unicast state change messages. Do not enable state delay unless you specifically experience such synchronization issues. Be aware of the caveats as listed above.

To set the unicast registry in Cisco Vision Director for the device:

1. Click **Configuration > System Configuration > Advanced Registry Settings** (Figure 24 on page 43).

2. In the **Key** column, click **Add.** The Create Configuration Setting dialog box appears.

Figure 24   Adding a Registry
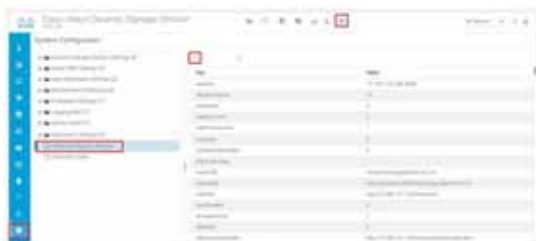
3. In the **Name** field, type **script.stateChange.nextStateDelay**.

4. In the **Value** field, type **n, w**here n is the number of seconds to delay state changes by.

5. Click **Save**.

State Delay Caveats

- State delay effects all DMPs in the system: DMPs using unicast and DMPs using multicast state change messages.

- State delay will cause all state changes to be delayed by that time, making it more difficult to make quick changes to the state.

- State delay is "best effort." There is no guarantee that the value chosen above will achieve synchronization of state change messages, given the network and system conditions.

- Do not make state changes while the state change is pending; unpredictable results may occur.

Troubleshooting Per-Script Multicast Configuration

This section includes information about troubleshooting the following behaviors when per-script multicast optimization is enabled:

-

-

Scripts Unable to Start or Stop

Verify that the multicast packets are reaching the DMPs using any or all of the following methods:

- Look at the sv_msg_mcast_trace.log available from the Troubleshooting menu of the TUI for Cisco Vision Director in the Control logs.

- Use a packet sniffer device at Cisco Vision Director and/or at the DMP.

- Inspect the multicast configuration of the Cisco Connected Venue switch by turning on debug for multicast group subscriptions.

Tip: It is valuable to know the multicast group/port that a specific DMP should be listening on. This can be validated using the dmpconfig debug feature, by going to the URL:

http://svd-ip:8080/StadiumVision/dmpconfig/000000000000?ipaddr=*x.x.x.x*,

where *x.x.x.x* is the IP address of the DMP to be debugged. In the XML output provided, you will see the multicast IP address and port in use.

DMPs Rebooting

DMPs rebooting or becoming unresponsive while per-script multicast is enabled is most likely due to some multicast video port overlap with the ports used for multicast control.

To diagnose this condition:

1. Inspect all multicast port numbers in the configuration to investigate any multicast group/port overlaps.

2. Using a packet sniffer, inspect network traffic on a separate box and via port span rather than on a DMP.

Configuring Multicast Support for Zone-Based Content Synchronization for the DMPs

Zone-based content synchronization provides enhanced recovery for video walls if a DMP reboots during the running of a playlist. Zone-based video wall synchronization is an alternative form of synchronization available for devices participating in a video wall. It makes use of a mechanism native to the devices that helps a group of media players stay in content sync with a leader device over multicast.

The general guideline is to use zone-based video wall synchronization for dedicated video walls that are playing video content longer than 15 minutes. While you can use this form of synchronization for all video walls, the synchronization benefit is best seen with longer-playing video wall content.

The default multicast address and ports are automatically configured to support zone-based content synchronization for the DMPs upon installation of the Cisco Vision Director software; however, the feature is not enabled by default.

Use this task to change the default multicast values as needed, when you assess your system-wide multicast addressing needs.

Note: By default, zone-based content synchronization is not enabled. For more information, see the "Working with Video Walls" section of the Cisco Vision Dynamic Signage Director Operations Guide, Release 6.3.

To configure multicast support for zone-based content synchronization for the DMPs:

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

2. Verify that the following default values for the following properties are compatible for your network, and change as required:

   – **Content sync multicast address**—239.193.0.253

   – **Content sync multicast port**—50001

3. Save your changes.

What To Do Next

After you have configured the system settings for your Cisco Vision Director servers, do the following:

■ Configure the backup environment between your primary and secondary servers. For more information, see Backing Up and Restoring Cisco Vision Director Servers, page 77.

■ For more information about configuring Cisco Vision Director to support multiple venues, see Configuring Cisco Vision Dynamic Signage Director for Multiple Venue Support, page 47.

What To Do Next