Cisco Vision Administration Guide

Dynamic Signage Director

Release 6.3

Last Updated: 2021-04-06
First Published: 2020-08-21

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Contents

About This Guide

This document describes the tasks involved in setting up and maintaining the Cisco Vision Dynamic Signage Director system.

The content is intended for Cisco Vision system administrators and technical field engineers who are responsible for designing and deploying Cisco Vision solutions. It is expected that readers of this document are familiar with basic IP networking, power over ethernet, multicast, and virtualized server environments for the simplest scenarios.

In the documentation for Cisco Vision Dynamic Signage Director, we changed the terms “master” to “lead, leader, or primary,” the term “slave” to “secondary,” the term “whitelist” to “allowlist,” and the term “blacklist” to “blocklist.” There are currently no changes to the product’s syntax, so these terms are still present in the documentation where the current code requires their use. Where an industry standard exists, such as IEEE terminology, we cannot alter the term until the standards change.

Document Revision History

Table 1 lists the technical changes made to this document since it was first published.

Table 1 Document Revision History

Date	Change Summary
Last Updated: 2021-04-06	Updated to simplify the procedure to set the system time zone. See Configuring the System Time Zone, page 31.
Last Updated: 2020-09-30	Updated content to remove racially-biased terms.
First Published: 2020-08-21	First release of this content for Cisco Vision Dynamic Signage Director Release 6.3. This release removes the **Management Dashboard** interface. That functionality moved to **System Status** and is accessed through **Configuration > System Configuration**) and **Device Management** for **DMP and TV Controls** settings. We added server deployment profiles and system backup and restore functions to the HTML UI in the **Manage Software** interface.

Document Organization

Chapter	Description
Cisco Vision Dynamic Signage Director On-Premise Architecture Overview, page 9	Describes the network architectures supported in Cisco Vision Dynamic Signage Director, including the centralized Cisco Vision Dynamic Signage Director network architecture, and the server platforms used to implement the solution.
Configuring the Cisco Vision Director Server System Settings, page 15	Describes how to configure the initial setup of the Cisco Vision Dynamic Signage Director server.
Configuring Cisco Vision Dynamic Signage Director for Multiple Venue Support, page 47	Describes how to enable and manage multiple venue support.
System Accounts on the Cisco Vision Dynamic Signage Director Servers, page 63	Describes the default system accounts implemented by Cisco Vision Dynamic Signage Director for access and control of certain server functions. Aside from the admin account, these system accounts are generally separate from the user accounts that secure access to the Cisco Vision Dynamic Signage Director feature configuration and operation.
User Management in Cisco Vision Dynamic Signage Director, page 71	Describes the Role-Based Access Control (RBAC) function in Cisco Vision Dynamic Signage Director to control user access to only the portions of the system for which they are trained and authorized to use.
Backing Up and Restoring Cisco Vision Director Servers, page 77	Describes how to setup and schedule backups between a primary and secondary server and restore data between them.
Configuring Failover Between Redundant Cisco Vision Director Servers, page 89	Describes the warm standby environment between two servers that run the Cisco Vision Dynamic Signage Director software, where one of the servers operates as the primary active server and the other server operates as a secondary backup server. This module explains how you can configure the backup server to become the active server if a failure occurs and also how to restore the primary server.
Cisco Vision Dynamic Signage Director Server Text-Based User Interface, page 103	Provides an overview of the Text Utility Interface (TUI). The TUI provides a console-based interface for use by system installers, administrators, and troubleshooting personnel to perform routine system tasks such as modifying system configurations, changing passwords, and checking system logs.
System State Reports, page 111	Provides information about the System State Report feature that enables easy capture and export of system state data for Cisco Vision Dynamic Signage Director servers. This information can be sent to a remote support engineer to help troubleshoot any issues that occur with the system.

Related Documentation and Resources

For more information about Cisco Vision hardware and software installation, configuration, and operation, see the Cisco Vision documentation available on Cisco.com at:

www.cisco.com/go/stadiumvisiondocs

See Release Notes for Cisco Vision Dynamic Signage Director Release 6.3.

Cisco Vision Dynamic Signage Director On-Premise Architecture Overview

In its most basic design, the Cisco Vision Dynamic Signage Director on-premise architecture consists of all components of the solution implemented at a single site or venue. The basic Cisco Vision Dynamic Signage Director design can be extended to a multi-venue architecture.

In a multi-venue design, a Cisco Vision Dynamic Signage Director server installed at a central location can be used to manage and control content for multiple sites. DMPs can be installed at remote venues but still controlled by the central Cisco Vision Dynamic Signage Director server.

This module describes the standard on-premise architectures associated with Cisco Vision Dynamic Signage Director standard and multi-venue designs. It includes the following topics:

Standard Cisco Vision Dynamic Signage Director Network Architecture

The three primary areas of the standard Cisco Vision Dynamic Signage Director network architecture include:

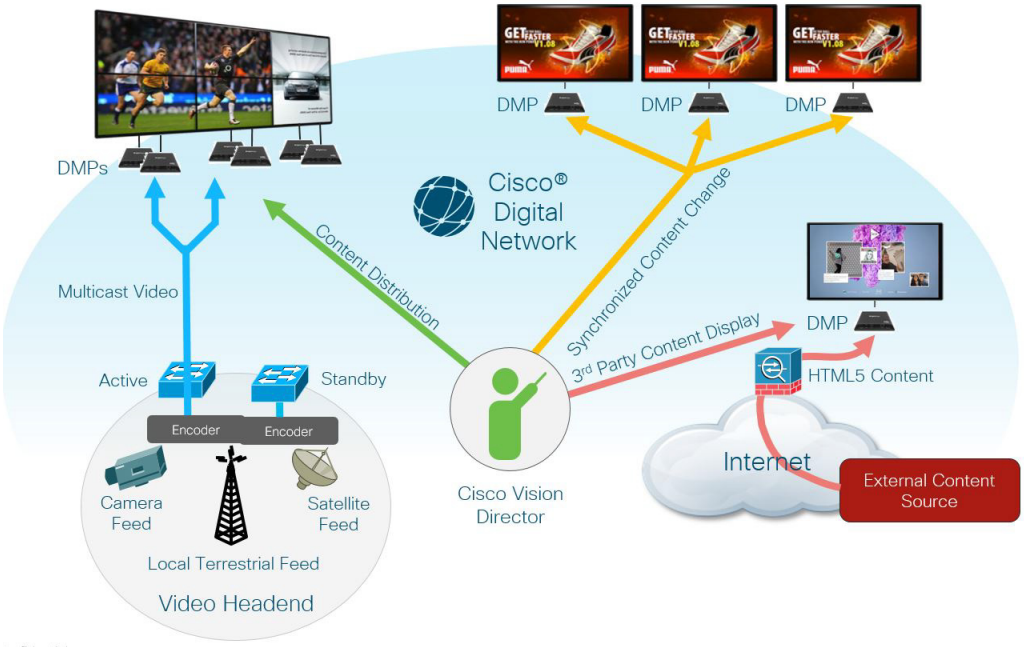
- Headend for video acquisition

  The Cisco Vision Dynamic Signage Director headend is designed to acquire, process, and encode the video content used in the Cisco Vision solution.

- IP network (Connected Venue)
- Endpoints (Digital Media Players)

Figure 1 on page 10 shows the basic network architecture for a Cisco Vision Dynamic Signage Director network.

Figure 1 Basic Cisco Vision Dynamic Signage Director Architecture



Cisco Vision Dynamic Signage Director Server Redundancy

Cisco Vision Dynamic Signage Director supports an environment of two servers that run the Cisco Vision Dynamic Signage Director software, where one of the servers operates as the primary active server and the other server operates as a secondary backup server. If a failure occurs, you can configure the backup server to become the active server, but the failover process is not automatic.

Cisco Vision Dynamic Signage Director supports two servers or a dual virtual server environment. Figure 2 on page 10 shows two virtual servers running Cisco Vision Dynamic Signage Director installed on a single subnet.

Figure 2 Cisco Vision Dynamic Signage Director Redundancy

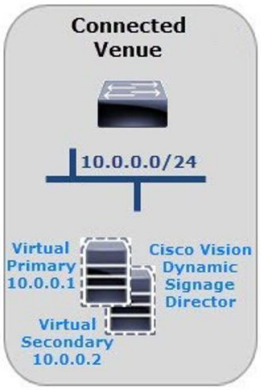


Figure 3 on page 11 shows the architecture of Cisco Vision Dynamic Signage Director server redundancy under normal network conditions and operation. The primary and secondary servers are addressed as independent hosts with two different IP addresses on the same subnet in the Cisco Connected Venue (Connected Stadium) network.

While the secondary server is still connected to the network, notice that communication and control only occurs between the primary Cisco Vision Dynamic Signage Director server and the rest of the network, including the Digital Media Players (DMPs) and any wireless access point.

The secondary server is only connected to the network to be made available as a backup to the primary should a failure occur. In addition, the secondary server can (and should) be configured to be backed up with data from the primary server on a scheduled basis so that it can be ready as a warm standby.

Figure 3 Cisco Vision Dynamic Signage Director Redundancy Under Normal Operation

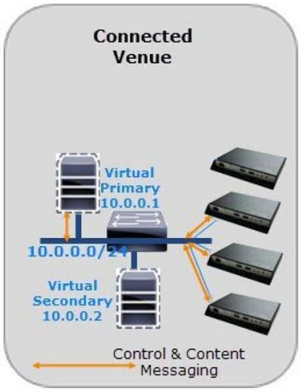
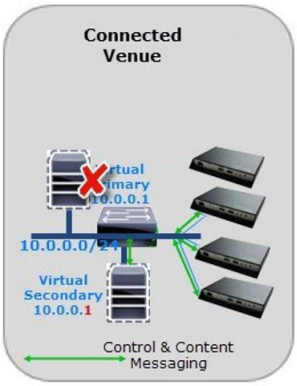


Figure 4 on page 11 shows the redundancy environment when connectivity from the primary Cisco Vision Dynamic Signage Director server fails. When the primary server fails, a manual process must take place to restore the secondary server from a backup, shut down the primary server, and activate the secondary server.

Figure 4 Cisco Vision Dynamic Signage Director Redundancy Under Manual Failover



Notice that the secondary server must be reconfigured to use the same IP address the original primary server. In this example, the secondary server IP address is changed to 10.0.0.1 (from 10.0.0.2) to match the primary server address. When the process is complete, communication and control only occurs between the newly activated secondary server and the rest of the network.

Note: The word “failover” does not mean automatic activation of a secondary server. The failover process is manual with the secondary server acting as a warm standby.

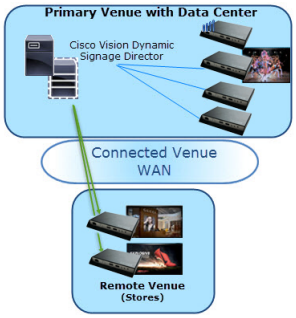
For more information about how to perform the failover process, see Configuring Failover Between Redundant Cisco Vision Director Servers, page 89.

Centralized Cisco Vision Dynamic Signage Director Network Architecture

Figure 5 on page 12 shows a central Cisco Vision Dynamic Signage Director server (that is connected to the headend), with network connections over the Cisco Connected Venue WAN to multiple remote sites.

The remote venue uses only DMPs that are remotely located from the primary venue, but control is retained by the central Cisco Vision Dynamic Signage Director server.

Figure 5 Centralized Cisco Vision Dynamic Signage Director with Remote Sites



Hierarchical Management

The centralized Cisco Vision Dynamic Signage Director architecture implements control of multiple venues using Hierarchical Management, which includes the following areas of functionality:

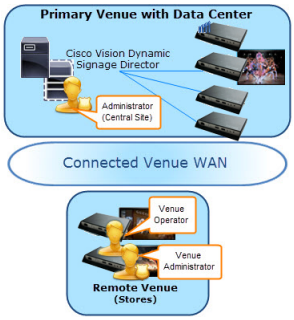
- Organization of Venue Administrator, Venue Operator, location, playlist, and script objects into site-specific groups by the central Administrator role using venue association to manage access and control.
- Use of the Venue Operator role to limit access and control of event operation at one or more assigned remote sites.
- Use of the Venue Administrator role to provide additional administrative, but limited permissions at the venues authorized by the central Administrator for that user, for the following areas of Cisco Vision Dynamic Signage Director:
  - Script Management
  - System Configuration—Read-only access with limited command support.
  - Device Management (Command Center Monitoring)—Read-only access.
  - Configuration > Devices (Display Specifications only); Read-only access to Groups & Zones, Channels, and Luxury Suites.

  Note: External content, channels, and Dynamic Menu Board (DMB) content are global to all venues. Therefore, these global content items also can be deleted/hidden by a Venue Administrator.

Figure 6 on page 13 shows the use of Hierarchical Management in Cisco Vision Dynamic Signage Director, where a central site user with administrator role-based access control (RBAC) permissions is located at the central site data center where the primary Cisco Vision Dynamic Signage Director server resides.

The remote venues can have venue operators and venue administrators, assigned by the primary administrator.

Figure 6 Hierarchical Management in Centralized Cisco Vision Dynamic Signage Director



The Primary Administrator can perform all venue-related functions, including assigning Venue Administrators, Venue Operators, content and scripts into their corresponding venue-specific scopes of control. At the remote venues, the remote Venue Operators can control the scripts associated to their assigned venue scope-of-control.

For more information, see the following modules of this guide:

- For a description of the supported user roles in Cisco Vision Dynamic Signage Director, see User Management in Cisco Vision Dynamic Signage Director, page 71.
- For information about configuring remote venues in a centralized Cisco Vision Dynamic Signage Director network architecture, see Configuring Cisco Vision Dynamic Signage Director for Multiple Venue Support, page 47.

Virtual Server Support

For information about virtual server requirements and installation in Cisco Vision Dynamic Signage Director, see:

- Release Notes for Cisco Vision Dynamic Signage Director Release 6.3
- Cisco Vision Software Installation and Upgrade Guide: Dynamic Signage Director Release 6.3

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

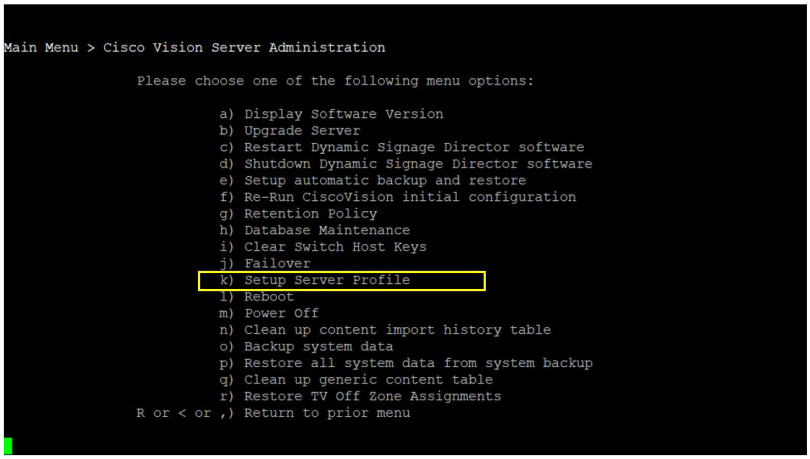
The Mini and Small differ in clock speed. During a full installation, the installer will detect and select a server size, based on resources available to the VM: RAM, CPU clock speed, and vCPU count. During an upgrade, the current configuration is unchanged. Use TUI to verify server is within these specifications.

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

To select a Cisco Vision Director deployment:

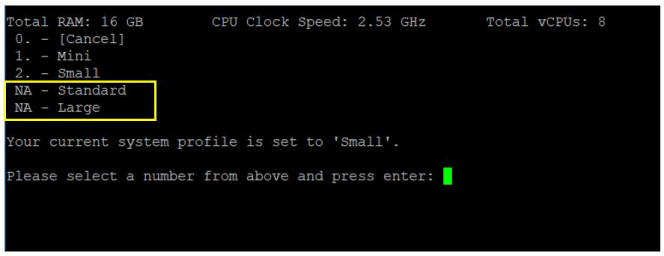
1. Log in using TUI.
2. Select **Cisco Vision Server Administration.**
3. Select **Setup Server Profile** (Figure 1 on page 16).

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:

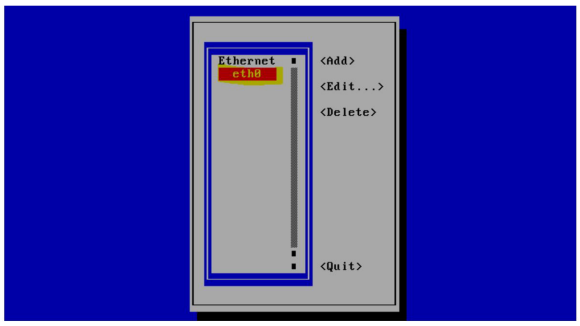
- New DSD Full ISO Installation–Mandatory, page 17 (required)
- Editing the Hosts File, page 23 (as required)
- Editing the Hosts File, page 23 (as required)
- Restarting the Network Service on the Server, page 24 (as required)
- Generating the SSL Certificate, page 24 (required)
- Configuring NTP on 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

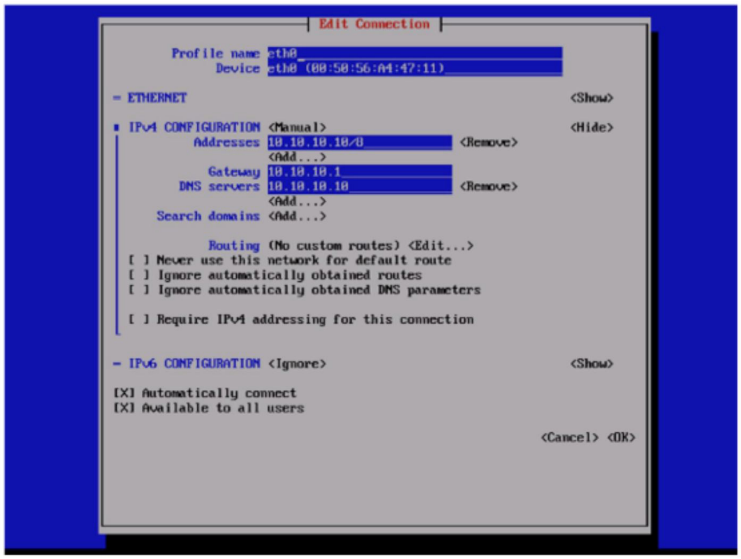


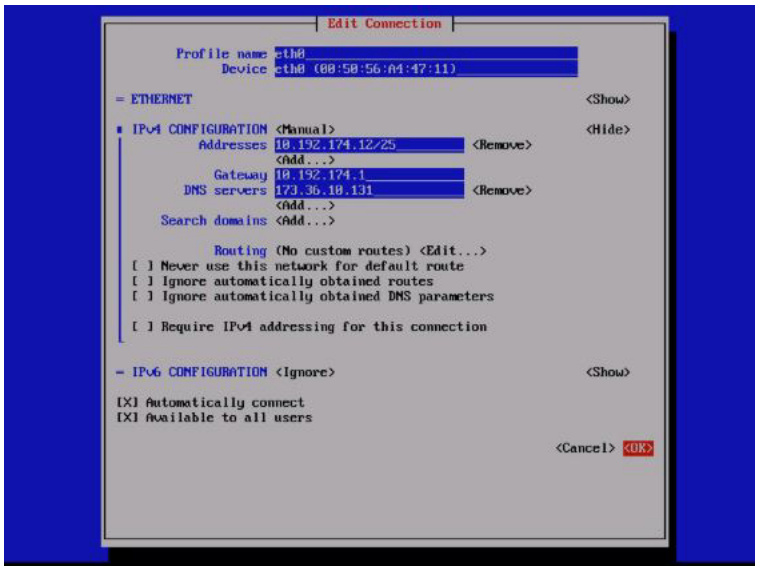
Note: Use left and right arrow keys to move the cursor to the previous or next fields. Use Space to make a selection (shown highlighted in red).

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.

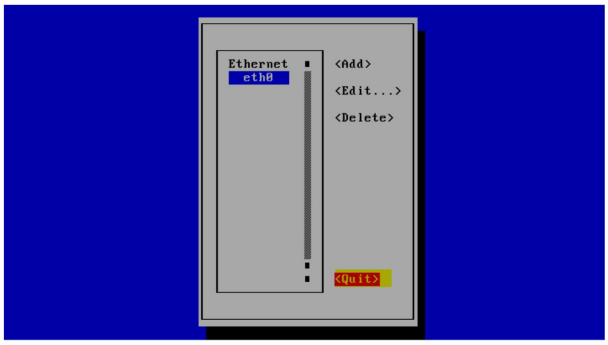
Figure 4 Edit Connection Address Update





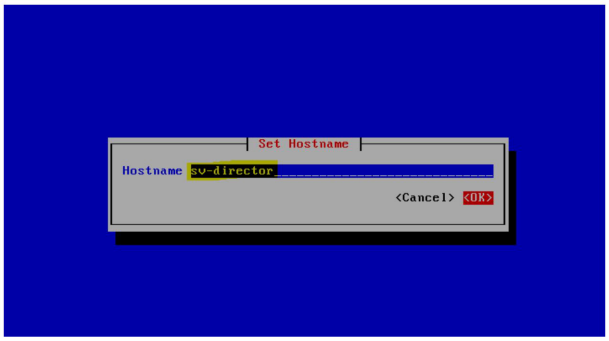
5. Select “Quit” to exit out of network configuration TUI (Figure 5 on page 20).

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.

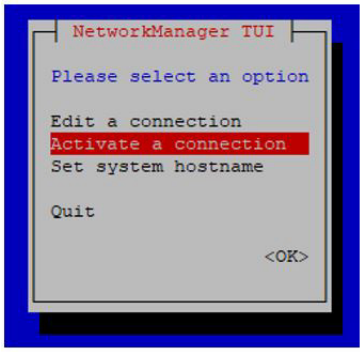
7. Click **OK** (Figure 7 on page 20). DSD components should begin installing.

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

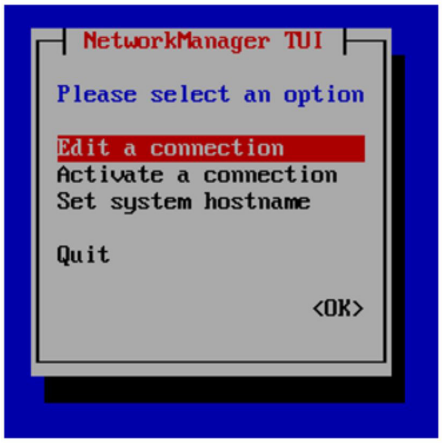
Tip: If you need to back out of the TUI menus for any reason, type `:q` or a comma.

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).

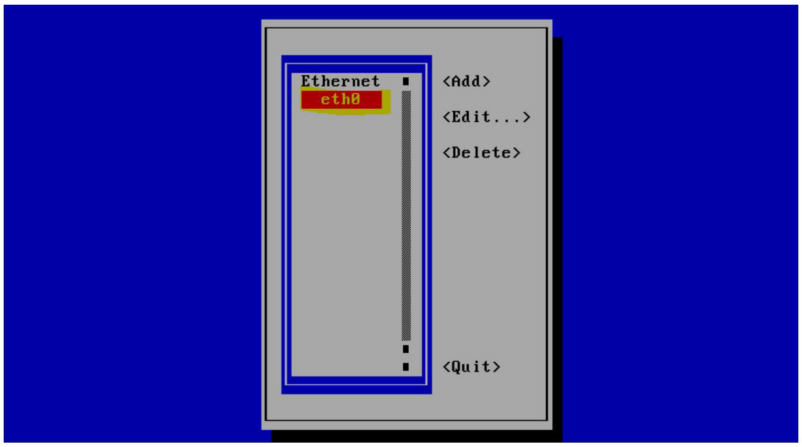
Figure 9 Edit a Connection



4. Select “eth0”

5. Select “Edit...”(Figure 10 on page 22).

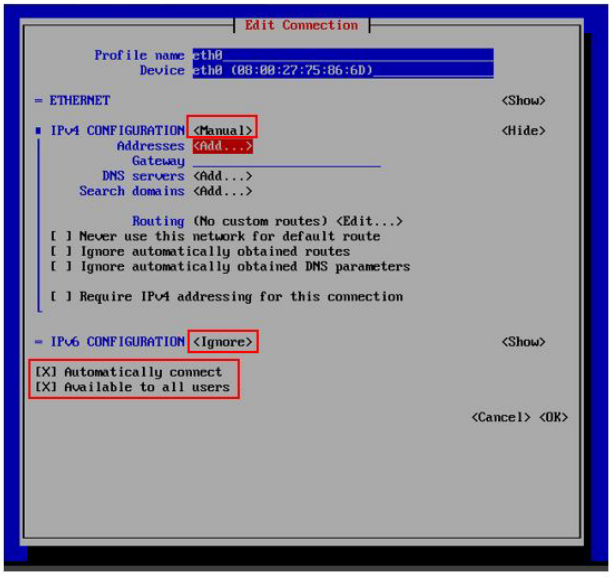
Figure 10 Editing the Network



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

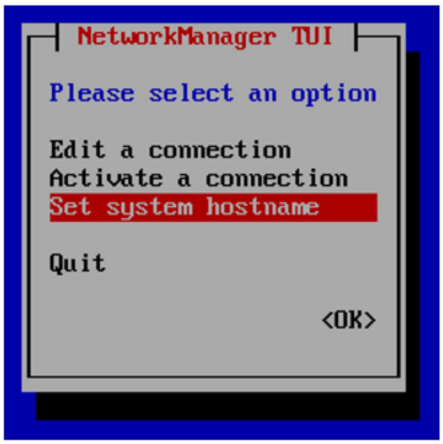


IMPORTANT: Verify the default values boxed above and listed below are checked or selected.

- Keep the name of “eth0”.
- Keep the IPv6 CONFIGURATION to “Ignore”.
- Keep the boxes for “Automatically connect” and “Available to all users” checked.

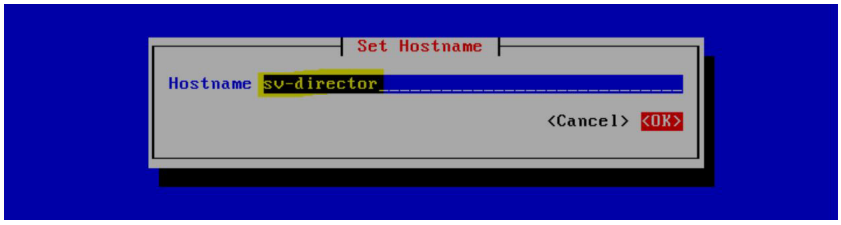
10. Navigate to **OK** and hit **Enter**.
11. Go back to Network Manager TUI main menu.
12. Select **Set system hostname** (Figure 12 on page 23).

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

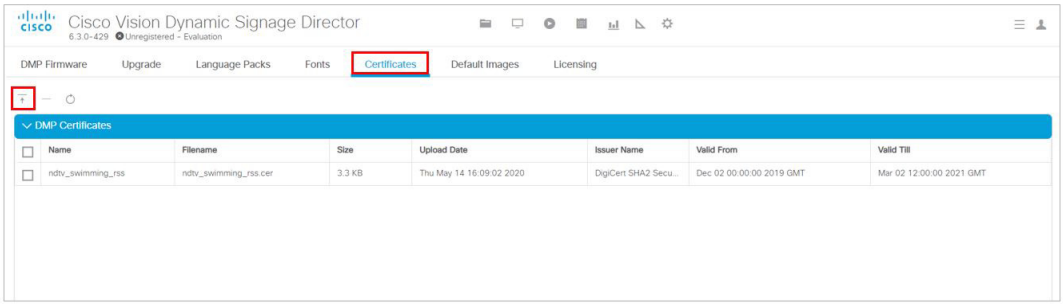
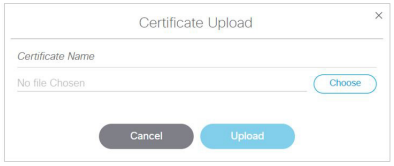


Figure 14 Certificates Upload Screen



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.

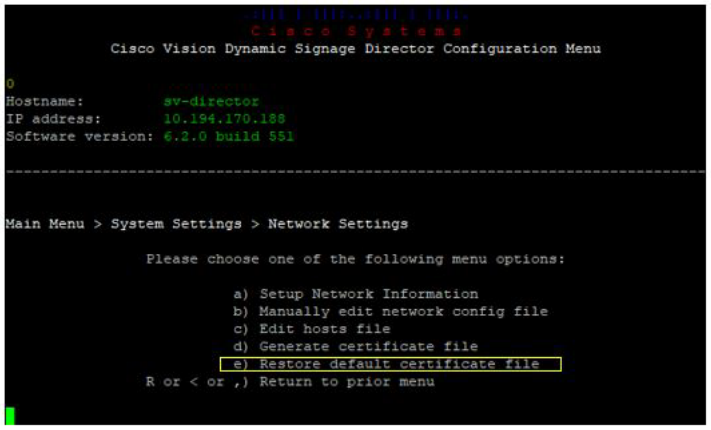
Importing Dynamic Signage Director (DSD) Certificates

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)

- 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!

```
# For more information about this file, see the man page ntp_auth(5).
#
# id    type    key
15      M       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:

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
server 192.168.69.70 iburst key 15
```

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**.

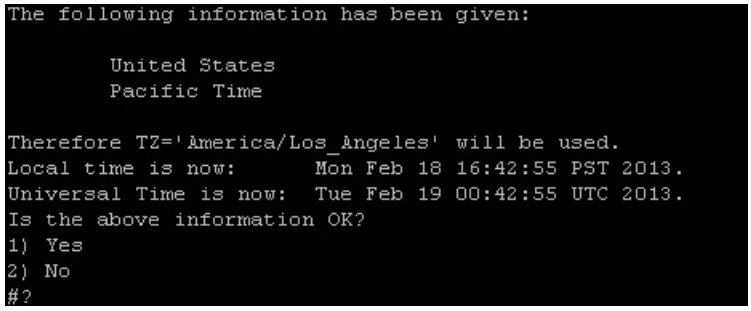
b. Type the number that corresponds to the applicable continent or ocean for the location of the server.

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).

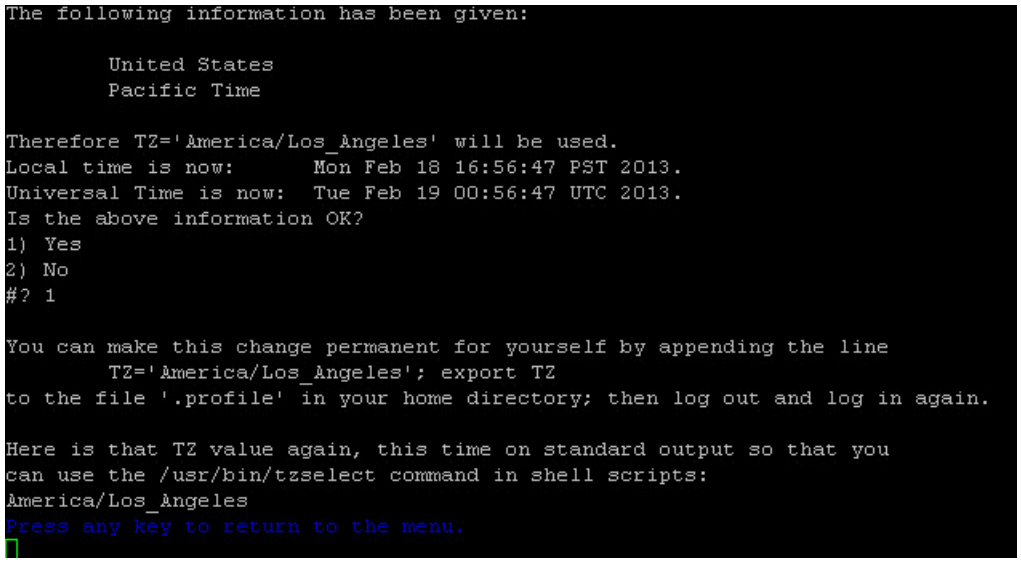
Figure 16 Time Zone Confirmation Prompt



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



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:

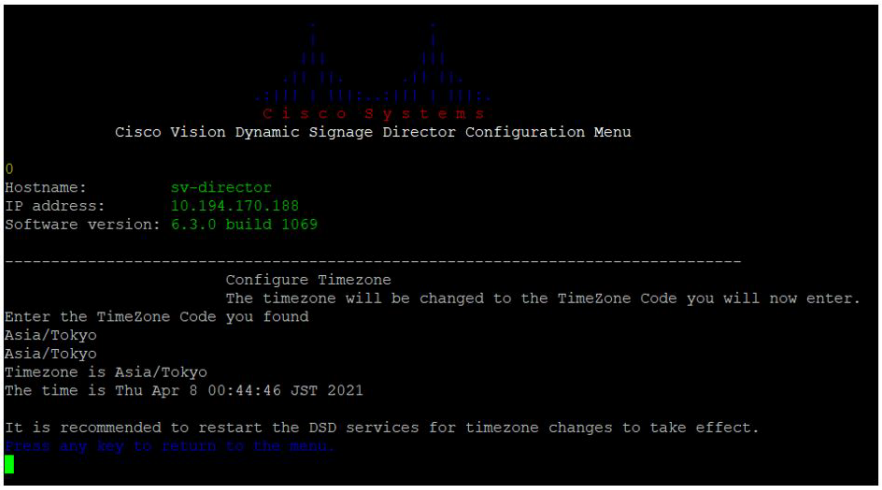
- How to use vi editor commands.
- The time zone code for the server location. If you need to look up the time zone code, see Finding the Time Zone Code for System Configuration, page 29.

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

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 Table 3 on page 34 and Table 4 on page 35.

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.

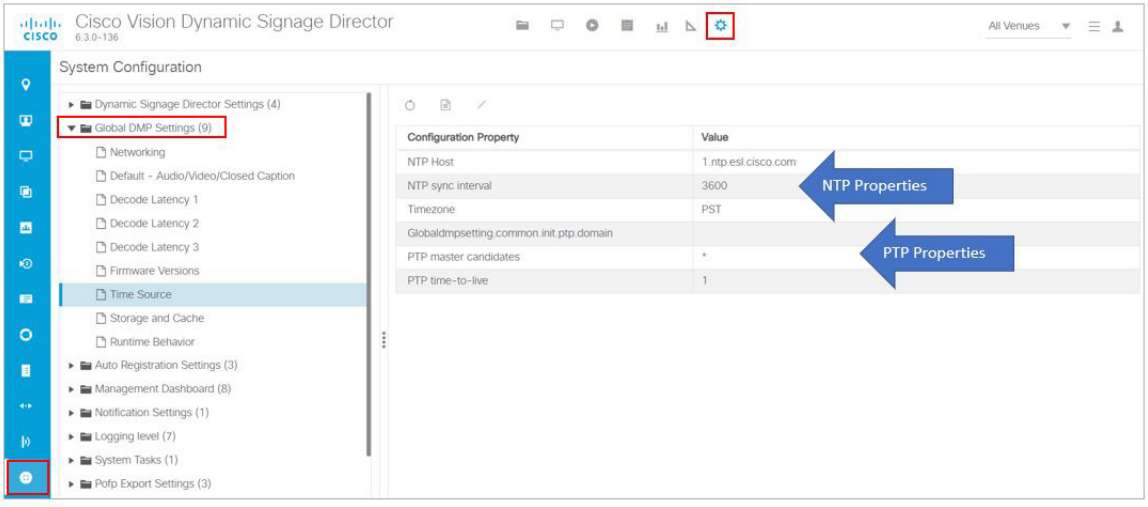
Table 4 Global DMP Settings–NTP Property Values

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:

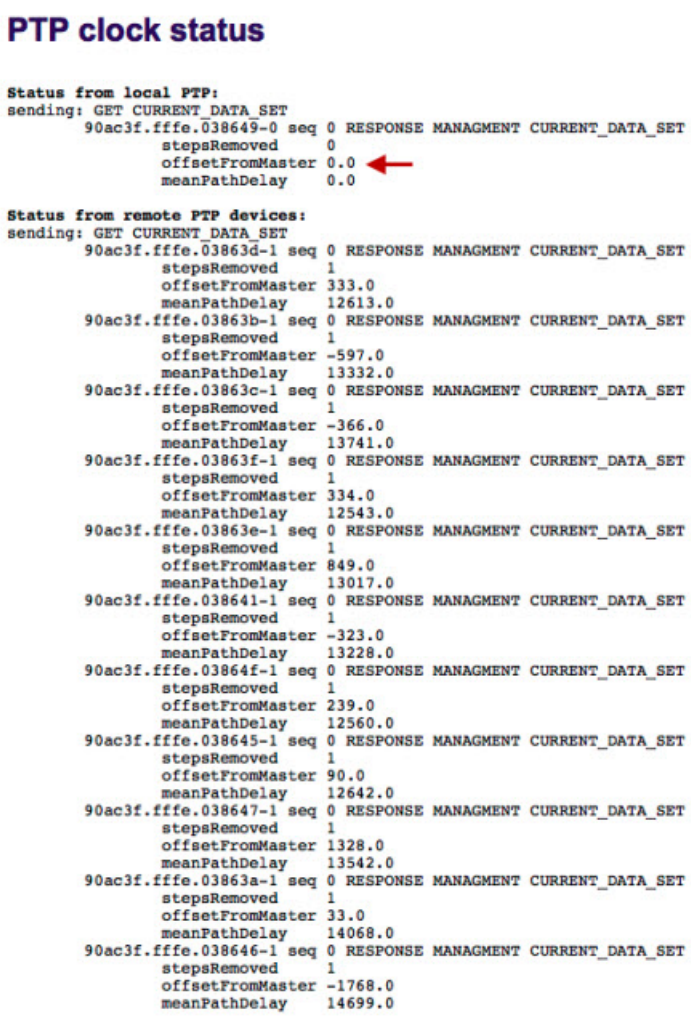
1. Open your browser and navigate to one of the DMPs:

   http://*sv4k-ip-address***/ptp.html**

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

Figure 20 on page 36 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

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

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:

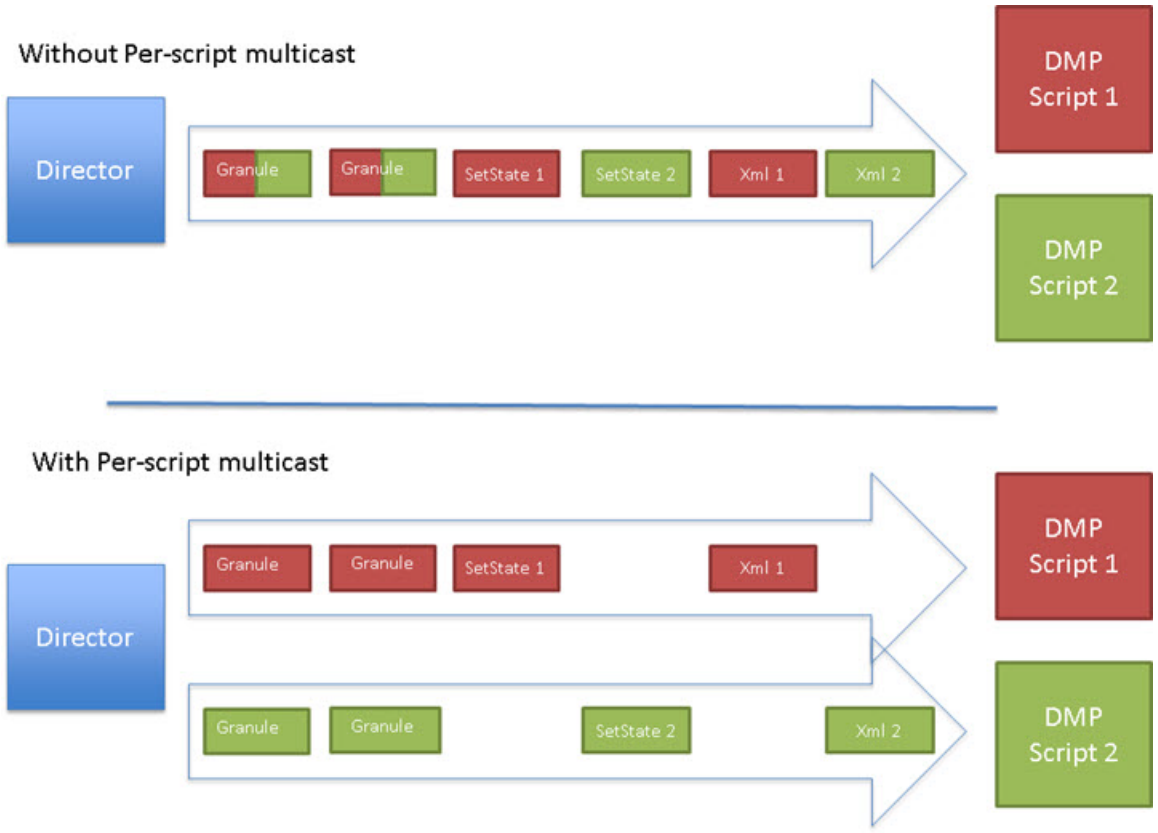
- Per script, you can use 20 maximum
- If you are running more than 20 scripts, then the first 20 scripts operate using per-script multicast channels, and the additional scripts are run over the global multicast host port.
- No remote servers required
- Default: disabled

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 Troubleshooting Per-Script Multicast Configuration, page 44.

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.

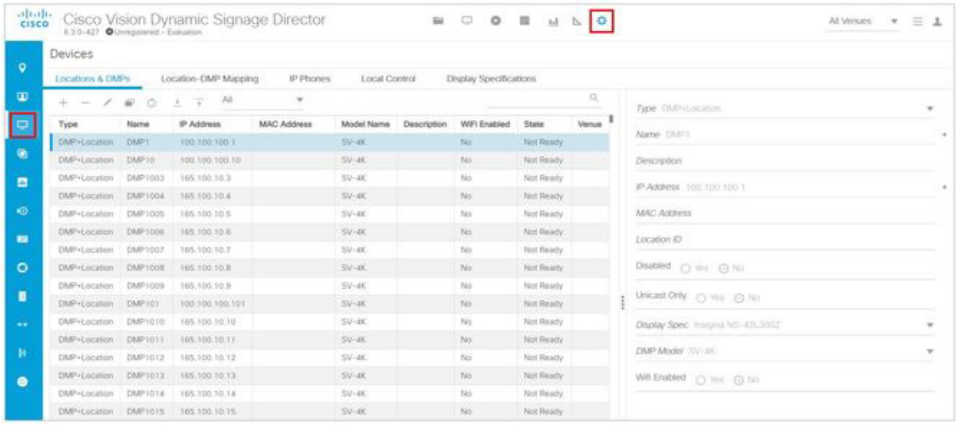
There are some limitations with unicast state change messages:

- 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:

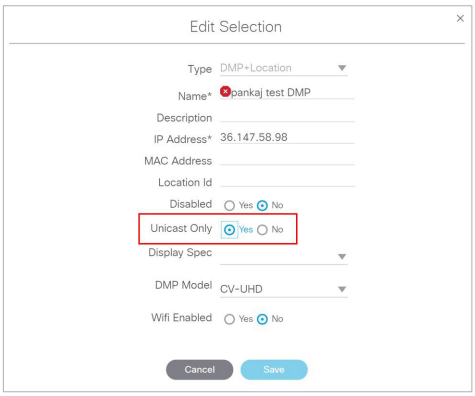
1. Click **Configuration > Devices > Locations & DMPs** tab (Figure 22 on page 42).

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.

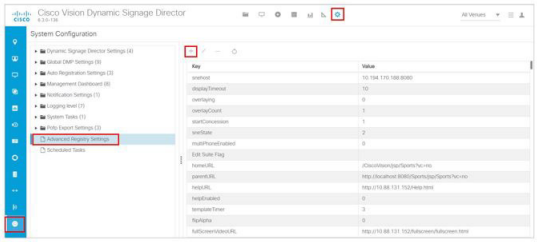
One possible workaround is for the system to delay the implementation of state changes, to try to allow the system to communicate to all unicast DMPs.

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, page 44
- DMPs Rebooting, page 44

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

Configuring Cisco Vision Dynamic Signage Director for Multiple Venue Support

A centralized server site can be deployed with multiple remote sites in a multi-venue architecture. This document is intended for Cisco Vision Dynamic Signage Director administrators and describes how to enable and manage multiple venue support.

Contents

Prerequisites for Configuring Multiple Venue Support

Before you configure multiple venue support, be sure that the following requirements are met:

- You have read Cisco Vision Dynamic Signage Director On-Premise Architecture Overview, page 9.
- You understand the deployment of zones, groups and locations and the use of playlists and scripts in Cisco Vision Dynamic Signage Director.
- The centralized Cisco Vision Dynamic Signage Director server is installed.
- You have planned the configuration for any new or changes to existing Locations. For existing Locations be sure that you are aware of current group/zone associations that will be disabled once you reassign an existing Location to a specific venue.

Restrictions for Configuring Multiple Venue Support

Before you configure Cisco Vision Dynamic Signage Director for multiple venue support, be sure that you consider the following restrictions:

- Any remotely-located DMPs are controlled by the central Cisco Vision Dynamic Signage Director server.
- The PTP lead for DMP time service must be co-located with those remote DMPs and on the same VLAN.
- Venue objects (such as locations, playlists, and scripts) are limited to a single-venue association, except for users who are assigned to the role of Venue Operator.

Caution: Once an existing Location is reassigned to a specific venue, any previous group/zone associations will be disabled and the Location will need to be reassigned to groups/zones.

- Only Venue Administrators or Venue Operators can be associated to one or more venues.
- Only certain areas of the Cisco Vision Dynamic Signage Director software are *venue aware*, which means that certain roles can apply venue-specific scope of control using the venue selector. These areas include:
  - **Device Management** (Command Center Monitoring)
  - **Library > Upload Assets**
  - **Script Management**

    Note: External content, channels, and Dynamic Menu Board (DMB) content items are global to all venues. Therefore, these global content items also can be deleted by a venue administrator.
  - **Event Management**
  - **System Status**

  For information about specific access allowed by user role, see Table 2 on page 75.

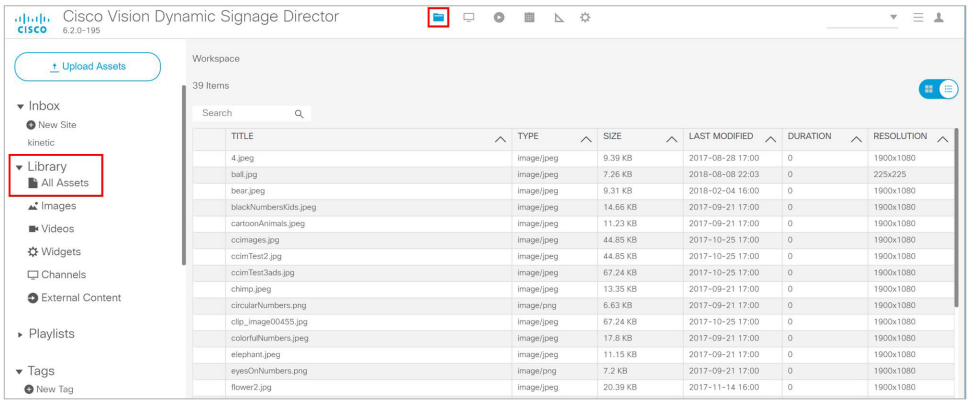
Note: The following areas of the **Configuration** interface are not directly venue-aware using the venue selector, but objects defined there can have a venue-specific relationship:

- Users—You can define all Users under **Configuration > Users**, but you can only associate venues to Venue Administrators or Venue Operators under the Venues tab. The Users interface is not venue aware.
- Groups & Zones—Zones and groups inherit their venue association through the Location. Locations are associated to venues under the Venues tab by the administrator.
- Triggers—Triggers can be applied to venue-associated scripts, but the Triggers interface itself is not venue aware, and all defined triggers in Cisco Vision Dynamic Signage Director are global in scope.
- Playlists imported using the Media Planner Import API need to be manually assigned to venues after import into Cisco Vision Dynamic Signage Director.

Caution: Cisco Vision Dynamic Signage Director does not support disabling of multiple venue support (set the "Multiple Venue Enabled?" property to false) after you have enabled it and associated objects.

Note: When multivenue is enabled the **All Assets** menu item will not display (Figure 1 on page 49).

Figure 1 All Assets Not Available with Multi-Venue Enabled



Information About Configuring Multiple Venue Support

This section includes the following topics:

Role-Based Access Control for Hierarchical Management of Multiple Venues

Cisco Vision Dynamic Signage Director Release 5.0 introduced a new role of Venue Administrator.

For more information about user management and Role-Based Access Control (RBAC), see User Management in Cisco Vision Dynamic Signage Director, page 71.

Administrator

The Cisco Vision Dynamic Signage Director administrator can perform all functions related to venue management.

Most of the configuration management for multiple venue support resides only with the Cisco Vision Dynamic Signage Director administrator role, which includes the addition of the following functions:

- Enabling Cisco Vision Dynamic Signage Director for multiple venue support.
- Creating venues in Cisco Vision Dynamic Signage Director.
- Creating users with role of Venue Administrator and Venue Operator.
- Capability for associating any venues to users, locations, content, playlists, scripts, tags, and folders.

Content Manager

In a multi-venue architecture, a Content Manager can perform all of the same functions as within a standard Cisco Vision Dynamic Signage Director environment, with the addition of the following capabilities:

- Selecting **Configuration > Venue**.

- Importing content to be associated with one or more venues by using venue tags.
- Creating playlists and scripts to be associated with the currently selected venue scope or all venues.

Note: Content Managers can only create new objects with venue assignment based on the currently selected venue in the venue selector. To reassign an object to a different venue, the Content Manager must remove the object and add it again.

Venue Administrator

The Venue Administrator role has limited permissions at the venues authorized by the central Administrator for that user, for the following areas of Cisco Vision Dynamic Signage Director:

- **Device Management**
- **Library > Upload Assets**
- **Script Management**
- **System Configuration**—Read-only access with limited command support
- **Configuration > Devices** (**Display Specifications** only); Read-only access to Groups & Zones, Channels Definitions, Luxury Suites

Venue Operator

The Venue Operator role is based on a subset of Event Operator and Help Desk roles, with the added functionality of venue-specific scope of control. The Venue Operator role supports the following capabilities:

- Changing the user password in **Configuration > Users**.
- Selecting venue scope for the venues for which permissions are granted.
- Viewing and monitoring information on the **System Status** with read-only access to the venues for which permissions are granted.
- Executing scripts and related state functions during an event at the venues for which permissions are granted.
- Running **Device Management**.

Note: In a multi-venue architecture, an Event Operator can perform all of the same functions as within a standard Cisco Vision Dynamic Signage Director environment. The Event Operator role is not venue aware. To support venue-specific scope of control for scripts, use the new Venue Operator role.

Understanding Venue Association

A centralized Cisco Vision Dynamic Signage Director site with multiple remote sites (venues) supports the following functionality:

- Association of venues to Users, Locations, Playlists, and Scripts (referred to collectively as *venue objects*).
- Inheritance of venue association from Locations for Groups, Zones, and Luxury Suites.

Tip: You can use the Bulk Administration Tool (BAT) to associate multiple locations to a venue.

Understanding Scripts and Staging Behavior in a Multi-Venue Environment

This section provides information about scripts when implementing them in a multi-venue environment.

Script Best Practices

When configuring scripts in a multi-venue environment, consider the following best practices:

- Configure scripts to control only a single venue.
- When creating venue-specific scripts, use the following process:
  a. Create the script first without any actions—Name it and save it.
  b. Assign the script to the venue.
  c. Edit the script to assign it to zones/groups.
  d. Use playlists that belong to the same venue.
  e. Edit the script to further define states.
- Be sure that scripts that are intended to run at a remote site are not also being run on any non-site DMPs.
- For optimal operation, avoid running multiple event scripts to the same DMPs at a site.

Note: If you move a script assignment from one venue to another, be aware that the zones/groups/playlists might still be associated with the old venue until they are manually reassigned. If a script is part of one venue and zones/groups/playlists are part of another venue, then the script will not start.

Script Staging Behavior

In Cisco Vision Dynamic Signage Director, script staging is always serialized. For example, if a manual staging job is running, a script-initiated staging job will begin after the manual staging has completed. The scripts will not start at the same time.

In the case of content replacement, content staging happens right away. If current staging is going on, content replacement staging will go into the queue. The DMP will play old content until confirmation of successful staging occurs, so there could be some time delay.

How to Configure Multiple Venue Support

This section includes the following tasks:

Enabling Multiple Venue Support in Cisco Vision Dynamic Signage Director

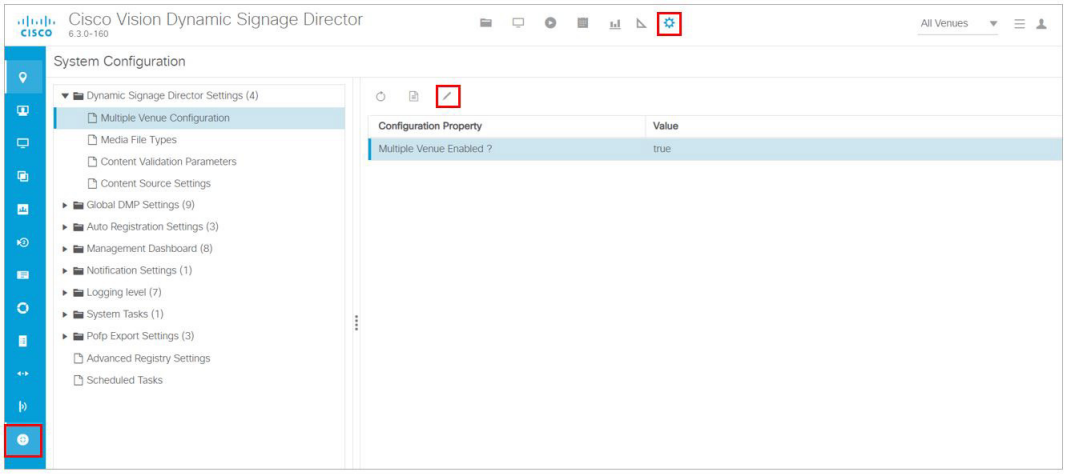
By default, Cisco Vision Dynamic Signage Director is not configured for multi-venue deployment. To support Cisco Vision Dynamic Signage Director with a centralized server and remote sites, you must configure the Multiple Venue Configuration property, which will set the corresponding registry key. Once this registry key is set, it will be preserved during an upgrade.

Caution: Cisco Vision Director does not support disabling of multiple venue support (set the "Multiple Venue Enabled?" property to false) after you have previously enabled it and associated objects. In other words, do not toggle between enabling multiple venue support and disabling it.

To enable multiple venue support in Cisco Vision Dynamic Signage Director:

1. Log into Cisco Vision Dynamic Signage Director as an administrator.
2. Click **Configuration > System Configuration** > **Dynamic Signage Director Configuration > Multiple Venue Configuration**.
3. Set the **Multiple Venue Enabled?** property value to "**true**." See Figure 2 on page 52. If it not set to "true," click **Edit**. The Edit – Configuration Setting dialog box appears. Set the **Value** to "true" and click **Save**.

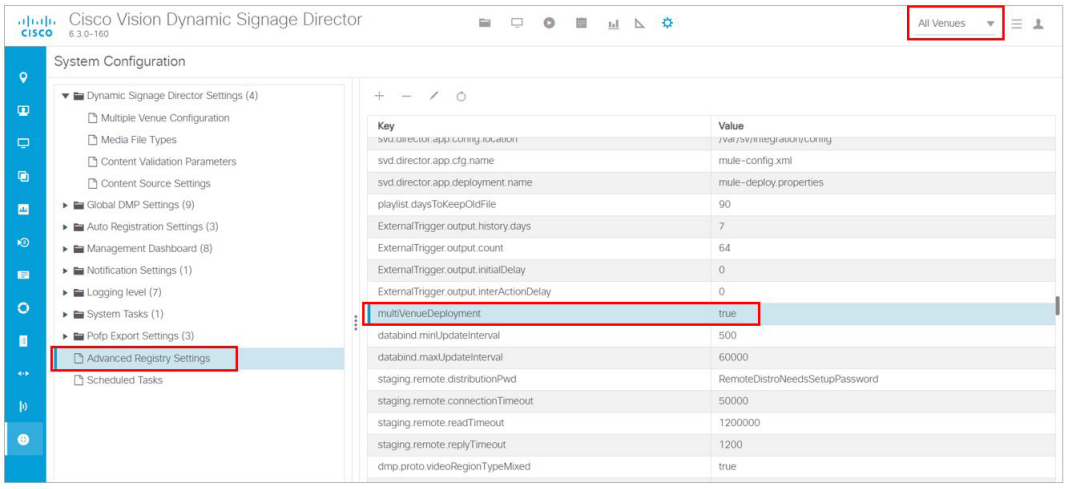
Figure 2 Enable Multiple Venue in Management Dashboard



4. Click the **Refresh** icon to update property values.
5. Click **Save**.

   Note: The multiple venue management functions are enabled in Cisco Vision Dynamic Signage Director and the registry key (Figure 3 on page 52) named "**multiVenueDeployment**."

Figure 3 Registry: multiVenueDeployment



6. Confirm that the "**All Venues**" control appears in the upper right corner of the **Main Menu** window.

7. Go to **Configuration** > **Venues** and confirm that the Venues icon is available.

Tip: If you already had **Configuration** open before enabling multiple venue support, refresh the window to display the **Venues** icon.

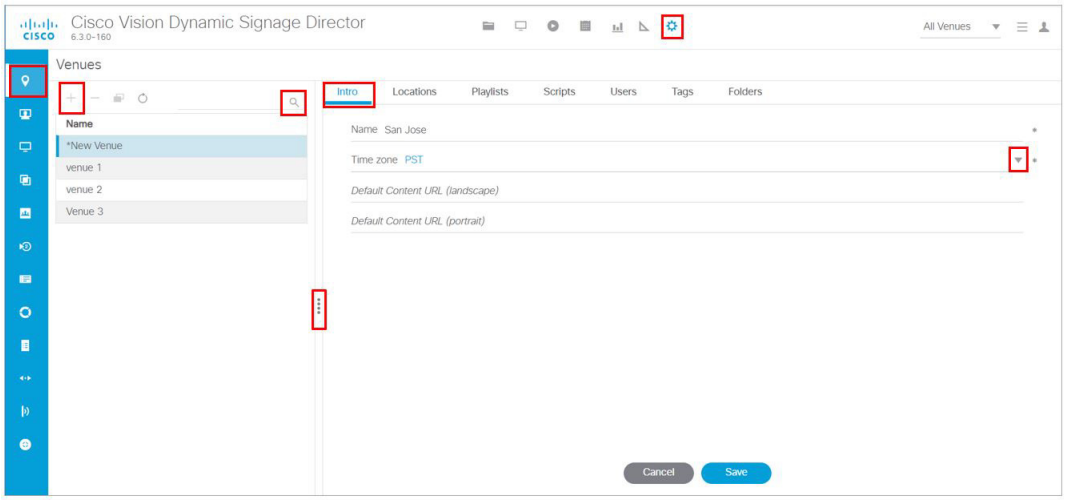
Adding Venues to Cisco Vision Dynamic Signage Director

After you enable multiple venue support in Cisco Vision Dynamic Signage Director, you can add remote sites as venues.

To add venues in Cisco Vision Dynamic Signage Director:

1. Log into Cisco Vision Dynamic Signage Director as an administrator.
2. Go to **Configuration > Venues** (Figure 4 on page 53).
3. Click the plus (**+**) icon.

Figure 4 New Venue Intro Panel



4. (Required) In the Name box, type a unique and identifiable name for the venue. “New venue” is the default.
5. (Required) In the Time zone box, click the arrow to open the drop-down box and select the time zone for the remote site.

   Note: This option is informational only and for proof-of-play reporting.
6. Set Default Content URL (landscape).
7. Set Default Content URL (portrait).
8. Click **Save**.

Associating Venues with Cisco Vision Dynamic Signage Director Objects

You can associate venues with Locations, Playlists, Scripts, and Users in Cisco Vision Dynamic Signage Director. Only the administrator can perform associations for all of these objects for all venues using **Configuration > Venues**.

After the initial multiple venue configuration and association is completed by the Cisco Vision Dynamic Signage Director administrator, other roles (Content Manager, Venue Administrator, and Venue Operator) can use the venue selector in Cisco Vision Dynamic Signage Director for their authorized functional areas of the interface to select their venue scope of control. Any related tasks will be based on that selected venue scope (All Venues or a specific venue).

This section includes the following topics:

Guidelines for Associating Venues

Before you associate venues in Cisco Vision Dynamic Signage Director, understand the following guidelines:

- Each object is limited to a single-venue association, except for users.
- Only users with the assigned role of Venue Administrator or Venue Operator can be assigned to one or more venues by the administrator.
- Only the following roles can see the venue selector in the Cisco Vision Dynamic Signage Director interface and use it to select the venue scope of control for their authorized areas:
  - Administrator
  - Content Manager
  - Event Operator
  - Venue Administrator
  - Venue Operator

Caution: If a location is already in a group/zone configuration, it will be forcibly removed from those groups and zones when you either associate or disassociate the location from a venue. Scripts might fail to start on those endpoints because they are not part of the group anymore.

- Refer to Script Best Practices, page 51 for guidelines on script creation and association.

Venue Association Procedure

To associate venues with Cisco Vision Dynamic Signage Director objects:

1. Log into Cisco Vision Dynamic Signage Director as an administrator.
2. Go to **Configuration** > **Venues**.
3. In the Venue list, click the name of the venue that you want to associate.
4. Do the following to assign object types to the selected venue:
   a. Click **Locations**, **Playlists**, **Scripts**, **Users**, **Tags**, or **Folders**.
   b. In the “Available” panel, select the name of the location, playlist, script, user, tag, or folder that you want to associate.

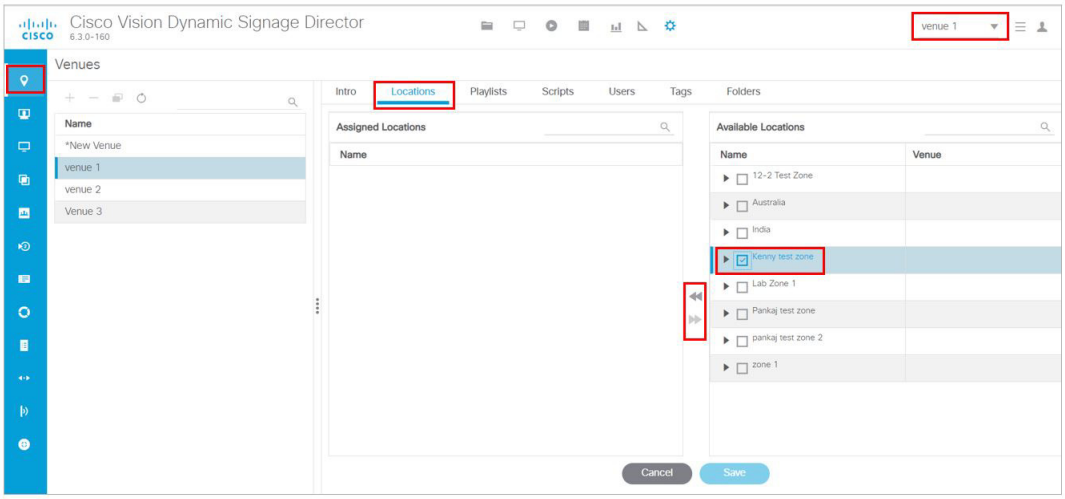
Tip: You can multi-select objects. Click the checkbox and **Ctrl+Click** to select additional objects.

c. Click the **"moving box icon"** icon, shown in red.

The object name is added to the Assigned panel.

d. Repeat from Step a. on page 54 or Step b. on page 54 for as many objects as you need to associate.

Figure 5 Associate Locations to Venue Example



5. (Optional) To remove an assigned object, select the name of the object in the "Assigned" panel and click the **move** button.

6. When associations are complete, click **Save**.

Troubleshooting Venue Association Conflicts

When you attempt to associate objects to venues, certain conditions can cause the system to warn about objects that are not optimally configured to be associated to the venue, such as a Location already being associated to a group or zone in another venue. The warning message identifies the objects, which allows you to do one of two things:

- Click **Close** to go back to the Cisco Vision Dynamic Signage Director configuration to confirm that the object best follows venue association guidelines and note or change the configuration.
- Click **Force** to permit the system to attempt to make the requested association for the objects in conflict.

  Note: The Force button might not work for all associations. The system attempts to force the specified user action but several factors influence its success. For best results, read the error message and see what objects are in conflict with the requested action. Take corrective steps to avoid the conflict within Cisco Vision Dynamic Signage Director.

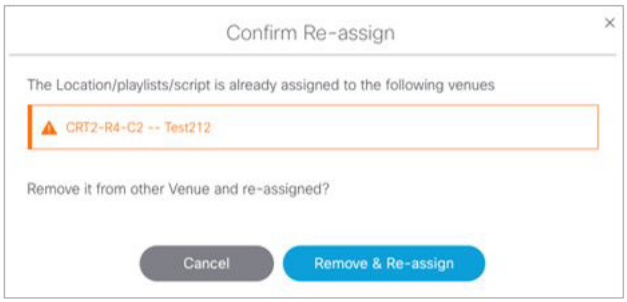
Figure 6 on page 56 shows an example of an error message that can appear when you attempt to associate venue objects and there are conflicts within the Cisco Vision Dynamic Signage Director configuration. Any other objects not in conflict will be associated to the venue as requested.

Figure 6 Venue Association Conflict Message Example

Figure 7 on page 56 shows an example of a venue assignment conflict message where the location, playlist, or script that you tried to assign to a venue is identified as already assigned to another venue. The original venue assignment is displayed in the message ("Cheyenne2" in this example). You can do one of two things:

- Click **Remove & Re-assign** to proceed with the new venue assignment and remove the specified object from its current venue assignment.
- Click **Cancel** to retain the original venue assignment and return to Cisco Vision Dynamic Signage Director.

Figure 7 Confirm Object Reassignment Message Example



Removing Venues From Cisco Vision Dynamic Signage Director

To remove a venue from Cisco Vision Dynamic Signage Director:

1. Log into Cisco Vision Dynamic Signage Director as an administrator.
2. Go to **Configuration** > **Venues** (Figure 5 on page 55).
3. Remove association from all objects that are linked to the venue that you want to remove.
4. In the Venue List panel, select the venue that you want to remove.
5. Click the **Delete** icon (dash).

Selecting Venue Scope

You can select venue scope in the **Configuration > Venues** interface and in the **Management Dashboard**. However only certain areas of the interface are venue aware. Once you have enabled the software for multiple venue support and added new venues, you can use the venue selector in those areas that are venue aware.

Venue status is indicated in the venue selector using a radio button that is colored red to indicate that the venue is disabled and green to show that the venue is online.

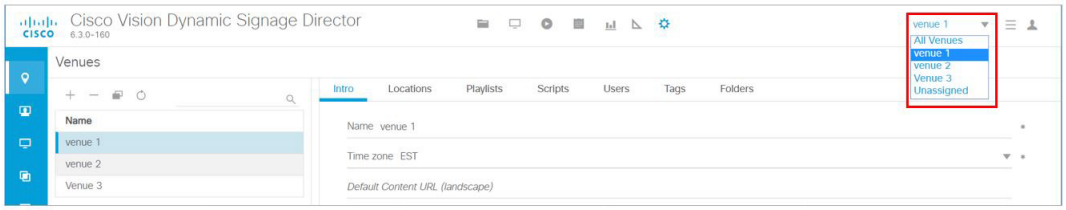
Caution: Take note that the venue selector will show the last venue that you selected, but the scope will not be limited to the selected venue if you are not in a venue-aware area of the interface. The global scope will apply (All Venues). For more information, see Understanding Venue Association, page 50.

To select venue scope:

1. Log into Cisco Vision Dynamic Signage Director as an administrator, content manager, venue administrator, or venue operator.
2. At the top of the window, look for the venue selector drop-down box.

Figure 8 on page 57 shows an example of the venue selector in the Cisco Vision Dynamic Signage Director.

Figure 8 Venue Selector Drop-Down Box



3. Do one of the following:
   - To apply the scope of operation to a specific venue, select the name of the venue in the drop-down box.
   - To apply the scope of operation to all venues, select **All Venues**.
4. Continue to the **Configuration** area that you want to configure.

Monitoring Venues From the Management Dashboard

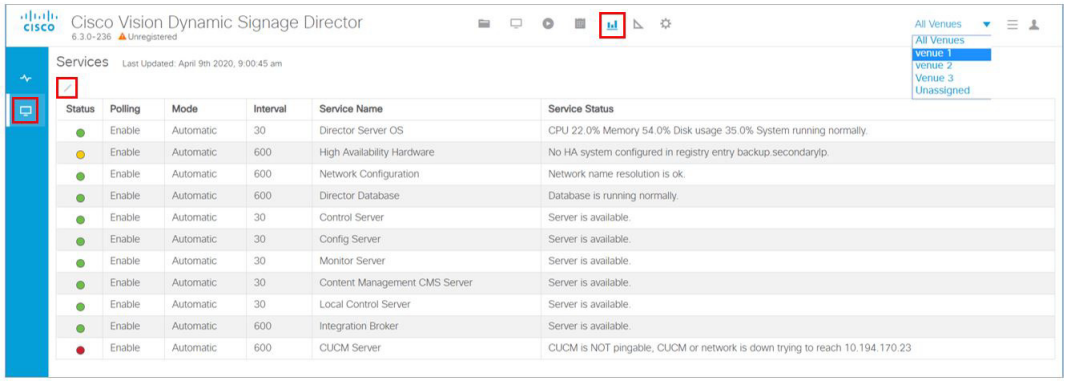
You can monitor the status of remote devices for selected venues from the **Management Dashboard**.

Traffic monitoring of remote DMPs in the **Management Dashboard** is performed using unicast messaging, so multicast optimization does not apply.

To monitor venues from the Management Dashboard:

1. Log into the Cisco Vision Dynamic Signage Director server as an administrator.
2. Click **System Status > Monitor and Status.**
3. At the top of the window, select the venue whose devices you want to monitor. The **Services** window shows the **Status, Polling, Mode, Interval, Service Name** and **Service Status** of each device (Figure 9 on page 58).

Figure 9 Monitoring Devices for a Specific Venue in the Services Window



How to Migrate Deployed Devices From a Single Venue to a Multiple Venue System

This section describes the best practices for migrating a large number of deployed devices and locations from a single venue to a multiple venue system using the Bulk Administration Tool (BAT).

For more information about the tasks referenced here for exporting, editing, and importing TSV files using BAT, see the Cisco Vision Director Bulk Administration Tool guide.

This section includes the following tasks:

- Prerequisites, page 58 (required)
- Exporting a Device List for the Original Configuration, page 59 (required)
- Creating New Venues, page 60 (required)
- Removing All Locations From Existing Groups, page 60 (required)
- Removing Locations From Existing Suites, page 60 (only required if DMPs are in suites)
- Associating Initial Locations to Venues, page 61 (required)
- Completing Venue-Specific Information and Association of Locations Using the BAT, page 61 (required)
- Populating Group Information in the New Device List, page 61 (required)

Prerequisites

Before you migrate deployed devices from Cisco Vision Dynamic Signage Director, be sure that the following requirements are met:

Caution: Cisco Vision Dynamic Signage Director does not support disabling of multiple venue support (set the "Multiple Venue Enabled?" property to false) after you have previously enabled it and associated objects. In other words, do not toggle between enabling multiple venue support and disabling it.

- You must be sure that the following object types are configured to be unique per venue:

  Groups, zones, locations, scripts, suites, and playlists.

- Use a naming convention that easily identifies the venue to which an object is associated by assigning a prefix to the object name. This makes it easier to find and track related objects.

For example, to name scripts, playlists, and locations that belong to a venue called “WEST-SIDE-VENUE” you could use the prefix “WE” such as WE-Script1, WE-Script2, WE-Playlist1, WE-Location1, and so on.

- If you have existing DMPs in a group that are targeted to be in multiple venues, they need to be split up so that each group contains DMPs *only for a single venue*.

  For example, if there is a group (ALL-DMPs) that consists of all of the DMPs in Cisco Vision Dynamic Signage Director, then sub-divide the group into smaller groups of DMPs by venue, such as “ALL-DMPs-Venue1,” “All-DMPs-Venue2,” “ALL-DMPs-No-Venue” and so on.

  This same rule applies to other objects like zones, scripts, suites, and locations. If any of these have objects that are targeted to be in different venues or to be global (that is, objects that are not part of any venues) then sub-divide them on a per-venue basis.

- (For DMPs in suites only) All suites must have a suite controller attached.

  Tip: You can easily verify whether or not a controller is defined for a suite by looking at the original exported device list (See Exporting a Device List for the Original Configuration, page 59.) If Column N (Suite Name) has a value and Column M (Suite Control Type) does not have a corresponding value in the same row, then you know that the Suite named in Column N does not have a device list attached to it.

  If a suite controller is not attached, assign a suite controller to it. If there are not any available suite controllers, create an artificial one and assign it to the suite. Delete these fake controllers after the migration process completes successfully:

  a. Go to **Configuration > Devices** > **IP Phones**.

  b. Create artificial IP phone entries with fake, non-pingable IP addresses.

  c. Go to **Configuration > Luxury Suites**.

  d. Select the suite that does not have a suite controller.

  e. Click the **Phone & Remote** tab on the right panel that has suite properties.

  f. Select the checkbox to the suite to assign the artificial IP phone that you created.

Exporting a Device List for the Original Configuration

Do this task to preserve initial single-venue system configuration information and to aid re-population of that information to the new multi-venue device list created later.

For more information, see the “Exporting and Downloading a TSV File for Locations and DMPs” topic in the Cisco Vision Director Bulk Administration Tool guide.

To export a device list for the original system configuration:

1. Go to **Configuration** > **Devices** > **Locations & DMPs**.
2. Click **Export**.
3. When the Export box displays, click **Download**.
4. When the “Select location for download” window appears, type the name of the .txt file that you want to save, or accept the default name and click **Save**.
5. **Be sure to save a principal copy** of the originally exported device list.

Creating New Venues

This task describes how to create a new venue with basic information, which will be further updated in a later task using BAT.

To create new venues:

1. Go to **Configuration** > **Venues.**
2. Click the "**+**" icon to Create a venue.
3. Specify the Name and Timezone for the venue.
4. Click **Save**.

Removing All Locations From Existing Groups

Note: Before you remove locations from existing groups, complete the requirements in the Prerequisites section to place all objects in unique groups per venue.

Before associating Locations to the new venues, remove them from existing groups.

To remove all Locations from Groups:

1. Go to **Configuration > Groups & Zones** > **Location<->Group**.
2. Click **Groups**.
3. Select an individual group.
4. In the Locations panel on the right, select all Locations for the selected group.
5. You can use **Ctrl+Click** or **Shift+Click** key sequences to multi-select the Locations.
6. Click **Remove From Groups**.
7. Repeat from Step 3. on page 60 for all groups that need locations removed.
8. Refresh the browser to reload the UI so that the changes update.

Removing Locations From Existing Suites

To associate locations to a venue, remove them from any existing suites. Add these locations back to the configuration using the BAT tool using the original Device list that was exported.

To remove Locations from existing suites:

1. Go to **Configuration > Luxury Suites**.
2. Select any suites that contain locations that are targeted to be moved to venues.
3. Select each location and click the '-' icon on the top to delete it from the suite.

   Tip: Click the '-' icon rapidly to delete DMPs quickly from the suite.
4. After all DMPs are removed from the suite, click **Save**.
5. Repeat from Step 2. on page 60 for each suite from which you need to remove locations.

Associating Initial Locations to Venues

To establish the venue-specific fields when you export the new multi-venue device list, associate at least one Location to each new venue that you created.

For more information, see Associating Venues with Cisco Vision Dynamic Signage Director Objects, page 54.

Completing Venue-Specific Information and Association of Locations Using the BAT

Perform this task to more easily complete configuration of any remaining venue-specific information and association of locations using the BAT.

To complete venue-specific information and association of Locations:

1. Export a new device list.

   After the association of at least one Location per venue, the newly exported device list file now contains the venue-specific field entries that can now be more easily populated with the remaining required configuration information.

   The venue-specific field entries in the BAT file are:

   - Venue Name
   - Venue Timezone
   - Venue JMX Password—The JMX password is saved in the venue information only when the system is disabled for global credentials.

   Note: The Venue JMX Username field is always ignored.

2. To complete association of Locations to venues, edit the TSV file using a spreadsheet application such as Microsoft Excel to:

   a. Complete the venue-specific information.

   b. Copy (or auto-fill) to add rows for new Locations that you want to add to the venues.

3. Import the device list.

   For more information, see the “Importing a TSV File” topic in the Cisco Vision Director Bulk Administration Tool guide.

4. Go to **Configuration** > **Venues** and confirm that the Locations are properly associated to their venues.

Populating Group Information in the New Device List

This step allows you to more easily re-populate the original system’s Group information to the new multi-venue device list.

To populate Group and other information from the original device list:

1. Export a new device list and open the file in your spreadsheet application.
2. Excluding the first row, select all rows and columns.
3. Sort the spreadsheet by the Name field (column E).
4. Obtain the copy of the principal device list that you exported in Step 1.

5. Sort the principal spreadsheet by the Name field.
6. From the original principal file, copy the columns that have Group information (Z, AA, AB, AC, and so on) and paste them appropriately into your new device list.

   Tip: When working with certain rows and columns in Microsoft Excel, use the hide/unhide columns or rows feature and freeze/unfreeze feature to efficiently do this job. For information about these features, see the Microsoft support site.
7. From the original principal file, copy columns that have Suites and Suite Controller information (J–Y).
8. Save the new device list.
9. Import the new device list into Cisco Vision Dynamic Signage Director.
10. After the import is complete, refresh the browser.

System Accounts on the Cisco Vision Dynamic Signage Director Servers

This module describes the default system accounts implemented by Cisco Vision Dynamic Signage Director for access and control of certain server functions. Aside from the admin account, these system accounts are generally separate from the user accounts that secure access to the Cisco Vision Dynamic Signage Director feature configuration and operation.

In addition, only a few of these accounts are intended for general modification after installation of the server. Other system accounts are reserved for special services or technical support and should not be modified unless you are instructed to do so, or you otherwise understand the impact to your server installation.

For information about user accounts and Role-Based Access Control (RBAC) in Cisco Vision Dynamic Signage Director, see User Management in Cisco Vision Dynamic Signage Director, page 71.

Contents

Information About System Accounts

All of the system accounts are automatically implemented upon installation of the Dynamic Signage Director software.

This section provides an overview of the default system accounts in Cisco Vision Dynamic Signage Director:

Common System Accounts

Table 1 on page 64 describes the common system accounts for Cisco Vision Dynamic Signage Director that are intended for you to modify after deployment of your server, and on which server platform they are supported. These common system accounts are automatically implemented upon installation of the Dynamic Signage Director software.

Table 1 Description of Common System Accounts

Account	Purpose	Server Platform
Admin	**Cisco Vision Dynamic Signage Director** Account that provides access to the administrator RBAC functions in the Cisco Vision Dynamic Signage Director user interface(UI).[1] It is automatically implemented upon installation of the Dynamic Signage Director software. The username is: **admin** The default password is: **C-V1$i0n** Using the Text Utility Interface (TUI) to change the admin account password allows an installer to recover access to the Cisco Vision Dynamic Signage Director UI. The password for the admin user account can also be changed in the Cisco Vision Dynamic Signage Director **Configuration > User** or by setting the option to force a password change upon initial login with the admin account.	Cisco Vision Dynamic Signage Director
Installer	Account that provides access to the TUI using a directly-connected console or SSH client. The username is: **installer** The default password is: **cisco!123**.[2]	Cisco Vision Dynamic Signage Director
TAC (Technical Assistance Center) Access	Account that provides access by Cisco TAC personnel to help troubleshoot an issue. A menu item under System Accounts in the TUI: **a) Enable/Disable TAC user.** For more information, see Enable/Disable TAC User, page 67.	Cisco Vision Dynamic Signage Director

1. For more information on the administrator role in Cisco Vision Dynamic Signage Director, see User Management in Cisco Vision Dynamic Signage Director, page 71.
2. For more information about the TUI, see Cisco Vision Dynamic Signage Director Server Text-Based User Interface, page 103.

Note: We *strongly recommend* you change the password as one of the post-installation tasks. Be advised: there is no way to recover it if lost.

2.

New Password Policies

For tighter security, users must set stronger passwords. When setting a new password, use the following rules:

- Must have at least 1 lower case character (a-z).
- Must have at least 1 upper case character (A-Z).

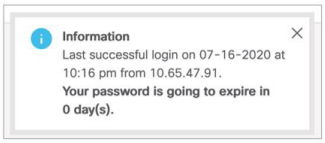
- Must have at least 1 numerical character (0-9).
- Must have at least 1 special character. Special characters are ! @ # $ %
- Must be 8-127 characters.
- Must not contain any of the following characters: space tab newline linefeed backslash (\).
- Must not contain a character sequence from a predefined list maintained in a dictionary.
- Must not have 3 sequential characters (for example: abc5#pqr is not allowed)
- Must not have a character repeat 4 times (for example: aaaa#2020! is not allowed)
- Dictionary words not allowed: words that look like “cisco,” “password,” and “admin.”

Note: There are two **Generate Password** buttons: when user first logs in and in the **User** screen to create a user (**Configuration > User**). The button provides a random password that meets the password rules. Use the “eye” icon to see the new password.

- After logging in to Cisco Vision Director, the UI displays a brief message about when you last logged in, successfully or not.
- If you try to login with failed passwords 5 times in 1 minute or less, your account is temporarily locked for 30 minutes. Upon next successful login, the message shows that the account was locked due to too many failed attempts.
- In **User** interface, the “admin” role cannot be deleted.

Notes:

1. Every user can change their own password by entering the current one as a challenge.
2. The Administrator can change anyone’s password without any challenge.
3. Except password, other fields of the user’s, like email, can be changed without any challenge.
4. Now password entry has an expiry notification.



5. Whenever a user is created or a password gets changed, the change date is logged.

Passwords after Upgrading

When upgrading an existing installation, existing passwords are kept.

Passwords after Fresh Install

Role: Admin

During fresh install, the default admin user is prompted to change the password on the first login. Starting with Release 6.1, the new password must adhere to the password policies or the password is rejected.

DMP Admin Password

The default password for fresh install is C-V1$i0n. If you do not choose a valid password, the error message indicates which rule is inviolate.

Other System Accounts

Table 2 describes some other default system accounts that are reserved for use in Cisco Vision troubleshooting or other specialized access.

Table 2 Description of Reserved System Accounts

Account	Purpose	Server Platform
admgr	Reserved for use by special agreement with Cisco Systems to support the Media Planner Import API.[1]	Cisco Vision Dynamic Signage Director
MySQL	Reserved for internal use only to access the MySQL database account.	Cisco Vision Dynamic Signage Director
TAC user[2]	Reserved for troubleshooting with remote shell access. This account should remain disabled and only activated when instructed by Cisco Technical Support for troubleshooting.	Cisco Vision Dynamic Signage Director

1. For more information about the Media Planner Import API and other API support in Cisco Vision Dynamic Signage Director, see the *Cisco Vision Dynamic Signage Director Operations Guide, Release 6.3*.
2. For more information about the TAC user account, see Enable/Disable TAC User, page 67.

Enable/Disable Browser Inspector

A new security enhancement includes disabling the DMPs browser inspector, by default. If you choose to add the registry setting to enable the browser inspector, it stays enabled until and unless you remove the registry data completely and reboot the DMPs. Disabling the browser inspector protects against network access to the DMPs.

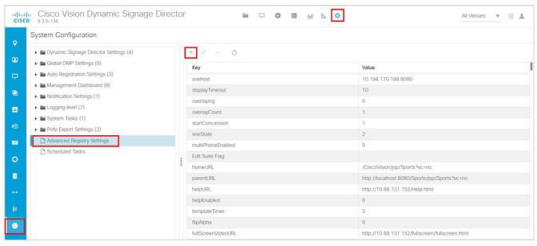
To enable browser inspector, contact Cisco Technical Assistance Center (TAC).

1. Click **Configuration > System Configuration > Advanced Registry Settings**.
2. In **Registry Data**, click **Add** (Figure 1 on page 67).
3. In the Create Configuration Setting dialog box, type **device.SvDmp.browser.inspector.addresses**.

   For example, the address of 192.168.1.1.10.1.1.1 will enable the browser inspector function on the DMPs with the IP address of 192.168.1.1.10.1.1.1.

   Note: For multiple addresses, separate the IP addresses with a comma.

Figure 1 Adding Browser Inspector Address to Registry Data



4. Reboot the DMP for changes to take effect.

To disable browser inspector capabilities:

1. Remove IP address from list.
2. Empty list or remove key to disable completely.
3. Reboot the DMP for changes to take effect.

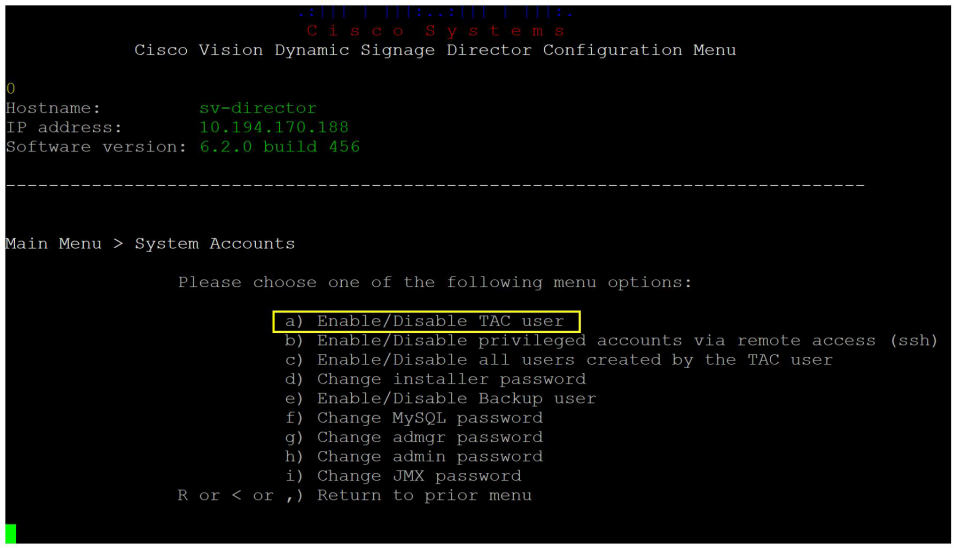
Enable/Disable TAC User

New to Release 6.2, you can create a Cisco TAC User account so Cisco can aid you in troubleshooting an issue. If you create a TAC case and grant access to Cisco TAC personnel, it is best practice to remove Cisco TAC access when the case is resolved.

To enable a TAC user:

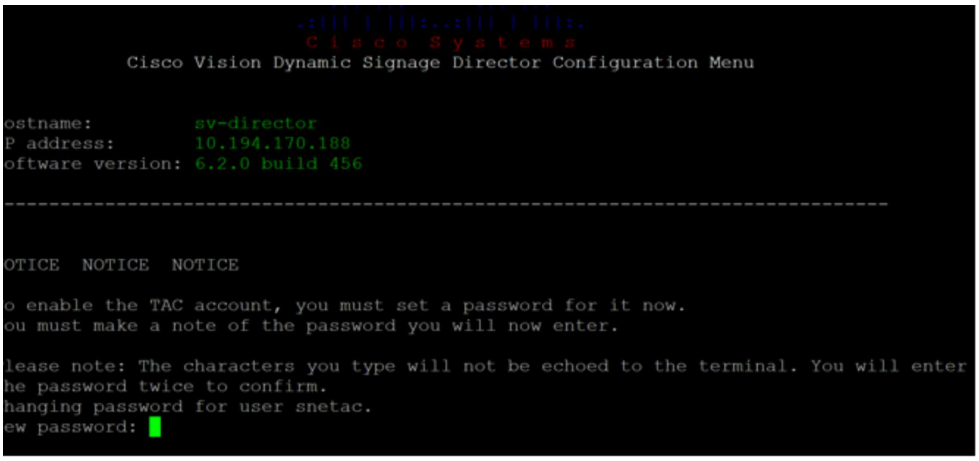
1. Login to the Director TUI using the valid user ID and password.
2. Type **b** for **System Accounts**.
3. Type **a** for **Enable/Disable TAC user** (Figure 2 on page 68).
4. Type **a** or **b**.

Figure 2 Enable/Disable TAC User



If you are using this option for the first time, you must set a password. Type it twice.

Figure 3 First Time TAC Account Password Change



Note: Choose a strong password with more than 8 characters, upper and lower case letters, numbers, and special characters. Read the instructions. Keep the credentials you choose because Cisco TAC will not have access to them and cannot recover them for you.

Note: To change the “installer” password (choice **d** above) requires the user to provide the current “installer” password.

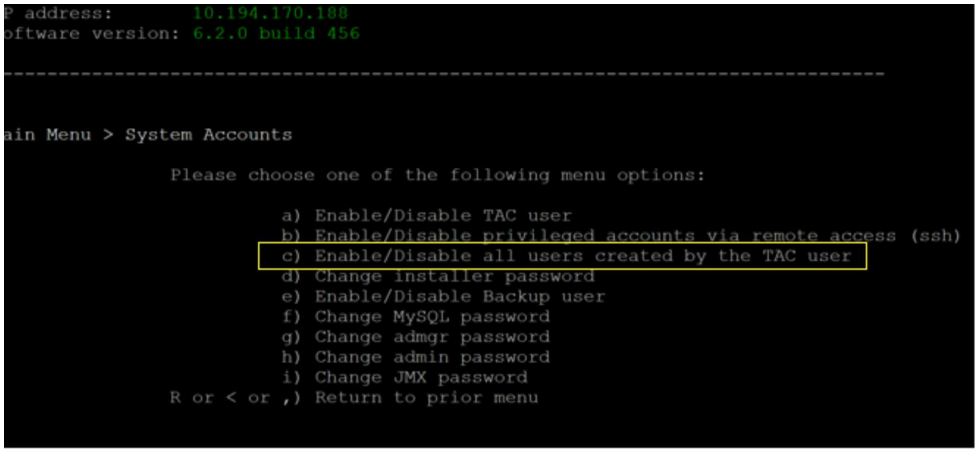
Enable/Disable all Users Created by TAC User

For added security, disable any and all accounts TAC may have enabled to help you solve an issue.

To disable any accounts created by a TAC user:

1. Login to the Director TUI using the valid user ID and password.
2. Type **b** for **System Accounts**.
3. Type **c** for **Enable/Disable all users created by the TAC user** (Figure 4 on page 69).
4. Type **a** or **b**.

Figure 4 Disable All Users Created by the TAC User



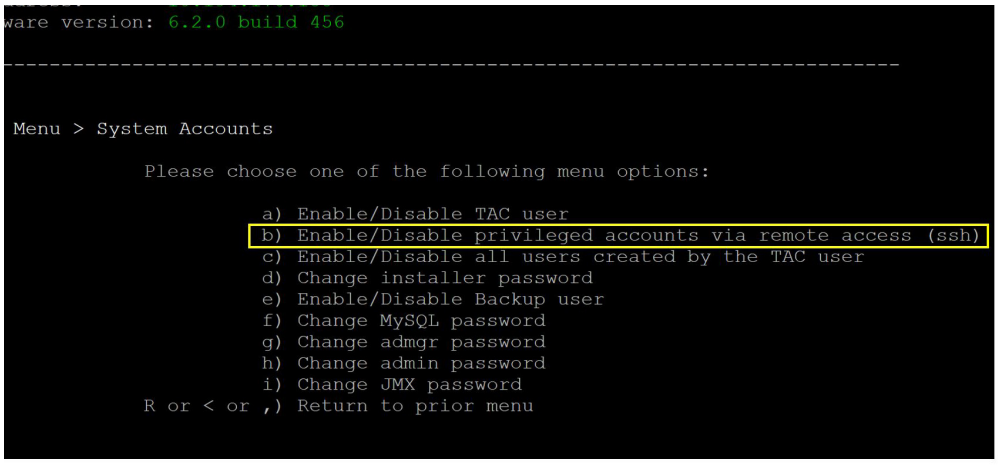
Enable/Disable Privileged Accounts Via Remote Access (SSH)

For added security, disable any remote access to your account.

To disable any remote access via SSH:

1. Login to the Director TUI using the valid user ID and password.
2. Type **b** for **System Accounts**.
3. Type **b** for **Enable/Disable privileged accounts via remote access ssh** (Figure 4 on page 69).
4. Type **a** or **b**.

Figure 5 Disable Privileged Accounts Via Remote Access



How to Change System Account Passwords

You can change system account passwords from the defaults in Cisco Vision Dynamic Signage Director using the TUI.

Note: To navigate through the TUI menus you must type the character that corresponds to the menu area where you want to go (a, b, c, and so on) and press Enter. To return to other menus, you must back out of the hierarchy of menus using one of the indicated keys to return you to prior menus.

To change system account passwords:

1. On the Cisco Vision Dynamic Signage Director, log into the TUI by doing the following:
   a. Use a directly connected console, or use an SSH client from a laptop computer that is connected to the Cisco Vision Dynamic Signage Director network to run a secure login to the primary Cisco Vision Dynamic Signage Director server using the IP address for your server.
   b. When the login prompt appears, enter the **installer** userid followed by the installer password at the password prompt.
2. From the Main Menu, go to **System Accounts**.
3. Select the system account whose password you want to change.
4. At the prompt, type the new password.
5. When prompted to confirm, retype the password.
6. Press any key to return to the System Accounts menu.
7. Return to the Main Menu and exit the TUI.

User Management in Cisco Vision Dynamic Signage Director

Cisco Vision Dynamic Signage Director deployments normally have a team of people who are responsible for different aspects of the site setup and event operation. For example, in addition to a system administrator, there is usually an event operator, a content manager, and a technical support person, among other personnel. Each person has different skills and needs for working with the Cisco Vision Dynamic Signage Director software.

The Cisco Vision Dynamic Signage Director software implements Role-Based Access Control (RBAC) to control permissions and user access to only the portions of the system for which they are trained and authorized to use. More than one user can be assigned to the same role in the software. However, only a single role can be assigned to each username.

For more details about RBAC in a multi-venue environment, see Role-Based Access Control for Hierarchical Management of Multiple Venues, page 49.

Information About User Management

This section includes the following topics:

Administrator Role Overview

Note: This section describes the primary (or central) Administrator role in a Cisco Vision Dynamic Signage Director system. A Venue Administrator has a subset of administrative permissions that are authorized on a per-venue basis. See Table 2 on page 75.

The primary Administrator role has unrestricted access to the Cisco Vision Dynamic Signage Director software, and is the only role that can add users and assign RBAC privileges to them. The Administrator role is pre-configured in Cisco Vision Dynamic Signage Director and cannot be deleted. However, you can change the password. You also can have more than one user assigned with Administrator privileges.

The Cisco Vision Dynamic Signage Director administrator is the person who is responsible for deploying the Cisco Vision solution throughout the venue.

The primary administrator has sufficient permissions to do the following functions:

- Installing, upgrading, backing up, and restoring Cisco Vision Dynamic Signage Director servers.
- Associating objects (including Venue Operators and Venue Administrators) to venues.

Note: Users assigned to the Administrator role have *global* access to all venues in a multi-venue environment. Venue Administrators only have access to those venues for which they are authorized by a primary Cisco Vision Dynamic Signage Director administrator.

- Creating additional users and assigning roles.
- Adding devices to Cisco Vision Director.
- Staging content.
- Configuring the channel lineup (Content Managers can also configure this area).
- Configuring local control areas such as luxury suites, back offices, and bars.
- Configuring Point of Sale (POS).
- Generating Proof of Play (PoP).
- Configuring the Dynamic Menu Board application.
- Configuring the TV Off custom application.
- Configuring Device Management, including rebooting DMPs and controlling TVs.

RBAC Roles Overview

Table 1 on page 73 provides an overview of the roles that can be assigned by the Administrator in Cisco Vision Dynamic Signage Director. For a complete mapping of permissions by role, see Table 2 on page 75.

Table 1 Cisco Vision Dynamic Signage Director Roles

Role	Overview
Concessionaire	Concessionaires have access only to the Dynamic Menu Board application, which allows modification of certain text-based and graphics items, and the background graphic on menus. ■ All content uploaded by the concessionaire is available to all users that have sufficient permissions based on the roles assigned to them. ■ The concessionaire role does not have permissions in the **System Configuration > User Administration** or the **System Configuration**, and they can only see the DMB themes that they create.
Content Manager	Content Managers are responsible for uploading content and ads provided by the creative services team. ■ They create event scripts so that the correct content displays in the proper area of the venue and the proper area of the TV screen according to the specified schedule. ■ The content manager role has permissions in Cisco Vision Dynamic Signage Director to configure event states/scripts, zones, groups, screen templates, playlists, and tickers. ■ Content managers also can assign gadgets for custom menus and create playlists for those menus.
Event Operator	Event Operators run the Cisco Vision Director event scripts during an event. The event operator role has permissions to start and stop scripts and modify their states. ■ They can change the transition of an event state from time-based to manual, move an event into one of the three ad hoc states (Inside Emergency, Outside Emergency, or Delay), and approve ticker content (legacy version). ■ Additionally, the event operator keeps track of which break states have played and is responsible for performing the pre-game walk-through.
Facility Operator	Facility Operators have access only to the TV Off application. ■ The facility operator must access this application directly using the http://*ipaddress*:9090/web/sv/home, where *ipaddress* is the IP Address of the Cisco Vision Dynamic Signage Director server.
Help Desk	Help Desk users have read-only permissions to view and monitor information on the System Configuration and to use **Device Management**. This role does not have permissions in the **System Configuration > User Administration**, except to change their own password.

Table 1 Cisco Vision Dynamic Signage Director Roles (continued)

Role	Overview
Support	Support users are responsible for first-level technical support. ■ They have limited access to the System Configuration to monitor DMP status, troubleshoot, and manage the DMPs on the Cisco Vision network. They also have access to **Device Management**. ■ The support role does not have permissions in the **System Configuration > User Administration**, except to change their own password.
Venue Administrator	Venue Administrators have limited permissions at the venues authorized by the central Administrator for that user, for the following areas of Cisco Vision Dynamic Signage Director: **Note:** New **System Configuration** and **Device Management** functionality is added for the Venue Administrator. ■ Script Management ■ System Configuration: – The Venue Administrator can issue all DMP and TV commands. – Read-only access with limited command support. ■ Device Management: – The Venue Administrator can run the Reboot Device command from Device Management to restart DMPs. – Read-only access. ■ System Configuration > Devices (Display Specifications only); Read-only access to Groups & Zones, Channels, Luxury Suites.
Venue Operator	Venue Operators have script control only, and only for venues authorized by the central Administrator for that user. ■ In the System Configuration, venue operators can view and monitor information on the System Configuration with read-only access to the venues for which permissions are granted. ■ They also have access to Device Management. **Note:** Venue Operators and Venue Administrators are the only roles that have venue-specific permissions. For more information, see the Configuring Cisco Vision Dynamic Signage Director for Multiple Venue Support, page 47

Access Summary by Role

Table 2 on page 75 provides a summary of the areas of access in the Cisco Vision Dynamic Signage Director software by each user role.

Note: “Yes” indicates that the user role has access to the corresponding functional area, and “–” means that the role does not have authorization there.

Table 2 Role Access Summary by Functional Area of Cisco Vision Dynamic Signage Director

Functional Area	Admin	Concessionaire	Content Manager	Event Operator	Facility Operator	Help Desk	Support	Venue Admin	Venue Operator
Device Management	**Yes**	–	–	–	–	**Read only**	**Read only**	**Yes**	**Read only**
Configuration									
Channel Definitions	**Yes**	–	**Yes**	–	–	–	–	**Read only**	–
Channel Guide									
Data Integration	**Yes**	–	**Yes**	–	–	–	–	–	–
Devices	**Yes**	–	–	–	–	–	–	**Limited**[1]	–
Groups & Zones	**Yes**	–	**Yes**	**Yes**	–	–	–	**Read only**	–
Menus	**Yes**	–	**Yes**	–	–	–	–	–	–
My Profile	–	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
Proof of Play	**Yes**	–	–	–	–	–	–	–	–
Stores	**Yes**	–	–	–	–	–	–	–	–
Luxury Suites	**Yes**	–					**Limited**[2]	**Read only**	–
System Configuration	Yes	–	–	–	–	Limited[5]	**Yes**	Limited[7]	Limited[8]
Triggers	**Yes**	–	–	–	–	–	–	–	–
User Admin	**Yes**	–	–	–	–	–	–	–	–
Venues	**Yes**	–	–	–	–	–	–	–	–
Script Management									
Content	**Yes**	–	**Yes**	–	–	–	–	**Limited**[3]	–
Control	**Yes**	–	–	**Yes**	–	–	–	**Limited**[4]	**Limited**[5]
Staging	**Yes**	–	–	**Yes**	–	–	–	**Yes**	–
Scheduling	**Yes**	–	**Yes**	–	–	–	–	**Yes**	–
Templates	**Yes**	–	**Yes**	–	–	–	–	–	–
Widgets	**Yes**	–	**Yes**	–	–	–	–	–	–
Dynamic Menu Boards	**Yes**	**Yes**	**Yes**	–	–	–	–	–	–
System Status	**Yes**	–	–	–	–	**Limited**[5]	**Yes**[6]	**Limited**[7]	**Limited**[8]
Scheduler Application	**Yes**	–	–	**Yes**	–	–	–	–	–
Software Manager	**Yes**	–	–	–	–	–	–	–	–

Table 2 Role Access Summary by Functional Area of Cisco Vision Dynamic Signage Director (continued)

Functional Area	Admin	Concessionaire	Content Manager	Event Operator	Facility Operator	Help Desk	Support	Venue Admin	Venue Operator
System State Reports	**Yes**	–	–	–	–	–	–	–	–
TV Off Application	**Yes**	–	–	**Yes**	**Yes**	–	–	–	–

1. Venue Administrators can only edit the Display Specifications panel.
2. Support users can set up TV control PINs and channel guides for suites.
3. Venue Administrators can delete content associated (tagged) to the venues for which that venue admin is authorized. External content, channels, and Dynamic Menu Board (DMB) content items are global to all venues. Therefore, these global content items also can be deleted by the venue admin.
4. Venue Administrators and Venue Operators have script control only, and only for venues authorized by the Administrator for that user.
5. Help Desk users can view and monitor information on the System Status with read-only access. They also can run Get Status, Ping, Display IP, and Ping Test commands for DMPs in the System Status.
6. Support users can run Get Status, Ping, Display IP, Ping Test, TV On/Off, Set Display Input, Set Display Banner, Set Closed Captions, Set Video Channel, Cabling Test using TDR, and Show TDR Test Results commands.
7. Venue Administrators can view and monitor information on the System Status with read-only access to the venues for which permissions are granted. They also can run Get Status, Ping, Display IP, and Ping Test commands in the System Status for the DMPs in the venues at which that Venue Administrator is authorized.
8. Venue Operators can view and monitor information on the System Status with read-only access to the venues for which permissions are granted. They also can run Get Status, Ping, Display IP, and Query Syslog commands in the System Status for the DMPs in the venues at which that Venue Operator is authorized.

Backing Up and Restoring Cisco Vision Director Servers

This module describes how to setup and schedule backups between a primary and secondary server and restore data between them.

Contents

Prerequisites for Backing Up and Restoring Cisco Vision Director Servers

Before you backup or restore Cisco Vision Director servers, be sure that the following requirements are met:

- You are familiar with using the Text-based User Interface (TUI) in Cisco Vision Director.

  For more information, see Cisco Vision Dynamic Signage Director Server Text-Based User Interface, page 103.
- You have a directly-connected console or an SSH client to access the primary active and secondary servers.
- You have the IP addresses of the active and secondary servers.
- You know the installer account credentials on the Cisco Vision Director active and secondary servers.

- The IP address of the secondary server must be reachable on the network from the active server or the TUI backup configuration will fail.
- You have determined an appropriate time on the network to schedule automatic backups and restores.

Restrictions for Backing Up and Restoring Cisco Vision Director Servers

Consider the following restrictions when backing up and restoring Cisco Vision Director servers:

Caution: The tasks described in this document apply only to a redundant server environment where *both* servers are running Cisco Vision Director software.

- If you have to fail over to your secondary Cisco Vision Director server due to a problem on the primary, then your original backup configuration will be invalid.

  Be aware that your scheduled backup process cannot fully operate by automatically transferring a copy of the backup to the secondary server until you use the TUI automatic backup configuration again to reset the backup configuration between the primary and secondary servers. However, a backup will continue to be saved on the primary server.

- When you fail back to the original primary server and are now using the original IP addressing configuration, use the TUI automatic backup configuration again, so that the backup directory can be re-established on the secondary server.

Information About Backing Up and Restoring Cisco Vision Director Servers

This section includes the following topics:

Backup Environment

While you can run a backup for a network environment where there is only a single Cisco Vision Director server, we recommended a redundant, virtualized environment. In a redundant environment, you run Cisco Vision Director on a primary server, with a secondary server connected to the same subnet where the backup data from the primary server is saved.

The backup process can be scheduled or run manually. When a backup completes, the Content Management System (CMS) is automatically restarted.

The backup task can run even while an event script is running. As part of this change, the database is no longer optimized or repaired during the backup process—a new TUI option is added to run database maintenance manually if needed.

Although it is not expected that database maintenance should be needed regularly, slow performance may indicate a need to run database maintenance.

Tip: You can look at the backup log (/var/log/svd-config/backup-YYYMMddHHMMSSz.log) to see if the table updates are “OK” and up-to-date. If not, then use the TUI option to run database maintenance. For more information, see the “Running Database Maintenance” topic in the Cisco Vision Dynamic Signage Director Operations Guide, Release 6.3.

What Cisco Vision Director Data is Backed Up

There are several areas of Cisco Vision Director that need to be backed up. The backup process backs up the following areas of the Cisco Vision Director server:

- Uploaded fonts
- Cisco Vision Director Content Management System (CMS)
- Cisco Vision Director database
- Cisco Vision Director system configuration files
- Content Integration data
- Dynamic Menu Board data
- Proof of Play report data in the /var/sv/pofp/data directory

  Caution: The proof of play raw data in the /var/sv/pofp/raw directory is *not* backed up.

Disk Storage and Maintenance

Note: To be sure that your system has enough disk space, Release 4.0 and later releases only retain one backup file by default.

For more information, see the “Managing Server Resources in Cisco Vision Director” module of the Cisco Vision Dynamic Signage Director Operations Guide, Release 6.3.

Restore Environment

As with backups, schedule the restore process or run it manually. When the manual restore screen is displayed, it lists backups from both the backup and restore directories, concatenated together. This allows you to run a manual restore on either the primary or the secondary server. An automated restore always uses the most recent backup file in the restore directory.

Also, the schedule of tasks to run in the primary database and the secondary database will be different, due to the existence of the backup and restore tasks. Therefore, the schedule itself is not automatically restored.

How to Backup a Cisco Vision Director Server

This section includes the following tasks:

- Enabling the Backup Account on the Secondary Server, page 80 (required)
- Setting Up the Primary Server for Automatic Backup and Restore, page 80 (required)
- Scheduling a Regular Backup, page 83 (required)
- Starting a Backup Manually for Immediate Execution, page 84 (optional)
- Verifying Backup Completion, page 85 (optional)

- Modifying the Number of Backup Files to Retain, page 86 (optional)

Enabling the Backup Account on the Secondary Server

Before you set up the primary Cisco Vision Director server for automatic backup and restore with a redundant secondary server, enable the backup account on the secondary server using the TUI.

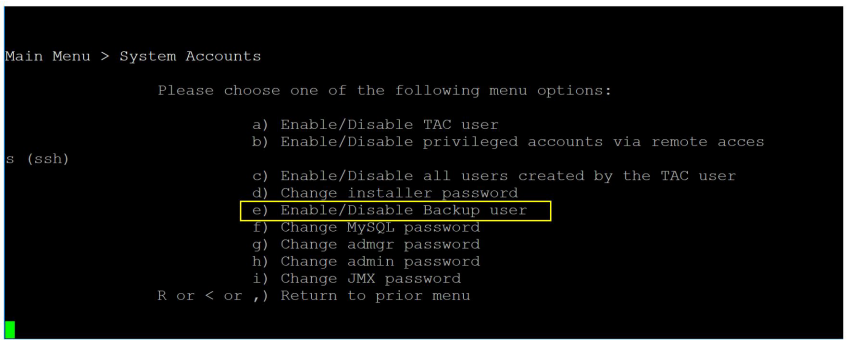
For more information about using the TUI, see Cisco Vision Dynamic Signage Director Server Text-Based User Interface, page 103.

To enable the backup account on the secondary server:

1. On the secondary server, log into the TUI by doing the following:
   a. Use a directly connected console, or use an SSH client from a laptop computer that is connected to the Cisco Vision Director server network to run a secure login to the secondary Cisco Vision Director server using the IP address for your server.
   b. When the login prompt appears, enter the **installer** userid followed by the installer password at the password prompt.
2. From the Main Menu, go to the **System Accounts** > **Enable/Disable Backup User** menu (Figure 1 on page 80).

   Tip: To navigate through the TUI menus, type the character that corresponds to the menu area where you want to go (a, b, c, and so on) and press Enter. To return to other menus, back out of the hierarchy of menus using one of the indicated keys to return you to prior menus.

Figure 1 Enable/Disable Backup User Menu



1. Select **Enable backup user account**.

   When successfully created, the following messages display:

   ```
   Backup user has been enabled.
   You must set up the backup user key from the primary system to use it.
   ```

2. Press any key to return to the Enable/Disable Backup user menu.
3. Continue to return to the Main Menu and exit the TUI.

Setting Up the Primary Server for Automatic Backup and Restore

Use a TUI menu option to automate the configuration of the backup accounts and directories between the primary and backup server. Use the TUI to setup the Cisco Vision Director Server environment to run the backup and restore processes.

Note: The TUI is only used to configure the backup environment. Use **System Configuration** to schedule or run any manual backups. For more information, see Scheduling a Regular Backup, page 83 and Starting a Backup Manually for Immediate Execution, page 84.

Prerequisites

Complete these few steps before performing a backup and restore:

- Determine the IP address of the DSD server which is the destination of the backup files
- On that server (the backup one), enable remote ssh access. Use the TUI on the backup DSD.
  a. Use a directly connected console, or use an SSH client from a laptop computer that is connected to the Cisco Vision Director Server network to run a secure login to the primary Cisco Vision Director server using the IP address for your server.
  b. When the login prompt appears, enter the **installer** userid followed by the installer password at the password prompt.
  c. From the Main Menu, choose **System Accounts** (Figure 2 on page 81) then choose **Enable/Disable privileged accounts via remote access (ssh)** (Figure 3 on page 82).

Figure 2 System Accounts in TUI

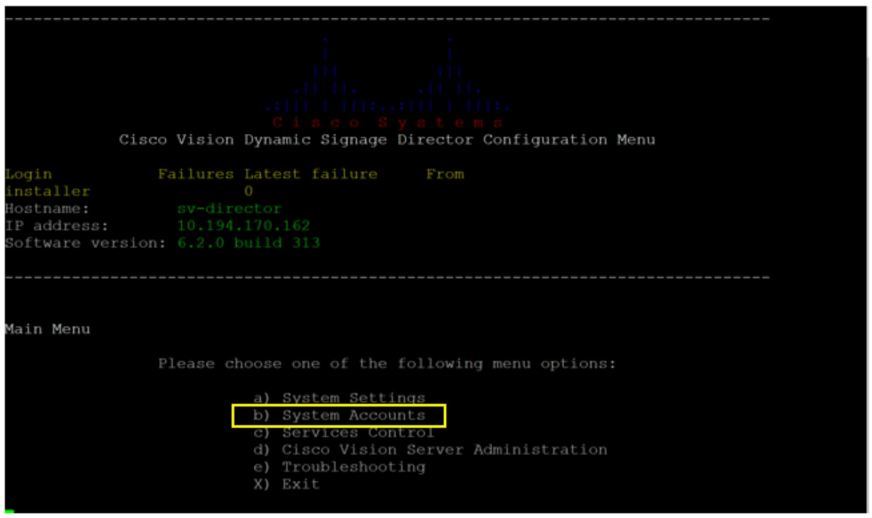
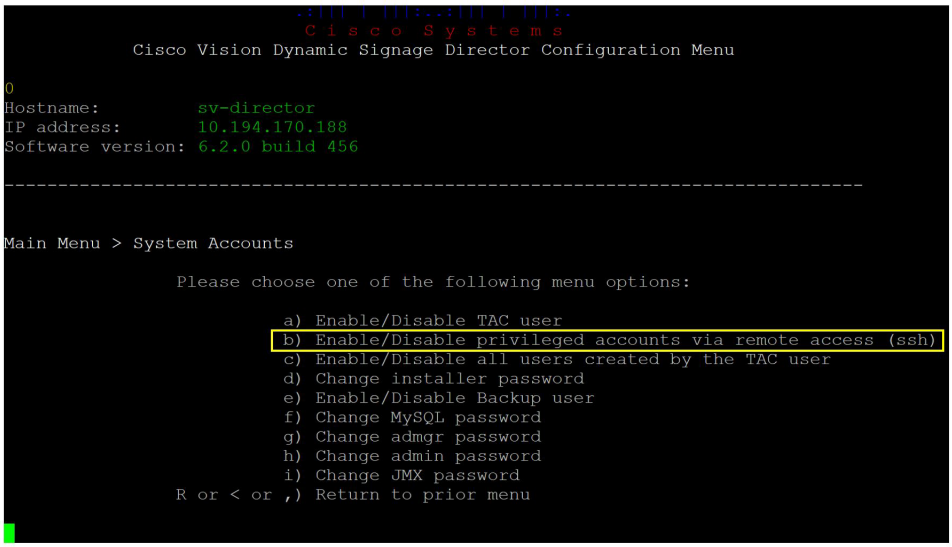


Figure 3 Enable Remote Access via SSH

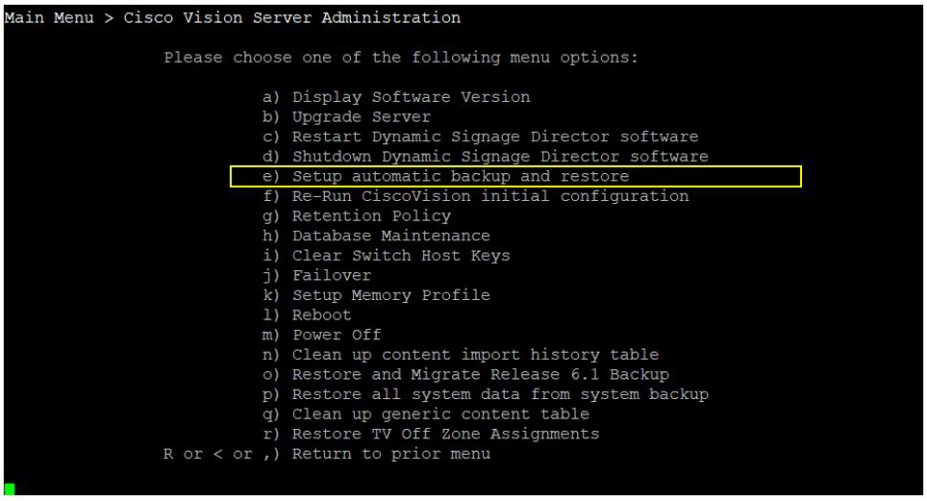


After enabling access on the remote (backup) server, go back to the primary DSD server and proceed.

To set up the primary server for automatic backup and restore:

1. On the primary server, log into the TUI by doing the following:
   a. Use a directly connected console, or use an SSH client from a laptop computer that is connected to the Cisco Vision Director Server network to run a secure login to the primary Cisco Vision Director server using the IP address for your server.
   b. When the login prompt appears, enter the **installer** userid followed by the installer password at the password prompt.
2. From the Main Menu, go to **Cisco Vision Server Administration > Setup automatic backup and restore**.

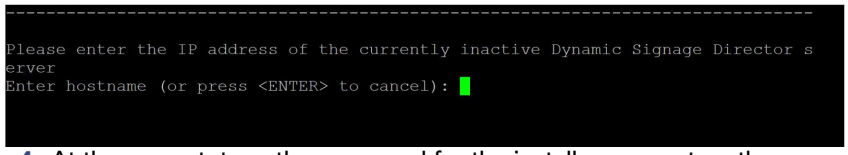
Figure 4 Setup Automatic Backup and Restore Menu Option



3. At the prompt type the IP address or hostname of your secondary (remote backup) server as shown in the example in Figure 5 on page 83.

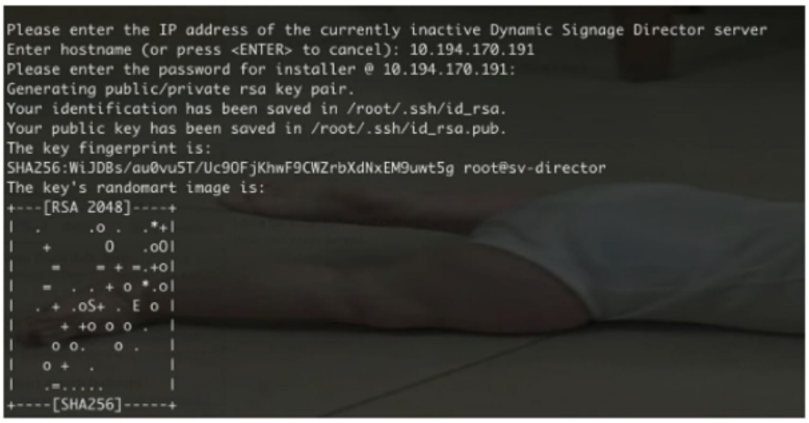
Note: Text shown in yellow in the screen (omitted in figure below) is instructions on what is done in Prerequisites, page 81 above.

Figure 5 Secondary Server IP Address Configuration



4. At the prompt, type the password for the installer account on the secondary backup server.
5. When accepted, the system generates the RSA keys and the public key is copied to the secondary server. Confirm that the keys are created without errors as shown in (Figure 6 on page 83).

Figure 6 Generate RSA Keys



6. Wait until the “Press any key” message appears (there may be a short delay before it displays).
7. Press any key to return to the Cisco Vision Server Administration menu.
8. Continue to return to the Main Menu and exit the TUI.

Scheduling a Regular Backup

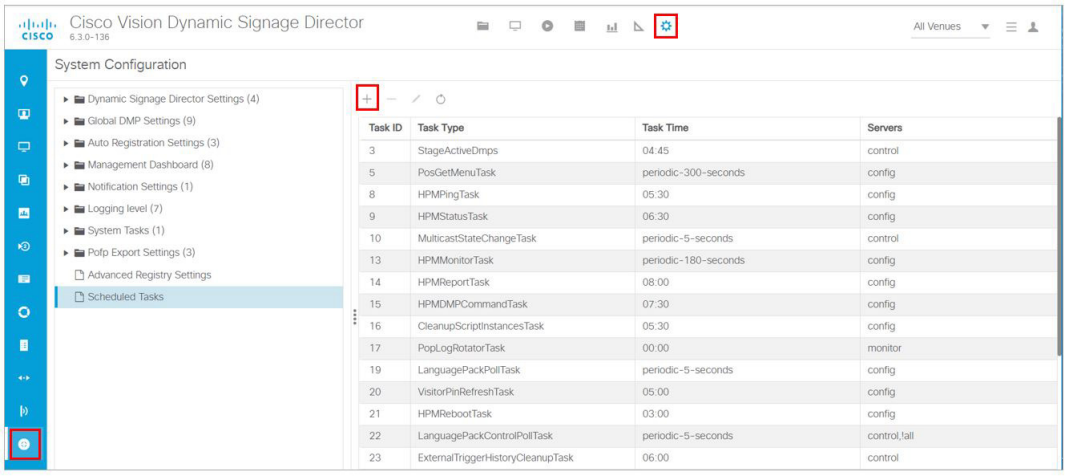
After you have configured the servers to support the backup process, schedule backups using **System Configuration** in the Cisco Vision Director software.

To configure a backup to run on a regular schedule:

1. Log into the primary Cisco Vision Director server as an administrator.
2. From the Cisco Vision Director click **Configuration > System Configuration > Scheduled Tasks** (Figure 7 on page 84).
3. Click the **Add** icon. The **Schedule Task – Add** dialog box appears (Figure 8 on page 84).
4. Click in the Task Type field and type **BackupTask** (Figure 8 on page 84).

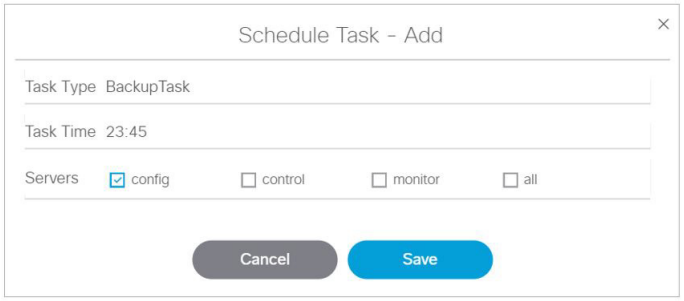
   Note: Be sure to type the name of the task ***exactly*** as shown with upper and lowercase characters.

Figure 7 Adding a Backup Task to Run on a Regular Schedule



5. Click in the Task Time field and specify the time (in 24:00 format) when you want the backup to run.

Figure 8 Schedule Task – Add Dialog Box



6. Click in the Servers field and choose **config**.
7. Click **Save**.

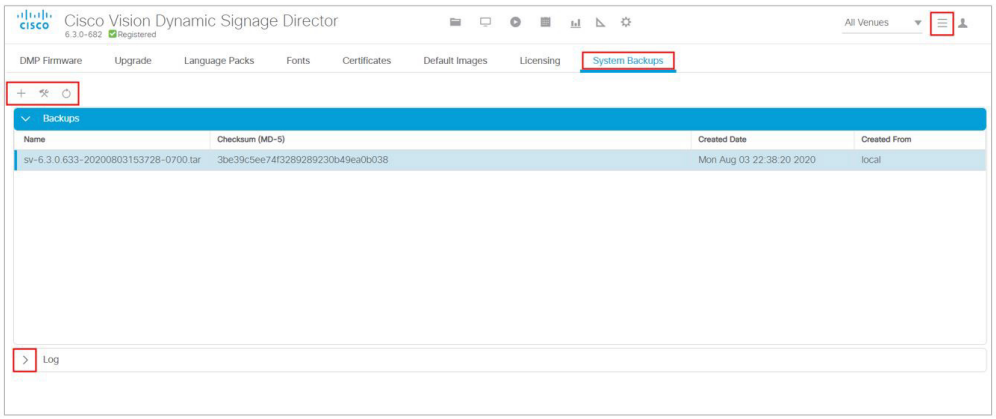
Starting a Backup Manually for Immediate Execution

If you want to start a backup right away, run a backup manually.

To start a backup manually for immediate execution:

1. Log into Cisco Vision Director as an administrator.
2. Click **More > Manage Software**.
3. Click the **System Backup** tab (Figure 9 on page 85).
4. Click the **+** icon to start creating a backup. The backup begins immediately.

Figure 9 Generating a System Backup



Use the Log arrow to see the log file information.

Note: The “success” message that appears means that the backup task started. It does not mean that the backup is completed.

Verifying Backup Completion

To verify backup completion, confirm that a backup file exists and also that no errors appear in the log file.

Verifying That a Backup File Exists

Note: Verifying the existence of a backup file only tells you that a backup was attempted. Check the file for errors.

To verify that a backup file exists:

1. Log into the TUI. When the login prompt appears, enter the **installer** userid followed by the installer password at the password prompt.
2. Choose **Cisco Vision Server Administration.**
3. Choose **Restore all system data from system backup.**
4. Verify that backup files with dates and times appear.

Finding Backup Errors in the Log File

Note: The messages “Starting backup” and “Backup completed” always appear in the log, even if unsuccessful.

To find backup errors in the log file:

1. Open the **/opt/sv/servers/config/logs/sv_dev_debug.log** file.

   Tip: You can access log files from the TUI, or by running a System State Report from the Cisco Vision Director **Library** (Main Menu). Click **More > System State Report**.

2. In the sv_dev_debug.log file, find messages that include the string “com.cisco.sv.backup.”

   These are the backup process messages.

3. Find the “Starting backup” message.

4. After the “Starting backup” message (but before the “Backup completed” message), look for a “com.cisco.sv.backup” message that also includes “ERROR” in the string.

   If you find this error, the backup did not complete successfully.

Modifying the Number of Backup Files to Retain

To reduce the amount of disk storage required in your system, the default backup retention policy is to keep one backup file. This retention policy can be modified to retain 2, 5, 7, or 10 days backup files.

Caution: Check your overall disk utilization and the size of your backup content so that your system resources support the number of backup files you keep.

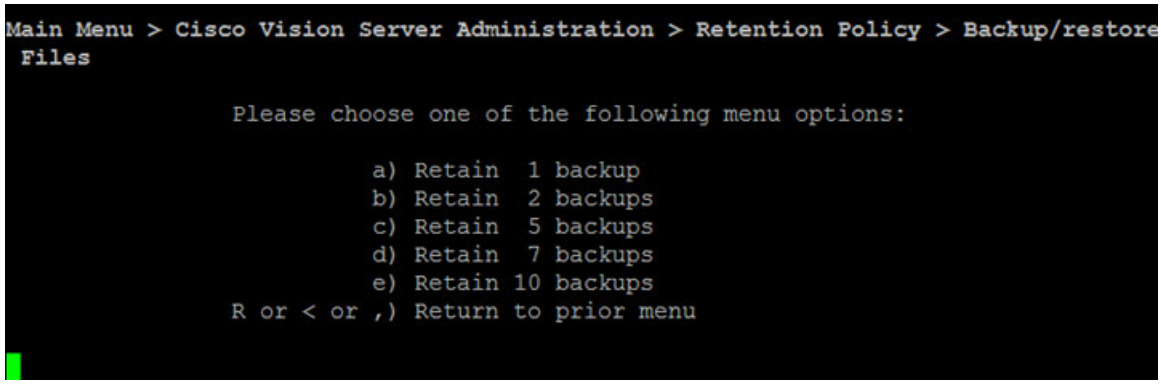
Note: Run this task on both the primary server and secondary backup server.

To modify the number of backup files to retain:

1. Log into the TUI by doing the following:
   a. Use a directly connected console, or use an SSH client from a laptop computer that is connected to the Cisco Vision Director server network to run a secure login to the primary Cisco Vision Director server using the IP address for your server.
   b. When the login prompt appears, enter the **installer** userid followed by the installer password at the password prompt.
2. From the Main Menu, choose **Cisco Vision Server Administration.**
3. Choose **Retention Policy.**
4. Choose **Backup/restore Files**.

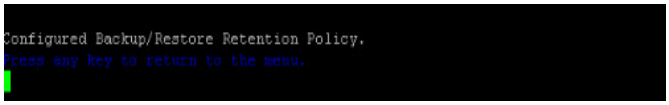
A menu of policy options is displayed (Figure 10 on page 86), where you can choose to retain 1 (the default), 2, 5, 7, or 10 backup files.

Figure 10 Backup Retention Policy Menu



5. Type the letter that corresponds to the number of days that you want to retain files and press **Enter**.
6. When the change of policy confirmation message displays, press any key to return to the Cisco Vision Server Administration menu.

Figure 11 Confirmation of Policy Change



7. Continue to return to the Main Menu and exit the TUI.

How to Restore a Cisco Vision Director Server

The Cisco Vision Director software automatically copies backup files between the primary and secondary servers and when the restore process starts, verifies the MD5 checksum.

If you need to failover to the secondary server and do a restore, follow the procedures in Configuring Failover Between Redundant Cisco Vision Director Servers, page 89.

Note: If you need to manually copy files between the servers, copy both the .tar and .chksum files. The restore process automatically uses both files to verify the MD5 signature.

This section includes the following tasks:

- Starting a Restore Manually for Immediate Execution, page 87 (optional)
- Restarting the Cisco Vision Director Software, page 88 (required after restore run)

Starting a Restore Manually for Immediate Execution

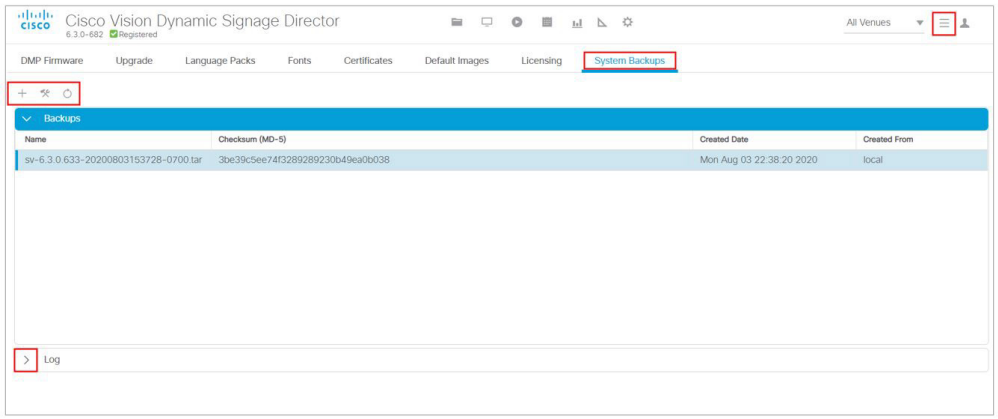
To start a restore other than at the regularly scheduled time, the Cisco Vision Director software also allows you to run a restore from backup to begin immediately.

Caution: You cannot successfully run the restore process while an event script is running. In addition, if your venue was running any script when the backup took place, then those scripts will begin running after the restore.

To start a restore manually for immediate execution:

1. Log in to Cisco Vision Director as an Administrator.
2. Click **More > Manage Software**.
3. Click the **System Backups** tab (Figure 12 on page 88).
4. Click **Restore**. The Confirm Restore dialog box appears.
5. Click **Yes**.

Figure 12 Restore the System from Backup



The system restore from backup process begins.

Or, if you prefer, you can still do the same process using TUI.

To start a restore manually for immediate execution:

1. Login to the TUI by doing the following:
   a. Use a directly connected console, or use an SSH client from a laptop computer that is connected to the Cisco Vision Director server network to run a secure login to the primary Cisco Vision Director server using the IP address for your server.
   b. When the login prompt appears, enter the **installer** userid followed by the installer password at the password prompt.
2. From the Main Menu, choose **Cisco Vision Server Administration**.
3. Choose **Restore all system data from system backup.**

   The restore begins immediately.

Restarting the Cisco Vision Director Software

After you perform any restore on a Cisco Vision Director server, you must restart the Cisco Vision Director software to resume normal operation of the services.

To restart the Cisco Vision Director software:

1. On the primary server, log into the TUI by doing the following:
   a. Use a directly connected console, or use an SSH client from a laptop computer that is connected to the Cisco Vision Director server network to run a secure login to the primary Cisco Vision Director server using the IP address for your server.
   b. When the login prompt appears, enter the **installer** userid followed by the installer password at the password prompt.
2. From the Main Menu, choose **Cisco Vision Server Administration.**
3. Choose **Restart Dynamic Signage Director Software**.
4. Return to the Main Menu and exit the TUI.

Configuring Failover Between Redundant Cisco Vision Director Servers

Cisco Vision Director supports an environment best described as *warm standby* between two servers that run the Cisco Vision Director software—one of the servers operates as the primary active server and the other server operates as a secondary backup server. If a failure occurs, you can configure the backup server to become the active server, but the failover process is not automatic.

Contents

Note: Restoring the primary server after failover to secondary requires a service interruption and should only be conducted during scheduled downtime. Be aware that until you change the IP address of the primary server to remove the addressing conflict with the newly active secondary server, you will be unable to schedule backups between the two servers. Reconfigure the backup/restore environment using the Text Utility Interface (TUI) after the restore. For more information, see Backing Up and Restoring Cisco Vision Director Servers, page 77.

Prerequisites for Configuring Failover Between Redundant Cisco Vision Director Servers

Before you promote a secondary server to become the primary active server, be sure that the following requirements are met:

- You have either physical console access or an SSH client such as PuTTY to log into both Cisco Vision Director servers.
- 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. To select a menu item, type the character that corresponds to the menu option and press **Enter**.
- Verify that you have a successful backup of the primary server on the secondary server. For more information, see Backing Up and Restoring Cisco Vision Director Servers, page 77.
- The Cisco Vision Director backup server is on the same subnet as the primary server.
- The servers are using the Eth0 interface for connection to the network.

- You have the IP addresses of the primary and secondary servers.

Tip: The IP address for the server is displayed on the screen when you log into the TUI. You also can view the /etc/hosts information on each server using the **TUI System Settings > System Information** menu option.

Restrictions for Configuring Failover Between Redundant Cisco Vision Director Servers

The Cisco Vision Director server redundancy architecture has the following restrictions:

- The Cisco Vision Director server architecture does not support automatic failover when a failure occurs on the active server.
- Depending on your environment, it takes 30 minutes or more to complete the manual failover process.
- In addition, after the manual failover process completes, perform a script push if you are in an active event, which depending on your deployment and content size, can take anywhere from minutes to an hour. When pushing the script again, there will be a service interruption.

Information About Failover Between Redundant Cisco Vision Director Servers

Figure 1 on page 91 shows the architecture of Cisco Vision Director server redundancy under normal network conditions and operation. The primary and secondary servers are addressed as independent hosts with two different IP addresses on the same subnet in the Cisco Connected Venue (Connected Stadium) network.

While the secondary server is still connected to the network, notice that communication and control only occurs between the primary Cisco Vision Director server and the rest of the network, including the DMPs.

The secondary server is only connected to the network as a backup to the primary, should a failure occur. Configure the secondary server to be backed up with data from the primary server on a scheduled basis.

Figure 1 Cisco Vision Director Redundancy Under Normal Operation

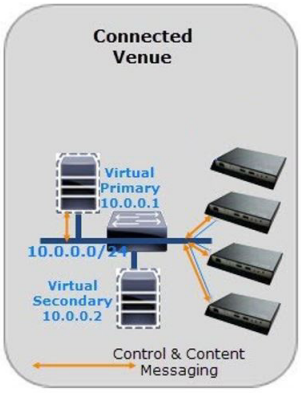
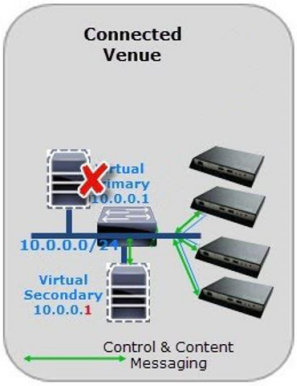


Figure 2 on page 91 shows the redundancy environment when connectivity from the primary Cisco Vision Director server fails. When the primary server fails, a manual process must take place to restore the secondary server from a backup, shut down the primary server, and activate the secondary server as the primary.

Notice that the secondary server must be reconfigured to use the same IP address as the original primary server. In this example, the secondary server IP address is changed to 10.0.0.1 (from 10.0.0.2) to match the primary server address. When the process completes, communication and control only occurs between the newly activated secondary server and the rest of the network.

Note: The word “failover” does not mean automatic activation of a secondary server. **The failover process is manual.**

Figure 2 Cisco Vision Director Redundancy Under Failover Operation



How to Promote a Standby Secondary Server to the Active Server

This section describes the related tasks to perform when a primary Cisco Vision Director server fails in a redundant server environment, or if you need to perform an upgrade of your Cisco Vision Director software. It includes tasks to activate the secondary server to replace the functionality of the primary server for Cisco Vision Director operation.

Note: To select a TUI menu item, type the character that corresponds to the menu option and press **Enter**.

This section includes the following tasks:

- Starting and Configuring the Services on the Secondary Server, page 92 (required)

Starting and Configuring the Services on the Secondary Server

To start and configure the services on the secondary server:

1. Log into the TUI as installer on the *secondary* server using a directly-connected console or SSH client.

   The TUI Main Menu displays.

2. Choose **Cisco Vision Server Administration.**
3. Choose **Failover**.
4. Choose **Promote as Primary/Active**.

   The Cisco Vision Director services are started and configured to start automatically when a reboot occurs.

Restoring the Secondary Server with System Data From a Backup File

To restore the secondary server with system data from a backup file:

1. Log into the TUI as installer on the *secondary* server using a directly-connected console or SSH client.

   The TUI Main Menu displays.

2. Choose **Cisco Vision Server Administration.**
3. Choose **Restore all system data from system backup.**
4. Select the components that you want to restore, and select the date of the backup file to use for the restore.
5. Click **Apply**.

   The restore begins. A dialog box appears notifying you when the restore process successfully completes.

6. When the restore is complete, look around the system to verify that everything looks as expected.

Stopping Services and Auto-Restart and Shutting Down the Primary Server

Note: If the primary server becomes unavailable for this task, power down the server so that it will not conflict with the newly active secondary server.

To stop services and auto-restart and to shut down the primary server:

1. Log into the TUI as installer on the *primary* server using a directly-connected console or SSH client.

   The TUI Main Menu displays.

2. Choose **Cisco Vision Server Administration.**
3. Choose **Failover**.
4. Choose **Configure as Secondary/Inactive**.
5. Press any key to return to the **Failover** sub-menu.
6. Return to the **Cisco Vision Server Administration** menu by typing **R** and pressing **Enter**.
7. Choose **Power Off**.

   The primary server shuts down.

Shutting Down Services on the Secondary Server

To shut down services on the secondary server:

1. Log into the TUI as installer on the *secondary* server using a directly-connected console or SSH client.

   The TUI Main Menu is displayed.

2. Choose **Cisco Vision Server Administration**.
3. Choose **Shutdown Dynamic Signage Director software**.

   All Cisco Vision Director services stop.

4. Return to the Main Menu by typing **R** and pressing **Enter**.

Changing the IP Address on the Secondary Server

Prerequisites

Before you change the IP address on the secondary server, be sure that the following requirements are met:

- You have the IP address of the primary server.
- You understand how to use the vi editor. For information about using the vi editor, see Cisco Vision Dynamic Signage Director Server Text-Based User Interface, page 103.

Note: The system will run if the localhost entry exists but the hostname entry is missing in the /etc/hosts file. However, when the secondary hostname exists, the IP address of the secondary server must be changed to match the IP address of the primary server.

Procedure

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

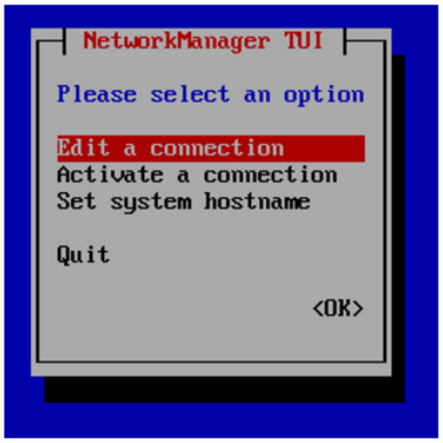
To change the IP address on the secondary server:

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, choose **System Settings.**
3. Choose **Network Settings.**
4. Choose **Setup Network Information**.

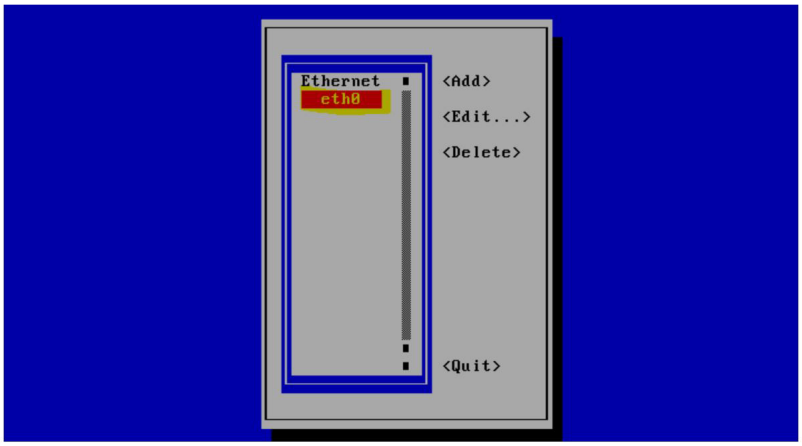
   Tip: To navigate through the TUI menus, type the character that corresponds to the menu area (a, b, c, and so on) and press **Enter**. To return to other menus, use one of the indicated keys to return to prior menus.
5. At the Network Manager TUI screen, select **Edit a Connection** (Figure 3 on page 94).

Figure 3 Edit a Connection



6. Select “eth0”
7. Select “Edit...”(Figure 4 on page 94).

Figure 4 Editing the Network

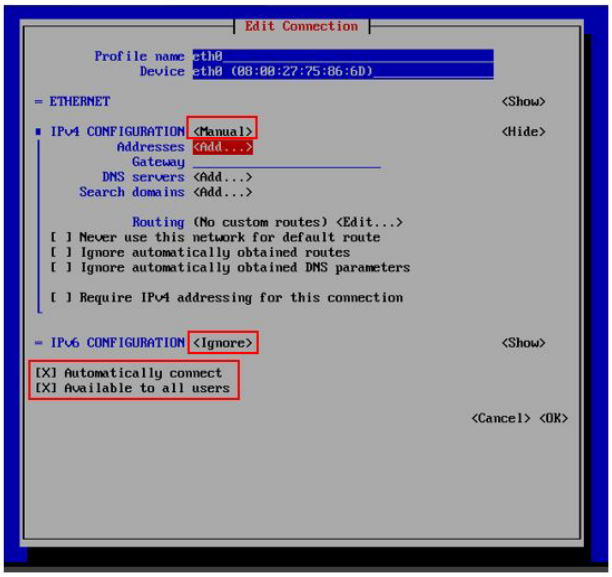


8. Set IPv4 CONFIGURATION to “Manual” (Figure 5 on page 95).
9. Select “Show” to provide details.
10. Press the tab key until the cursor is positioned on the Static IP address line.
11. Press the backspace key to go to the beginning of the line and type in the IP address of the primary server.

    Format is: *ip address/prefix*

In our example from Figure 2 on page 91, this would be 10.0.0.1. Use the actual IP address of your primary server.

Figure 5 Network Setup



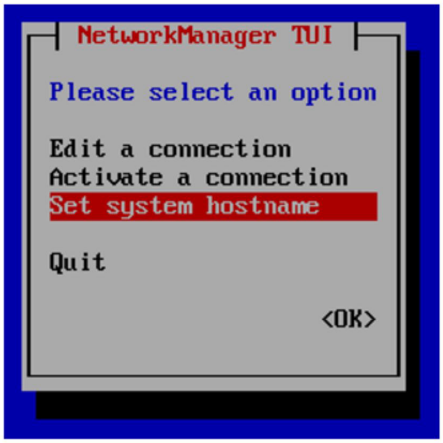
Notes:
Do not change the name of “eth0”.
Keep the IPv6 CONFIGURATION to “Ignore”.
Leave the boxes for “Automatically connect” and “Available to all users” checked.

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

13. Press any key to return to the **Network Settings** sub-menu.

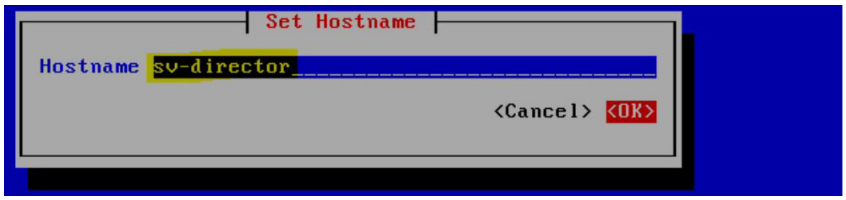
14. Select **Set system hostname** (Figure 6 on page 95).

Figure 6 Set System Hostname



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

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



16. See Editing the Hosts File, page 23.
17. Replace this server's IP address with the IP address of the primary server.
18. Save the configuration and exit vi using the following command:

    ```
    :wq
    ```

Restarting the Network Service on the Secondary Server

To restart the network service on the secondary server:

1. From the TUI Main Menu on the secondary server, go to the **Services Control** sub-menu.
2. Select the **Networking** option.

   The Networking sub-menu is displayed.
3. Select the **Restart networking** option.

   The network daemon is restarted and the IP address change is put into effect on the secondary server.

Note: If you are connected to the server through the network using SSH, your session disconnects. Reconnect using the IP address of the primary server.

Verifying Network Connectivity to the Secondary Server

To verify network connectivity to the secondary server:

1. From the TUI Main Menu on the secondary server, go to the **Troubleshooting** sub-menu.
2. Select the **Ping a host** option.
3. At the "Enter hostname" prompt, type the hostname or IP address of the secondary server and press **Enter**.
4. Look for successful transmission and receipt of PING packets.

   Note: If you cannot reach the secondary server, go to Clearing the ARP Cache on the Switch, page 96.
5. Press **Ctrl-C** to stop sending PING packets.
6. Press any key to return to the Troubleshooting menu.

Clearing the ARP Cache on the Switch

This task is optional; the ARP cache on the switch will refresh in 5-10 minutes. However, if you cannot access the secondary server after changing its IP address, clear the ARP cache for that IP address on the switch using the **clear ip arp** privileged EXEC command.

To clear the ARP cache on the switch:

1. Use a directly-connected console, or if you know the IP address of the switch, use Telnet to access the switch as shown in the following example, where *ip-address* is the address of your switch:

   ```
   telnet ip-address
   ```

2. At the corresponding prompts, enter your login information as shown in the following example, where *yourname* and *yourpass* are your username and password:

   ```
   Username: yourname
   Password: yourpass
   switch>
   ```

3. Enter privileged EXEC mode using the **enable** command and corresponding password:

   ```
   switch> enable
   Password: enablepassword
   switch#
   ```

4. To clear the ARP cache of the newly-assigned IP address now used by the secondary server, use the **clear ip arp** command as shown in the following example:

   ```
   clear ip arp 10.0.0.1
   ```

Restarting Cisco Vision Director on the Secondary Server

To restart Cisco Vision Director on the secondary server:

1. Do one of the following on the *secondary* server:
   - If still logged into the TUI, go to the Main Menu.
   - If not still logged into the TUI as installer on the secondary server, use the new IP address and log in again using a directly-connected console or SSH client.

   The TUI Main Menu displays.

2. Choose **Cisco Vision Server Administration**.
3. Choose **Restart Dynamic Signage Director software**.

   All Cisco Vision Director services are started.

4. Press any key to return to the Cisco Vision Server Administration sub-menu.
5. Press **R** and **Enter** until you return to the Main menu.
6. Press **X** to exit the TUI.

Verifying the Cisco Vision Director Configuration on the Secondary Server

To verify the Cisco Vision Director configuration on the secondary server:

1. Log into Cisco Vision Director on the ***secondary*** server using an administrator account.
2. From the Cisco Vision Director main menu, click **Device Management > Get Status**.
3. Click **Play** (**Send Command**).

   Confirm that you have successful communication between the DMPs and Cisco Vision Director.

4. Verify that all of the content is on this server.
5. To establish control of the DMPs, start a script without any content and with **No Staging** selected. This should require less than 10 minutes.

   Note: You can push a script with content, but that means longer downtime.

How to Restore the Primary Server to Active

Note: This task requires a service interruption.

At a scheduled downtime, restore the primary server as the active server to re-establish your normal operating environment to clean up the original primary server from a failure or prepare to do a software upgrade, make IP addressing changes, and have regularly scheduled backups again between the two servers.

Note: To select a TUI menu item, type the character that corresponds to the menu option and press **Enter**.

This section includes the following tasks:

Prerequisites to Restoring the Primary Server to Active

If you make any administrative changes on the active secondary server, run a successful backup.

While the secondary server is still active, re-configure the backup environment and run a manual backup from the Cisco Vision Director **Manage Software > System Backups**. The latest backup will then be copied to the primary (inactive) server. For more information, see Backing Up and Restoring Cisco Vision Director Servers, page 77.

Note: Smart Software Licensing requires that you register both servers. See the Cisco Vision Software Installation and Upgrade Guide.

Stopping Services and Auto-Restart on the Secondary Server

To stop services and auto-restart of them on the secondary server:

1. Log into the TUI as installer on the ***secondary*** server using a directly-connected console or SSH client.

   The TUI Main Menu displays.

2. Choose **Cisco Vision Server Administration** > **Failover**.
3. Choose **Configure as Secondary/Inactive**.
4. Press any key to return to the Failover sub-menu.
5. Return to the **Cisco Vision Server Administration** menu by typing **R** and pressing **Enter**.
6. Choose **Shutdown Dynamic Signage Director software**.

Changing the IP Address on the Secondary Server

Prerequisites

Before you change the IP address on the secondary server, be sure that the following requirements are met:

- You have the IP address of the secondary server.
- You understand how to use the vi editor. For information about using the vi editor, see Cisco Vision Dynamic Signage Director Server Text-Based User Interface, page 103.
- See procedure Changing the IP Address on the Secondary Server, page 93.

Verifying Network Connectivity on the Secondary Server

To verify network connectivity to the secondary server:

1. From the TUI Main Menu on the ***secondary*** server, go to the **Troubleshooting** sub-menu.
2. Choose **Ping a host**.
3. At the “Enter hostname” prompt, type the hostname or IP address of the secondary server and press **Enter**.
4. Look for successful transmission and receipt of PING packets.

   Note: If you cannot reach the secondary server, go to Clearing the ARP Cache on the Switch, page 96.
5. Press **Ctrl-C** to stop sending PING packets.
6. Press any key to return to the Troubleshooting menu.

Starting and Configuring the Services on the Original Primary Server

To start and configure the services on the original primary server:

1. Power on the original ***primary*** server.

   Note: It might take a few minutes for SSH to be available as the server boots.
2. Log into the TUI as installer on the original ***primary*** server using a directly-connected console or SSH client.

   The TUI Main Menu displays.
3. Choose **Cisco Vision Server Administration** > **Failover**.
4. Choose **Promote as Primary/Active**.

   The Cisco Vision Director services are started and also configured to start automatically when a reboot occurs.

5. Press any key to return to the Failover sub-menu.
6. If a script is running on the original primary Cisco Vision Director server, end the script.

Verifying Network Connectivity to the Primary Server

To verify network connectivity to the primary server:

1. From the TUI Main Menu on the original ***primary*** server, go to the **Troubleshooting** sub-menu.
2. Choose **Ping a host**.
3. At the "Enter hostname" prompt, type the hostname or IP address of the primary server and press **Enter**.
4. Look for successful transmission and receipt of PING packets.

   Note: If you cannot reach the secondary server, go to Clearing the ARP Cache on the Switch, page 96.
5. Press **Ctrl-C** to stop sending PING packets.
6. Press any key to return to the Troubleshooting menu.
7. Press **R** and **Enter** until you return to the Main menu.
8. Press **X** to exit the TUI.

Restoring the Original Primary Server with System Data From a Backup File

If any administrative changes were made to the system while in failover to the other server, restore the backup from the secondary.

Note: This step requires that a backup was run from the secondary server to the primary, before reactivating the primary server.

To restore the original primary server with system data from a backup file:

1. Log into Cisco Vision Director on the original ***primary*** server using an administrator account.
2. From the Cisco Vision Director Main Menu, click **Configuration > System Configuration**.
3. From the Dashboard drawers, select **Tools > Advanced > Restore system data from backup**.
4. Select the components that you want to restore.
5. Select the date of the backup file to use for the restore.
6. Click **Apply**. The restore begins.

Restarting the Cisco Vision Director Software

After you perform any restore on a Cisco Vision Director server, restart the Cisco Vision Director software to resume normal operation of the services.

To restart the Cisco Vision Director software:

1. Log into the TUI as installer on the original ***primary*** server using a directly-connected console or SSH client.

   The TUI Main Menu displays.
2. Go to **Cisco Vision Server Administration > Restart Cisco Vision Director Software**.

3. Press **R** and **Enter** until you return to the Main menu.
4. Press **X** to exit the TUI.

Verifying the Cisco Vision Director Configuration on the Original Primary Server

To verify the Cisco Vision Director configuration on the original primary server:

1. Log into Cisco Vision Director on the original ***primary*** server using an administrator account.
2. From the Cisco Vision Director Main Menu go to **More > Management Dashboard**.
3. From the Dashboard drawers, select **DMP and TV Controls > Monitoring > Get Status**.

   Confirm that you have successful communication between the DMPs and Cisco Vision Director.
4. Verify that all of the content is on this server.
5. Test the system by looking at the status in the **Management Dashboard**.
6. Run a test script to verify operation of the system.

Upgrading the Primary Server Software

Note: This task is only necessary when performing a software upgrade on redundant servers according to the instructions in Cisco Vision Software Installation and Upgrade Guide: Dynamic Signage Director Release 6.2.

After you restore the original ***primary*** server to active status after an upgrade of the software on the ***secondary*** server, upgrade the primary server software.

Reconfiguring the Backup Environment After Upgrades

After you complete software upgrades for both the secondary and primary servers, reconfigure the backup environment to re-enable the backup account on the ***secondary*** server and to configure the ***primary*** server for automatic backup and restore. For more information, see Backing Up and Restoring Cisco Vision Director Servers, page 77.

Cisco Vision Dynamic Signage Director Server Text-Based User Interface

The text-based user interface (TUI) provides a console-based interface for use by system installers, administrators, and troubleshooting personnel. The TUI replaces the requirement for any low-level system command line (shell) access and performs routine system tasks such as modifying system configurations, changing passwords, and checking system logs. Remote TAC access and troubleshooting can both be done from the TUI in the event of an outage or failure.

Contents

Information About the TUI

This section includes the following topics:

Overview of the TUI Menus

The TUI is a nested structure of menus with options that allow you to drill down to specific system tasks to perform on the server. The primary menus are:

- Main Menu
- System Settings
- System Accounts
- Services Control
- Cisco Vision Server Administration
- Troubleshooting

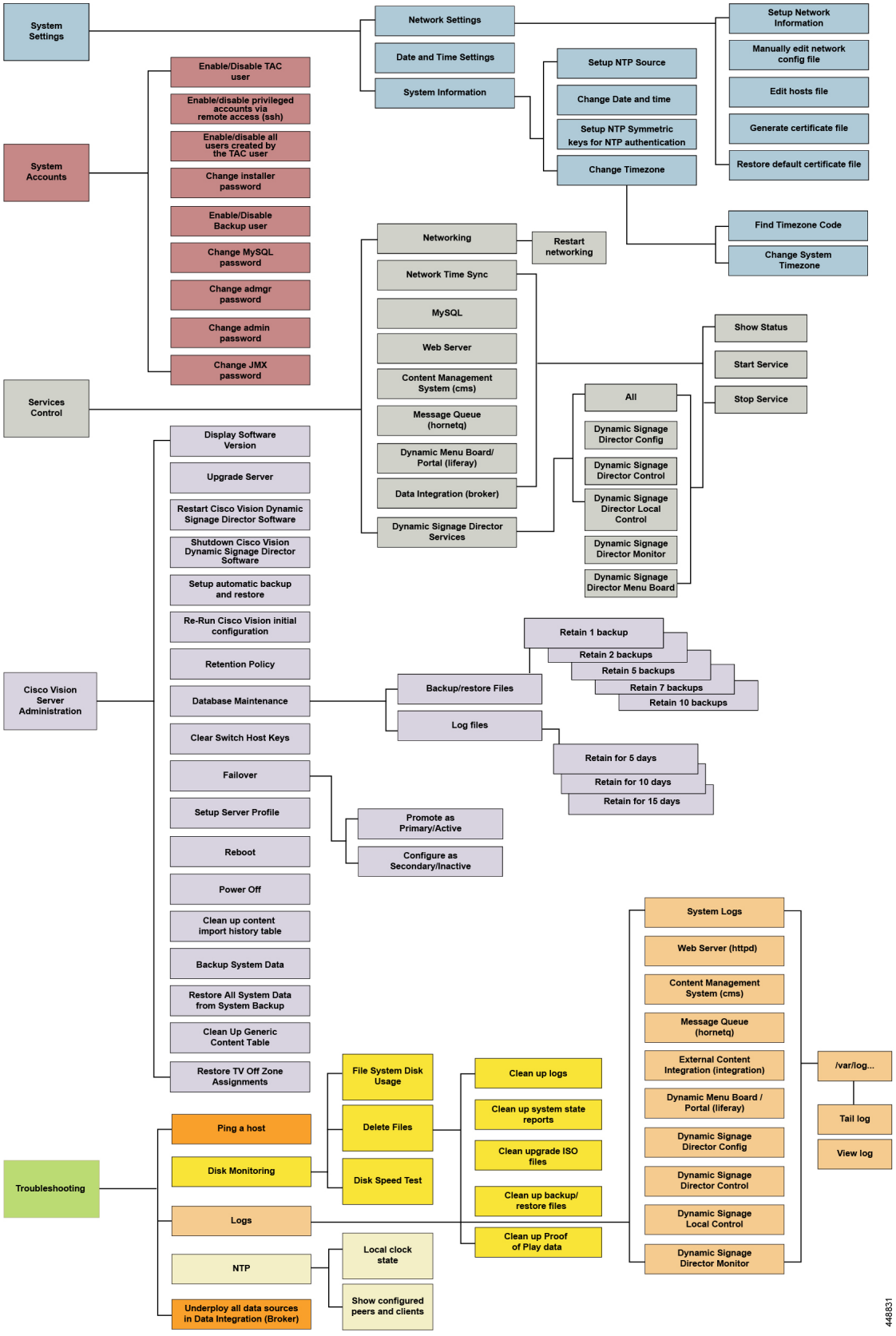
Table 1 on page 104 provides a description of the primary menus included in the Cisco Vision Dynamic Signage Director TUI.

Table 1 Description of the Primary TUI Menus

Menu Name	Use this menu to . . .
Main Menu	Access all other menus or exit the TUI.
System Settings	Change server network configuration, system date/time, or display system information.
System Accounts	Manage default system passwords. For more information about system accounts and modifying them, see System Accounts on the Cisco Vision Dynamic Signage Director Servers, page 63.
Services Control	Access services running on the server to start, stop, or show status.
Cisco Vision Server Administration	Manage the operation and software configuration of the server.
Troubleshooting	Run a **ping** command, monitor disk space usage, clean up files to free up disk space, test disk speed, display system logging information, or get NTP information.

Figure 1 on page 104 shows a map of the new Cisco Vision Dynamic Signage Director TUI menu system and options.

Figure 1 TUI Map for Cisco Vision Dynamic Signage Director Servers


System Settings
Network Settings
Setup Network Information
Manually edit network config file
Edit hosts file
Generate certificate file
Restore default certificate file
Date and Time Settings
Setup NTP Source
Change Date and time
Setup NTP Symmetric keys for NTP authentication
System Information
Change Timezone
Find Timezone Code
Change System Timezone
System Accounts
Enable/Disable TAC user
Enable/disable privileged accounts via remote access (ssh)
Enable/disable all users created by the TAC user
Change installer password
Enable/Disable Backup user
Change MySQL password
Change admgr password
Change admin password
Change JMX password
Networking
Restart networking
Network Time Sync
MySQL
Web Server
Content Management System (cms)
Message Queue (hornetq)
Dynamic Menu Board/ Portal (liferay)
Data Integration (broker)
Dynamic Signage Director Services
Services Control
Show Status
Start Service
Stop Service
All
Dynamic Signage Director Config
Dynamic Signage Director Control
Dynamic Signage Director Local Control
Dynamic Signage Director Monitor
Dynamic Signage Director Menu Board
Cisco Vision Server Administration
Display Software Version
Upgrade Server
Restart Cisco Vision Dynamic Signage Director Software
Shutdown Cisco Vision Dynamic Signage Director Software
Setup automatic backup and restore
Re-Run Cisco Vision initial configuration
Retention Policy
Database Maintenance
Backup/restore Files
Retain 1 backup
Retain 2 backups
Retain 5 backups
Retain 7 backups
Retain 10 backups
Log files
Retain for 5 days
Retain for 10 days
Retain for 15 days
Clear Switch Host Keys
Failover
Promote as Primary/Active
Configure as Secondary/Inactive
Setup Server Profile
Reboot
Power Off
Clean up content import history table
Backup System Data
Restore All System Data from System Backup
Clean Up Generic Content Table
Restore TV Off Zone Assignments
Troubleshooting
Ping a host
Disk Monitoring
Logs
NTP
Underploy all data sources in Data Integration (Broker)
File System Disk Usage
Delete Files
Disk Speed Test
Local clock state
Show configured peers and clients
Clean up logs
Clean up system state reports
Clean upgrade ISO files
Clean up backup/ restore files
Clean up Proof of Play data
System Logs
Web Server (httpd)
Content Management System (cms)
Message Queue (hornetq)
External Content Integration (integration)
Dynamic Menu Board / Portal (liferay)
Dynamic Signage Director Config
Dynamic Signage Director Control
Dynamic Signage Local Control
Dynamic Signage Director Monitor
/var/log...
Tail log
View log
448831

Working with the TUI Interface

This section includes the following topics:

Menu Navigation

The Main Menu displays when you log in. To navigate through the menus, type the character that corresponds to the menu area item (**a**, **b**, **c**, and so on) and press **Enter**.

To return to other menus, use one of the indicated keys to return you to prior menus.

Caution: Avoid pressing Ctrl-c from the TUI. If services were started during the session they might stop running. Use the TUI menu system to exit the interface.

File Editor

Several of the TUI options open server system files for you to modify using the Unix system vi editor. The following configuration files are editable from the TUI:

- DNS information—/etc/resolv.conf
- NTP server information—/etc/ntp.conf
- Server host information—/etc/hosts

Before modifying configuration files, you should be familiar with the simple editing techniques used within the vi editor. Table 2 on page 106 describes some of the more common vi editor commands.

Table 2 Common vi Editor Commands

Command	Description
ZZ or **:wq**	Exit vi and save changes.
:q!	Exit vi without saving changes.
Esc key	Exit current mode and enter vi command mode.
Cursor Movement	
h	Move left (backspace).
j	Move down.
k	Move up.
l	Move right.
Enter key	Move to the beginning of the next line.
Inserting	
a	Append character after cursor.
i	Insert character before cursor. Enters INSERT mode.
r	Replace character under cursor with next character typed.
R	Keep replacing character until [Esc] is pressed.
Deleting	
db	Delete word before cursor.

Table 2 Common vi Editor Commands (continued)

Command	Description
dd	Delete line under cursor.
dw	Delete word under cursor.
x	Delete character under cursor.
Put	
P	Undo deletion of characters, words, or lines before cursor.
p	Undo deletion of characters, words, or lines after cursor.

How to Use the TUI

This section provides information about how to use some of the areas of the TUI interface. It includes the following topics:

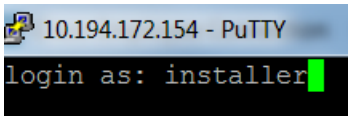
Logging Into the TUI

To access the TUI, use either physical console access or an SSH client such as PuTTY.

To log into the TUI:

1. Do one of the following:
   - Access the server using a directly-attached console.
   - In the SSH client software, specify the IP address of the server that you want to access.
2. When the “login as:” prompt appears, type **installer** and press **Enter** (Figure 2 on page 107):

Figure 2 TUI Login Prompt

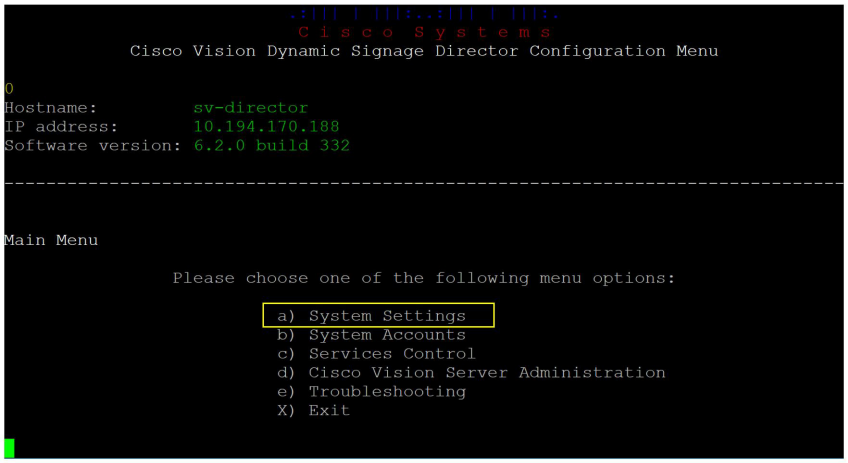


3. At the password prompt, type the installer password and press **Enter**.

Note: In a PuTTY terminal, the keystrokes for your password entry are not shown.

When the login is successful, the Main Menu displays along with some basic system information at the top of the screen (Figure 3 on page 108).

Figure 3 Cisco Vision Dynamic Signage Director TUI Main Menu



Note: Once logged in, you can change the installer password from the **System Accounts** > **Change installer password** menu option.

Note: Keep a good record of the changed installer password. Cisco cannot recover the password, If you lose the password, a re-install could be required.

Displaying System Information

The **System Settings** > **System Information** option allows you to obtain information about the current network configuration, hosts file, DNS configuration, NTP server, system date and time, and UUID for the server.

To display system information:

1. Go to the TUI Main Menu.
2. Choose **System Settings** and press **Enter** (Figure 3 on page 108).
3. From the **System Settings** menu, type the letter corresponding to the **System Information** option and press **Enter**.

   The system information is displayed on your screen.
4. To return to the **System Settings** menu, press any key.

Exiting the TUI

Caution: Avoid pressing Ctrl-c from the TUI. If services were started during the session they might stop running. Use the TUI menu system to exit the interface.

To exit the TUI:

1. Go to the TUI Main Menu.

   Note: If you are in a TUI submenu, type **R** or **<** or **,** and press **Enter** to go back to the Main Menu.
2. Type **X** and press **Enter**.

Related Documentation

The following documents provide details about using some of the specific areas of the TUI:

- Other modules in this Cisco Vision Dynamic Signage Director Server Administration Guide

- Cisco Vision Software Installation and Upgrade Guide: Dynamic Signage Director Release 6.3

System State Reports

The System State Report application enables easy capture and export of system state data for Cisco Vision Dynamic Signage Director servers. Send this information to a remote support engineer to help troubleshoot issues with the system.

Information About System State Reports

Figure 1 on page 111 shows the System State Report screen.

Figure 1 System State Report Screen

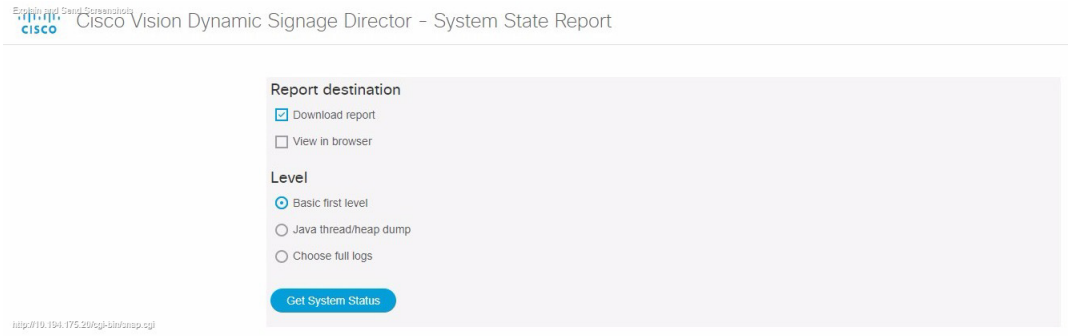


Table 1 on page 112 describes the options provided on the System State Report screen.

Table 1 System State Report Screen Description

Category	Description
Report Destination	Allows you to choose whether you want to download the report or view it in your browser window. If you check **Download report**, your browser will download the resulting report when the system state report is ready. You can save this file on your computer, view its contents, and mail it to support personnel. If you check **View in browser**, the resulting report is available for immediate viewing online via the link provided.
Level	Selects the level of detail you want in the report. ■ **Basic First Level**: Provides detailed information of the system state, including information on configuration and current performance of the hardware, the operating system, the database, the Java VM, and the SV application. ■ **Java Heap Dump**: Displays a report indicating the internal activities of the selected Java Virtual Machine (JVM). Before running the report, you will see a selection screen showing the process ID, the name of the JVM, and its command line. Select one of the JVMs that you wish to get the heap dump for, then click **Get Heap Dump**. The heap dump report will generate. Be careful in taking a heap dump. While this is running, it can affect system performance. ■ **Full SVD Logs**: Displays a list of system log files available for retrieving from the server and copying to your local drive or sending to Cisco Support. If you select **View in Browser**, view the logs online, too.
Previous Reports	Lists up to 15 of the most recent exports of the system state reports that were collected. The reports are collected from someone accessing this request page, or from a system scheduled task. Select one of the links to download to your local drive to view or email to Cisco support.

How to Run a System State Report

This section includes the following tasks:

■ Running a System State Report Manually, page 113

■ Scheduling a System State Report, page 113

■ Viewing Reports, page 113

Running a System State Report Manually

To run a system state report manually:

1. From the Cisco Vision Dynamic Signage Director server Main Menu, go to **More > System State Report**.
2. Select one or both report destination types, **Download report** and/or **View in browser**.
3. Under **Level**, select the type of report that you want to run.
4. Click **Get System Status**. A status bar displays while the report is generating.

Scheduling a System State Report

You can extract the system state data on a periodic basis. Go to Tools > Management Dashboard. Click the **Tools** drawer **> Advanced > Scheduled Tasks** function. View the reports generated under **Previous Reports** on the main **System State Report** page.

To create a scheduled task:

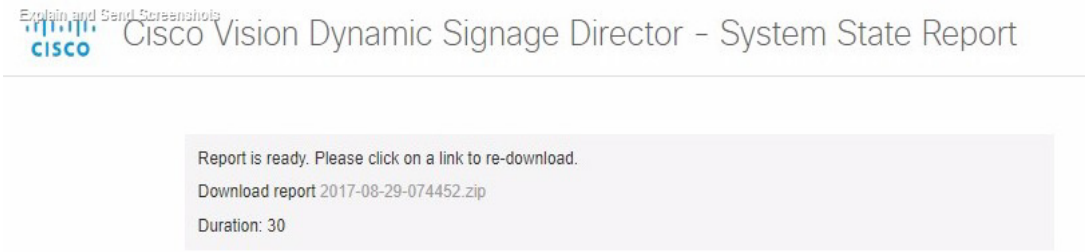
1. Go to **More > Management Dashboard** and select **Tools** drawer **> Advanced** tab **> Scheduled Tasks**.
2. Click **Add Row** and add a row with the task type being **SystemStateExtractorTask**.
3. Enter a task time as desired.
4. Click **Apply**.

   View the reports generated under **Previous Reports** on the main **System State Report** page.

Viewing Reports

After manually running a report, the screen displays “Report is ready” as shown in Figure 2 on page 113.

Figure 2 Report is Ready



Depending on the option(s) that you selected before running the report, you can view the report in your browser by selecting the link provided.

If you downloaded the report, then depending on your browser and its settings, you will get a dialog box to save the report on your local machine. If the automatic download does not work, click on the link after the word **Download** to download the file again. The report downloads as a compressed file (.zip) containing multiple parts to the report.

Note: The heap dump report type is a compressed report file which you can save to your local drive and forward to support personnel for troubleshooting.It is packaged like the Basic Level report.

Viewing Scheduled Reports and Previous Reports

View scheduled reports under **Previous Reports** on the **System State Report** screen. The format of the file name is the date and time that the report was run.

Click one of the timestamps under **Previous Reports** to download the report that ran at the scheduled time. You may get a dialog box to save the report on your local machine. If so, save it as desired. This is a compressed file containing multiple parts to the report.

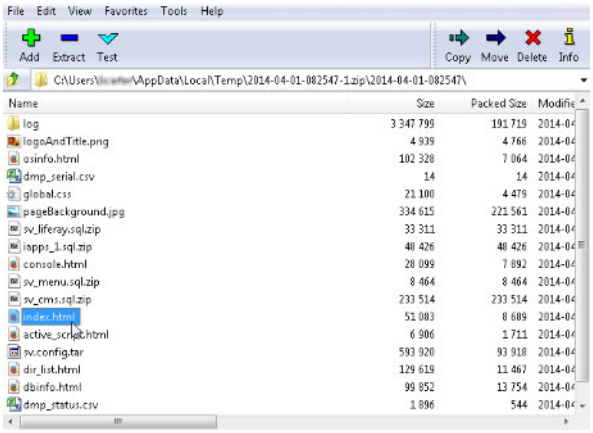
Viewing the Contents of the Zip File

Once you have downloaded the report file to your PC, you will have a .zip file. You can email it to Cisco support as is.

To view the contents of a downloaded file:

1. Double-click the file to open the .zip file archive manager. The contents of this file depends on the file compression software program installed on your PC. Figure 3 on page 114 shows an example of a common Microsoft Windows compression file manager, where the .zip file is opened to view the contents.

Figure 3 Windows Compression File Manager Example



2. Click **Extract** and load all of the files in the archive to a new directory on your local drive.
3. Navigate to the directory that you just created and locate a file named **index.html**. Double-click the file and it will open in your internet browser.
4. Click links from the browser page to view the rest of the report.

   Tip: In the case of the heap dump and log file reports, there is not an “index.html” file. Navigate down the levels of folders until you see the log files of interest.