Cisco Video Surveillance Management Console Administration Guide

Cisco Video Surveillance Manager, Release 7.14
October 2019

Cisco Systems, Inc. www.cisco.com

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.

Cisco Video Surveillance Management Console Administration Guide, Release 7.14

Preface vii

Overview vii

Related Documentation vii

Obtaining Documentation and Submitting a Service Request vii

CHAPTER 1

Overview 1-1

Overview 1-2

Using the Management Console 1-2

Understanding the Initial Setup Wizard 1-3

Management Console Feature Summary 1-4

Requirements 1-5

Logging In 1-7

Changing the Cisco VSM Management Console Password 1-8

CHAPTER 2

Server Administration 2-1

Server Settings 2-2

General Information 2-2

Services 2-2

Network Information 2-4

VSOM High Availability 2-5

Time Settings (NTP Information) 2-7

Set Date Time 2-8

SSL Certificate 2-9

Using a SSL Certificate 2-9

SNMP Settings 2-12

Clear Restrictions for Failed Login Attempts 2-14

System Settings 2-15

Server Upgrade 2-15

Log Level 2-19

Setting the Process Log Levels 2-19
Setting the Platform Service Log Levels 2-21
Manage Drivers 2-22
Backup & Restore 2-24
Backup Usage Notes 2-24
Backup Procedure 2-25
Backup Settings 2-26
Restoring a Backup 2-27
Backup File Format 2-28
Backup File Information 2-29
Failed Backups 2-29
Deleting a Backup File 2-29
Active Users 2-30
Local User 2-31

CHAPTER 3 **Troubleshooting** 3-1
Software Status 3-2
Hardware Status 3-3
Hardware Information 3-3
System Resources 3-4
Hardware Alerts 3-5
RAID Status 3-6
Support Report 3-9
Media Server 3-10
Devices 3-10
Recordings 3-12
Media Out 3-14
Streams 3-15

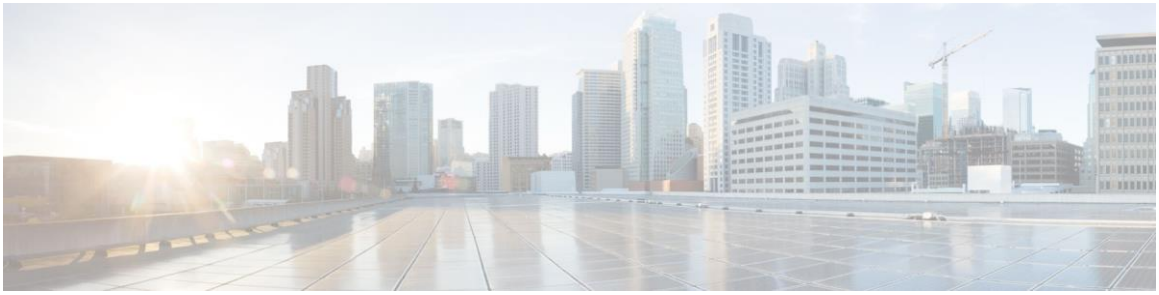
CHAPTER 4 **History** 4-1
Jobs 4-1
Understanding Job Status 4-4
Audit Logs 4-5
System Logs 4-6
System Log Descriptions 4-7

CHAPTER 5 **Restarting and Shutting Down** 5-1
Restart Services 5-1

Reboot Server 5-1
Shutdown Server 5-2

CHAPTER 6 Monitor Video 6-1

APPENDIX A Related Documentation A-1



Preface

Revised: October 2019

Overview

This document describes the procedures used to access the Cisco Video Surveillance Management Console browser-based user interface (UI) that is used to setup, monitor, and administer a single Cisco Video Surveillance server.

Related Documentation

See the Cisco Video Surveillance 7 Documentation Roadmap for descriptions and links to Cisco Video Surveillance documentation, server and storage platform documentation, and other related documentation.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to What's New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Overview

The Cisco Video Surveillance Management Console (Management Console) is a browser-based user interface used to manage, monitor, and troubleshoot a single physical or virtual Cisco Video Surveillance server.

Refer to the following topics for more information:

Contents

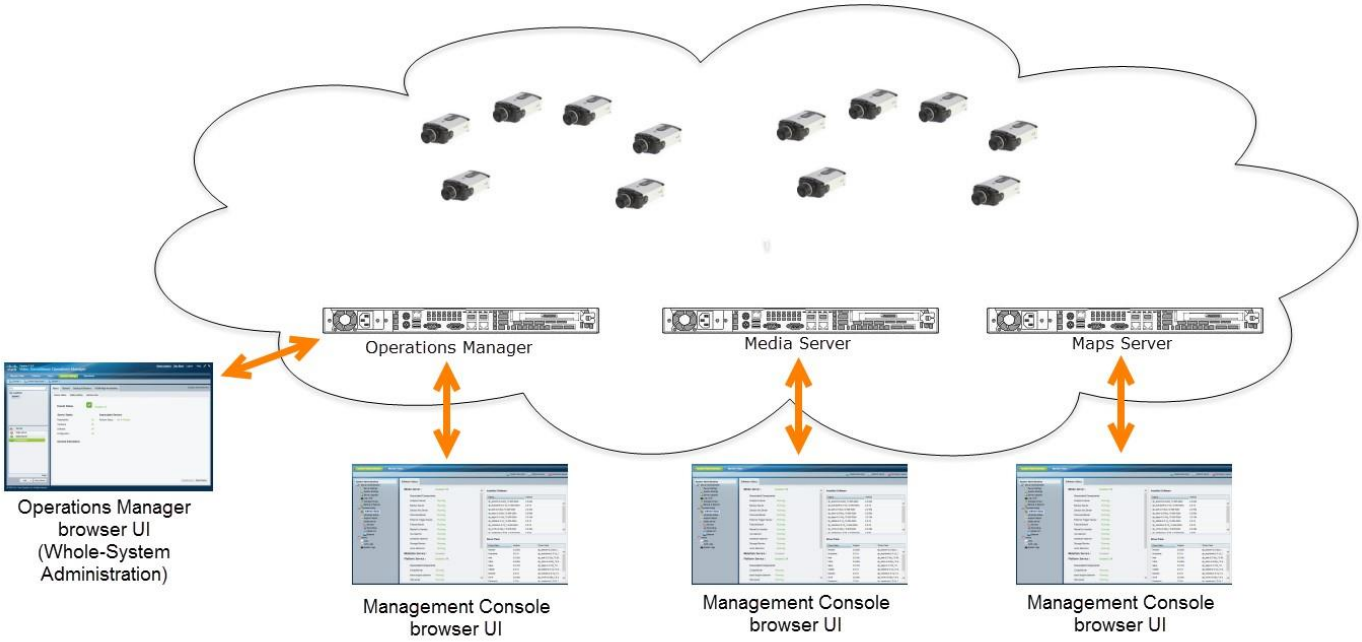
- Overview, page 1-2
  - Using the Management Console, page 1-2
  - Understanding the Initial Setup Wizard, page 1-3
  - Management Console Feature Summary, page 1-4
  - Requirements, page 1-5
- Logging In, page 1-7
- Changing the Cisco VSM Management Console Password, page 1-8

Using the Management Console

The Cisco VSM Management Console is used by system administrators to perform infrequent administration tasks on a single physical or virtual machine. For example, use the Management Console to complete the initial server Setup Wizard, monitor system logs and resources, troubleshoot hardware and system software issues, and gather information about the installed hardware and software components.

The Management Console user interface is available for each instance of system software installed on either a physical server (such as the Cisco Connected Safety and Security UCS Platform Series servers) or as a virtual machine (Figure 1-1).

Figure 1-1 Management Console UI for Each Cisco VSM Server



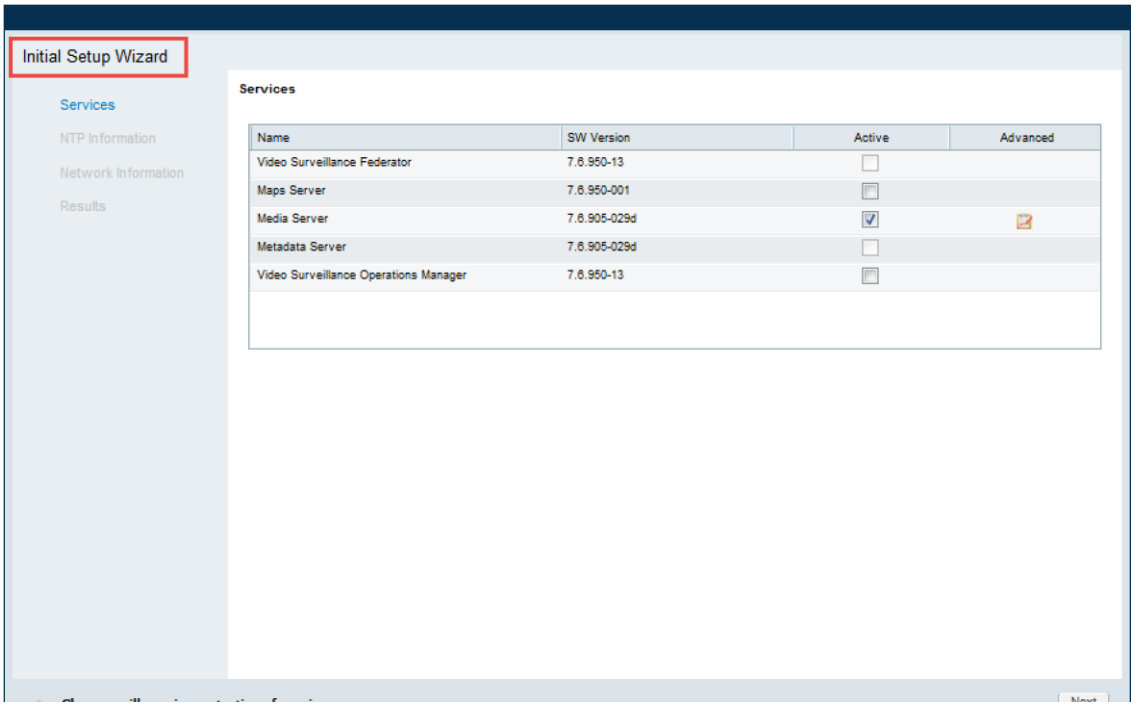
Note After a server is added to the Operations Manager configuration, the Management Console cannot be used to activate or deactivate the server services. Use the Operations Manager to manage server services, such as the Operations Manager (VSOM), Federator service, Maps Server or Media Server.

Caution Never modify the Cisco Video Surveillance server settings using the Linux CLI. Always use the Cisco Video Surveillance Management Console as described in this document. Settings made using the Linux CLI can result in inconsistent system performance and other issues.

Understanding the Initial Setup Wizard

When you access a Cisco VSM server for the first time (by entering the IP address or hostname in a web browser), you are automatically redirected to the Management Console, and prompted to complete the Initial Setup Wizard (Figure 1-2). This setup wizard appears only once.

Figure 1-2 Initial Setup Wizard



Follow the on-screen prompts to enter or accept the basic settings such as the server services, NTP source, and network settings. You may be prompted to restart the server services when the wizard is complete to activate the changes.

Usage Notes

- Some fields require server services to restart when the wizard is complete.
- —Appears when a step is completed (Figure 1-2).
- Click **Back** to return to the previous step to revise or correct entries, if necessary.

Completing the Setup Wizard

Step 1 Log in to the Management Console.

See the "Logging In" section on page 1-7.

Step 2 When the Initial Setup Wizard appears, select the Services that will run on the server, and click **Next**.

Step 3 Revise the NTP server and timezone, if necessary, and click **Next**.

See the "Time Settings (NTP Information)" section on page 2-7 for more information.

Step 4 Enter the Network Information (IP address used by network cards), if necessary, and click **Next**.

Step 5 Click **Finish** and wait for the Wizard results to appear.

Step 6 Click **Reboot**, **Restart**, **or Close** when prompted.

- Restarting services can take up to 90 minutes or more depending on number of devices managed by the Operations Manager and Media Server. Installed products will be offline during this time.

Step 7 (Optional) Re-login to the Management Console, if necessary, to perform additional configuration or administrative tasks.

Step 8 (Recommended) Use the Operations Manager browser-based interface for most additional tasks, including server upgrades, network and NTP settings, and other tasks. See the Cisco Video Surveillance Operations Manager User Guide for more information.

Management Console Feature Summary

The Cisco VSM Management Console can perform the following server setup, administration and monitoring tasks:

Table 1-1 Feature Summary

Feature	Description	More information
Setup Wizard	The **Setup Wizard** guides you through the process to enable the server services such as the (Media Server and Operations Manager), configure network settings, configure the NTP server, and other basic settings.	Understanding the Initial Setup Wizard, page 1-3
Server Administration	Allows you to enter basic system properties, define the log levels, upgrade the server software and device drivers, backup or restore the server configuration. **Note** Although many configuration, backup and upgrade tasks are available using the console, we highly recommend using the Operations Manager for most tasks. The Operations Manager manages all servers in the system, and ensures that system software, NTP settings, are in sync.	Server Administration, page 2-1

Table 1-1 Feature Summary (continued)

Feature	Description	More information
Troubleshooting	Provides summaries of the installed software packages and drivers, including the software status. Also provides the status of the hardware and RAID components, and allows you to generate support reports if instructed by your support representative. The Media Server links provide lists of the cameras and encoders associated with the server, video stream and recording information, and other system details.	Troubleshooting, page 3-1
History	Provides details regarding the administrative jobs triggered by users, audit logs that track the actions taken by users, and system logs for the services enabled on the server.	History, page 4-1
Restart or shutdown the server	Use the buttons in the top right to restart, reboot or shut down the server.	Restarting and Shutting Down, page 5-1

View Video	View video from a single Cisco Video Surveillance camera.	Monitor Video, page 6-1

Requirements

The Cisco Video Surveillance Management Console requires the following.

Table 1-2 Requirements

Requirement	Requirement Complete? (✓)
A PC or laptop with the following: • Windows 7 (32-bit or 64-bit), 8.1 (64-bit), or 10. • Minimum resolution of 1280x1024 • You must log in with a standard Windows user account. Logging in with a Guest account can prevent video streaming and result in an error to be displayed in the video pane: "Cannot create RTSP connection to server. Check network connection and server health status." See the Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification for the complete baseline performance specifications for a video surveillance monitoring workstation.	☐
The Internet Explorer (IE) web browser. • Windows 7 supports IE 10 or 11. • Windows 8 supports IE 10, desktop version (the Metro version of IE 10 is not supported). • Windows 8.1 supports IE 11 See the Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification for the complete baseline performance specifications for a video surveillance monitoring workstation.	☐

Table 1-2 Requirements (continued)

Requirement	Requirement Complete? (✓)
A physical or virtual server running Cisco Video Surveillance 7.6 (or higher). **Note** The Cisco VSM Management Console interface in release 7.6 (or higher) is different than the console in Cisco VSM release 7.5 and lower. See the Cisco Video Surveillance Management Console Administration Guide for your release. **Server Platform Information** • Physical Servers: – (Systems pre-installed with Release 7.2 or higher) See the Cisco Physical Security UCS Platform Series User Guide for more information. – (Systems pre-installed with Release 7.0.0 or 7.0.1) See the Cisco Physical Security Multiservices Platform Series User Guide for more information. • Virtual Machines—See the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms for instructions to install the server software .ova image as a virtual machine (VM).	☐

At least one static IP address used to access the server. The address will be assigned to the Eth0 or Eth1 port. • Redundant Operations Manager servers in an HA config must use the same Ethernet port for network access.	☐
Complete the server initial configuration (including network settings) using the Setup Wizard. **Note** Adding a Media Server directly to the Operations Manager configuration without completing the Management Console **Initial Setup Wizard** will cause the Media Server to use the Operations Manager IP address (instead of the hostname).	☐
Verify that only one interface is enabled and active on the server configured with the Operations Manager service (including co-located servers). Although the Management Console UI allows enabling both interfaces when the Operations Manager service is running, this configuration is not supported.	☐
Verify that the Operations Manager server hostname resolves to only one (correct) address. **Note** Dual-homed/NAT server configurations are not supported on any server running the Operations Manager service (including co-located servers). Dual-homed/NAT server configuration is supported only for stand-alone Media Servers.	☐
Each server must run the same version of system software. If a critical driver pack mismatch error occurs, then the driver packs on all Media Servers must be upgraded to the same version.	☐

Logging In

The Cisco VSM Management Console password is used for the following:

- Access the Management Console browser-based utility.
- Add the Media Server to the Operations Manager configuration (see the Cisco Video Surveillance Operations Manager User Guide for more information).
- Monitor video with for cameras supported by a specific Media Server.

Notes

- The default username localadmin is read-only and cannot be changed.
- You can also enable the Local User username. This provides access to the Monitor Video page so users can view video on the Media Server if the Operations Manager is down or unavailable.
- A local user account can be created to allow users to monitor video for cameras supported by the Media Server. This can be used to give users access to local video only, or if the Cisco VSM Operations Manager is down or unavailable. The local user can only access the Monitor Video page. See Local User, page 2-31.

Procedure

Step 1 Launch the 32-bit version of Internet Explorer on your Windows computer.

See the "Requirements" section on page 1-5 for supported versions.

Step 2 Enter the server URL.

For Release 7.6 and higher, the syntax is: **http://**<server-ip-address or hostname>**/cdaf/**, where the server address is one of the following:

Platform	Server Address
Physical servers	The default (factory) static IP address is 192.168.0.200 For example, the URL is **http://192.168.0.200/cdaf/**
Virtual Machines: Cisco Unified Computing System (Cisco UCS) platform	The Cisco VSM server includes two network ports with the following default configuration: • Eth0 port—static IP address 192.168.0.200 • Eth1 port— DHCP See the "Configuring the Network Settings" section of the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms for more information.

Step 3 Enter the Cisco VSM Management Console password.

Platform	Username / Password
Physical servers	• The default username **localadmin** is read-only and cannot be changed. • The default password is **secur4u**.
Virtual Machine—Cisco USC platform	• The default username **localadmin** is read-only and cannot be changed. • A new password is entered during the VM setup. See the "Changing the Default Password" section of the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms for more information.

Step 4 Click **Log In**.

Step 5 (First login only, or after a factory restore):

a. Enter and re-enter a new password.

b. Complete the Initial Setup Wizard (see the "Understanding the Initial Setup Wizard" section on page 1-3).

c. Re-login when prompted.

d. Click **Get Certificate** , when prompted.

Changing the Cisco VSM Management Console Password

Click the **localadmin** username at the top if the screen, then enter and re-enter your new password.

Note The username cannot be changed.

Server Administration

Contents

- Server Settings, page 2-2
- System Settings, page 2-15
- Server Upgrade, page 2-15
- Log Level, page 2-19
- Manage Drivers, page 2-22
- Backup & Restore, page 2-24
- Active Users, page 2-30
- Local User, page 2-31

Server Settings

General Information

General settings define the server name and installed location.

This information is read-only if the server is managed by the Operations Manager. Use the browser-based Operations Manager interface to change the following settings, if necessary. **Table 2-1 General Server Settings**

Setting	Description
Name	(Required) Enter a descriptive name that can help you identify the server. For example, enter the location of the server or its primary use. The name can include any combination of characters and spaces.
Tags	(Optional) Enter the tags that help identify the server using the Find function.
Description	(Optional) Describe the purpose or use of the server. For example: “Support for Building B cameras and associated video”.

Services

This information is read-only if the server is managed by the Operations Manager. Use the browser-based Operations Manager to manage the server services.

Procedure

Step 1 Click the **Server Settings** tab (Figure 2-1).

Step 2 Click Select or de-select the Operations Manager or VSF (Federator) service

- Use the Operations Manager to enable or disable the other services.

Step 3 Click **Save**.

Step 4 Restart the system services, if prompted.

- Changes require you to restart server services and log back in.

- Restarting services can take up to 90 minutes or more depending on number of devices managed by the Operations Manager and Media Server. Installed products will be offline during this time.

Disassociate a Server

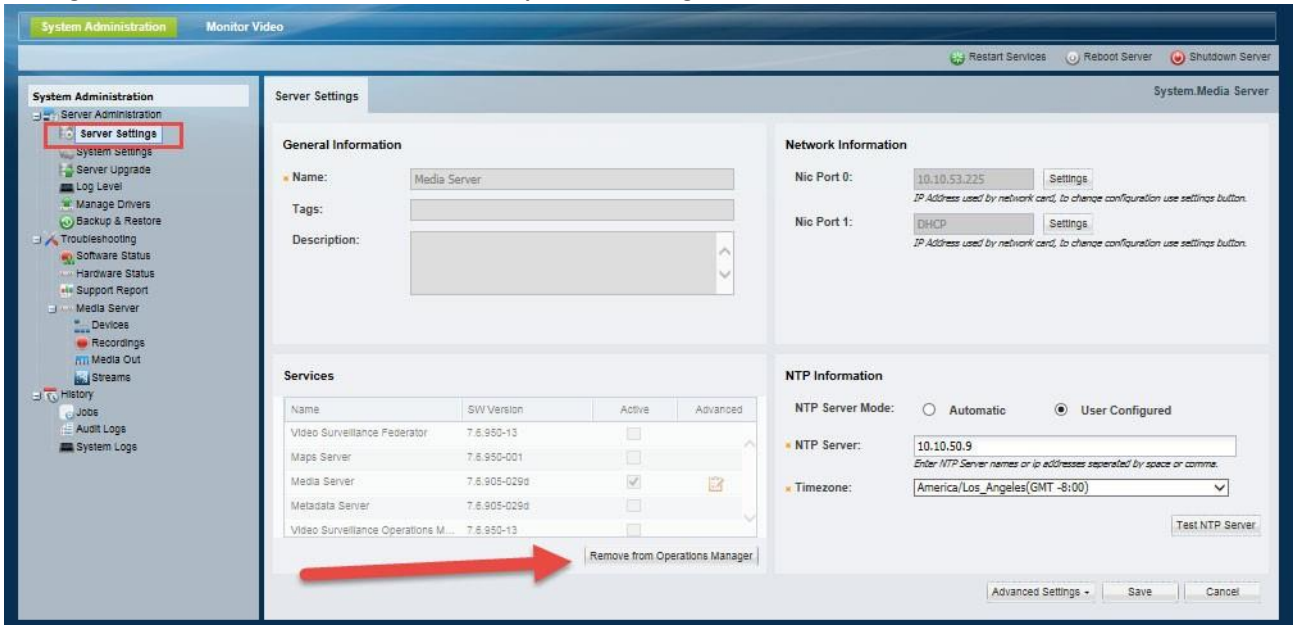
Click the **Remove from Operations Manager** button to disassociate the server and all server services from the Operations Manager (Figure 2-1). This allows the server (and running services) to be added and managed by a different Operations Manager.

You can deactivate the Operations Manager (VSOM) service even if the Media Server is running on the same server, or if the Operations Manager is managing other Media Servers. The Operations Manager (VSOM) will stop managing the Media Servers and associated cameras, so that another Operations Manager can take ownership of these Media Server and associated cameras and start managing them.

Note

- If the Media Server is co-located on the same server as the Operations Manager, the **Remove from Operations Manager** button is disabled. Log in to the Operations Manager and remove the Media Server service.
- The **Advanced** icon displays additional read-only configurations for the service. Use the Operations Manager to change these settings if necessary.

Figure 2-1 Remove a Service From Operations Manager



Server Settings

Network Information

The **Network Information** settings are used to configure the Ethernet network interface cards (NIC). These settings are configured during the initial server configuration and should only be changed by a network administrator or similar user.

Caution Incorrect network settings will cause a loss of network connectivity, loss of camera control, and the inability to view live or recorded video. Do not change these settings without a clear plan and reason. In addition, the use of certain settings, such as a static IP vs. DHCP, depends on the server applications supported on the server hardware. See the Cisco Video Surveillance Operations Manager User Guide for more information.

Tip

- If multiple VMs are deployed on the same network using the default Eth0 IP address (192.68.0.200), the Eth0 address setting in the Management Console will not be set (the field will be blank). This is because the operating system cannot configure the actual physical interface with duplicate IP addresses. To resolve this, enter a unique value for the Eth0 port on each deployed VM.
- You can also use CLI commands to change the default Eth0 network settings. See the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms for more information.

Click **Settings** next to each NIC port to change the following network settings:

Table 2-2 Network Settings

Setting	Description
Name	The NIC name.
Hostname	Enter the host name used to access the server over the network.
Domain	Enter the network domain name. For example: `cisco.com`
Configuration type	Select one of the following options based on the enabled server applications. • **Disabled**—disables the interface. • **DHCP**—the IP address and other fields will be disabled and defined by a DHCP server. • **Static** —enter the **IP address**, **Subnet Mask** and other network settings. **Note** The Ethernet ports must be configured with static IP address or DHCP depending on the enabled applications. See the Cisco Video Surveillance Operations Manager User Guide for more information.
Gateway	(Static IP configuration only) Enter the IP address of the default gateway and click **Add**.

Table 2-2 Network Settings (continued)

DNS Servers	(Optional) Enter up to three domain name service (DNS) servers. Separate multiple entries with a comma (,).
Searchable Domains	Enter the domain name. Separate multiple entries with a comma (,).

VSOM High Availability

If your Operations Manager is configured for high availability, a split brain scenario can occur when the communication between the Primary and Peer servers is lost and both servers try to independently assume the Primary role. This is called a “Split Brain” scenario.

Cisco VSM will automatically detect a Split Brain scenario and direct all traffic to the server that was Primary at
the time of communication loss. The Peer server is put in standby and a Health alert is sent.

Since there can be a delay up to 90 seconds for the issue to be detected, users logging in to the virtual IP server may have their requests sent to the Peer server (since, during this time, it is possible that user traffic will go to both servers).

When the communication link between the servers is reestablished, log in to the Operations Manager using the virtual IP/host name, and verify that the Peer server is reachable. If the Peer server is reachable, you must return the server to a normal state by doing the following:

- Clear the split brain issues
- Replace the HA configuration on the Peer server

You can clear the split brain issue using either the Operations Manager or the Cisco VSM Management Console.

Procedure

To use the Console to clear a split brain issue:

Step 1 Correct the issue causing the loss of communication between the Primary and Peer servers.

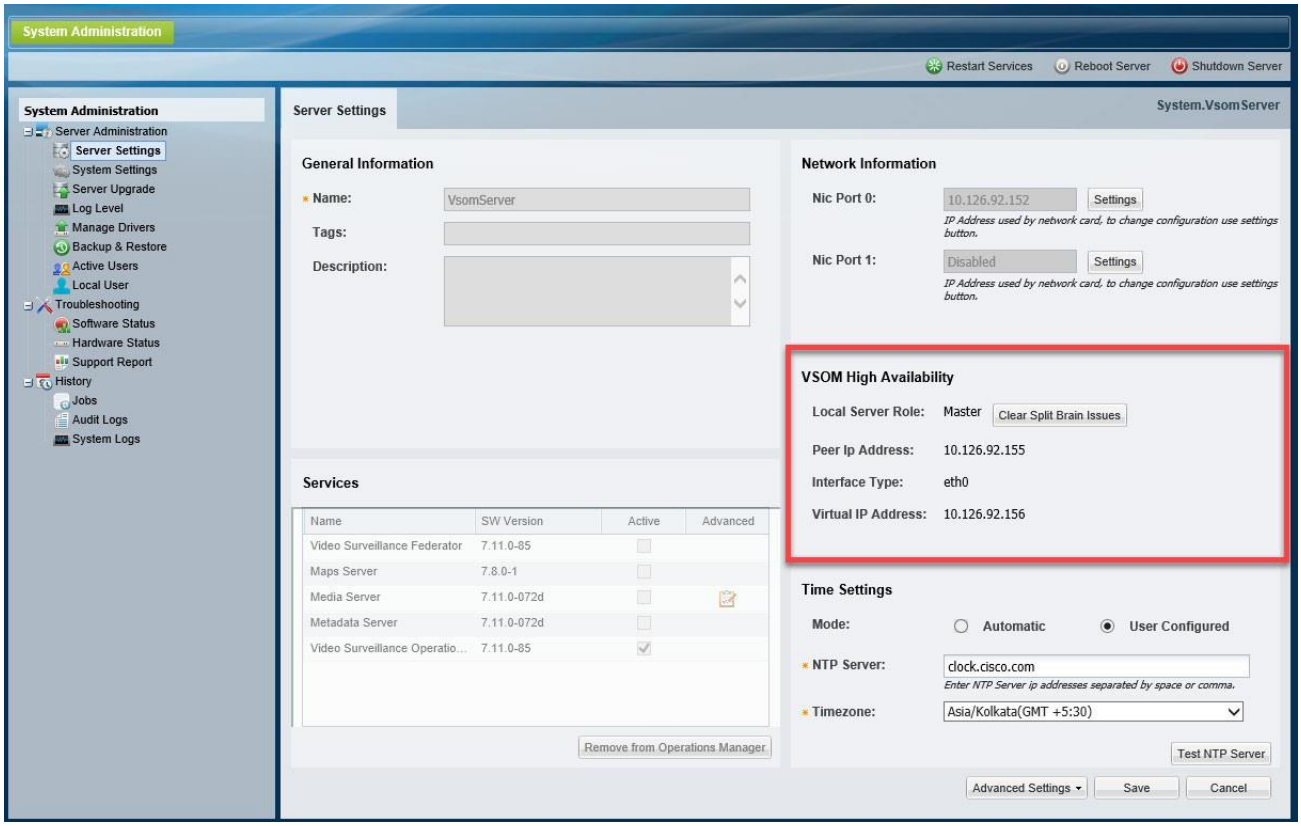
Step 2 Log in to the Cisco VSM Management Console.

Step 3 Select **Server Administration** > **Server Settings** (Figure 2-2).

Step 4 Under VSOM High Availability, click **Clear Split Brain Issues**.

Step 5 Click **OK** and verify the alert and issue are cleared.

Figure 2-2 VSOM High Availability



Time Settings (NTP Information)

The server time synchronizes server operations, defines recording timestamps and backup schedules. The network time protocol (NTP) server automatically sets the server time and date.

Table 2-3 NTP Configuration Options

Server Type	NTP Setting
Operations Manager Stand-alone servers	Use the Management Console or Operations Manager to change the NTP settings, if necessary.
Co-located server (Operations Manager and other services hosted on a single server)	Only the **User Configured** option is enabled. Enter NTP server hostname(s) or IP address(es), if necessary.
• Stand-alone Metadata server • Stand-alone Media Server • Co-located Media Server/Maps Server	Use the default (and recommended) **Automatic** mode to use the Operations Manager server as the NTP server. This ensures proper operation since all components will use the same time, date, and timezone.

Usage Notes

- Changes to the server time can affect video recording schedules and timestamps.
- A warning alert is generated if the time difference between the server and Operations Manager is more than 2 minutes.

- A warning message is also displayed to operators when logging in if the time difference between their workstation and the server is more than 2 minutes.
- Never modify the time and NTP settings using the Linux CLI. Settings made using the Linux CLI can result in inconsistent system performance and other issues.
- The server's NTP information (including the NTP server or time zone) is updated using the Management Console, the information is saved, but, a "config mismatch" is displayed in the Cisco VSM Operations Manager. To resolve this issue, you can either update the NTP information again using the Operations Manager or select **Device Settings** > **Replace Configurations** (in a device configuration page) to repair the config mismatch.

Table 2-4 NTP Server Settings

Mode	Settings
Automatic	Recommended for the servers containing stand-alone Metadata Servers or servers containing only Media Server and/or Maps Server. The Operations Manager server is used as the NTP server. The Operations Manager also defines the server timezone. This ensures proper operation since all components use the same time, date, and timezone. **Note** Automatic mode is disabled for co-located servers (Operations Manager and Media Server hosted on a single server). No other changes or settings are required when using Automatic mode.

Table 2-4 NTP Server Settings (continued)

Mode	Settings
User Configured	ws you to enter a custom NTP server and time zone for the current server. • Co-located servers—(Default and required) Enter the NTP server hostname(s) or IP address(es). Separate entries with a space or comma and select the Co-located server's time zone. • Stand-alone Metadata Servers or servers containing only Media Server and/or Maps Server—(Optional) This option may be necessary based on proximity of the server. For example: if your deployment spans numerous countries or timezones, the Media Servers may need to use local NTP servers. Enter one or more NTP server hostnames or IP addresses separated by a space or comma and select the Media Server time zone. **Note** If multiple NTP servers are used, a hierarchy of servers should ensure that the times on the various components are close. **Note** We recommend using the same network time protocol (NTP) server on all Media Servers to ensure the time settings are accurate and identical.

Set Date Time

Select **Advanced Settings** > **Set Date Time** to manually change the date and time on the server.

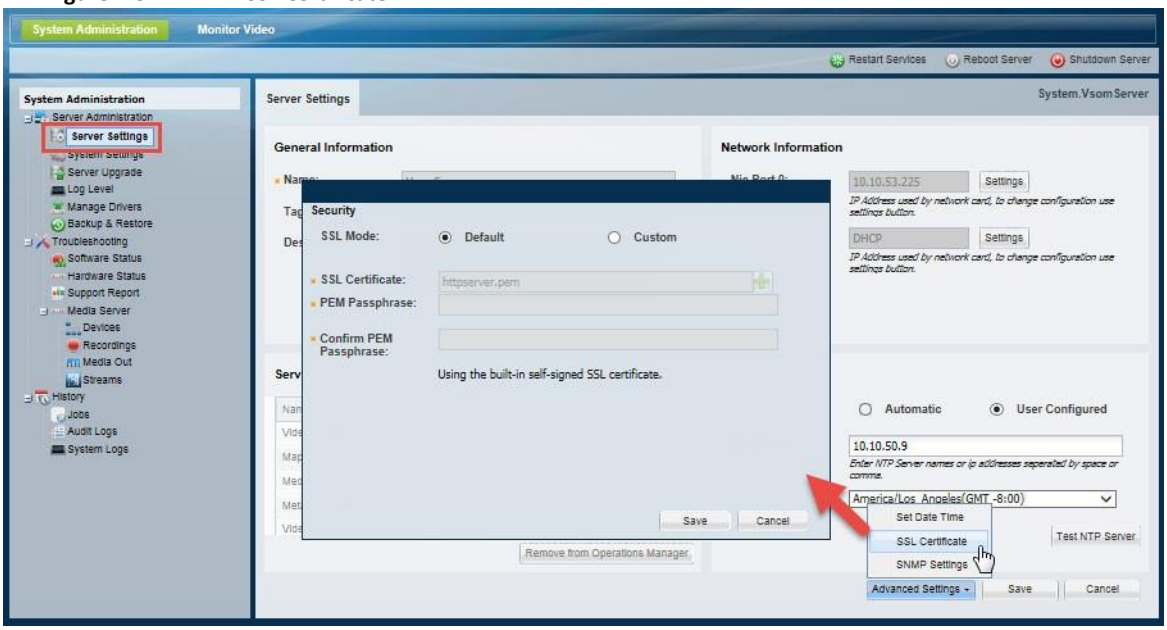
Caution Changing the system time requires a reboot and may affect video recording retention, recording schedules, and backup schedules. We highly recommend using the NTP server to define the server system date and time. See the "Time Settings (NTP Information)" section on page 2-7.

SSL Certificate

Network communication between the browser (client) and the Operations Manager or the Management Console is encrypted using SSL and HTTPS. The SSL certificate is also used for back-end communication between Cisco Video Surveillance components, such as between the Operations Manager, Media Server and/or Management Console.

By default, all Cisco Video Surveillance servers use a self-signed SSL certificate, and no additional action is necessary (Figure 2-3). To create and use a custom `.PEM` SSL certificate file issued by a Certificate Authority, see the "Using a SSL Certificate" section on page 2-9.

Figure 2-3 SSL Certificate



Using a SSL Certificate

Complete the following instructions to create and install the SSL certificate.

Usage Notes

- The digital certificate must be a Privacy Enhanced Mail (PEM) file with the `.PEM` extension.
- Upload a single certificate file that includes both a valid certificate and a valid private key.
- Web server certificates also require a pass phrase, which protects the certificate if stolen. Enter the pass phrase during conversion of the `.PFX` file to `.PEM` format, and when the `.PEM` certificate is uploaded to the server.
- If you upload a Web server certificate, you can click **Default** to revert to the self-signed certificate (Figure 2-3).
- The security certificate is included in Media Server backups (see the "Backup & Restore" section on page 2-24). If the database is restored, the backed up certificate is also restored. If the certificate changed since the last backup, you must reinstall the new certificate to replace the outdated version restored in the backup.

Using Web Server Certificates in an Operations Manager HA Configuration

An Operations Manager HA server configuration includes two servers: a Primary and a Peer. Each server is assigned an IP address and hostname. An additional virtual IP address and hostname is also added to the HA configuration, and is used by

operators to log in to the Operations Manager. The virtual address connects those operators to whichever server has the Primary role. See the Cisco Video Surveillance Operations Manager User Guide for more information.

By default, all Cisco VSM server include a self-signed certificate. Using the self-signed certificate on the Operations Manager server causes a security warning to appear when users log in the Operation Manager.

To avoid this, you can create and install a web server certificate for the Operations Manager servers. The certificate must point to the HA virtual IP address and be installed on both Operations Manager servers (Primary and Peer) used in the HA configuration.

For example, an HA configuration includes two servers: vsom-server1 and vsom-server2. A third virtual IP address and hostname vsom-server3 is used by operators to log in to the Operations Manager.

1. Obtain a signed certificate by a Certification Authority. This certificate should contain the host name mapped to the virtual IP. For example: vsom-server3.
2. Install the certificate on both the Primary and Peer servers using the Cisco Video Surveillance Management Console. For example, vsom-server1 and vsom-server2.
3. Wait for the services to be restarted.
4. Log in again to the Operation Manager using the virtual IP address. The certificate error should not appear.

Obtaining a Signed Certificate by a Certification Authority

Refer to the information from a Certification Authority to obtain a signed certificate. For example:

- Symantec
- Thawte

Creating a Self-Signed Certificate in .pem Format (Example)

Although each server includes a self-signed certificate, you can also create an alternative self-signed certificate using the following example.

Note There are multiple ways to create self-signed certificates. The following example describes one possible option.

Step 1 Generate server key which will expire after a year (without any encryption) and server certificate.

openssl req -nodes -days 365 -newkey rsa:1024 -keyout server.key -x509 -out server.crt

Step 2 Bundle the certificate and key together and generate a `.PEM` file:

a. Generate a `.PFX` file that includes the certification and key. For example: **openssl pkcs12 -in server.crt -inkey server.key -export -out vsmserver.pfx -passout pass:**MyPassword

b. Convert the `.PFX` file to `.PEM` format. For example: **openssl pkcs12 -in vsmserver.pfx -out vsmserver.pem -passin pass:**MyPassword **-passout pass:**MyPassword

Tip *`MyPassword`* is the password entered in Step 1. .

Step 3 Continue to "Installing a Security Certificate".

Installing a Security Certificate

After a self-signed or CA certificate is created, you must install it on the server.

- The SSL certificate "issued to", "subject name", and "subject alternate name" must contain a valid FQDN (Fully Qualified Domain Name).
- The certificate validity cannot be more than 3 years.

  Validity is the period from Start date to End date.

  - Certificates older than this will be rejected.
  - A warning message is displayed at the top of the Cisco VSM Management Console if the SSL certificate on the server is expired or will expire within 90 days.

Step 1 Select **Server Settings**.

Step 2 Click **Advanced Settings** > **SSL Certificate** (Figure 2-3).

Step 3 Select **Custom**.

Step 4 Click the + icon and select the `.PEM` SSL certificate file used for encrypted communication.

Step 5 Enter and re-enter the PEM Pass Phrase.

Step 6 Click **Save**.

Step 7 Click **Restart Services** to activate the changes and use the new certificate.

Note You must restart the services after any change to the certificate (uploading a custom certificate or reverting to the default self-signed certificate (click **Restart Services** and log back in to the Management Console). Restarting services can take up to 90 minutes or more depending on number of devices managed by the Operations Manager and Media Server. Installed products will be offline during this time.

Revert to the Self-Signed Certificate

Step 1 Select **Server Settings**.

Step 2 Click **Advanced Settings** > **SSL Certificate**

Step 3 Click **Default** to revert to the default certificate (Figure 2-3). You do not need to enter a pass phrase 'ifreverting' to the default certificate.

Step 4 Click **Save**.

Step 5 Click **Restart Services** to activate the changes and use the new certificate.

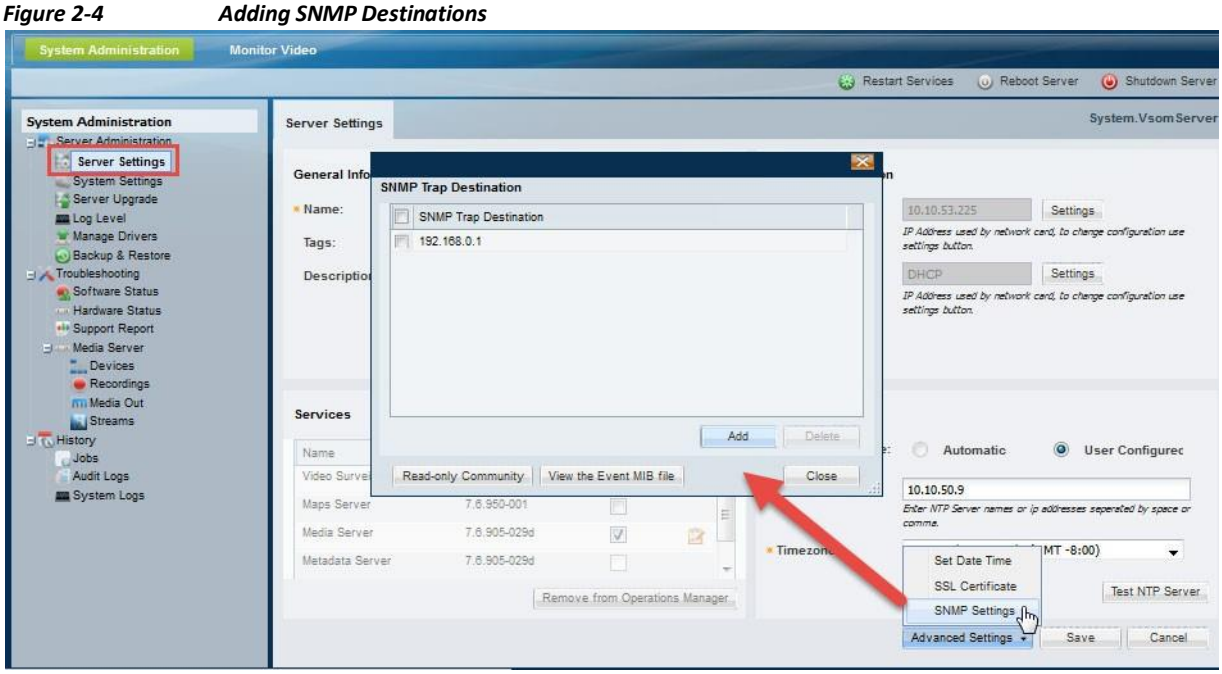
SNMP Settings

Click **Advanced Settings** > **SNMP Settings** to configure up to five SNMP trap destinations (Figure 2-4). All Cisco Video Surveillance server SNMP traps will be forwarded to these destination addresses.

SNMP Usage Notes

- To view the supported traps and descriptions, click the link "**View the Event MIB file**".
- Cisco Video Surveillance supports SNMP version 2 (Inform)
- Running a third-party trap receiver on a Cisco Video Surveillance host is not supported.
- To view or change the read-only community string, see (Optional) Change the SNMP Read Only Community String, page 2-13.

Figure 2-4 Adding SNMP Destinations



Adding SNMP Destinations

Step 1 Select **Server Settings**.

Step 2 Click **Advanced Settings** > **SNMP Settings**.

Step 3 Click **Add** to add a destination address. You can configure up to five SNMP trap destinations.

Tip To delete an entry, select the entry check box and click **Delete**.

Step 4 Enter the IP address or host name for the destination server.

- The entry must be a valid IP address or host name and cannot include `http://` or port numbers.
- Leading protocol strings (for example, http://) and port numbers (for example, 8080) are not allowed.

Step 5 Click **Close**.

Step 6 Repeat these steps for up to 5 destination addresses.

(Optional) Change the SNMP Read Only Community String

The read only community string is used to retrieve SNMP MIB OID values pertaining to system resources such as CPU, memory, and traffic usage on the server. For example, using SNMP GET, GETBULK operations.

The default string is a randomly generated value created during installation. You can change this string if necessary (Figure 2-5).

Step 1 Select **Server Settings**.

Step 2 Click **Advanced Settings** > **SNMP Settings**.

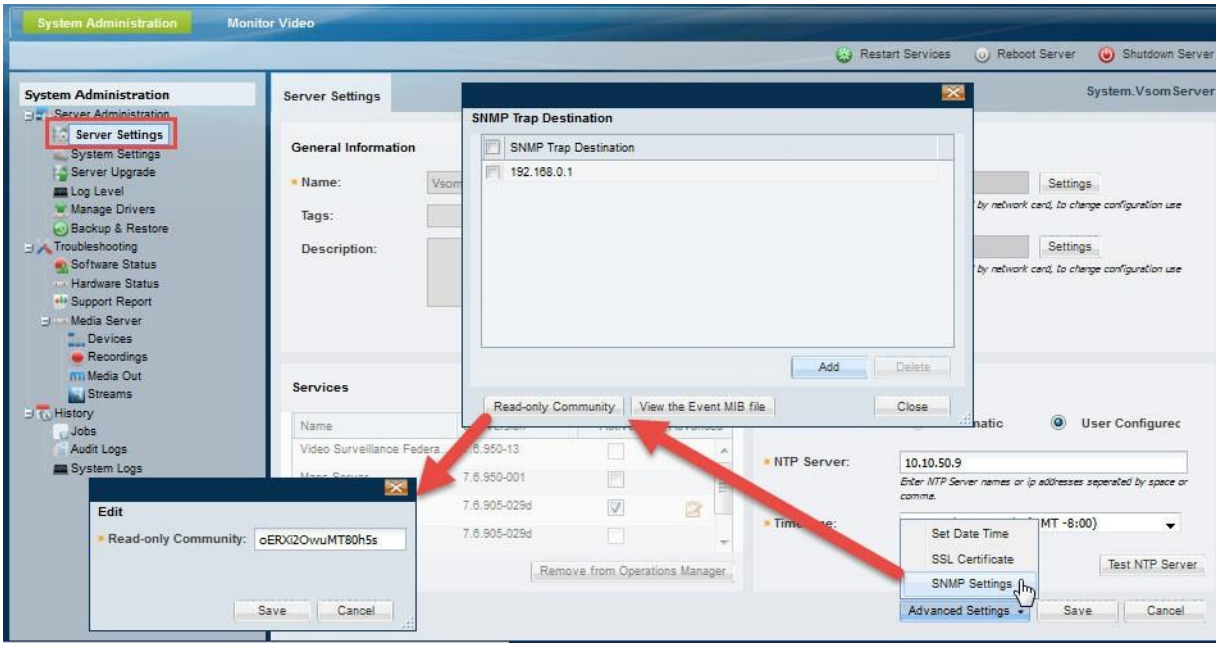
Step 3 Click Read-Only Community (Figure 2-5).

Step 4 Enter a new read-only community string.

Step 5 Click **Save**.

Step 6 Click **Close**.

Figure 2-5 Changing the SNMP Community String

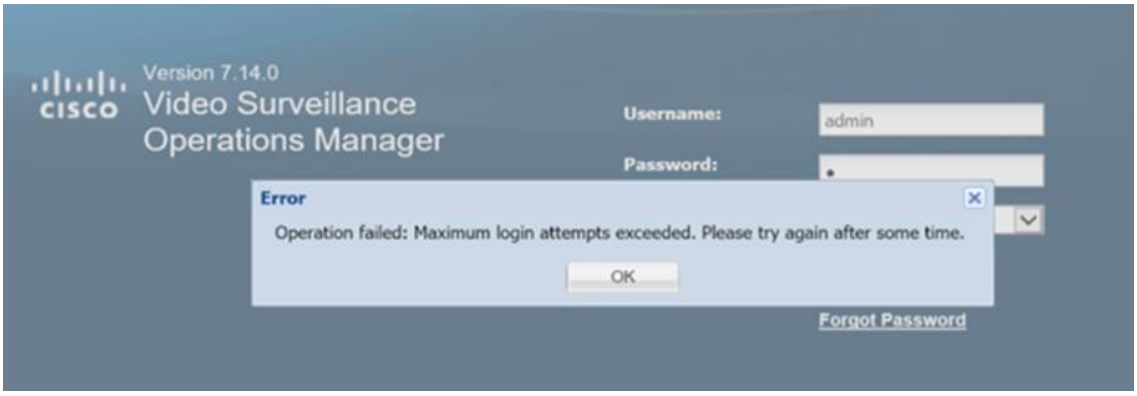


Clear Restrictions for Failed Login Attempts

If a user enters an incorrect login credentials too many times, their access can be blocked.

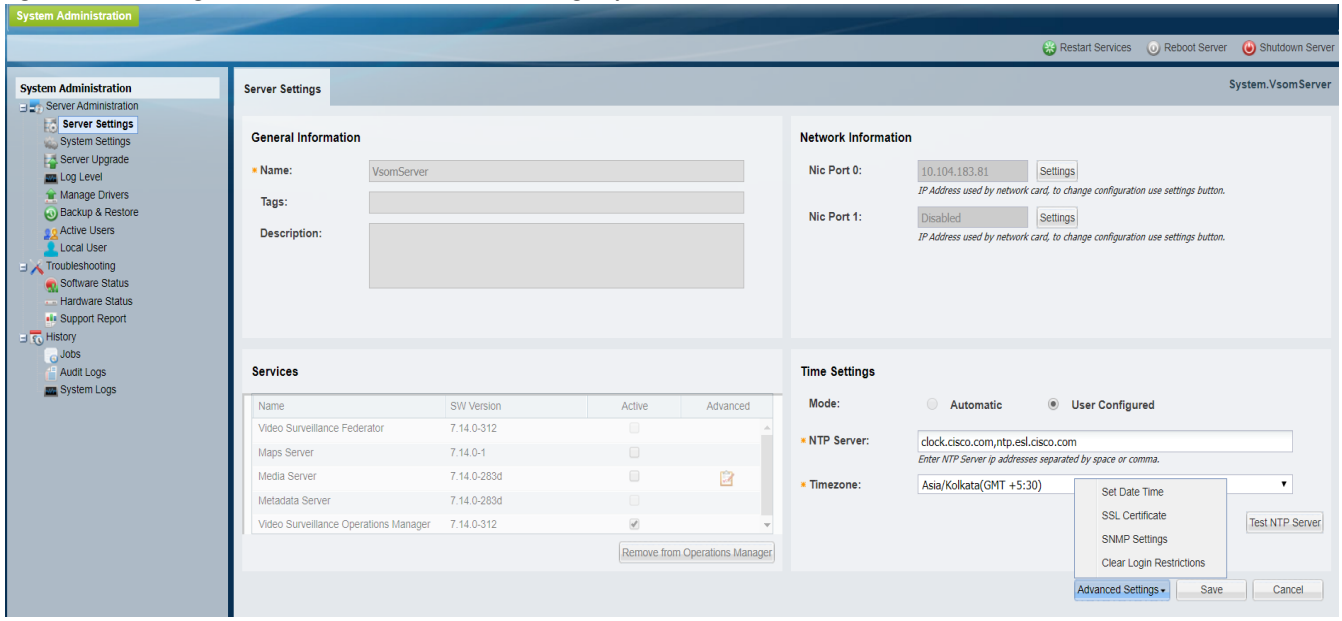
User will get a lock out error message in such a case as shown below:

Figure 2-6 Lockout Error Message



To override this block, and allow the user to attempt to login again, select **Server Settings > Advanced Settings > Clear Login Restrictions**.

Figure 2-7 Clear Login Restrictions as an Advanced Settings Option



System Settings

The system settings define basic properties that apply to the current server and its users.

Note The System Settings can also be defined using the Operations Manager (recommended).

Table 2-5 General Settings

Setting	Description
User Timeout	(Required) The number of minutes before a user is automatically logged out due to inactivity. After this period, users must re-enter their username and password to log back in. **Note** The maximum value is 10080 minutes (168 hours / 7 days). The default is 30 minutes.

Server Upgrade

Complete the following procedure for each server that hosts any Cisco VSM service.

Note Since all servers should run the same version of system software, we highly recommend using the Operations Manager to upgrade the servers in your deployment. See the Cisco Video Surveillance Operations Manager User Guide for more information.

The Cisco VSM server software upgrade file is a `.zip` file that includes all required software packages.

Server Upgrade Sequence

Cisco VSM servers should be upgraded in the following recommended order (depending on server type) to maximize access to video, minimize downtime, and ensure the integrity of video and configuration data.

1. Federator server
2. Operations Manager server
3. Map Server
4. Failover Media Servers
5. Primary Media Servers
   a. Servers acting as Dynamic Proxy servers
   b. Servers not acting as Dynamic Proxy servers
   c. Redundant Media Servers
6. Long-term Storage Media Servers
7. Metadata Server

Upgrading Language Packs

Use the Operations Manager to manage language packs (see the Cisco Video Surveillance Operations Manager User Guide).

Usage Notes

Use the following procedure to upgrade the server software for a single server.

- We recommend using the Operations Manager **Software Management** page to upgrade multiple servers. See the Cisco Video Surveillance Operations Manager User Guide for more information.

- Upgrading the server software may also require camera or encoder firmware upgrades. Failure to upgrade device firmware can cause camera failure after the server upgrade is complete.
  - See the Release Notes for Cisco Video Surveillance Manager for information on the supported firmware versions.
  - See the Cisco Video Surveillance Operations Manager User Guide instructions to upgrade Cisco device firmware on multiple servers.
- In rare scenarios, a PC workstation firewall can cause the upgrade process to fail. If this occurs, temporarily disable the workstation firewall software until the upgrade is complete.
- The server upgrade process automatically restarts server services.
- Installation is supported only if the RAID is in a non-bad, non-failed state.

Upgrading a Linux Red Hat Server From Release 7.0.0 to 7.0.1

If your Cisco VSM server is running the Linux Red Hat operating system, complete the following steps to update the date that the password was last set for the root user.

Tip Open the **Hardware Status** page to determine the server operating system.

Step 1 Use an SSH client to access the Cisco VSM server and log in as localadmin user.

Step 2 Enter the following command to update the date that the root user password was last set, where date is the current date in yyyy-mm-dd format:

[localaddmin@linux:~]# **sudo change -d** date **root**

For example: `[localadmin@linux:~ ]# sudo change -d 2013-03-06 root`

Upgrade Procedure for Server Software

Use the following procedure to upgrade the server software for a single server.

Tip We recommend using the Operations Manager **Software Management** page to upgrade multiple servers. See the Cisco Video Surveillance Operations Manager User Guide for more information.

Step 1 Determine the server that will be upgraded according to the "Server Upgrade Sequence" section on page 2-15

Step 2 Download the server software file.

- For example, navigate to the Video Surveillance Media Server Software section from the Cisco Video Surveillance Manager download page.
- See the Release Notes for Cisco Video Surveillance Manager, Release 7.14 for more information on downloading software and the packages included in a release.

Step 3 Complete the "Upgrading a Linux Red Hat Server From Release 7.0.0 to 7.0.1" section on page 2-16, if necessary.

Step 4 Upload the upgrade software image to the server:

a. Click **Add Software Pack** and choose **From Local** or **From Remote**.

b. If uploading from an FTP or SFTP server, enter the server details and click **List**. Select a valid `.zip` driver pack file and click **Add**.

c. If uploading from a PC, click + and select a valid `.zip` driver pack file from a local or network disk. For example: `Cisco_VSM-7.6.0-020d.zip`

Step 5 Wait for the software file to upload to the server.

Tip You can copy the software to the server without installing it. This allows you to stage the software on a server without performing the upgrade, if necessary.

Step 6 Click **Update Server** to install the system software package.

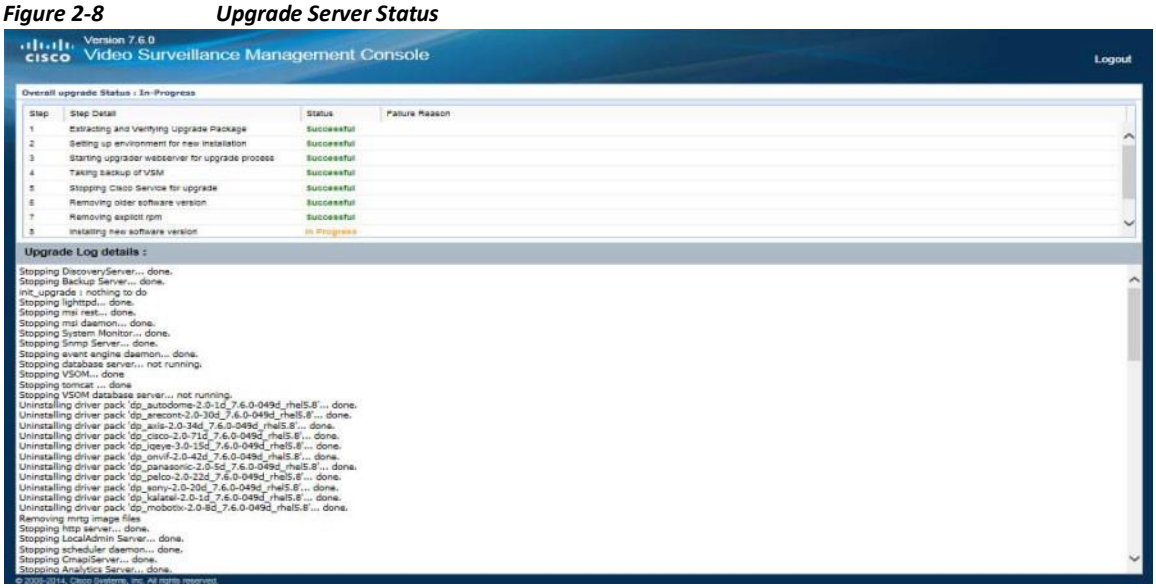
Step 7 To view the upgrade status screen:

a. Wait for the "upgrade status server" to be available. You will be asked to log in again.

b. Enter your password for the localadmin username when promoted.

c. The upgrade status screen is displayed until the upgrade is complete.

Figure 2-8 Upgrade Server Status



Step 8 Wait for up to 90 minutes for the operation to complete and the server to restart.

Note If the upgrade fails, see the "Recovering From a Failed Upgrade" section on page 2-18.

Step 9 Re-login to the server when the login screen appears.

Step 10 Repeat these steps for each server according to the "Server Upgrade Sequence" section on page 2-15 (log in to the Management Console for each server and upgrade the software to the same version).

Step 11 Upgrade the camera or encoder firmware, if required by the software release.

Recovering From a Failed Upgrade

If the upgrade fails or is interrupted, an error message ("work order file exists") may appear when you attempt to perform the upgrade again. This can be caused by a corrupted or incomplete upgrade file.

To address this issue, do the following:

Procedure

Step 1 Resolve the issue that caused the upgrade to fail. For example:

- Make sure the upgrade file is complete and not corrupted. Re-download the file again, if necessary.
- Make sure the upgrade can complete without interruption.

Step 2 Log in to the Cisco VSM server that was being updated and execute the server clean-up script.

Note This script cleans up the system so the upgrade can be attempted again. The script does not resolve the specific issue(s) that caused the upgrade failure. Resolve the cause of the upgrade failure first before attempting it again.

a. Log in using the localadmin username and password (the same credentials used to access the Cisco VSM Management Console).

b. Enter the following command to perform the server cleanup:

```
[localadmin@linux:~ ]# sudo /usr/BWhttpd/upgrade/server/bin/upgrade_cleanup.sh
```

Step 3 Repeat the "Upgrade Procedure for Server Software".

Log Level

Log Levels define the type of information that the system writes to the server log. Once set, the log contents can be viewed using the **History** > **System Logs** page (see System Logs, page 4-6).

You can define the log levels for the following processes:

- Setting the Process Log Levels, page 2-19—defines the Media Server processes (and modules under these processes) that generate log entries for more focused logging and debugging. The log levels can be set as a numerical value from 0 to 10. To set the Media Server log levels, you must have prior knowledge about different processes and modules running on the system. See the "Setting the Process Log Levels" section on page 2-19 for more information.
- Setting the Platform Service Log Levels, page 2-21—defines the log level for the server services on the server. For example: ERROR, WARN (Default), INFO, DEBUG, or TRACE.

Note Logs are typically used by Cisco technical support for debugging purposes. Wait approximately 1 minute for changes to the log levels to take effect.

Setting the Process Log Levels

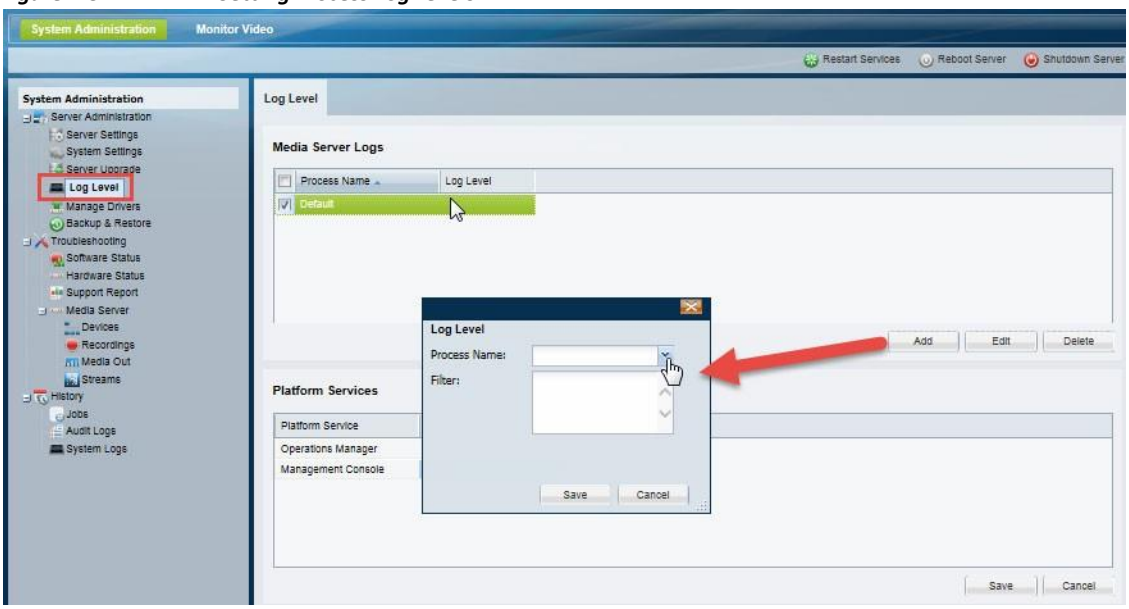
To set the Process log levels, create a new entry for the process name, and define the log level .

Usage Notes

- You must have prior knowledge about different processes and modules running on the system.

- The Platform Service log levels are always present, even if the Media Server service is not enabled.

Figure 2-9 Setting Process Log Levels



Procedure

Step 1 Click **Add** to create a new log level entry.

Step 2 Select a Process Name or enter a value.

Step 3 Enter the filter text string, in the format "name=value".

For example, to set the log level for all processes named proxy, enter **proxy** in the Process Name field and **PROXY=10** in the filter field.

To set the default log level to 1 for all Media Server processes, leave the Process Name field blank and enter **DEFAULT=1** in the filter field.

The log levels are:

- 0 = no logging
- 1 = (default) error logging only
- 2 - 9 = various levels of debug logging
- 10 = trace logging

Step 4 Click **Save**.

Step 5 Wait approximately one minute for the changes to take effect.

Step 6 Click **History** > **System Logs** to view the log information. See System Logs, page 4-6.

Tip To delete an entry, select the entry check box and click **Delete**.

Setting the Platform Service Log Levels

To define the log level for the server services on the server (ERROR, WARN (Default), INFO, DEBUG, or TRACE), do the following. The following options are available:

- Operation Manager— select ERROR, WARN (Default), INFO, DEBUG, or TRACE.
- Management Console—select ERROR, WARN (Default), INFO, DEBUG, or TRACE.
- GeoServer—select ERROR, WARN (Default), INFO, DEBUG, or TRACE.
- VSF—select ERROR, WARN, INFO, DEBUG (Default), or TRACE.

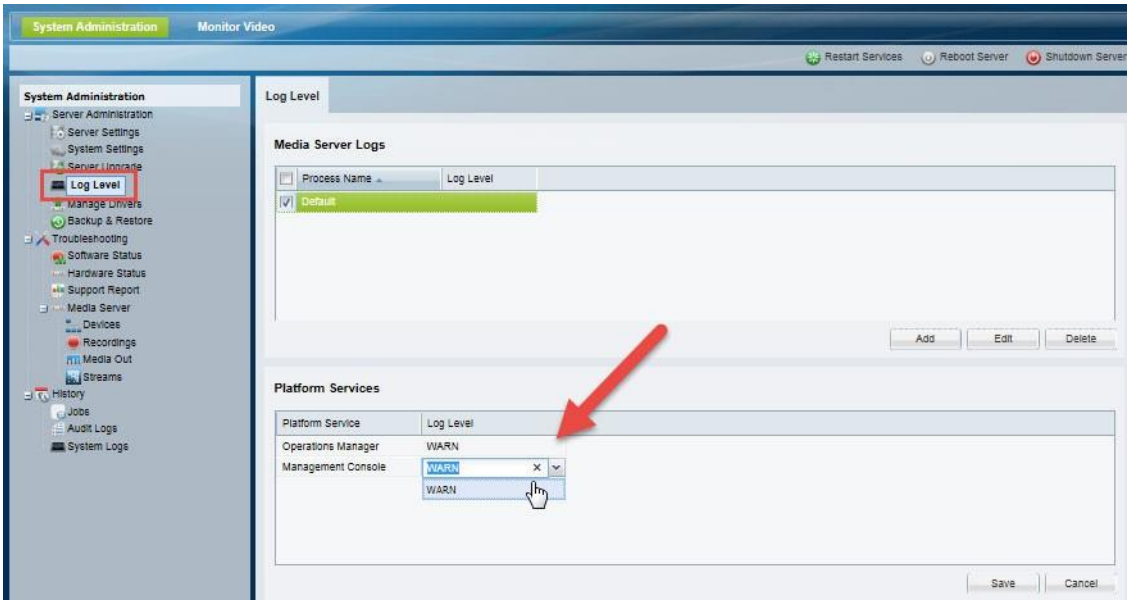
Procedure

Step 1 Choose of the following log levels from the drop-down menu to enable logging of Operations Manager and Management Console processes .

- ERROR—error events that might still allow the service to continue running.
- WARN—(default) potentially harmful situations.
- INFO—informational messages that highlight the progress of the service at coarse-grained level.
- DEBUG—fine-grained informational events that are most useful to debug a service. Also includes messages from all other log levels. The Debug log level captures the most data but may cause the system to run slower.
- TRACE—finer-grained informational events than DEBUG

Step 2 Click **Save**.

Figure 2-10 Setting Platform Service Log Levels



Manage Drivers

Device driver packs are the software packages used by Media Server and Operations Manager to inter-operate with video devices. Driver packs are included with the Cisco VSM software, or may be added to a server at a later time to add support for new devices or features.

- Install new driver packs to add support for additional devices.
- Upgrade existing driver packs to enable support for new features.

Driver Pack Versions and Mismatch

You can install the new version on all Media Servers, or only the Media Server(s) that support the affected devices. If the driver pack version is different on the Media Servers in your deployment, a driver pack mismatch error can occur:

- A warning message appears if the driver pack is different on the Media Servers, but the functionality or compatibility of the system is not impacted. Cameras and encoders can be configured and operate normally.
- A critical message appears if the driver pack mismatch will impact the functionality or compatibility between the Operations Manager, Media Servers, and the video device. The upgrade is not allowed. Camera and encoder templates cannot be revised until the same driver pack version is installed on all Media Servers.

Note We strongly recommend upgrading driver packs using the Operations Manager interface. This allows you to upgrade multiple servers at once. The Management Console interface described in this section allows you to upgrade the driver packs for the current server only. Using the Management Console, you must log in to each server to upgrade the drivers.

Usage Notes

- Driver packs can be upgraded but not downgraded.
- The driver pack file format is `.zip`. For example:
  `dp_cisco-2.0-59d_7.6.905-029d_sles10-sp1-i686.zip`
- See the Release Notes for Cisco Video Surveillance Manager, Release 7.14 for more information on the supported driver packs.

Device Upgrade Procedure

Step 1 Obtain the new driver pack from the Cisco website.

- For example, navigate to the Video Surveillance Device Driver Software from the Cisco Video Surveillance Manager download page.
- See the Release Notes for Cisco Video Surveillance Manager, Release 7.14 for more information.
- Be sure to use the correct drivers for the server operating system. To determine the server OS, go to **Monitor** > **System Summary** > **OS Type**. For example, the SUSE Linux Enterprise Server (SLES).

Step 2 Select **Manage Drivers.**

Step 3 Upload the new driver pack software file to the server.

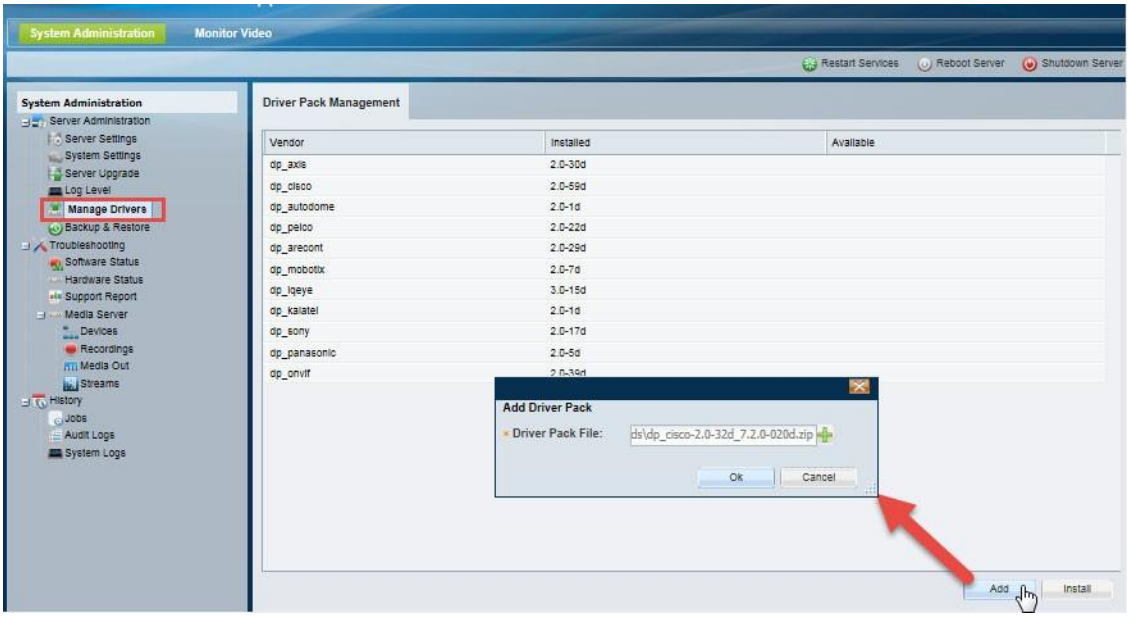
a. Click **Add**.

b. In the pop-up window, click icon and select a valid `.zip` driver pack file from a local or network disk. For example: `dp_cisco-2.0-59d_7.6.905-029d_sles10-sp1-i686.zip`

Manage Drivers

c. Click **OK** and wait for the upload to complete.

Figure 2-11 Manage Drivers



Step 4 The Available column shows the uploaded version that is available for the upgrade.

Step 5 Click **Install** to install all available driver pack file on the current server.

Caution Do not refresh the browser while the driver installation is in progress.

Step 6 Complete these steps for each server that hosts a Media Server or Operations Manager.

- (Recommended) Use the Operations Manager interface to upgrade multiple servers at once. See Driver Pack Versions and Mismatch, page 2-22.
- (Alternative) Log in to the Management Console for each server and upgrade the driver pack software.

Backup & Restore

Use the Management Console to perform a one-time manual backup of the configuration and historical data for the services running on the server. Each backup creates:

- A separate backup file for each server service running on that server (such as the Media Server and Operations Manager).
- A backup file for the CDAF (Management Console) service.

To restore a backup, you must restore the files for each server service, and restore the CDAF backup file. We highly recommend the following:

- Back up all servers on a regular basis to ensure configuration and event data is not lost if a hardware failure occurs. Backups are also used to restore configurations and historical data when upgrading or moving to a new system. Backup files can be saved to the server ("local") or to a valid FTP/SFTP server.
- Use the Operations Manager to schedule automatic backups and perform other backup maintenance tasks. The Operations Manager is used to manage multiple server backups.

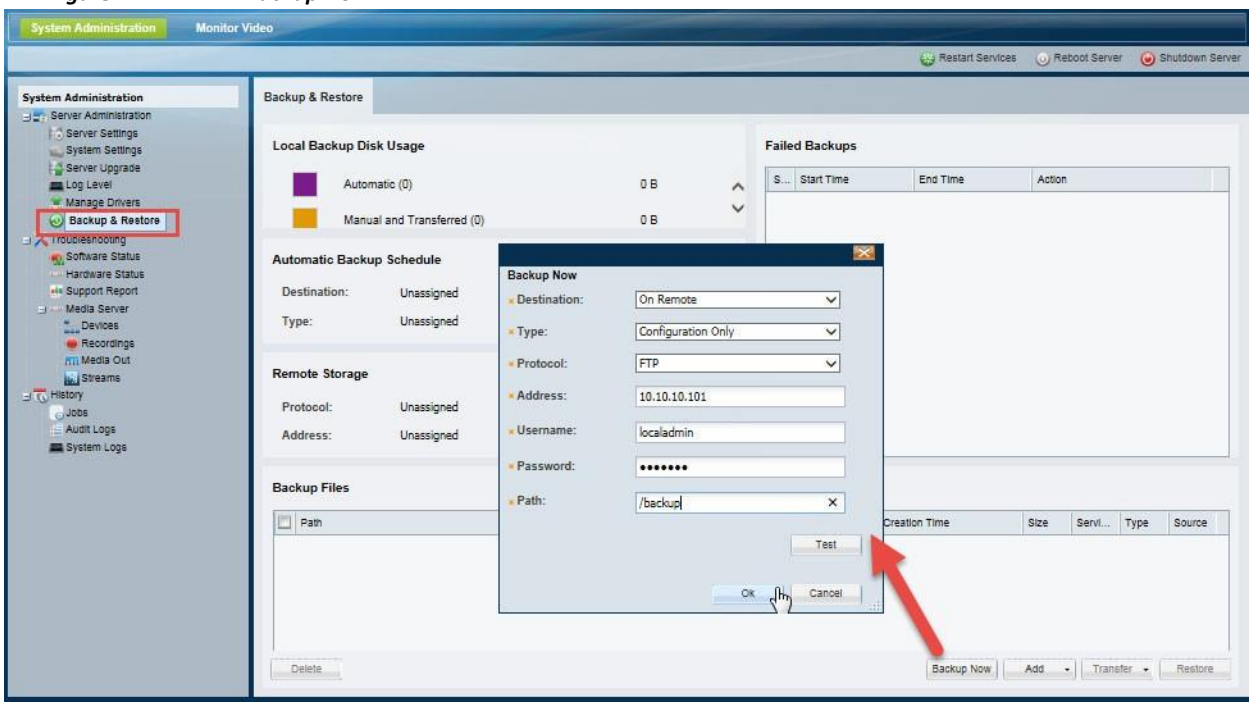
Backup Usage Notes

- Backups include services on the current server only, and do not include data from other servers. Use the Operations Manager to backup multiple servers. See the Cisco Video Surveillance Operations Manager User Guide for more information.
- Use the Operations Manager interface to schedule recurring backups. Automatic backup schedule details and Remote storage details are read-only field in the Management Console. See the Cisco Video Surveillance Operations Manager User Guide for more information.
- Each backup includes a separate backup file for each active service on the server, plus a file for the CDAF service.
- CDAF runs on all servers and provides the Cisco VSM Management Console user interface and features. CDAF backups include the server database, system information, console jobs and other data. The CDAF service must be restored along with the other server services or information may be missing and system errors can occur.
- Backups do not include video files. Use the high-availability feature to back up video files, as described in the Cisco Video Surveillance Operations Manager User Guide.
- Configuration data includes user-configured settings, such as camera configurations. Historical data includes all user entered data plus logs and events.
- The Media Server configuration data is backed up automatically to the local server every day by default (and cannot be disabled).
- The security certificate is included in Media Server backups. If the database is restored, the certificate included in that backup is also restored. If the certificate has changed since the backup was created, the old certificate is also restored and you must reinstall the new security certificate.

Backup Procedure

Note We highly recommend backing up all services when any major configuration changes are made. Backups ensure the system data can be restored to the present state, if necessary. The Media Server configuration data is backed up automatically to the local server every day by default (and cannot be disabled). Automatic backups are not supported for other services using the Management Console.

Figure 2-12 Backup Now



Procedure

Step 1 Select **Backup & Restore.** .

Note When the maximum number of backups is reached, an existing backup file must be deleted to make room for the new backup file.

Step 2 Click **Backup Now**.

Step 3 From the pop-up, select or enter the backup settings, as described in Table 2-6 on page 2-26.

Step 4 Click **OK**.

Step 5 Backup files are saved to the selected destination.

- See the "Backup File Format" section on page 2-28 for a description of the file name
- If saved locally, the backup files are saved to the Backup File list. See the "Backup File Information" section on page 2-29.
- Failed backups are displayed in the Failed Manual Backups field. See the "Failed Backups" section on page 2-29.

Backup Settings

The Table below describes the server backup and restore settings.

Table 2-6 Server Backup Settings

Field	Description
Destination	Select where the backup file will be stored: • **On Local**—(Default) Saves the backup file to the server hard drive. • **On Remote**—Saves the backup file to a remote storage network server.
Type	Select the type of data to back up: • **Configuration Only**—Backs up the user-defined configuration, including device settings (for cameras, encoders, and Media Servers), user accounts, and other attributes. • **Configuration Plus Historical Data**—(Default) Backs up the configuration plus events, health notifications, logs, and other data containing information regarding the status, use and health of the system.
Remote Storage	
Note These settings define the remote server used to store backup files if the **On Remote** option is selected.	
Tip Click **Test** to verify the settings are correct and the remote server can be accessed.	
Protocol	Select the type of remote server: **FTP** or **SFTP**.
Address	Enter the server network address.
Username	Enter the username used to access the server.
Password	Enter the server password.
Path	Enter the directory path where the backup file will be stored

Automatic Backups (Single Server)

Use the Operations Manager to schedule recurring backups.

Restoring a Backup

Restoring a server backup requires that you restore the backup file for each service running on that server, and the CDAF service.

Note The CDAF service provides the server's Management Console functionality, including the server database, system information, console jobs and other data. If the CDAF service is not restored at the same time as the other services, information may be missing and system errors can occur.

For example, if the server is running Operations Manager (VSOM) and Media Server (VSMS) services, a separate backup file is created for each service plus the CDAF (Console) service. You must restore each service backup file, one service at a time.

Caution Restoring a backup deletes any existing configurations, settings and historical data.

Note Failed backups are displayed in the Failed Backup field. Double-click an entry to display details.

Procedure

To restore the server configuration from a backup file, do the following.

Step 1 Select **Backup & Restore**.

Step 2 (Optional) Select **Restore System Config** to exclude the server configuration from the restore operation.

Step 3 The server configuration is the non-Cisco VSM portion of the backup data that includes OS-related settings, such as the server network configuration. Excluding the system configuration can be used to replicate a server configuration on additional servers: create a backup from the original server and restore it to a new server while selecting the **Restore System Config** option.

Step 4 (Optional) If the backup file does not appear in the list, select **Add** > **From Remote** or **From PC** to copy a backup files stored on a PC or remote server.

From PC

- Select a backup file stored on a PC or remote server.

From Remote

- Enter the remote server settings in the pop-up window. See the "Backup Settings" section on page 2-26 for more information.
- Click List to view the backup files available at the remote location.
- Select one or more backup files.
- Click **Add**.

Step 5 Select the backup file for the service you want to restore.

- The Service Type displays the server service: For example: VSOM (Operations Manager), VSMS (Media Server), CDAF (Console), Geoserver, or Metadata.

Step 6 Click **Restore**.

Step 7 Click **Yes** to confirm the backup and server restart.

Note The system configuration is included by default, which restores system configurations such NTP and network configurations. Deselect this option if necessary.

Step 8 Click **OK** when the restore process is complete.

Step 9 Re-login to the server.

Step 10 Repeat these steps to restore the configurations and data for additional service on the server.

Step 11 Repeat these steps to restore the backup for the CDAF (Console) service.

Backup File Format

Backup files are saved to a `.tar.gz` file in the following formats:

Table 2-7 Backup File Formats

Backup Data	Format
Config and Historical	**VSMS_**HostName_yyyyMMdd_HHmmss**.DbBackup.tar.gz** **Example:** `VSMS_vsm-server_20121126_105943_1.0.62.DbBackup.tar.gz`
Config Only	**VSMS_**HostName_yyyyMMdd_HHmmss.**configOnlyDbBackup.tar.gz** **Example:** `VSMS_vsm-server_20121126_103509_1.0.62.configOnlyDbBackup.tar.gz`

- HostName—the host name of the server running the service.
- yyyyMMdd_HHmmss—the date and time when the backup file was created.

For example, if the vsm-bldg14 server configuration and historical data was backed up on August 17, the resulting filename would be: `VSMS_vsm-bldg14_backup_20120817_174250.tar.gz`

- VSOM=Operations Manager service
- VSMS=Media Server service

Backup File Information

Each backup file saved on the server displays the following summary information:

Step 1 Select Backup & Restore.

Step 2 (Optional) To first save the file to a PC disk or remote server, click **Transfer** and then **To Remote** or **To PC**.

- **To PC**—select the location for the backup file

Table 2-8 Backup Files

Column	Description
Path	The server directory path where the backup files are stored.
File Name	The file name. See Backup File Format, page 2-28.
Creation Time	The date and time when the backup file was created.
Size	The size of the backup file.
Service Type	The server service types included in the backup. For example: • VSOM (Operations Manager) • VSMS (Media Server) • CDAF (Console) • Geoserver • Metadata
Type	Configuration or configuration plus historical data. See Backup Settings, page 2-26.
Source	Automatic or manually triggered backup.

Failed Backups

The failed backup field displays the following information:

- Failed manual backups—failed manually executed backups. No additional information is available.
- Failed scheduled backup — failed automatic backups. Double click an entry to open a window that lists all failed scheduled backups.

Deleting a Backup File

Deleting a backup file permanently removes the file from the system. The file cannot be used to restore the database.

Tip To archive the backup for later use, save the backup file to your PC or a remote server before deleting it.

Procedure

Step 1 Select **Backup & Restore**.

Step 2 (Optional) To first save the file to a PC disk or remote server, click **Transfer** and then **To Remote** or To PC.

To PC—select the location for the backup file**.**

To Remote—the file will be transferred to the location specified in the Remote Storage section of the Configure tab. See the "Backup Settings" section on page 2-26 for more information.

Step 3 Select the backup file from the list.

Step 4 Click **Delete** (bottom left).

Step 5 Confirm the operation, when prompted.

Active Users

The Active Users page displays information about the user accounts that are currently logged in to the Cisco Video Surveillance system.

To discontinue an active user session, select an entry and click **Logout Session**. Users that are logged out in this method can continue watching the video they are currently viewing. But they will be automatically logged out if they attempt to access new video streams or open or a new video pane.

Table 2-9 Active User Fields

Setting	Description
Username	The username of the account used to access the system.
First Name	The first name in the user account
Last Name	The last name in the user account
User Group(s)	The user groups the user is assigned to. User groups define the user role and location for member users, which defines the cameras and resources they can access.
Super-admin	Indicates if the user account is assigned the super-admin role.
Logged-In Time	The date and time when the user logged in.
Last Access Time	The date and time the user last performed any action on the system.
From IP	The IP address of the device or computer used to access the system.

Tip To view a history of user activity, go to **History** > **Audit Logs** (see Audit Logs, page 4-5).

Local User

The localuser account can be enabled on a Cisco Media Server to allow operators to log in to that server and monitor video. This can be used to give users access to local video only, even if the Cisco VSM Operations Manager is unavailable.

The localuser can do the following:

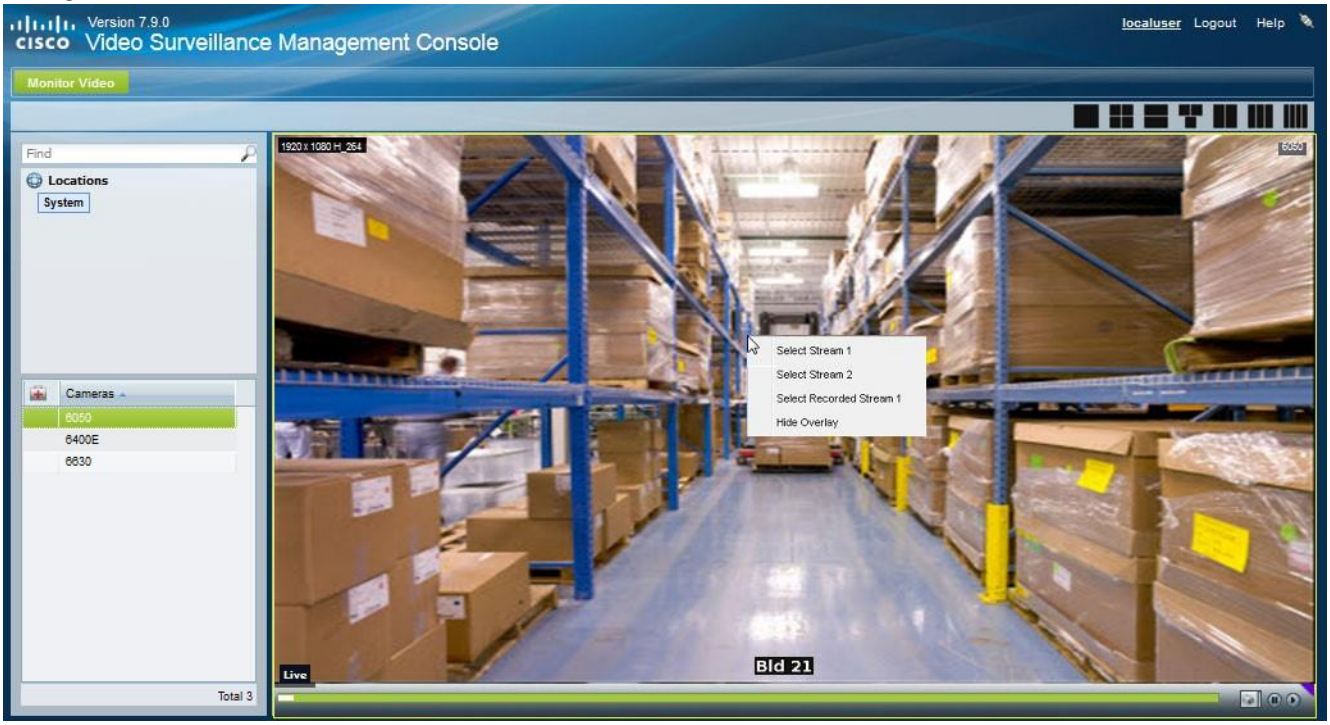
- Monitor video from the cameras supported by the Media Server
- Create cva clips

The localuser cannot:

- Access any administrative functions or settings
- Create MP4 or virtual clips

For example, in the below Figure the localuser can only access the Monitor Video tab, allowing them to view video from the cameras supported by the Cisco Media Server and create cva clips.

Figure 2-13 Local User Access to Monitor Video



Procedure to Enable the Local User

The localuser account is disabled by default.

To enable the localuser, enter a password and save the changes.

Step 1 Log in to the Cisco VSM Management Console for the Cisco Media Server (see Logging In for more information).

Step 2 Select **Server Administration > Local User.**

Step 3 Enter and re-enter a password.

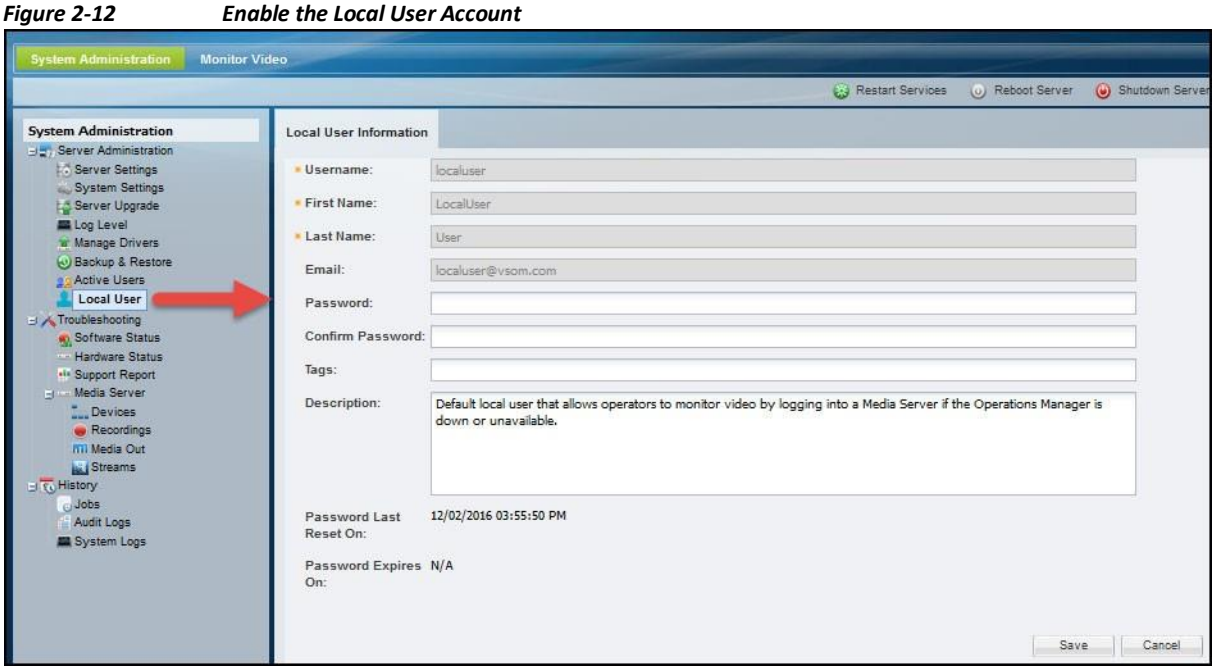
- The password does not expire.
- The localuser cannot change the password (only the localadmin can).

Step 4 (Optional) Enter a tag and description.

Note The other fields are read-only and cannot be changed.

Step 5 Click **Save**.

Figure 2-12 Enable the Local User Account



Step 6 Log out and log back in using the localuser credentials you just created.

Step 7 Verify that only the Monitor Video tab appears.

Limitations

- The localuser is not notified if a camera is in covert mode.
- If a camera is in covert mode for the live stream in the Operations Manager, the localuser will not be able to view the live or recording stream in the Management Console.
- If a camera is in covert mode for the recorded stream in the Operations Manager, none of the camera recordings will be available to the localuser in the Management Console.

Troubleshooting

The Troubleshooting pages allow you to gather information about the state of the server, hardware and software components, RAID drives, and video that is recorded or streamed on the Media Server. You can also use the Support Report to generate detailed information for analysis by your Cisco support representative.

Refer to the following topics for more information:

- Software Status, page 3-2
- Hardware Status, page 3-3
  - Hardware Information, page 3-3
  - System Resources, page 3-4
  - Hardware Alerts, page 3-5
  - RAID Status, page 3-6
- Support Report, page 3-9
- Media Server, page 3-10
  - Devices, page 3-10
  - Recordings, page 3-12
  - Media Out, page 3-14
  - Streams, page 3-15

Software Status

The Software Status page displays a summary of the Cisco VSM services (and related components), installed software, and device driver packs (Figure 3-1).

Figure 3-1 Software Status

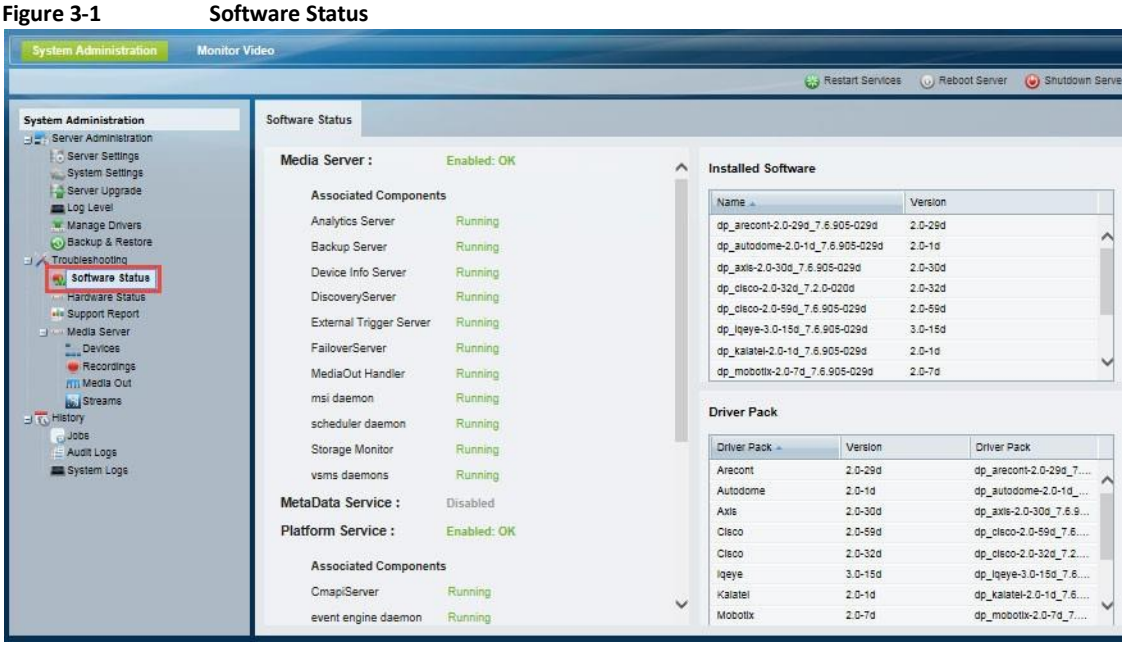


Table 3-1 Software Status

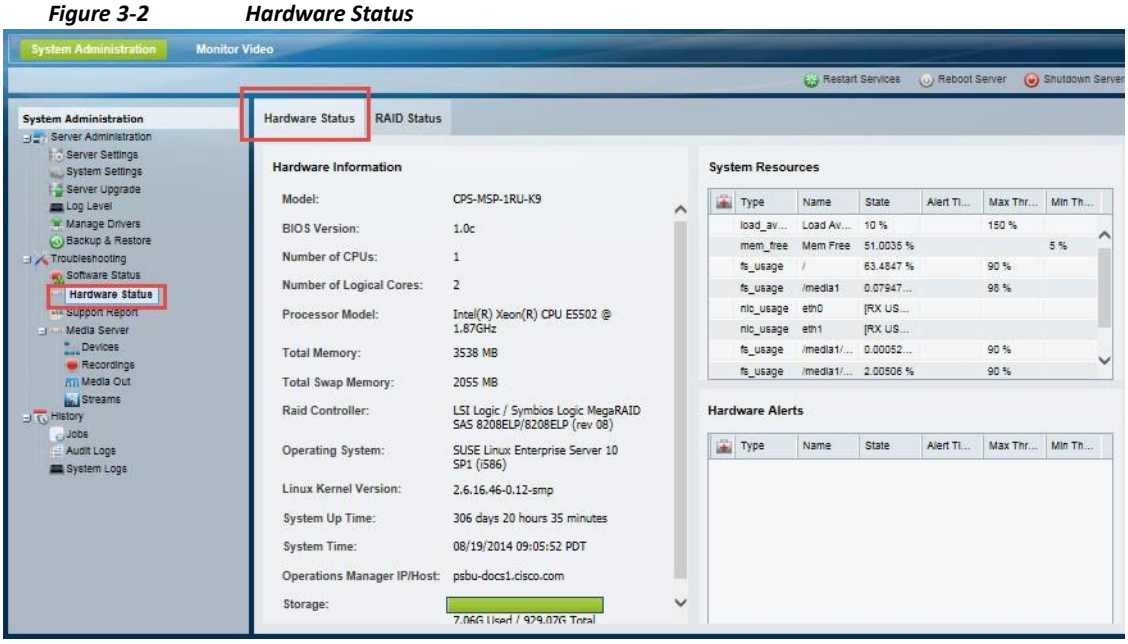
Field	Description
Server services	Specifies if the server service is running or disabled on the server.
Installed software	Additional software (such as driver packs) that are installed on the server. See Manage Drivers, page 2-22 for more information.
Driver Pack	The name, version and file name of the installed driver packs. See Manage Drivers, page 2-22 for more information.

Hardware Status

Hardware Status (Figure 3-2) displays information about system resources, hardware, or RAID disks, including alarms that are created if a hardware component exceeds a minimum or maximum threshold. For example, if the server is not responding properly, use Hardware Status to determine if the available memory is low, the system load is high, or the disk space is full.

Alarms are created if either the minimum or maximum threshold for the component is crossed.

Figure 3-2 Hardware Status



Hardware Information

The System Summary window displays server hardware details, uptime, system time, and other details. Below Table describes the information displayed in each field. The information on this page refreshes every one (1) minute.

Table 3-2 Hardware Information

Platform Origin Version	(VM installations only)
Model	The server model. For example, CIVS-MSP-1RU is a Cisco Multiservices Platform server that requires 1 rack unit.
BIOS Version	The system BIOS version number.
Number Of CPU	The number of CPUs in the Linux system.
Number of Logical Cores	The number of processing cores in the system.
Processor Model	The processor model. For example: `Intel(R) Core(TM)2 Duo CPU E4300 @ 1.80GHz`
Total Memory	The total amount of physical memory.
Total Swap Memory	The total amount of memory available for paging.
RAID Controller	The type of RAID controller on the server.
Operating System	The Linux operating system and version number used to boot and operate the server. For example, SUSE or RHEL.
Linux Kernel Version	The version number of the Linux kernel.
Fiber Channel Port Name	

Fiber Channel Port ID	Servers with FC card only. **Note** The Cisco Connected Safety and Security UCS series servers do not display the status of FC port-0. **Note** The Cisco Connected Safety and Security UCS series servers require a service restart to see updated FC link status.
Fiber Channel Port Link State	
Fiber Channel Port Type	
System Up Time	The number of days and hours the server has been running without a reboot.
System Time	The time configured on the server. The time can be entered manually or set automatically using a network time protocol (NTP) server. The time is used to timestamp video and synchronize system operations with other servers and components in the deployment.
Operations Manager IP/Host Name	The IP address or host name of the Cisco VSM Operations Manager used to configure and monitor the Cisco Video Surveillance deployment.
Storage	The total available storage on the server, and the amount of storage used.

System Resources

Table 3-3 describes the information included in the System Resources table.

Table 3-3 System Resource Status

Field	Description
Type	The system resource type.
Name	The descriptive name of the system resource.
State	The current overall status of the item. For example, the percentage of free system memory.
Alarm Time Stamp	The day and time the alarm occurred. If any of the resource types, such as mem_free (free memory) has crossed a threshold, then an alarm is generated and an Alarm Timestamp is displayed.

Table 3-3 System Resource Status (continued)

Max Threshold	The maximum alarm value. If the component exceeds this value, an alarm condition is created and an Alarm Timestamp is displayed.
Min Threshold	The minimum alarm value. If the component is lower than this value, an alarm condition is created and an Alarm Timestamp is displayed.

Note For “nic_usage", bare metal servers display the correct network bandwidth usage, but data for virtual machines (VMs) is not supported.

Hardware Alerts

Table 3-4 describes the information included in the Hardware Status table.

Table 3-4 Hardware Status

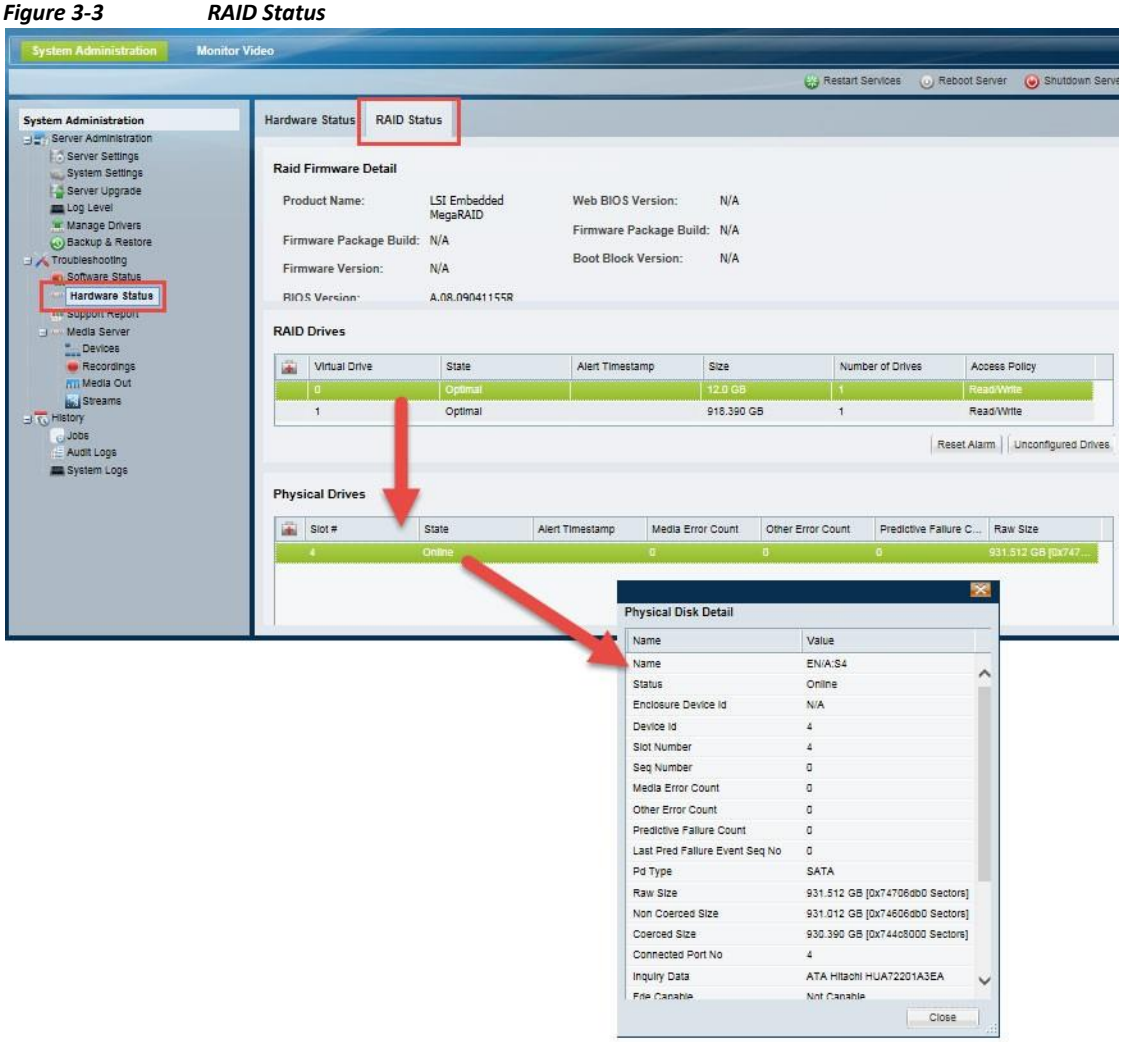
Field	Description
Type	The hardware type or device.
Name	The descriptive name of the hardware or the type of status shown.
State	The current overall status of the hardware item.
Alert Timestamp	The day and time the alarm occurred. If any of the resource types, such as mem_free (free memory) has crossed a threshold, then an alarm is generated and an Alarm Timestamp is displayed.
Max Threshold	The maximum alarm value. If the component exceeds this value, an alarm condition is created and an Alarm Timestamp is displayed.
Min Threshold	The minimum alarm value. If the component is lower than this value, an alarm condition is created and an Alarm Timestamp is displayed.

RAID Status

Click the **RAID Status** tab (Figure 3-3) displays information if a RAID is installed on a Cisco server that includes a compliant RAID controller. This page also lets you silence alarms that occur when a RAID failure occurs or when the RAID array is rebuilding, and generate a debug package.

Figure 3-3 shows a sample RAID Status page. A Virtual Drive is selected to show the physical drives.

Figure 3-3 RAID Status



RAID information is provided only for Cisco VSM servers that support RAID.

Procedure

To view details about the virtual and physical drives in a RAID configuration, do the following:

Step 1 Select **Hardware Status**.

Step 2 Select the **RAID Status** tab.

Step 3 Select a Virtual drive to display information about the associated physical drives (Figure 3-3).

Step 4 Click a virtual or physical drive number to display additional drive details in a pop-up window (Figure 3-3).

Virtual Drive Information

Table 3-5 describes the information displayed for each virtual RAID drive.

- Select a virtual drive to display the physical drives.
- Click **Reset Alarm** to refresh the alarm status.
- Click **Unconfigured Drives** to display the additional drives not configured for RAID.

Table 3-5 RAID Drive Status

Field	Description
Alarm	The alarm icon is displayed if an alarm occurs for one or more physical drives. • View the physical drive(s) that caused the alarm. • Click **Silence Alarm** to silence the RAID controller alarm. The timestamp is updated for virtual drives only.
Virtual Drives	The RAID drives configured on the server. The possible states are: • Optimal—the RAID is working normally • Degraded—one or more RAID drives are missing or not operational but is still operating with reduced performance • Offline—two or more RAID drives are missing or not operational, making the RAID inoperable.
State	The current drive status. • Missing—Provides information when a hard drive is not detected. • Rebuild—Provides information when hard drive is rebuilding. • Optimal—Provides information when a hard drive is rebuilt and operating.
Alarm Timestamp	The time when a non-optimal condition was recognized. A timestamp is displayed only if the drive is in an alarm state and has not rebuilt successfully or been replaced. The timestamp is updated for virtual drives only.
Size	The amount of storage available on the drives.
Number of Drives	The number of physical drives.
Access Policy	Read/Write access to the drive.

Physical Drive Information

Double-click on a physical drive entry to view additional information about the physical drive (Figure 3-3).

Table 3-6 Physical Drive Status

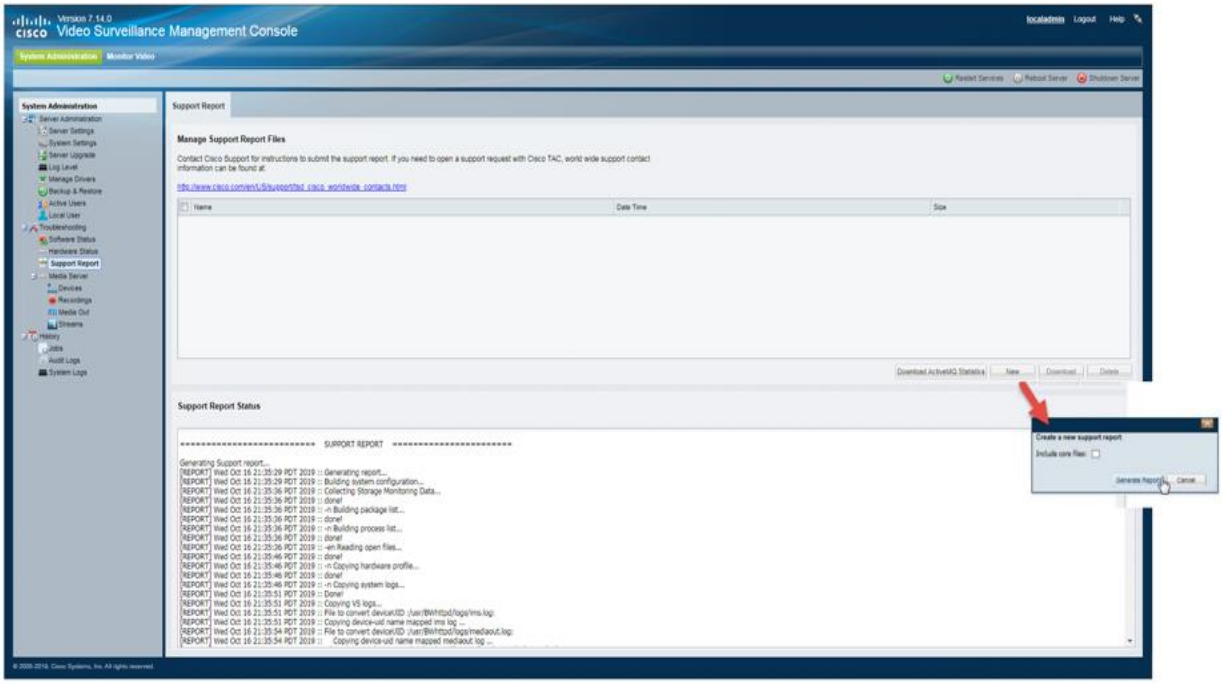
Field	Description
Slot Number	The physical slot location in the server.
State	The current drive status. For example: `Online`, `Spun Up`, or `Rebuilding`.

Alarm Timestamp	The time when a non-optimal condition was recognized. A timestamp is displayed only if the drive is in an alarm state and has not rebuilt successfully or been replaced. The timestamp is updated for virtual drives only.
Media Error Count	The number of errors that occurred when reading, writing, or accessing data on the hard drive. These errors are usually related to the drive platters (media) and related mechanism.
Other Error Count	All other hard drive behaviors, such as failed commands, the drive resetting or needing to be reset, and any other error not included in the Media or Predictive error counts.
Predictive Error Count	Predictive errors are similar to SMART errors, which indicate possible future failure of the drive to the hard drive or RAID controller.
Raw Size	The size of the disk drive.

Support Report

Support reports contain detailed information about the server for use in troubleshooting and system analysis. These reports are used by your support representative and should be generated only when requested (Figure 3-4).

Figure 3-4 Generating a Support Report



Procedure

Step 1 Select **Support Report**.

Step 2 Click **New**.

Step 3 (Optional) Select **Include Core Files** to generate core files on the system. This is useful if any Media Server processes crashed at runtime.

Step 4 Click **Generate Report** to create a new support report (as a `.zip` archive file).

Step 5 Wait for the report to be generated.

Step 6 (Optional) Click the report entry to view details about the report generation process.

Step 7 Select a report entry and click **Download** to save the `.zip` file to a local drive.

Step 8 Contact Cisco Support for instructions to submit the support report.
If you need to open a support request with Cisco TAC, world wide support contact information can be found at: http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Note: You can download Active MQ statistics i.e. list of active connections between brokers and clients using **Download Active AMQ Statistics.**

Media Server

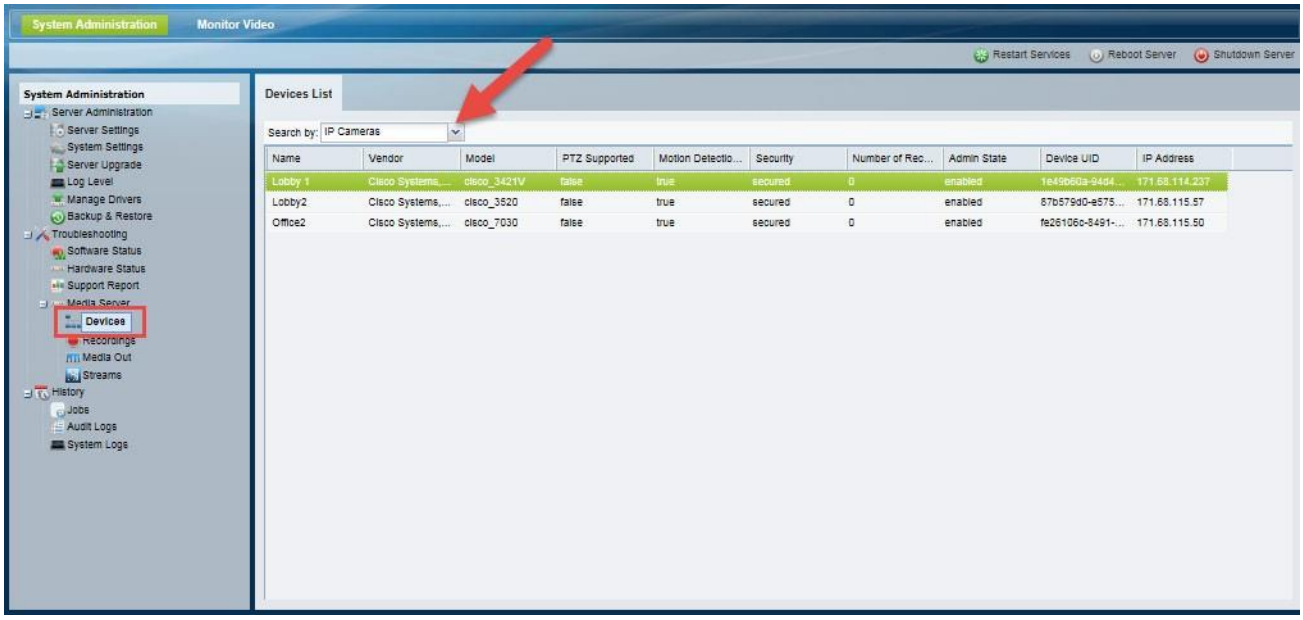
The Media Server options provide information about the cameras, encoders, recordings and video streams managed by the server. Refer to the following topics for more information:

- Devices, page 3-10
- Recordings, page 3-12
- Media Out, page 3-14
- Streams, page 3-15

Devices

Select **Devices** to display a list of all IP cameras, analog cameras and encoders associated with the Media Server (Figure 3-5).

Figure 3-5 Device List



Procedure

Step 1 Select **Media Server** > **Devices**.

Step 2 Select a device type from the Device Filter menu (Figure 3-5):

- **IP camera**
- **Analog Cameras**
- **Encoders**

Step 3 Use the column headings to sort the results.

Table 3-7 describes the available device information:

Table 3-7 Device List

Field	Devices	Description
Name	All devices	The meaningful name assigned to the device using Cisco VSM Operations Manager. For example: `Lobby Door Camera`
Vendor	All devices	The device manufacturer. For example: `Cisco Systems, Inc`
Model	All devices	The device model. For example: `Cisco 4300E`
PTZ Supported	IP and analog cameras	Indicates if the camera supports pan, tilt and zoom (PTZ) movements. See the camera documentation for more information. The possible values are true or false.
Motion Detection Supported	IP and analog cameras	Indicates if the camera supports motion detection. See the camera documentation for more information. The possible values are true or false.
Security	All devices	Indicates if the network communication is secured or unsecured.
Number of Recordings	IP and analog cameras	Indicates the number of recordings associated with the camera on the current Media Server.
Admin State	All devices	The administrative state of the device. For example, Enabled, Pre-provisioned, Disabled, or Soft-Deleted. See the Cisco Video Surveillance Operations Manager User Guide for more information.
Device UID	All devices	The unique ID assigned to each device. See the Cisco Video Surveillance API Programming Guide located on the Cisco Developers Network (CDN) for more information on using the device UID.
Encoder	Analog Cameras	The encoder associated with the analog camera. The encoder provides network connectivity for the camera.
IP Address	IP cameras and encoders	The network address of the device. **Note** Analog cameras are attached to an encoder, which provides network connectivity for the device. Analog cameras are not assigned IP addresses.

Recordings

The Recordings page provides information about the recording archives on the Cisco Video Surveillance server.

Procedure

Step 1 Select **Media Server** > **Recordings**.

Step 2 Select a camera from **Device** (or select **All** to display information for all cameras).

Step 3 Review the information (Table 3-8).

Table 3-8 Recordings Information

Item	Description
Recording Name	Unique ID of the recording.
Device Name	The camera name. Click an entry to view additional camera details, such as the camera make and model, IP address, PTZ and motion detection support, and the number of recording associated with the camera.
Stream Name	Unique ID of the camera video stream. Click the name to display stream properties, including the camera admin state, transport type and video configuration details (resolution, codec, etc.).
Type	Recording types include the following: • Regular—The recording is configured as a regular archive, which runs for a set duration • Loop—The archive is configured as a loop archive, which repeats contains data for a set duration
Duration	For a regular archive, indicates how long the archive runs. For a loop archive, indicates the length of time in the loop.
Expiration Time	The number of days before a loop recording will expire and be deleted. For example, a value of 1 indicates that the most recent 24 hours of loop recording is available for viewing. Recorded video older than 1 day is deleted.
Event Expire Time	The number of days before an event recording (such as motion detection events) will expire and be deleted. For example, a value of 30 indicates that event recordings such as motion events will be saved for 30 days. After 30 days the recordings will be deleted.
Frame Rate	The number of frames per second (for JPEG recordings).
State	The current state of the recording. The possible values are: • CONFIG • RUNNING • SHELVED • PAUSED • FAILED

Table 3-8 Recordings Information (continued)

Item	Description
Clip Sub Type	Indicates the file format of a recording clip (if the recording is a clip). The possible values are: • notaclip (the recording is a system recording and was not saved as a clip). • native • mp4 • bwm • bwx
Create Time	The time when the recording was created.
Dead Time	Defines when the recording stops (due to a schedule or the recording being put into "No Recording" mode). A dead time with no value indicates the recording is still active.
Last Start Time	The time when the recording was last started.
Storage Estimation	The estimated storage space required by the recording.
Current Storage	The amount of storage space currently used by the recording.
Location	The server partition where the recording is stored.
First Frame Time	The timestamp of the first frame.
Last Frame Time	The timestamp of the last frame.
Scheduled	True/False. Indicates if the recording is a scheduled recording. This value is false if the recording is a continuous loop or an event.
Admin State	The admin state of the recording.
Codec	The recording codec. For example: • mpeg4 • JPEG • h264
Video Format	Indicates if the recording is in the NTSC or PAL format.
Video Width	The image width, in pixels.
Video Height	The image height, in pixels.
Start Immediate	Indicates if recordings will start immediately or are scheduled for a later time.

Secured	True/False. Indicates if the recording data will be transferred using a secure channel.

Media Out

Mediaout statistics display information about video that the Media Server is serving.

Procedure

Step 1 Select **Media Server** > **Mediaout**.

Step 2 Select the following:

- Device Name—Select the camera name.
- Stream—Select live or recorded.
- Stream—Select the stream name.

Step 3 Wait for the information to refresh. Mediaout information is provided for each camera that is serving video (Table 3-9).

Table 3-9 Mediaout Connection Details

Item	Description
Connection Type	The network protocol used to deliver video (RTSP or HTTP).
Device Name	The camera name. Click an entry to view additional camera details, such as the camera make and model, IP address, PTZ and motion detection support, and the number of recording associated with the camera.
Stream	Indicates if the stream being viewed is live or recorded.
Stream Name	The name of the live or recorded stream that is being viewed. Click the name to display stream properties, including the camera state, transport type and video configuration details (resolution, codec, etc.). See the "Streams" section on page 3-15 to view information on the available streams for a camera.
Sub Session Type	The format used for video recording, compression, and distribution. For example, H.264 is used for high-definition video and Internet streaming.
IP Address	The destination network address for the video stream.
Up Time (in Seconds)	The number of seconds that the Media Server has been sending the video stream to the endpoint.
Transport	Transport protocol used for the stream (TCP or UDP).
Port	Port on the server from which the stream is being sent.
Average Throughput (in Bps)	Average bandwidth used by the stream, in bytes per second.
Average FPS	Average frames per second send in the stream.
Lost Frames	Number of frames dropped by the stream.

Lost RTP	Number of RTP packets dropped by the stream.

Streams

The Streams page provides information about the live video streams on the Cisco Video Surveillance server.

Procedure

Step 1 Select **Media Server** > **Streams**.

Step 2 Select a camera name from the **Device Name** menu (all cameras are displayed by default).

Step 3 Table 3-10 describes the information for each stream.

Table 3-10 Streams Information

Item	Description
Stream Name	Unique ID of the camera video stream. Click the name to display stream properties, including the camera admin state, transport type and video configuration details (resolution, codec, etc.).
Device Name	The camera name. Click an entry to view additional camera details, such as the camera make and model, IP address, PTZ and motion detection support, and the number of recording associated with the camera.
Channel	Indicates if the stream is the primary (1) or Secondary (1), if multiple streams are available from the camera.
Port	Port on the server from which the stream is being sent
Transport Type	Indicates if the stream data is sent using unicast or multicast.
Codec Type	The format used to encode and decode the video stream for transmission, storage, encryption, or playback.
Format	The format used for distribution. For example, H.264 is used for high-definition video and internet streaming.
Video Name	The name of the video stream format. For example, 720p indicates a progressive HDTV signal with 720 horizontal lines.
Width	The number of vertical lines in the video. For example, 1280.
Height	The number of horizontal lines in the video. For example, 720.
Frames per Second	The number of video frames displayed in one second. For example, 6 means that 6 still images are sent each second to create the video image.
CBR	The constant bitrate used to ensure a high quality image. Displayed only if the stream is configured for a CBR.
VBR Upper Cap	The maximum allowed variable bitrate. Displayed only if the stream is configured for a VBR.
VBR Lower Cap	The minimum allowed variable bitrate. Displayed only if the stream is configured for a VBR.

Sample Rate	(Audio streams only) The sampling rate for the audio stream.

Table 3-10 Streams Information (continued)

Item	Description
Secured	If True, the stream can only be viewed using a security token
Admin State	The admin state of the camera, indicating if the device is meant to stream video. For example, the ENABLED state means that the camera should be streaming video (even if there is an error that results in a critical error that prevents the camera stream). The DISABLED state means that the camera is offline and does not provide video.

History

- Jobs, page 4-1
- Audit Logs, page 4-5
- System Logs, page 4-6

Jobs

Many user actions (such as editing a camera template) trigger a Job that must be completed by the Cisco VSM system. These Jobs are completed in the background so you can continue working on other tasks while the Job is completed. Although most Jobs are completed quickly, some actions (such as modifying a camera template) may take longer to complete if they affect a large number of devices.

Note Jobs are pruned (removed) automatically on a regular basis.

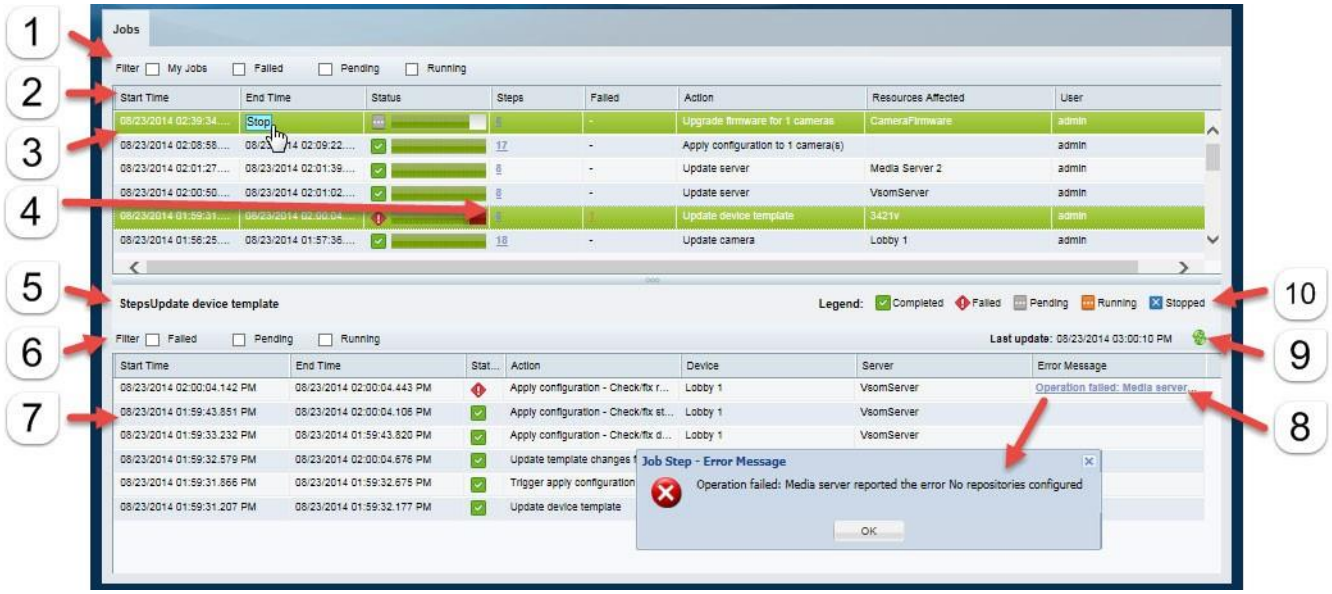
Click **History** > **Jobs** (Figure 4-1) to view a summary of recent Jobs, filter and sort the Job entries, and view detailed Job Steps and error messages.

For example, if a camera template that is assigned to 100 cameras is modified, the revised configuration must be applied each device and the cameras may need to be restarted. Although a single Job is created, there will be 100 Job Steps (one step for each affected camera). If the action fails for a single camera, there will be 99 Completed steps, and one Failed step. Click the error message for the failed step to view additional information that can help you resolve the issue.

Tip Click the number under the Steps or Failed columns to display Job Step information in the bottom pane.

Jobs

Figure 4-1 Jobs



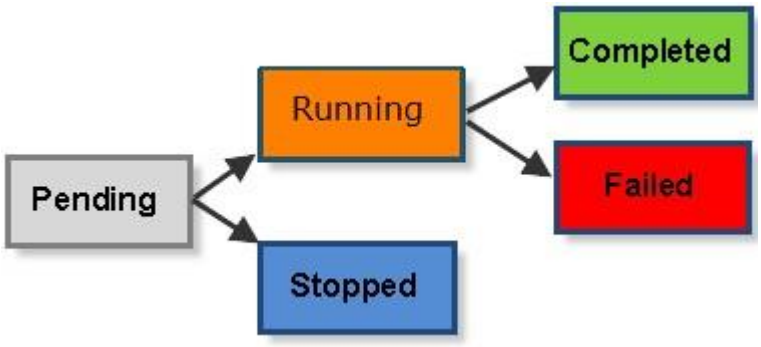
	Feature	Description
1	Filter	Select a filter to limit the Job types displayed. For example, click **Failed** to display only failed Jobs. **Note** Click **My Jobs** to view only the Jobs you initiated. This option is only available to super-admin. Most users can only view their own Jobs by default.
2	Job events	Lists the Jobs in the system. Use the filter to narrow the Jobs displayed or click the column headings to sort the information. **Note** The Job list automatically refreshes to display up-to date status information. Each Job includes the following information: • Start Time—The date and time when the Job was initiated by the user. • End Time—The date and time when the Job ended. A Job can end when it is completed or fails. Jobs with at least one pending Job Step can be stopped (click the **Stop** button). See the "Understanding Job Status" section on page 4-4 for more information. • Status—Indicates the Job status. Refer to the legend for a description of each color. See the "Understanding Job Status" section on page 4-4. • Steps—The number of Job Steps required to complete the Job. Click the number to display the step details in the bottom pane. • Failed—The number of Failed Job Steps. Click the number to display only the failed Job Steps in the bottom pane. • Action—The action or system change performed by the Job. • Resources Affected—The resources affected by the Job. For example, name of the Media Server or the template that is modified by the Job. • User—The user who triggered the Job.
4	Job Steps	Lists the sub-steps performed for a Job (click the Steps number to display Job details).

5	Job Steps filter	Select a filter to limit the steps displayed. For example, click **Running** to display only Job Steps that are still in progress.
6	Job Steps detail	Lists each sub-step that is performed for the selected Job. Click the number under the Step or Failed column to display the steps for a Job. **Note** The Job Step list does not automatically refresh. Click the refresh icon to renew the display and view up-to-date information. Use the filter to narrow the Jobs steps displayed or click the column headings to sort the information. Each Job Step includes the following information: • Start Time—The date and time when the step began to process. • End Time—The date and time when the step ended. A step can end when it is completed or fails. • Status—Indicates the Job Step status. Refer to the legend for a description of each color. • Action—The action or system change performed by the Job Step. • Device—The resources affected by the Job Step. For example, a camera. • Server—The server affected by the Job Step.
7	Error Message	Click the error message (if available) to open a pop-up window with additional details.
8	Refresh icon	Click the refresh icon to renew the display and view up-to-date Job Step status. The Last Update field shows when the information was last updated.
9	Legend	Describes the meaning of each status color. For example, a green Job status bar means the Job was successfully completed. Legend: Completed Failed Pending Running Stopped

Understanding Job Status

Each Job and Job Step has a status as shown in Figure 4-2.

Figure 4-2 Job Status



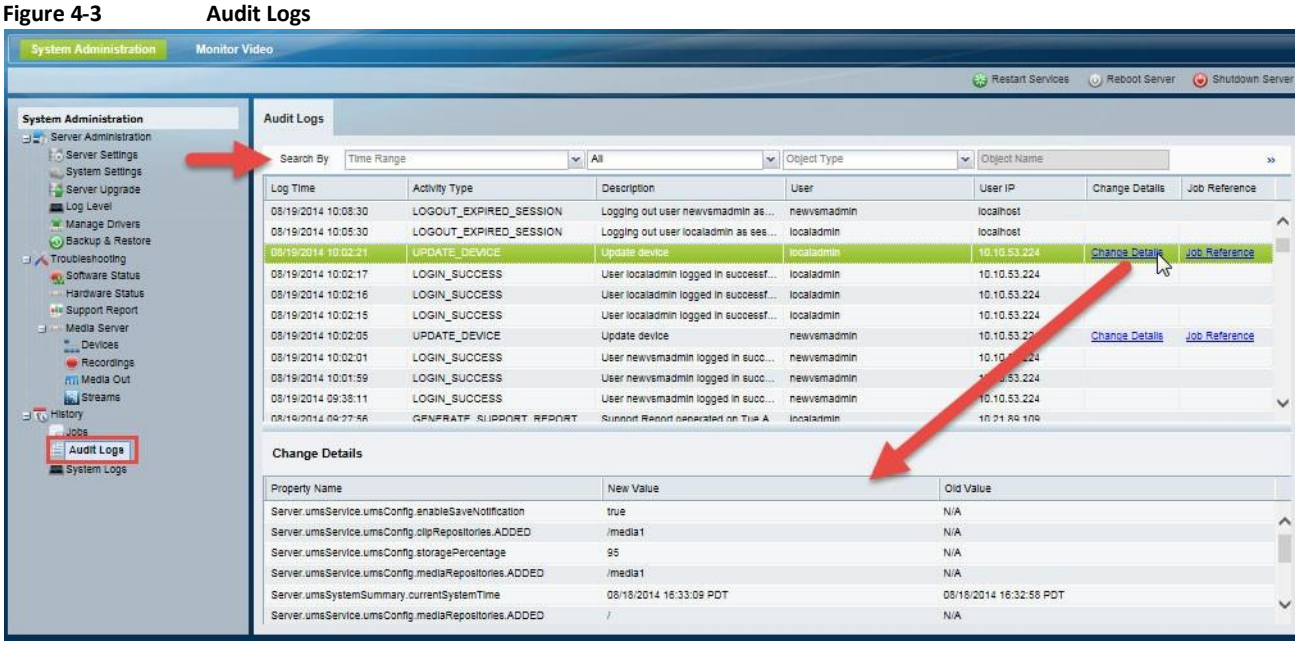
Status	Color	Description
Pending	Gray	A Job or Job Step that has not begun to process. Only Pending Jobs or Job Steps can be stopped.
Running	Orange	The Job or Job Step has begun to process. The action cannot be stopped and will continue until it either succeeds or fails.

Stopped	Blue	A pending Job or Job Step that was stopped by the user.
Completed	Green	A Job or Job Step that was successfully completed.
Failed	Red	A Job or Job Step that failed to complete. Click the Error Message for more information regarding.

Audit Logs

Audit Logs display a history of user configuration actions in the Cisco Video Surveillance deployment (Figure 4-3). The most common operations are setting up the system resources such as Ethernet IP addresses, date & time, enabling or disabling the Operations Manager and Media Server. The Audit Logs also record numerous other activities.

Figure 4-3 Audit Logs



Procedure

Step 1 Select **History** > **Audit Logs**. All logs are displayed by default.

Step 2 Use the Search By fields narrow the results.

- Time Range
- Activity Type
- Object Type
- Object Name (enabled only when an Object type is selected)
- Object Location
- User Name

- User IP address.

For example, you can select a time range 24 hours and Activity Type Create_Role to view all roles that were created in the last 24 hours. Click **Reset Filter** to clear your selections.

Step 3 (Optional) Click the **Change Details** link (if available) to view additional information about the event (Figure 4-3).

Step 4 (Optional) Click the **Job Reference** link (if available) to view the related Jobs summary.

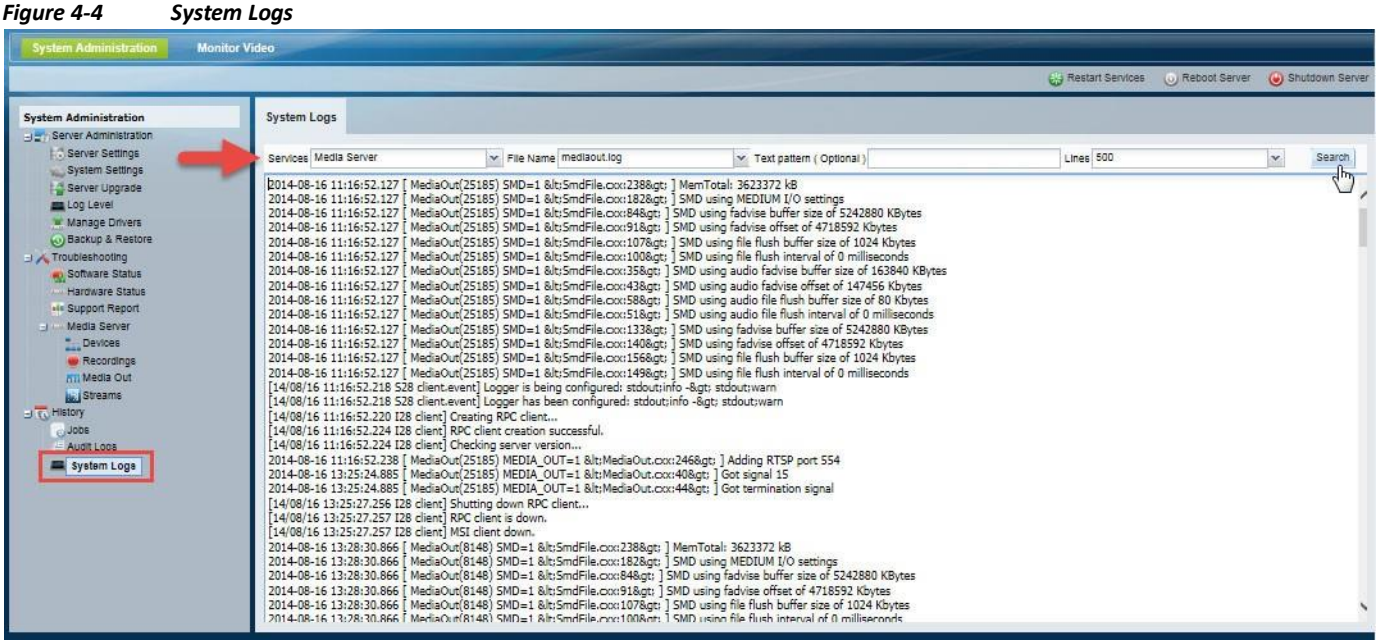
See the "Jobs" section on page 4-1 for more information.

Step 5 Click the column headings to sort the list.

System Logs

Logs are used by Cisco technical support or other support representatives to gather server log output for troubleshooting purposes (Figure 4-4). See the "System Log Descriptions" section on page 4-7 for descriptions of the available log files.

Figure 4-4 System Logs



Procedure

Step 1 Select **History** > **System Logs**.

Step 2 Select a **Service**, such as the **Operations Manager** (VSOM) or **Media Server**.

Step 3 Select a log File Name.

- For example: `mediaout.log`.
- See the "System Log Descriptions" section on page 4-7".

Step 4 (Optional) Enter search text in the Text Pattern field to display only the log lines that includes that text.

Step 5 Select the number of lines to display.

The system can display the most recent 500 or 1000 entries.

Step 6 Click **Search** to display the log records. The results are displayed from the most recent log entry.

System Log Descriptions

Table 4-1 Log Files and Descriptions

Service	Service or Process	Description
Map Server	geoserver.log	Log generated by Map Server service, if enabled on the server.
Media Server	cmapi.log	Log generated by cmapi server which handles most of the incoming http requests.
	failover.log	Log generated by failover server that runs on all Media Servers.
	groom.log	Log indicated a list of files groomed by the recorder on its grooming cycles.
	mediaout.log	Logging information for the RTSP server and HTTP media-related requests, such as MJPEG streaming and thumbnail generation.
	mediaout_access.log	List of incoming request handle by the mediaout process.
	mp4groom.log	Log indicating when MP4 grooming was done.
	msi.log	Log generated by the Cisco msi subsystem, which is used for auto-discovery of Cisco cameras.
	scheduler.log	Log generated by the scheduler when it handles incoming scheduler requests and when it runs a scheduled job.
	snmpd.log	Includes information about the SNMP daemon, such as when the SNMP daemon starts, stops, the snmpd.conf configuration file is read by the daemon.
	xvcrman.log	Contains logging information for the recorder process.
Metadata	vmgs.log	Log generated by the Metadata service, if enabled on the server.
Operations Manager	amqbroker.log	Log file for the ActiveMQ broker running on any Cisco VSM server.
	gc.log	Log file which captures the memory usage and cleanup of memory done by the JVM (Java Virtual Machine).
	mysql.log	Log file for the Operations Manager database server process.
	mysql_install.log	Log file for capturing the install time info for the Operations Manager database.
	slow_sql.log	Log file which captures slow transactions happening in the Operations Manager database. Meant for debugging only.
	vsom_be.log	The log file for the Operations Manager backend process. This file will be empty on a media-server only server

Table 4-1 Log Files and Descriptions (continued)

Service	Service or Process	Description
Platform Services	httpserver.log	Includes HTTP requests that the Operations Manager or Media Server host sends to the Apache server.
	httpserver_access.log	List of all incoming HTTP requests sent to the Media Server HTTP server.
	ims.log	A general log that captures general debug and error information that does not belong to the other logs.
	mysql.log	Log file for the Media Server database server process.
	mysql_install.log	Log generated when MySQL is installed on Media Server.
	mysql_upgrade.log	Log generated when MySQL is upgraded on Media Server.
	mysql_slow_query.log	Log of long running MySQL queries.
	rpm_install.log	Log of the RPM packages installed on the server.
	cdaf_be.log	Management Console backend log.

Restarting and Shutting Down

- Restart Services, page 5-1
- Reboot Server, page 5-1
- Shutdown Server, page 5-2

Restart Services

A restart is required to activate configuration changes to settings such as the server services and network settings. You must also restart services after a Media Server restore.

- Changes to some fields require you to restart server services and log back in.
- Restarting services can take up to 90 minutes or more depending on number of devices managed by the server. Installed products will be offline during this time.

Procedure

Step 1 Click **Restart Services** at the top right corner of the page.

Step 2 Click **Yes** to confirm and continue.

Step 3 Wait for the operation to complete.

Step 4 Re-login to the server.

Reboot Server

Use **Reboot Server** to power cycle the server. A server reboot restarts the Linux operating system and all services, and can be used to recover from system errors or other issues that are not resolved by restarting the services.

Note The reboot process results in system downtime and a loss of connectivity between the server and all associated devices and users. During this time, the Cisco Video Surveillance server will be offline and inaccessible.

Procedure

Step 1 Click **Reboot Server** at the top right corner of the page.

Step 2 Click **Yes** to confirm and continue.

Step 3 Wait for the operation to complete.

Step 4 Re-login to the server.

Shutdown Server

Use **Shutdown Server** to power down the Cisco Video Surveillance server. Shutting down the server halts all Cisco Video Surveillance services and terminates the connections between the server and all associated devices and users until the server is brought back online. The Cisco Video Surveillance server will be offline and inaccessible until powered on.

Procedure

Step 1 Click **Shutdown Server** at the top right corner of the page.

Step 2 Click **Shutdown Now**.

Step 3 Click **Yes** to confirm and continue.

Step 4 The page will continue to show an "Attempting to shut down the server" message until the server is powered on again.

Step 5 After the server shuts down, power on the server. See the server hardware user guide for more information.

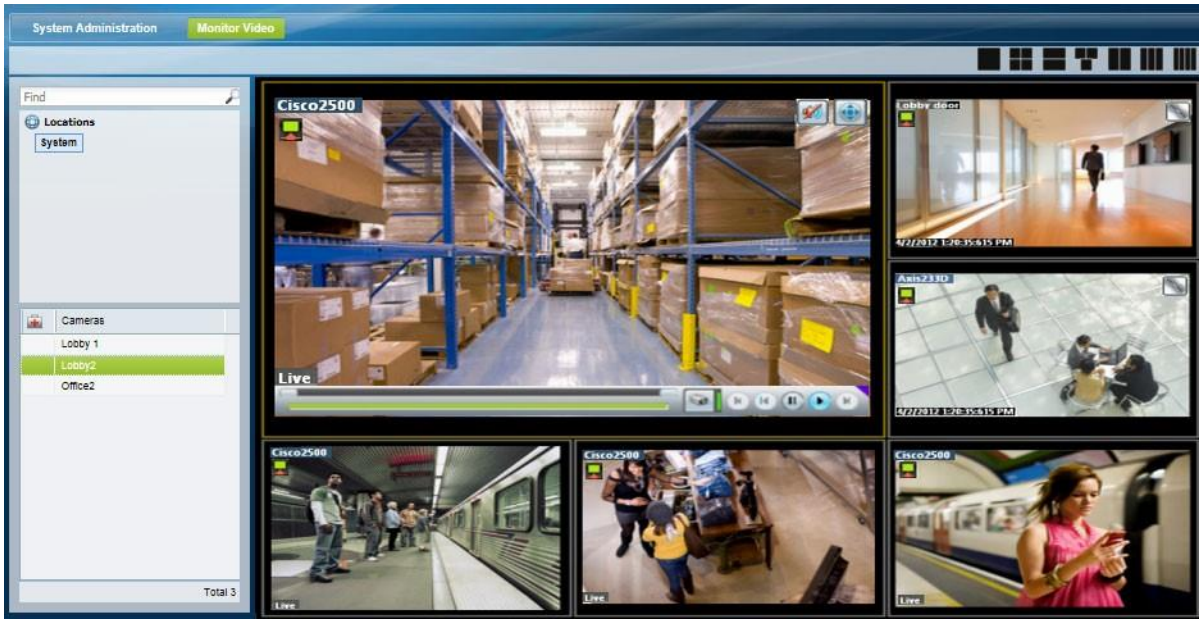
Monitoring Video

Select the **Monitor Video** tab to view video from the cameras supported by the Cisco Media Server, even if the Cisco VSM Operations Manager is unavailable. You can also create cva clips.

Usage Notes

- The ActiveX player be installed on a supported browser, such as Internet Explorer. See the Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification for more information. The Firefox browser can also be used for basic video monitoring using HTML.
- You cannot create MP4 or virtual clips.
- Use the browser-based Cisco VSM Operations Manager or the Cisco Video Surveillance Safety and Security Desktop applications. See the "Related Documentation" section on page A-1 for more information.
- If the live or recoded steam is in covert mode by an Operations Manager user, the video may not be displayed.

Figure 6-1 Monitor Video



Procedure

Step 1 Log in to the Cisco VSM Management Console (see the "Logging In" section on page 1-7).

Step 2 Verify that you are using a compatible browser (such as Internet Explorer) with the ActiveX player installed.

Step 3 Click **Monitor Video** (Figure 6-1).

- Other console options are not available if you signed is as a localuser.

Step 4 Select the System location and a view. Only cameras supported by the server are displayed.

Step 5 Double-click a camera name from the list.

Step 6 Use the video controls to view recorded video and create cva clips.

See the Cisco Video Surveillance Operations Manager User Guide for more information.

Related Documentation

Use one of the following methods to access additional Cisco Video Surveillance (Cisco VSM) documentation:

- Click **Help** at the top of the screen to open the online help system.
- Go to the Cisco Video Surveillance documentation web site.
- See the Cisco Video Surveillance 7 Documentation Roadmap for descriptions and links to Cisco Video Surveillance documentation, server and storage platform documentation, and other related documentation.