Cisco Video Surveillance Management Console Administration Guide

Release 7.0

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-27092-03

Cisco Video Surveillance Management Console Administration Guide

CONTENTS

Preface

Revised: April 16, 2013

Overview

This document describes the procedures used to setup, monitor, and administer the Cisco Video Surveillance server software. It also describes the procedure to configure basic network settings, and enable the Media Server and Operations Manager applications.

Revision History

Table 1 Cisco Video Surveillance API Programming Guide Revision History

Release	Document Revision Date	Change Summary
Release 7.0.0	October, 2012	Initial draft. See the Release Notes for Cisco Video Surveillance Manager for more information.
Release 7.0.0	February, 2013	• Revised the "Creating a Custom Certificate in .pem Format (Example)"section. • Added information about virtual machine (VM) installation requirements (OVA image on the Cisco UCS platform) to the "Overview"section, including requirements for network and password settings. • Various minor edits.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information about obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*. This document also lists all new and revised Cisco technical documentation. It is available at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Also see the "Related Documentation" section.

CHAPTER 1

Overview

Overview

The Cisco VSM Management Console is used by system administrators to perform infrequent server administration tasks, such as initial server setup, backups, and log monitoring. The Management Console is used to enable the following applications:

- Operations Manager—A browser-based interface used to configure, manage and monitor a Cisco Video Surveillance deployment, including Media Servers.The Operations Manager is used for multi-user configuration, administration and monitoring tasks. The Operations Manager login credentials are different than the Management Console credentials. See the *Cisco Video Surveillance Operations Manager User Guide* for more information.
- Media Server—An application that processes and stores video from cameras assigned to that Media Server. Multiple Media Servers can be managed by a single Operations Manager. The Media Server credentials are the same as the Management Console.

Note The Operations Manager and Media Server applications can be run on the same server, or separate servers. One server in the deployment must run the Operations Manager, either *co-located* on the same physical server as a single Media Server application, or as a standalone Operations Manager server (to support multiple Media Servers).

The following combinations are supported.

- Co-located—The Operations Manager and a single Media Server are enabled on the same server. Co-located servers only support a single Media Server.
- Multiple Media Servers—In larger deployments, a single Operations Manager is used to configure and administer multiple Media Servers. The Operations Manager and each Media Server is installed in a stand-alone 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.

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 Media Server and/or Operation Manager applications, configure the Ethernet and network settings, define the system time (or NTP server), and other basic settings.	System Setup, page 2-1
Monitoring	Use the **Monitor** links to view lists of the cameras and encoders associated with the server, the installed software packages, logs, hardware status, video stream and recording information, and other system details.	Monitoring a Cisco Video Surveillance Server, page 3-1

Table 1-1 Feature Summary (continued)

Feature	Description	More information
Media Server Administration	Use the **Administration** pages to define the following: • Mediaout ports used to serve video. • The storage, recording and backup repositories. • SNMP trap destinations. • Other Media Server settings.	Media Server Administration, page 4-1
Server Maintenance	Restart or shutdown the server define the log levels, upgrade the server software and device drivers, backup and restore the server configuration.	Maintaining the Cisco Video Surveillance Server, page 5-1
View Video	View video from a single Cisco Video Surveillance camera.	Camera View, page 6-1

Requirements

The Cisco Video Surveillance Management Console requires the following.

Table 1-2 Requirements

Requirements	Requirement Complete? (✓)
A physical or virtual Cisco Video Surveillance 7.x server installed in the network where the other Cisco Video Surveillance components are deployed. • Physical Servers—See the Cisco Physical Security Multiservices Platform Series User Guide for instructions to install a physical server. • Virtual Machines—See the Cisco Video Surveillance Virtual Machine Deployment Guide for UCS Platforms, Release 7.0 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. **Note** All hostnames (Operations Manager, Media Servers, cameras and encoders) must either resolve to a local address (inside a NAT) or public address (outside a NAT). Having a mix of hostnames/IP addresses inside and outside a NAT can cause connection errors and other issues (such as camera discovery problems). See the "Configuring the Server Ethernet Ports" section on page 1-7	☐
A PC or laptop running Windows 7 (32-bit or 64-bit), with a minimum resolution of 1024x768.	☐
The 32-bit Internet Explorer (IE) 8 web browser (the 64-bit IE browser is not supported in this release).	☐

Understanding Cisco Video Surveillance Software

The following table summarizes the software that can be upgraded in a Cisco VSM deployment.

Table 1-3 Cisco Video Surveillance Software Types

Software Type	Description
System Software	*System Software* denotes the Cisco VSM software, including Media Server, Operations Manager, Management Console, and Cisco Video Surveillance Safety and Security Desktop clients. • The Operations Manager and all associated Media Servers must run the same software version. • See the "Server Upgrade" section on page 5-6 for upgrade instructions. To repair or restore the Cisco VSM server software, see the Cisco Video Surveillance Manager Flash Drive Recovery Guide. • Repair: reinstalls the Operating System files and partitions without erasing video files stored on the server. You must backup the Cisco VSM database before using the recovery image, and then restore the database after the recovery process is complete. This action also preserves the RAID configuration. • Factory Restore: Restores the server to its factory default settings, reinstalls the operating system, and clears and reconfigures the RAID. This action deletes all data, configurations, software and video files from the appliance, and then reinstalls the operating system and Cisco VSM software. Perform this procedure only if necessary.
OVA image (for VM installations)	OVF template files are used to install the server software as a virtual machine (VM) on a supported Cisco Unified Computing System (UCS) platform. • OVA template files are downloaded from the Cisco website. • The file format is .ova. For example: `Cisco_VSM-7.0.0-331d_ucs-bc.ova` • See the Cisco Video Surveillance Virtual Machine Deployment Guide for UCS Platforms, Release 7.0 for instructions to install the .ova image and perform the initial VM setup. • After the VM setup is complete, the the Management Console described in this guide to complete the configuration.
Device *driver packs*	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. • *Driver pack* versions must be the same on the servers that host the Media Server and Operations Manager or a *driver pack mismatch* error will occur. Templates cannot be revised when a *driver pack mismatch* error is present. • See the "Manage Drivers" section on page 5-11 for upgrade instructions.
Device *firmware*	Device *firmware* is provided by the device manufacturer. The firmware for Cisco devices can be upgraded using Operations Manager. Firmware for other manufacturers is upgraded using a direct connection. See the Cisco Video Surveillance Operations Manager User Guide for instructions to upgrade Cisco device firmware, or refer to the device documentation.

Logging In

The Cisco VSM Management Console username and password are 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).

Note The default username **localadmin** is read-only and cannot be changed.

Procedure

Step 1 Launch the 32-bit version of Internet Explorer 8 on your Windows 7 computer.

Step 2 Enter the server URL. The syntax is: **http://**<*server-ip-address or hostname*>**/vsmc/**

Platform	Server Address
Physical server : Cisco Multiservices Platform (Cisco MSP)	The default (factory) static IP address is: **http://192.168.0.200/vsmc/**
Virtual Machine: 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 The network settings can also be changed using the guest OS console when installing the server software OVA image. See the "Configuring the Network Settings" section of the Cisco Video Surveillance Virtual Machine Deployment Guide for UCS Platforms, Release 7.0 for more information.

Step 3 Enter the Cisco VSM Management Console password.

Platform	Server Address
Physical server —Cisco Multiservices Platform (Cisco MSP)	• 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 Guide for UCS Platforms, Release 7.0 for more information.

Step 4 Click **Log In**.

Step 5 Enter and re-enter a new password, if prompted (if logging in for the first time or after a factory restore operation).

Step 6 Complete the Initial Setup Wizard, if prompted (see the "Using the Initial Setup Wizard" section on page 2-2).

Changing the Cisco VSM Management Console Password

Note The username *localadmin* cannot be changed.

Procedure

Step 1 Click the **Administration** tab and then click **Reset Password**.

Step 2 Enter the current password.

Step 3 Enter and re-enter the new password.

Step 4 Click **Save**.

Configuring the Server Ethernet Ports

The Ethernet ports on a Cisco Video Surveillance server can use a combination of static, DHCP and disabled ports. The supported port configuration depends on the applications enabled on the server.

Refer to the following topics for more information.

- Default Ethernet Interface Settings, page 1-7
- Network Settings in a Virtual Machine (OVA File) Installation, page 1-7
- Supported Ethernet Port Configurations, page 1-8
- Using DHCP, page 1-9

Note After the Media Server is associated with an Operations Manager, the network settings are disabled in the Cisco VSM Management Console and can only be modified using the browser-based Operations Manager tool. See the "Network" section on page 2-7 and the Cisco Video Surveillance Operations Manager User Guide for more information. You must add the Media Server to the Operations Manager configuration to edit the settings.

Default Ethernet Interface Settings

The default Ethernet port configuration is:

- Eth0— configured with a private static IP address (`http://192.168.0.200/`)
- Eth1— configured for DHCP (the IP address and other settings are received from a DHCP server, if available).

These settings are applied in new servers, or servers that have been restored using the recovery USB stick. Use either of these addresses to access the Cisco VSM Management Console and complete the *Setup Wizard* (see the "Completing the Setup Wizard" section on page 2-2). At least one of these interfaces must reachable from the network where the workstation is installed.

Network Settings in a Virtual Machine (OVA File) Installation

The default network settings, including the server address, can be changed during the installation of a virtual machine (VM) on the Cisco Unified Computing System (UCS) platform. This is done if you cannot access either of the default addresses with a web browser.

If necessary, see you system administrator for the address assigned to the server using the guest OS console.

See the "Configuring the Network Settings" section of the Cisco Video Surveillance Virtual Machine Deployment Guide for UCS Platforms, Release 7.0 for more information.

Supported Ethernet Port Configurations

Cisco Multiservices Platform servers include two built-in Ethernet ports that support a combination of disabled, static or DHCP settings. The supported Ethernet port settings depend on the application(s) enabled on the server, as shown in Table 1-4.

Usage Notes

- At least one static interface must be configured.
- See the "Using DHCP" section on page 1-9 for information regarding DHCP interfaces.
- See the "Network" section on page 2-7 for interface configuration instructions.
- You must restart the server services after changing network settings. 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. See the "Restart Services" section on page 5-2.

Table 1-4 summarizes the supported configuration depending on the running applications.

Table 1-4 Supported Ethernet Configurations

Server Application	Ethernet Port Configuration
Co-located system (Operations Manager and Media Server hosted on the same server)	At least one Ethernet port must be enabled. The following combinations are supported: • Both interfaces configured static • One interface configured static and the other DHCP • One interface static and the other disabled **Note** The Media Server must be added to the browser-based Operations Manager configuration to access the network settings.
Media Server-only system	At least one Ethernet port must be enabled. The following combinations are supported: • Both interfaces configured static • One interface static and the other disabled • One interface configured static and the other DHCP
Operations Manager-only system	• Both interfaces configured static • One interface static and the other disabled

Using DHCP

A DHCP server can be used to automatically assign the IP address, default gateway and DNS server for an Ethernet port. If DHCP is enabled, then the other network fields are disabled and the required settings must be provided by the DHCP server.

To manually assign the IP address, default gateway, or DNS server, de-select **DHCP** by selecting the **Static IP** option, as described in the "Network" section on page 2-7.

Usage Notes

If the Media Server interface used in the Operations Manager configuration is set to DHCP, the connection can be lost when the Media Server reboots and receives a different IP address. To restore communication, update the Operations Manager configuration in with the new Media Server IP address. To avoid this situation, we recommend using a DNS hostname for the DHCP interface, or using a static IP address.

CHAPTER 2

System Setup

Complete the following procedures to set up a Cisco Video Surveillance server for the first time, or to revise the setup settings for a running server.

The *Initial Setup Wizard* runs the first time you log on to the Cisco VSM Management Console. After the server is configured, you can access the same settings pages under the Administration tab, or by clicking the **Setup Wizard** link in the top right of the screen.

System setup includes the following:

Using the Initial Setup Wizard

Refer to the following topics to access and complete the Initial Setup Wizard.

Accessing the Setup Wizard

The Setup Wizard appears the first time you log in to the Cisco Video Surveillance Management Console (see Logging In, page 1-5 and Default Ethernet Interface Settings, page 1-7).

After the initial configuration, you can also click the **Setup Wizard** link in the top right of the Management Console screen. The **Setup Wizard** link appears only in the following configurations:

- Systems that run only the Operations Manager application.
- Systems where the Media Server has not yet been added to the Operations Manager configuration.

Note The **Setup Wizard** link is not available in Media Server-only systems that are managed by the Operations Manager. Use the browser-based Operations Manager to revise the configuration, as described in the Cisco Video Surveillance Operations Manager User Guide.

Usage Notes

- —Appears next to fields that require a server services to restart, if changed. The restart is performed at the end (see Step 6) unless you enable the Media Server on a running system. 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 that time.
- —Appears next to any step that contains incorrect entries. Correct the settings and try again.
- —Appears next to step numbers that are successfully completed (Figure 2-1).
- Click **Back** to return to the previous step, if necessary.

Completing the Setup Wizard

Step 1 Enter the *Applications, Date and Time* settings and click **Next**.

See the "Applications" section on page 2-4 and the "Date and Time" section on page 2-10 for more information.

Step 2 Enter the *Network* settings and click **Next**.

See the "Network" section on page 2-7 and the "Configuring the Server Ethernet Ports" section on page 1-7 for more information:

Step 3 Enter the *System Language, Date and Time Format* settings and click **Next**.

See the "Language Settings" section on page 2-12.

Step 4 (Operations Manager and co-located servers only) Enter the SMTP server settings used to send server generated emails.

- Required if the Operations Manager application is enabled (see Step 1).

- See the "SMTP (Email)" section on page 2-8 for more information.

Step 5 Click **Finish** and wait for the Wizard results to appear (Figure 2-1).

Figure 2-1 Wizard Result

Step 6 Click **Restart Services Now** if 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) Continue to additional configuration or administrative tasks.

- Security, page 2-14—create and install a custom SSL certificate, if required (a self-signed certificate is used by default).
- System Setup Settings, page 2-4—revise the settings entered in the Initial Setup Wizard.
- Monitoring a Cisco Video Surveillance Server, page 3-1—display system status, hardware, software, installed Cisco Video Surveillance packages, and system activity.
- Media Server Administration, page 4-1—manage Media Server attributes such as Mediaout ports, storage, security, recording, serial ports, SNMP trap destinations and other settings.
- Maintaining the Cisco Video Surveillance Server, page 5-1—set log levels, backup and restore the database, perform server upgrades and manage device drivers.
- *Cisco Video Surveillance Operations Manager User Guide*—use the Operations Manager browser-based administration utility to configure the Media Server (including network port addresses), configure cameras, users, and other Cisco Video Surveillance parameters.

System Setup Settings

The system setup settings can be entered using the Initial Setup Wizard, or from the Administration > System Setup links.

Refer to the following topics for more information:

Applications

Use the Applications setting to enable or disable the Cisco VMS Media Server or Operations Manager.

At least one application must be enabled.

- Enable only the Operations Manager to create a stand-alone server that manages multiple Media Servers.
- Enable only the Media Server to use the server exclusively for hosting cameras and processing video. The server must be associated with a Operations Manager server.
- Enable both Operations Manager and the Media Server to create a *co-located* configuration.

Note Changes to fields marked with a  require the restarting of server services (click **Restart Services** and follow the on-screen instructions). 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.

Procedure

Step 1 Click the **Administration** tab and then click **Applications** (Figure 2-2).

Step 2 Enable the server applications (Figure 2-2).

- **Media Server**—Enables the Media Server application for camera hosting and video processing.
- **Operations Manager**—Enables the browser-based Cisco VSM Operations Manager administration and configuration tool.

Step 3 Enter the *Operations Manager IP / Host Name*.

- If both the Media Server and Operations Manager are selected, *localhost* is automatically entered and cannot be changed.
- If the Media Server and Operations Manager are on different servers, enter the IP address or hostname for the Operations Manager.

- The DHCP server can also provide the Operations Manager IP address, and auto-register the Media Server server with the remote Operations Manager. In this case, you do not need to configure the Media Server Ethernet ports using the Cisco VSM Management Console. Instead, use the Operations Manager web UI to configure the server Ethernet ports, as described in the *Cisco Video Surveillance Operations Manager User Guide*. See the "Using DHCP" section on page 1-9 for more information.

Note If you enter a hostname for the Operations Manager application, a DNS server is required. See the "Network" section on page 2-7. In addition, the Media Server must be able resolve the IP address for the Operations Manager hostname.

All hostnames (Operations Manager, Media Servers, cameras and encoders) must either resolve to a local address (inside a NAT) or public address (outside a NAT). Having a mix of hostnames/IP addresses inside and outside a NAT can cause connection errors and other issues.

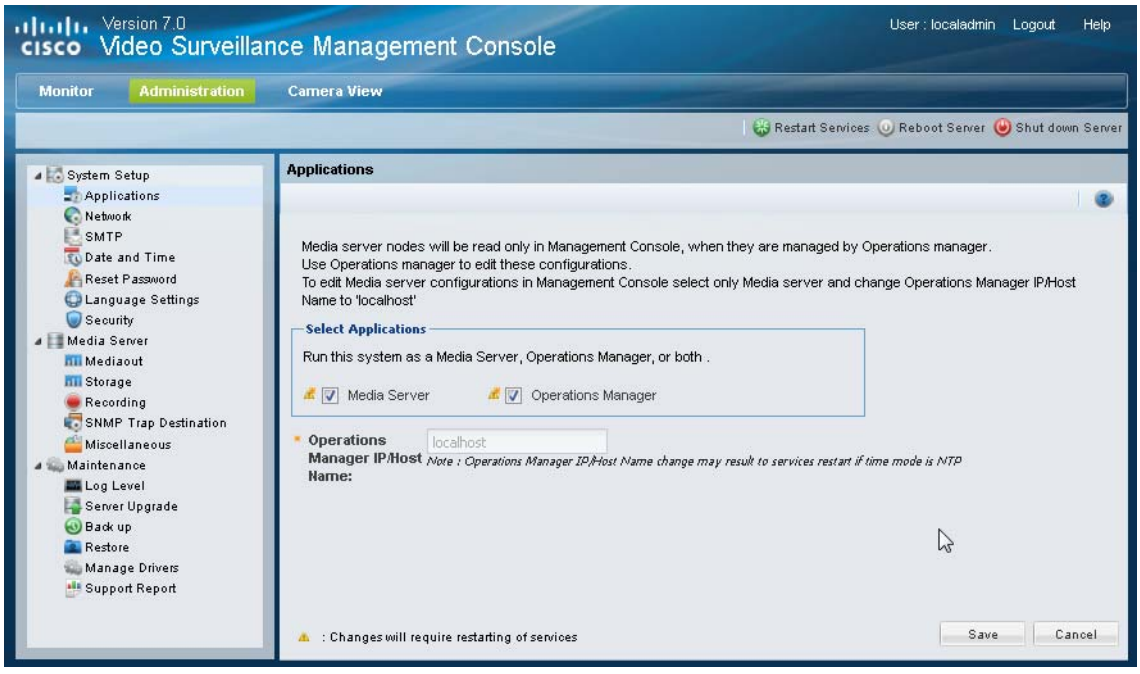
- All Media Servers in a deployment must point to the same Operations Manager.

Step 4 Click **Save**.

Step 5 Restart the system services, if prompted.

- Changes to fields marked with a 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.

Figure 2-2 Applications



Related Topics

- Logging In, page 1-5

- Feature Summary, page 1-2
- Configuring the Server Ethernet Ports, page 1-7
- Restart Services, page 5-2

Network

The *Network* settings (Table 2-1) define the server host name, domain name and Ethernet port configuration.

Note

- At least one interface must be set to static. See the "Configuring the Server Ethernet Ports" section on page 1-7 for information regarding the Ethernet port settings used to support the applications enabled on the server.
- Configuring an interface as DHCP may cause connectivity issues if no DHCP server is present in the network. For example, if an interface is configured for DHCP, and a DHCP server is not available in the network, then the network settings (such as the IP address and default gateway) will fail to populate and network communication cannot occur.
- After the Media Server is associated with an Operations Manager, the network settings are disabled in the Cisco VSM Management Console and can only be modified using the browser-based Operations Manager tool. See the Cisco Video Surveillance Operations Manager User Guide for more information.
- Operations Manager-only systems can include one static interface and one DHCP interface.
- Changes to fields marked with a require the restarting of server services (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.

Table 2-1 Network Settings

Setting	Description
Host Name	Enter the host name used to access the server over the network.
Domain Name	Enter the network domain name.
Interface (Eth0 and Eth1)	Select one of the following options based on the enabled server applications. See the "Configuring the Server Ethernet Ports" section on page 1-7 for more information. • **Static IP**—if selected, you must also enter the **IP address** and **Subnet Mask** for the interface. • **DHCP**—the IP address, Default Gateway, DNS Servers, and Search Domain(s) are disabled and will be defined by a DHCP server. See the "Using DHCP" section on page 1-9. • **Disable**—disables the interface. **Note** At least one interface must be set to static for proper functioning of the system.
Default Gateway	(Disabled when DHCP is enabled) Enter the IP address of the default gateway and click **Add**.

Table 2-1 Network Settings

DNS Servers	(Optional, Disabled when DHCP is enabled) Enter up to three domain name service (DNS) servers. **Note** If the Operations Manager address entered in the "Applications" section on page 2-4 is a hostname, a DNS server is required for Media Servers to resolve the associated IP address. To add a DNS entry, enter the IP address in the entry field and click **Add**. To remove an entry, highlight the IP address and click **Remove**.
Search Domain(s)	(Optional, Disabled when DHCP is enabled) Enter the domain name to search in the entry field and click **Add**. To remove an entry, highlight the domain and click **Remove**.

Procedure

Step 1 Click the **Administration** tab and then click **Network**.

Step 2 Edit the network settings described in Table 2-1.

Step 3 Click **Save** to apply the changes.

Step 4 Restart the system services, if prompted.

- Changes to fields marked with a  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.

Step 5 (Optional) Modify the server network configuration using the browser-based Operations Manager.

a. Log in to the browser-based Operations Manager.

b. Add the Media Server (click **Settings** > **Media Servers**).

c. In the Network Information section, click **Settings** (next to the NIC port).

d. Change the settings as necessary (see Table 2-1).

Related Topics

- Logging In, page 1-5
- Configuring the Server Ethernet Ports, page 1-7
- Restart Services, page 5-2

SMTP (Email)

The SMTP server settings are used to send email notifications. For example, the health notifications that are sent when a critical device error occurs.

Usage Notes

- The SMTP settings are required if the Operations Manager application is enabled.
- The SMTP settings are disabled if only the Media Server is enabled.

- Changes to the SMTP settings are reflected in the Operations Manager configuration.

Table 2-2 SMTP Settings

Setting	Description
SMTP Server	The IP address or hostname if the SMTP server used to send emails.
SMTP From Address	The email address that appears in the *from* field. User replies will be sent to this address. This field is required to send e-mails when an SNMP event occurs.

Procedure

Step 1 Click the **Administration** tab and then click **SMTP**.

Step 2 Enter the SMTP server settings (Table 2-2).

Step 3 (Optional) Click **Send test email** to verify the settings.

Step 4 Click **Save** to apply the changes.

Date and Time

The server time synchronizes server operations, defines recording timestamps and backup schedules. We strongly recommend using the same network time protocol (NTP) server on all servers to ensure the time settings are accurate and identical.

Setup Wizard NTP Options

Only the NTP server option is enabled when using the Setup Wizard. You can accept the default NTP server value, or enter a different NTP server.

- The localhost and IP address of the current server are not supported.
- By default, Media Server-only servers use the Operations Manager IP address as the NTP server. This ensures that all system components are synchronized to the same time. In the browser-based Operations Manager configuration tool, this is called the **Automatic** NTP mode.

Recommended Settings

All servers are configured to use an NTP server during the initial setup. We highly recommend using the NTP server option for all servers to ensure proper system operation.

- Operations Manager-only and *co-located* servers should use an NTP server such as `pool.ntp.org`.
- Media Server-only servers should use the Operations Manager IP address as the NTP server (default).

Note Localhost or same-server IP address is not supported.

Revising the Time and Date Settings After the Initial Setup

The time and date configuration options depend on the applications hosted by the server.

- **Operations Manager-only servers**
  - Always use the **NTP** server option (see Table 2-3).
  - If the **Manual** option is selected, a configuration mismatch can occur. To clear the configuration mismatch error, use the Management Console to enter an NTP server.
- **Co-located servers**
  - The *Date and Time* settings (in the Management Console) are disabled after the Media Server is added to the Operations Manager configuration.
  - To change the NTP server settings in a co-located server, use the Operations Manager browser-based interface. See the Cisco Video Surveillance Operations Manager User Guide for more information.
- **Media Server-only servers**
  - Once a Media Server is added to the Operations Manager configuration, the *Date and Time* settings in the Management Console are disabled. Use the Operations Manager browser-based interface to revise the Media Server NTP setting, if necessary. By default, all Media Server use the **Automatic** NTP mode (meaning the Media Server uses the Operations Manager server as the NTP server). This ensures that the timestamp on all Media Servers is the same.
  - If a different NTP server is required for a Media Server, use Operations Manager to modify the Media Server NTP configuration. Select the **User Configured** option to enter an NTP server different that the Operations Manager. See the Cisco Video Surveillance Operations Manager User Guide for more information.

Usage Notes

- Never modify the time and NTP settings using the Linux CLI. Always use the Cisco Video Surveillance Management Console interface as described in the following procedure. Settings made using the Linux CLI can result in inconsistent system performance and other issues.
- Changes to the server time can affect video recording schedules and timestamps.
- A warning alert is generated if the time difference between the Media 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.
- You will also be prompted to restart the server services (or cancel) if you enter a time or date that is different than the current server setting.

Settings

Table 2-3 Time Mode Settings

Mode	Settings
Manual	Select the date, time and time zone for the server.
NTP	(Recommended) Click **Add** to add the network time protocol (NTP) server that will automatically set the server date and time. You must also select a time zone.

Procedure

Step 1 Click the **Administration** tab and then click **Date and Time**.

Step 2 Enter the Time Mode and related settings (Table 2-3):

Step 3 Click **Save** to apply the changes.

Step 4 Restart the system services, if prompted, to activate the changes.

Note Changes to fields marked with a require the restarting of server services (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.

Reset Password

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

- Log in to the browser-based Cisco VSM Management Console GUI.
- Entered in the Cisco VSM Operations Manager configuration for the Media Server. The correct password must be entered to allow the Operations Manager to connect and communicate with the Media Server.

Usage Notes

- The password can include uppercase characters, lowercase characters, special characters and digit characters:
- The default Cisco VSM Management Console username *localadmin* cannot be changed.

Procedure

To reset the currently configured password, do the following:

Step 1 Click the **Administration** tab and then click **Reset Password**.

Step 2 Enter the current password.

Step 3 Enter and re-enter the new password.

Step 4 Click **Save**.

Step 5 Log in to the browser-based Operations Manager and update the password in the Media Server configuration.

Language Settings

Language settings define the user interface language, the date and time formats, and the first day of the week.

Tip To add or upgrade *System Language* packages, see the "Server Upgrade" section on page 5-6.

Procedure

Step 1 Click the **Administration** tab and then click **Language Setting**.

Step 2 Enter the *Language Settings* (Table 2-4).

Step 3 Click **Save**.

Step 4 Restart the system services.

Changes to fields marked with a require the restarting of server services (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

Settings

Table 2-4 Language Settings

Setting	Description
System Language	Select a supported language for the user interface text.
Date Format	Select the date format displayed in system messages, alerts, and other generated information. For example, **MM/DD/YYYY** means that dates will appear as month, day, and year. • d, dd = day • M = Month • y = year
Time Format	Select the time format displayed in system messages, alerts, and other generated information. For example, **h:mm:ss tt** means that the time will be displayed as hours, minutes, and seconds, and include the AM/PM notation. • h = hour • m = minute • s = second • tt = A.M. or P.M. • h/H = 12/24 **Note** Select **hh, mm, ss** to display the leading zero (or **h, m, s** if the display leading zero should not be displayed).
Calendar	Select the day that should be considered the first day of the week. For example, **Monday**.

Security

Network communication between the browser (client) and the Operations Manager or the Management Console is encrypted using SSL and HTTPS. Each server includes a default self-signed SSL certificate, or you can upload a custom .PEM certificate file issued by a Certificate Authority (see Figure 2-3).

The self-signed or custom 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.

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

- Creating a Custom Certificate in .pem Format (Example), page 2-14
- Installing the .pem Certificate, page 2-15

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.
- If you upload a custom certificate, you can click **Switch to self-signed certificate** to revert back to the default certificate.
- Custom 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.
- The security certificate is included in Media Server backups (see the "Database Backup and Restore" section on page 5-8). 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.

Creating a Custom Certificate in .pem Format (Example)

The following procedure is an example to create a custom self-signed certificate.

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

Sample Procedure

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 the "Installing the .pem Certificate" section on page 2-15.

Installing the .pem Certificate

Procedure

Step 1 Go to **Administration > Security**.

Step 2 Change the certificate used by the server for secure SSL communication.

- To use a custom certificate, click **Browse** and select the `.PEM` SSL certificate file used for encrypted communication.
- Click **Switch to self-signed certificate** to revert back to the default certificate (this option is enabled only if a custom certificate was previously applied). You do not need to enter a pass phrase if reverting to the default certificate.

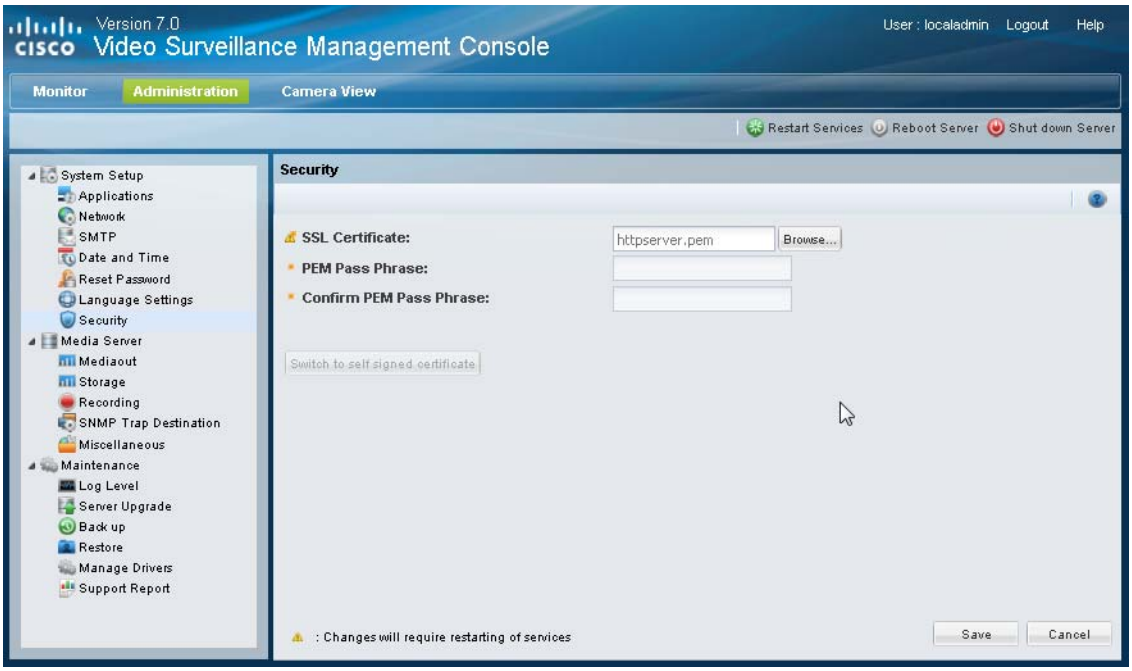
Step 3 (Custom certificates only) Enter and re-enter the *PEM Pass Phrase*.

Step 4 Click **Save**.

Step 5 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.

Figure 2-3 Security



CHAPTER 3

Monitoring a Cisco Video Surveillance Server

The **Monitor** tab displays system status, hardware, software, installed server packages, and system activity. For example, the System Trends page displays a set of graphical reports that show various information about system performance and resource use.

Refer to the following topics for more information:

System Summary

The System Summary window displays server hardware details, uptime, system time, and other details. Table 3-1 describes the information displayed in each field. The information on this page refreshes every one minute.

Table 3-1 System Summary

Field	Description
Server Model	The server model. For example, *CIVS-MSP-1RU* is a 1RU model is a server that requires 1 rack unit.
BIOS Version	The system BIOS version number.
Number Of CPU	The number of CPUs in the Linux system.
RAID Controller detail	The type of RAID controller on the server.
OS Type	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.
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.
Media Server Last Modified	(Media Server-only systems) The date and time the Media Server configuration was last modified. For example, Mediaout ports or storage.
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. You can enable the Operations Manager on any Cisco Cisco Video Surveillance server, but only one instance of Operations Manager is used to manage all of the Media Servers. See the "Feature Summary" section on page 1-2 for more information. To enable or disable Operations Manager on a server, see the "Applications" section on page 2-4.
Service Status	Displays the status of the services running on the server. Click the  icon to show or hide the status details. Services shown in red are in the down state.

Tip To access the System Summary page, log in to the Cisco VSM Management Console (see the Logging In, page 1-5). The System Summary appears by default.

Device List

The Device List displays a list of all IP cameras, analog cameras and encoders associated with the server.

Procedure

Step 1 From the **Monitor** tab, click **Device List**.

Step 2 Select a device type from the Device Filter menu (such as **IP camera**).

Step 3 Click **Search Now**.

Step 4 Use the column headings to sort the results. Details include the following:

Table 3-2 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*.
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.
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.

Installed Packages

The Installed Packages window displays the RPM software packages installed on the server, and the additional camera and encoder driver packages.

Procedure

Step 1 From the **Monitor** tab, click **Installed Packages**.

Step 2 Use the column headings to sort the results.

Tip Packages are updated as a group. See the "Server Upgrade" section on page 5-6 for instructions to update and manage the installed software packages. See the "Manage Drivers" section on page 5-11 to update the *driver packs* used by Media Server and Operations Manager to interoperate with video devices.

Logs

Logs are used by Cisco technical support or other support representatives to gather server log output for troubleshooting purposes.

The Logs page lets you display up to 1000 lines from the Media Server log files.

Note To define the log levels for the Operations Manager, Cisco VSM Management Console, or Media Server processes, see the "Log Level" section on page 5-4.

Procedure

To display information from a system log, follow these steps:

Step 1 From the **Monitor** tab, click **Logs**.

Step 2 Select an application or process from the first drop-down menu. The results are displayed from the most recent log entry.

Table 3-3 Log Options and Descriptions

Application or Process	Description
MS IMS	Primary Media Server log file. Includes system error messages and system activity messages.
MS Mediaout	Includes HTTP requests that the Operations Manager or Media Server host sends to the Apache server.
MS Recording	Captures log messages for recording-related activities.
MS Cmapi	Log generated by cmapi server which handles most of the incoming http requests.
SNMP	Includes information about the SNMP daemon, such as when the SNMP daemon starts, stops, the snmpd.conf configuration file is read by the daemon.
Operations Manager	Captures log messages for Operations Manager activities.
Management Console	Captures log messages for activities in the Management Console.
Tomcat	Captures log messages for Tomcat, which hosts the different web applications.
failover.log	Log generated by failover server that runs on all Media Servers.
scheduler.log	Log generated by the scheduler when it handles incoming scheduler requests and when it runs a scheduled job.
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.
httpserver.log	Log generated by the MS httpserver when it processes incoming HTTP requests.
groom.log	Log indicated a list of files groomed by the recorder on its grooming cycles.
mediaout_access.log	List of incoming request handle by the mediaout process.

Table 3-3 Log Options and Descriptions (continued)

Application or Process	Description
httpserver_access.log	List of all incoming HTTP requests sent to the Media Server HTTP server.
MS_mysql_install.log	Log generated when MySQL is installed on Media Server.
MS_mysql_slow_query.log	Log of long running MySQL queries.
amqbroker.log	Log file for the ActiveMQ broker on a Media Server-only server. (Operations Manager takes over the role of ActiveMQ broker on a Operations Manager-only or co-located server and the logs will be in `vsom_be.log`)
gc.log	Log file which captures the memory usage and cleanup of memory done by the JVM (Java Virtual Machine).
VSOM_mysql.log	Log file for the Operations Manager database server process.
VSOM_mysql_install.log	Log file for capturing the install time info for the Operations Manager database.
VSOM_slow_sql.log	Log file which captures slow transactions happening in the Operations Manager database. Meant for debugging only.

Step 3 (Optional) Enter search text in the *Text Pattern* field to display only the log lines that includes that text.

Step 4 Select the number of lines to display.

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

Step 5 (Optional) Click the *refresh* check-box to automatically perform the search every 30 seconds.

Step 6 Click **Search Now** to display the log records.

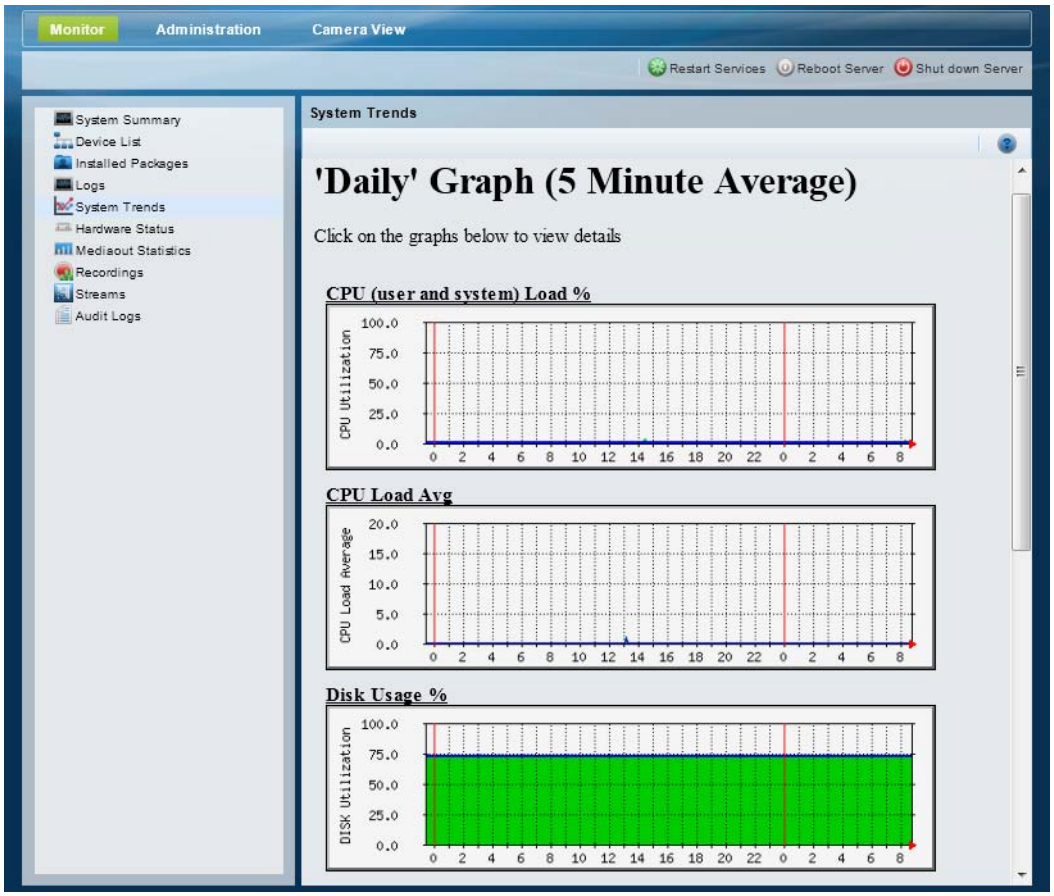
System Trends

The System Trends page displays information about system performance, hardware resource usage, and other data over time. The information is presented as a set of graphical reports, as shown in Figure 3-1.

Refer to the following topics for more information:

- Viewing Current Reports, page 3-8
- Viewing Historical Reports, page 3-8
- Understanding Graph Data and Colors, page 3-9

Figure 3-1 System Trends



Viewing Current Reports

By default, the System Trends page displays the following information. To update the reports, refresh your browser.

Table 3-4 System Trends

Field	Description
CPU Load Avg	Displays the average CPU resources that are consumed by user applications (the same value as displayed in the Linux "uptime" command output). The graph shows CPU Load Avg of 1 minute interval.
CPU (user and system) Load %	Displays the CPU resources that are consumed by user applications and by system operations, as a percentage of total CPU capacity.
Disk Usage %	Displays the amount of disk space used on the root and /usr disks for system files, archives, and related files, as a percentage of total capacity of these disks.
Used Physical Memory	Displays the amount of physical memory being used.
Used Swap Memory	Displays the amount of Swap memory being used.
Traffic Analysis	Displays the amount of incoming and outgoing network traffic, in bytes per second.

Viewing Historical Reports

Click the report name or graph to display historical versions of any System Trends report. Historical reports include the following:

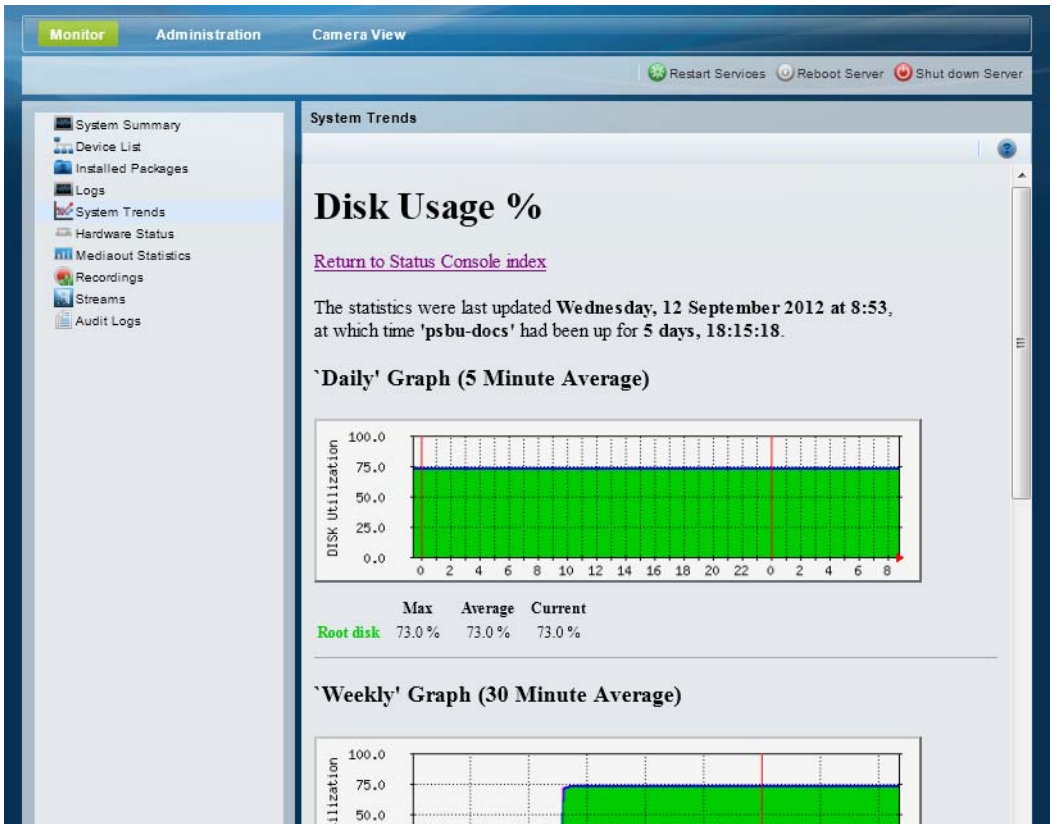
- Daily graph—Provides information for the past 32 hours, calculated by averaging values every 5 minutes. The information in this graph is the same as the default page (see the "Viewing Current Reports" section on page 3-8).
- Weekly graph—Provides information for the past 8 days, calculated by averaging values every 30 minutes.
- Monthly graph—Provides information for the past 4 weeks, calculated by averaging values every 2 hours.
- Weekly graph—Provides information for the past 12 months, calculated by averaging values every 1 day.

Some reports also include a table of maximum, average, and current values.

See the "Understanding Graph Data and Colors" section on page 3-9 for more information.

Figure 3-2 shows a detail view for the Daily CPU Utilization graph.

Figure 3-2 Graph Detail



Tip Click **Return to Status Console index** at the top or bottom of the page to return to the Status Console Overview page.

Understanding Graph Data and Colors

The time scale at the bottom of a graph progresses from left to right, as indicated by a small red arrow at the right of the scale. The time that the report generates appears at the far right of the time scale.

- The vertical *red* line indicates a start of a new period as follows:
  - Daily report—12:00 a.m. (00:00)
  - Weekly report—12:00 a.m. (00:00) on Monday
  - Monthly report—First day of the month
  - Yearly report—First day of the year (January 1)

Table 3-5 describes the information provided by each report:

Table 3-5 Data and Line Color Descriptions

Color	Description
CPU (user and system) Load %	
Green	Displays the CPU resources that are consumed by user applications and system operations, as a percentage of total CPU capacity.
Blue	Displays the server CPU use, as a percentage of total CPU capacity.
Dark Green	The dark green line displays the maximum value for incoming traffic, calculated every 5 minutes.
Magenta	The dark green line displays the maximum value for outgoing traffic, calculated every 5 minutes.
CPU Load Avg	
Green	Displays traffic load on the server, as a percentage of total CPU capacity.
Blue	Outgoing Traffic in Bytes per Second
Dark Green	The dark green line displays the maximum value for incoming traffic, calculated every 5 minutes.
Magenta	The dark green line displays the maximum value for outgoing traffic, calculated every 5 minutes.
Disk Usage %	
Green	Displays the amount of disk space, as a percentage of total disk capacity.
Dark Green	The dark green line displays the maximum value for incoming traffic, calculated every 5 minutes.
Blue	Displays the amount of space that is used for incoming traffic, as a percentage of total disk capacity.
Traffic Analysis	
Green	Displays the amount of outgoing network traffic, in bytes per second.
Blue	Displays the amount of outgoing network traffic, in bytes per second.
Used Physical Memory	
Green	Used Physical memory, excluding buffers and cached, in bytes
Dark Green	The dark green line displays the maximum value for incoming traffic, calculated every 5 minutes.
Used Swap Memory	
Green	Used Swap memory in bytes
Dark Green	The dark green line displays the maximum value for incoming traffic, calculated every 5 minutes.

Hardware Status

Hardware Status 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.

Refer to the following for more information:

- Viewing System Status, page 3-11
- Viewing Hardware Status, page 3-12
- Viewing RAID and Physical Drive Status, page 3-13

Viewing System Status

Procedure

Step 1 From the **Monitor** tab, click **Hardware Status**.

Step 2 Select **System Resources** from the drop-down menu.

Step 3 Click **Go**.

Step 4 See Table 3-6 for descriptions of each field.

Table 3-6 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.
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.

Viewing Hardware Status

Procedure

Step 1 From the **Monitor** tab, click **Hardware Status**.

Step 2 Select **Hardware** from the drop-down menu.

Step 3 Click **Go**.

Step 4 See Table 3-7 for descriptions of each field.

Table 3-7 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.
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.
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.

Viewing RAID and Physical Drive Status

Select **RAID** from the drop-down menu and click **Go** to display a list of *Virtual* drives that represent hard disk RAIDs. Expand the virtual drives to view information about the physical drives (see Figure 3-3).

Table 3-8 describes the information displayed for each RAID drive.

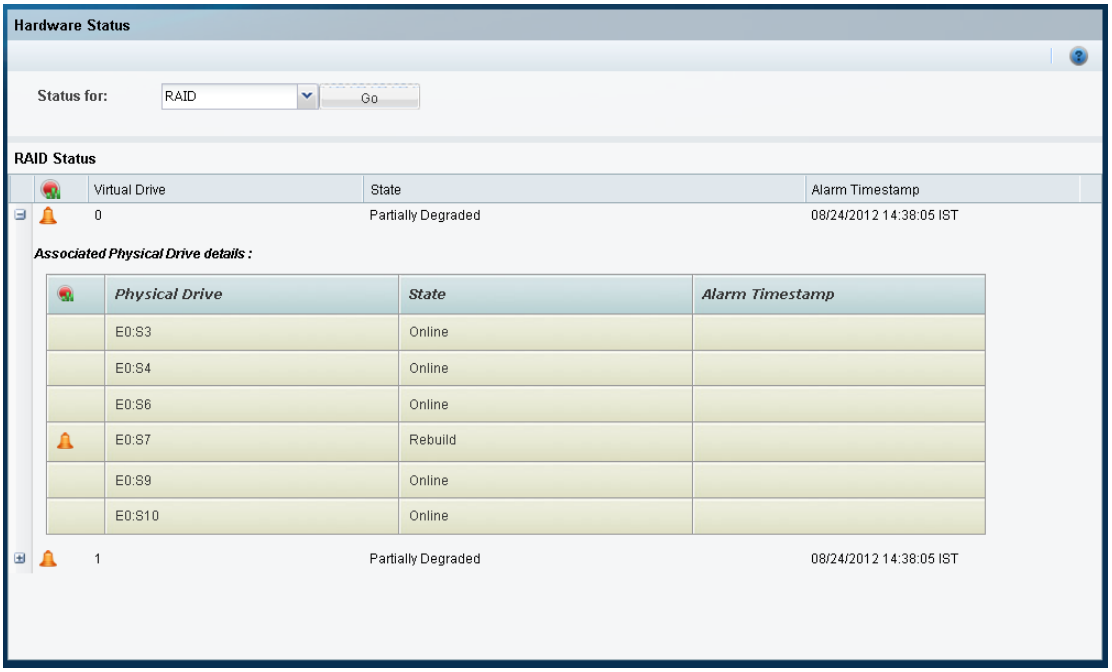
Note RAID information is provided only for Cisco Video Surveillance Multiservices Platform and Cisco Physical Security Multiservices Platform servers that support RAID. For example, CIVS-MSP-2RU, CIVS-MSP-4RU, CPS-MSP-1RU (4 hard drives), CPS-MSP-2RU.

Table 3-8 RAID Drive Status

Field	Description
Alarm	The alarm icon is displayed if an alarm occurs for one or more physical drives. Expand the virtual drive to view the physical drive(s) that caused the 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.
Physical Drives	Physical drives are listed by their physical location. For example: *Sx*=the slot and enclosure number. **Note** Cisco Video Surveillance Multiservices Platform and Cisco Physical Security Multiservices Platform servers have a single enclosure, and the hard drives lots are numbered 0-n.
State	The current drive status. For example: `Online`, `Spun Up`, or `Rebuilding`.
Alarm Time	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.

Figure 3-3 shows a sample Raid Status page. The Virtual Drive is expanded to show the physical drives. An alarm has occurred for the physical drive in slot 7.

Figure 3-3 Raid Status



Mediaout Statistics

Mediaout statistics display information about video that the Media Server is serving. The information on this page refreshes every 5 minutes.

Mediaout Summary

Select the **Mediaout Summary** radio button to view a summary of all connections that live or archived video is being served to.

Tip All devices, streams types and stream names are selected by default.

Table 3-9 describes the summary information.

Table 3-9 Mediaout Summary Information

Item	Description
Connection Type	The network protocol used to deliver video (RTSP).
Total	Total number of RTSP or HTTP connections that live or archived video is being served to. This field indicates the number of users who are viewing video through an RTSP connection.
Bandwidth	Total bandwidth that is consumed by all Mediaout connections.

Detailed Information

Step 1 Select the **Mediaout Detail** radio button,

Step 2 Select the following:

- Device Name—Select the camera name.
- Stream Type—Select the network protocol used to deliver the video, such as Real Time Streaming Protocol (RTSP).
- Stream Name—Select the stream name. See the "Streams" section on page 3-19 to view information on the available streams for a camera.

Step 3 Click **Go**.

Mediaout information is provided for each camera that is serving video (Table 3-10).

Table 3-10 Mediaout Connection Details

Item	Description
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.
Connection Type	The network protocol used to deliver video (RTSP or HTTP).
Stream Type	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.).

Table 3-10 Mediaout Connection Details (continued)

Item	Description
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 Bandwidth	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.

Recordings

The Recordings page provides information about the recording archives on the Cisco Video Surveillance server. The information on this page refreshes every 5 minutes.

Procedure

Step 1 From the **Monitor** tab, click **Recordings**.

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

Step 3 Click **Go**.

Step 4 Review the information (Table 3-11).

Table 3-11 Recordings Information

Item	Description
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.
Recording Name	Unique ID of the recording.
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.
Expire Time (in Days)	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 (in Days)	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.
JPEG 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 3-11 Recordings Information (continued)

Item	Description
Clip SubType	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
Created 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.
Estimated Storage	The estimated storage space required by the recording.
Current Storage	The amount of storage space currently used by the recording.
Current 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 Type-	The recording codec. For example: • mpeg4 • JPEG • h264
Video Format	Indicates if the recording is in the NTSC or PAL format.
Video Height	The image height, in pixels.
Video Width	The image width, 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.
Record iFrame	Indicates if the video is recording IFrames only.

Streams

The Streams page provides information about the live video streams on the Cisco Video Surveillance server. The information on this page refreshes every 5 minutes.

Procedure

Step 1 From the **Monitor** tab, click **Streams**.

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

Step 3 Click **Go**.

Table 3-12 describes the information that the list provides.

Table 3-12 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 for video recording, compression, and 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 3-12 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.

Audit Logs

Audit Logs display a history of user configuration actions in the Cisco Video Surveillance deployment. 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.

Procedure

Step 1 From the **Monitor** tab, click **Audit Logs**.

Step 2 Select the audit log file to be viewed or searched (this includes archived files for the past 12 months).

a. Select a **Feature Type** (such as *Authentication* or *System Setup*).

b. Select an **Activity Type** (such as *Login Succeeded*).

Step 3 Click **Go**.

The time of the activity, IP address of the user, and other details are displayed in the list

CHAPTER 4

Media Server Administration

Use the Media Server options to manage the following attributes:

Note

- The Media Server options are only available on servers running the Media Server application. See the "Applications" section on page 2-4 for instructions to enable or disable the Media Server.
- The Mediaout, Storage, Recording and Miscellaneous settings are read-only when the Media Server is managed by the Operations Manager. Use the browser-based Operations Manager interface to revise these settings, if necessary.

Mediaout

The Mediaout page defines the ports and other settings used to serve video. (Table 4-1).

Note Only the Live QoS and Playback QoS settings are editable when the Media Server is co-hosted with the Operations Manager. Use the browser-based Operations Manager interface to revise the read-only settings, if necessary.

Table 4-1 Mediaout Settings

Field	Description
HTTP Port	(Read-only) The port used for HTTP out connections. The default is 80.
HTTPs Port	(Read-only) The port used for secure (encrypted) HTTP sessions. The default is 443.
RTSP Port	The port used for Real Time Streaming Protocol (RTSP) out connections. Valid values are integers 1 through 65535. The default value is 554. Unless there is a network requirement it is recommended that the default port be used because it is the standard RTSP port.
RTP Min Port	The lowest port number used for Real-time Transport Protocol (RTP) out connections. The default is 1024.
RTP Max Port	The highest port number used for Real-time Transport Protocol (RTP) sessions. The default is 65535.
RTP Window Length	The maximum number of packets the Media Server buffers per stream to determine packet loss (before declaring a lost packet). This is also known as the jitter window length. This setting may need to be changed on a system with excessive packet delay on the network. **Note** This value is normally set to 1 but may need to be increased on networks where packets can get delayed.
Live QoS	The default Quality Of Service level that should be applied to RTP packets when playing *live* video streams. This setting is specific to your network, as each network may include a custom QOS setting. The value is based on the priority a network gives to certain types of traffic. For example, priority for video data over voice.
Playback QoS	The default Quality Of Service level that should be applied to RTP packets when playing *recorded* video streams. This setting is specific to your network, as each network may include a custom QOS setting. The value is based on the priority a network gives to certain types of traffic. For example, priority for video data over voice.

Storage

Use the Storage page to define the repositories (partitions) used to store media and backup files.

- Storage *Repositories* are mounted partitions on the server dedicated to storing media files (such as video).
- At least one media repository must be enabled.

Note These settings are read-only when the Media Server is managed by the Operations Manager. Use the browser-based Operations Manager interface to revise these settings, if necessary.

Procedure

Step 1 From the **Administration** tab, click **Storage**.

Step 2 Select the Storage options for the video files stored on the server (Table 4-2).

Table 4-2 Storage Repository Settings

Max Storage Utilization(%)	The maximum amount a disk can be full before it is declared unusable for any further recording. When the disk reached this percentage, the 200 oldest media files are groomed (deleted), until the free disk space is less that the Max Storage Utilization (%). • The maximum (and default) value is 98% (also the default). **Note** We recommend keeping this setting at or below the default value. • 0% means that the repositories are not available to store video archives. For example, if the Max *Storage Utilization* is set to 90%, and a camera template *Retain event recordings* setting is **Max Possible**, event recordings will be deleted once the disk repositories are 90% full.
Media Repositories	(Required) The repositories (partitions) used for video recordings generated by cameras associated with the Media Server. • At least one media repository must be enabled. • The size of the repository is displayed next to the selection. For example: `/media0(Size:687G)`
Backup Repositories	(Optional) The repositories (partitions) used for system backup files.

Table 4-2 Storage Repository Settings

Storage Estimation(%)	The amount of available storage required to ensure enough storage space is available on the Media Server for a scheduled recording. When the **Enable Storage Estimation** option is selected in a camera configuration, the Media Server verifies that enough disk space exists to complete the entire recording. For example, if a camera is configured to record a continuous H264 stream at 15mbps for 30 days, the Media Server would first verify that there is enough free disk space for the full recording length (30 days). If not, then recording will not start. In this example, 15 mbps of video uses approximately 2 megabytes of storage space per second, so 30 days of recording would require roughly 5 terabytes of disk storage.
Clip Repository	Choose one or more repositories (partitions) where video clips are stored. **Note** If multiple partitions are selected, the partition with the most available space is used to create video clips. CVA/CVX clips are downloaded immediately to the client workstation and not saved on the server. MP4 clips are saved on the server for 24 hours, and then deleted if they have not been downloaded. See the "Creating Video Clips" section on page -10 for more information.

Step 3 Click **Save**.

Recording

The Recording settings define how recorded video is managed by the server.

Note These settings are read-only when the Media Server is managed by the Operations Manager. Use the browser-based Operations Manager interface to revise these settings, if necessary.

Table 4-3 Recording Settings

Field	Description
Recording Queue Size	The maximum number of frames per recording that can be in queue waiting to be written to disk. The default is 150 and should only be increased if it is determined there is large I/O wait to the disk.

Table 4-3 Recording Settings

Maximum Event Duration	The maximum duration for a motion or other event recording. This option should be set to the maximum number of seconds of continuous activity that any camera in a deployment might capture. Valid values are integers 1 through 86400. The default value is 7200 seconds (2 hours).
Recording Default Groom Only	If selected, grooming based on the expiry time of recordings and events is not performed. Recordings and events are only groomed when the **Max Storage Utilization(%)** is reached (see Table 4-2).

SNMP Trap Destination

You can configure up to five SNMP additional trap destinations. All Cisco Video Surveillance server SNMP traps will be forwarded to these destination addresses.

Note
- Cisco Video Surveillance supports SNMP version 2 (Inform)
- Running a third-party trap receiver on a Cisco Video Surveillance host is not supported.

Procedure

Step 1 From the **Administration** tab, click **SNMP Trap Destinations**.

Step 2 Do one of the following to add, edit, or remove the destination entries:

- Click the Add icon to add a destination address. You can configure up to five SNMP trap destinations.
- Double-click the entry to edit an existing address (or select the entry check box and click the Edit icon).

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

Step 3 Enter the IP address or host name for the destination server.

Note Leading protocol strings (for example, http://) and port numbers (for example, 8080) are not allowed.

Step 4 Click **Add** or **Update**.

Step 5 Click close when the success message appears, or correct your entry and try again. The entry must be a valid IP address or host name and cannot include `http://` or port numbers.

Step 6 Repeat these steps for each trap that you want to configure.

Miscellaneous

Note These settings are read-only when the Media Server is managed by the Operations Manager. Use the browser-based Operations Manager interface to revise these settings, if necessary.

Table 4-4 Miscellaneous Settings

Field	Description
Security	Select one of the following: • **Secured**—The video streams from Media Server to ActiveX client (used to display video) will use a secure channel. • **Open**—The video streams from Media Server to ActiveX client (used to display video) will not be secure.
Camera Control Lockout	Designates how a camera behaves if PTZ contention occurs. (Contention occurs when two resources simultaneously attempt to access a camera PTZ operations.) In this case, the camera responds to PTZ commands from the first resource. It accepts PTZ commands from the next resource when the first resource is idle for the amount of time that this option defines. The default value is 5 minutes.

CHAPTER 5

Maintaining the Cisco Video Surveillance Server

Restarting, Rebooting, and Shutting Down the Server

Use the following instructions to restart server services after a configurations change, reboot (power cycle) the server, or shut down the server.

Restart Services

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

- Changes to fields marked with a  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.

Procedure

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

Step 2 Follow the on-screen instructions to complete the restart.

Step 3 Log back in to the Management Console.

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 Wait for the operation to complete. A success message appears when the server has rebooted.

Step 5 Power on the server by pressing the power button on the server appliance. See the *Cisco Multiservices Platform for Physical Security User Guide* for more information.

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 Monitoring tab. See the "Logs" section on page 3-5 for instructions to view system logs. Logs are typically used by Cisco technical support for debugging purposes.

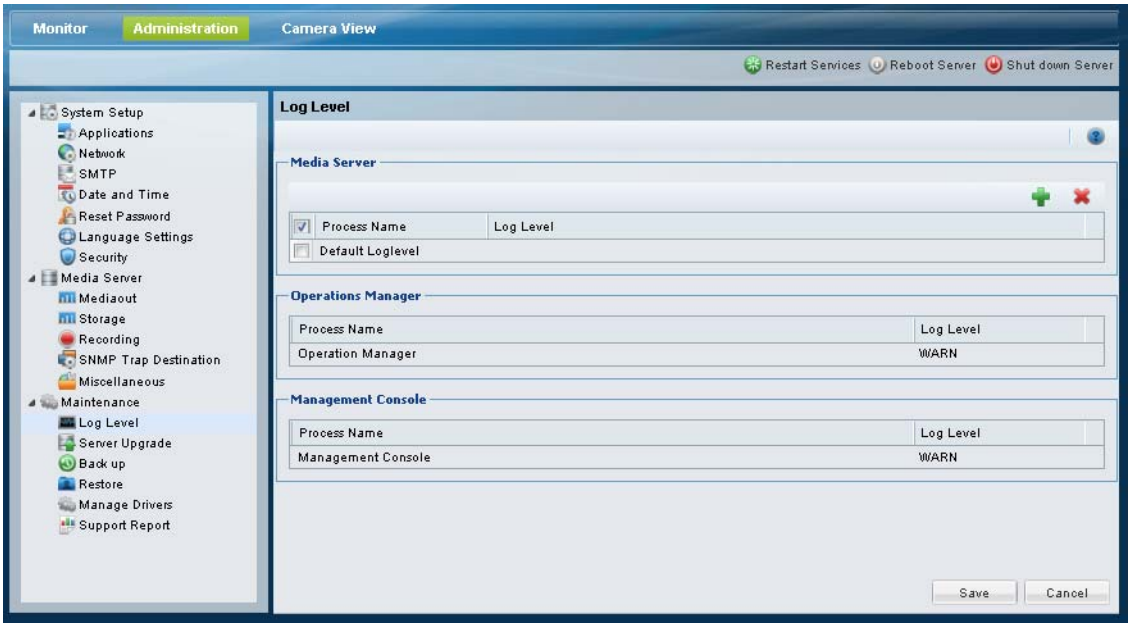
You can define the log levels for three types of processes:

- Media Server—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 Media Server Log Levels" section on page 5-4 for more information.
- Operation Manager— select ERROR, WARN, INFO, DEBUG, or TRACE.
- Management Console—select ERROR, WARN, INFO, DEBUG, or TRACE.

Note

- Wait approximately 1 minute for changes to the log levels to take effect.
- The default log level for all processes is WARN.

Figure 5-1 Setting Log Levels



Setting the Media Server Log Levels

To set the Media Server log levels, create a new entry for the process name, and define the log level:

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

- 10 = trace logging

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

Procedure

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

Step 2 Enter the Process Name in the entry field.

Step 3 Enter the Log Level using the following syntax:

Process=Log_Level_Number

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

Step 4 Click **Save**.

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

Step 6 Click the **Monitor** tab and then **Logs** to view the log information. See the "Logs" section on page 3-5 for more information.

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

Setting the Cisco VSM Operations Manager and Cisco VSM Management Console Log Levels

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

- ERROR—(default) error events that might still allow the application to continue running.
- WARN—potentially harmful situations.
- INFO—informational messages that highlight the progress of the application at coarse-grained level.
- DEBUG—fine-grained informational events that are most useful to debug an application. 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

Server Upgrade

The Cisco VSM server software includes the software packages for the Media Server, Operations Manager, Management Console, and Cisco Video Surveillance Safety and Security Desktop clients. The Operations Manager and all associated Media Servers must run the same software version. See the "Understanding Cisco Video Surveillance Software" section on page 1-4 for more information.

Upgrading Language Packs

The Server Upgrade feature is also used to upgrade or add language packages. You must upgrade the language packs on all servers in your deployment.

Download the language pack from the cisco.com and complete the following procedure (see the Release Notes for Cisco Video Surveillance Manager for software download instructions). After the system is restarted, login to the Management Console and select the System Language from **Administration > Language Settings > System Language**.

Usage Notes

- 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, Release 7.0 for instructions to upgrade Cisco device firmware.
- The server upgrade process automatically restarts server services. See the "Restart Services" section on page 5-2 for more information.
- To repair or restore the Cisco VSM server software, see the Cisco Video Surveillance Manager Flash Drive Recovery Guide.

Procedure

Step 1 Download the server software file.

See the Release Notes for Cisco Video Surveillance Manager, Release 7.0 for more information.

Step 2 Select **Administration > Server Upgrade**.

Step 3 Select an option to choose a file from your PC drive, or from an FTP server

- **Use file on PC**—Click **Browse** and select the file.
- **Use file on FTP**—Enter the server address, file path including the filename where the upgrade file is stored, and the FTP username and password.

Step 4 Click **Start Upgrade**.

Step 5 Click **Yes** to confirm and continue.

Note You cannot cancel the upgrade once it begins. This ensures that the server is not left in an unstable state.

Step 6 Wait for up to 90 minutes for the operation to complete and the server to restart.

Step 7 Re-login in the server when the login screen appears.

Step 8 Complete these steps for each server that hosts a Media Server or Operations Manager (log in to the Management Console for each server and upgrade the software to the same version).

Database Backup and Restore

Use the following procedures to backup and restore configuration data for the Media Server. We recommend backing up the Media Server data on a regular basis to ensure it is not lost in the event of a hardware failure, or to restore your configuration when upgrading or moving to a new system.

Usage Notes

- Backups include the current Media Server only, and do not include data from other Media Servers or the Cisco VSM Operations Manager.
- Configuration data includes user-configured settings, such as camera configurations. Historical data includes all user entered data *plus* logs and events.
- Automatically scheduled backups are not supported.
- 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. See the "Security" section on page 2-14 for more information.
- To create a scheduled Operations Manager back ups, or to back up video recordings, refer to the Cisco Video Surveillance Operations Manager User Guide.

Backup File Format

Backup files are saved using the following formats:

Table 5-1 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 Cisco VSM Operations Manager application.
- *yyyyMMdd_HHmmss*—the date and time when the backup file was created.

For example, if the *PSBU-ENG14* server configuration and historical data was backed up on August 17, the resulting filename would be: `VSOM_psbu-eng14_backup_20120817_174250.tar.gz`

Backup Procedure

Use the Backup feature to backup either the Media Server or Operations Manager configuration to a `.tar.gz` file. You can back up the configuration data only, or the configuration data plus the historical data.

Note We highly recommend backing up both the Operations Manager and Media Server applications when any major configuration changes are made. Backups ensure the system data can be restored to the present state, if necessary.

Procedure

Step 1 (Co-installed servers only) Select the **Operations Manager** or **Media Server** radio button.

Step 2 Select **Configuration Only** or **Configuration Plus Historical Data**.

Step 3 Select an option to save the file to your PC drive, or to an FTP server

If FTP server is selected, enter the server address, file path where the file will be saved, username and password.

Step 4 Click **Transfer File**.

Step 5 If saving the file to a PC, select the location for the file.

Step 6 Wait for the process to complete.

Restore

Use the Restore feature to restore a previously saved backup file and recreate a configured server state.

Note 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. See the "Security" section on page 2-14 for more information.

Procedure

Step 1 (Co-installed servers only) Select the **Operations Manager** or **Media Server** radio button.

Step 2 Select **Restore System Configs** to restore all system configurations such as network settings, language settings, date time, log level, SMTP, and the enabled applications.

Step 3 Select **Use file on PC** or **Use file on FTP**.

- If PC is selected, click Browse and select the `.tar.gz` backup file.
- If FTP server is selected, enter the server address, file path including the `.tar.gz` filename where the file is stored, and the FTP username and password.

Step 4 Click **Restore**.

Step 5 Click **Yes** to confirm and continue.

Step 6 Wait for the operation to complete and the server to restart. A success message appears when the server has restarted.

Step 7 Re-login to the server when prompted.

Manage Drivers

Device *driver packs* are the software packages used by Media Server and Operations Manager to interoperate 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.

Tip See the "Understanding Cisco Video Surveillance Software" section on page 1-4 for more information.

Usage Notes

- Driver packs must be upgraded to the same version on each server where the Media Server and Operations Manager applications are enabled. For example, if your deployment includes a stand-along Operations Manager, the Operations Manager server must have the same driver pack versions as the Media Servers associated with that Operations Manager. If the versions are different, a *driver pack mismatch* error can occur, which prevents camera template revisions.
- Upgrading a driver pack requires server services to restart.
- The driver pack file format is .zip. For example: `dp_cisco-2.0-16d_7.0.0-331d_sles10-sp1.zip`
- To view information about a driver, select a driver from the list. Information is displayed in the right side panel (Figure 5-2).
- See the Release Notes for Cisco Video Surveillance Manager, Release 7.0 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 7.0 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 **Administration > Manage Drivers**.

Step 3 Install a new driver pack to upload the software file to the server.

a. Click **Install New Driver**.

b. In the pop-up window, click **Browse** and select a valid *.zip* driver pack file from a local or network disk. For example: `dp_cisco-2.0-16d_7.0.0-331d_sles10-sp1.zip`

c. Click **Install New Driver**.

Step 4 Wait for the driver installation process to complete.

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

Step 5 (Optional) Select the driver pack to display important information about the driver pack release, and the impact of upgrading to the new driver pack (Figure 5-2).

Step 6 Upgrade the driver pack to apply the software on the server.

a. Select the driver pack.

b. Click **Upgrade Driver**.

c. In the pop-up window, click **Browse** and select a valid driver pack file from a local or network disk.

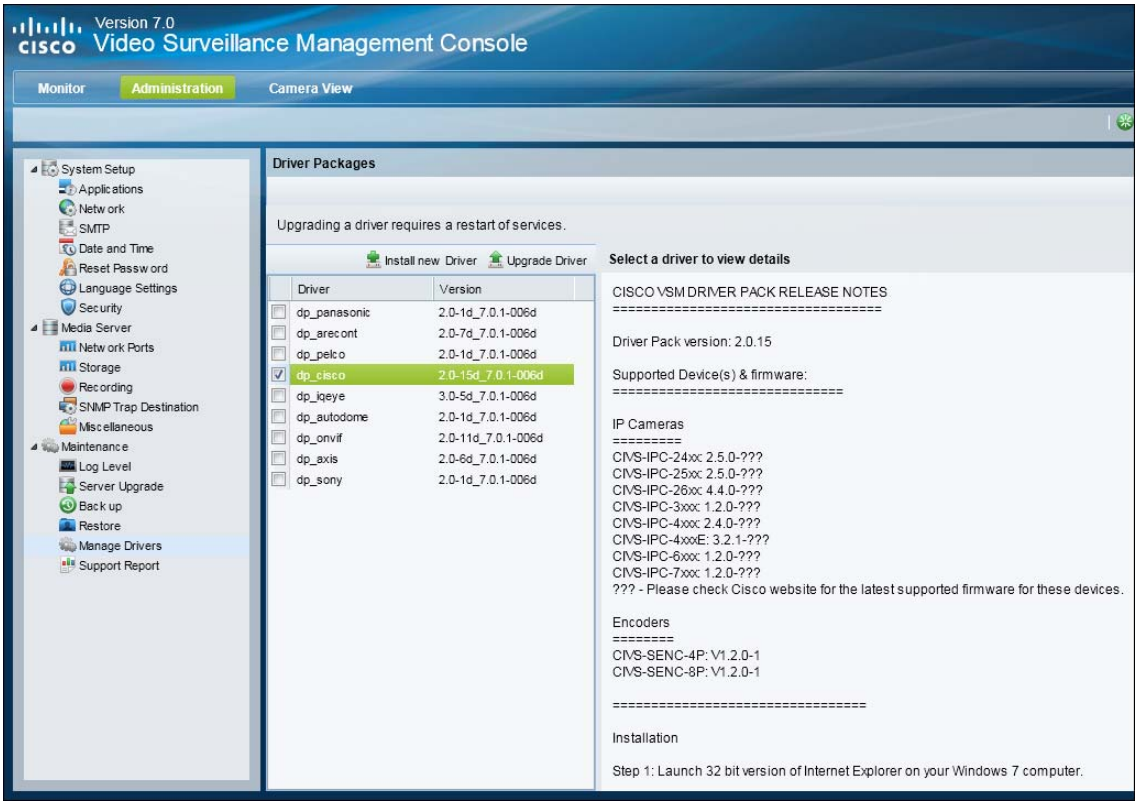
d. Click **Upgrade Driver**.

Step 7 Follow the onscreen prompts to restart the 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.

Step 8 Complete these steps for each server that hosts a Media Server or Operations Manager (log in to the Management Console for each server and upgrade the driver pack software to the same version).

Figure 5-2 Manage Drivers



Support Report

Click **Generate Report** to create and downloads a new support report (as a ZIP archive file).

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

Do not navigate away from or refresh this page until you receive the browser's **Save File** dialog box. Processing can take a few minutes.

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

CHAPTER 6

Camera View

Use the **Camera View** tab to view video from a Cisco Video Surveillance cameras.

Usage Notes

- You can view video from the primary stream of a single camera.
- To view video from multiple cameras or secondary streams, use the 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.

Procedure

Step 1 Log in to the Cisco VSM Management Console (see the "Logging In" section on page 1-5).

Step 2 Click **Camera View** (Figure 6-1).

Step 3 Double-click a camera name from the list.

All Cisco Video Surveillance cameras are included in the list.

Step 4 Use the video controls to view recorded video.

See the Cisco Video Surveillance Operations Manager User Guide or Cisco Video Surveillance Safety and Security Desktop User Guide for more information.

Figure 6-1 Camera View

APPENDIX A

Related Documentation

Use one of the following methods to access the 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 (the documents and direct links are summarized below).

Documentation Summary and Links

Refer to the following documentation for additional information about Cisco Video Surveillance, including server installation, system configuration, video monitoring, and other features.

Topic	Related Document	Description
All Documents	Cisco Video Surveillance documentation web site	Links to all of the documents described in this table.
Data Sheet	Cisco Video Surveillance Manager 7.0 Data Sheet	Describes the main features and part numbers for the Cisco Video Surveillance solution.
Release Notes	Release Notes for Cisco Video Surveillance Manager, Release 7.0	Describes the new and changed features, open and resolved caveats, and other information.
Design and planning	Cisco Video Surveillance Solution Reference Network Design Guide	Summarizes high-level design recommendations and best practices for implementing IP Video Surveillance on the enterprise network infrastructure. Also includes information on implementing high-availability, Medianet, virtual machines on the Cisco UCS platform, and security best practices.
Physical server installation	Cisco Physical Security Multiservices Platform Series User Guide	Instructions to physically install and set up the **Cisco VSM server appliance**. Each server can run the Media Server application, the Operations Manager application, or both.
Virtual machine (VM) deployment	Cisco Video Surveillance Virtual Machine Deployment Guide for UCS Platforms, Release 7.0	Deploy a virtualized Cisco VSM on a supported Cisco Unified Computing System platform.
	VMware HA for Cisco VSM 7.0 Operations Manager on UCS B- and C-Series Platforms	Describes the key requirements and instructions for deploying a highly available Cisco Video Surveillance Manager (VSM) 7.0 Operations Manager in a virtualized environment on a UCS B- and C-Series server using VMware HA.

Topic	Related Document	Description
Management Console	Cisco Video Surveillance Management Console Administration Guide	Use the browser-based **Cisco VSM Management Console** to set up and maintain a Cisco VSM server. Tasks include server software and driver pack upgrades, Media Server backups.
Browser-based configuration and monitoring	Cisco Video Surveillance Operations Manager User Guide	Use the browser-based **Operations Manager** to configure and manage a Cisco VSM deployment. The Operation Manager can also be used to monitor live and recorded video.
Workstation video monitoring	Cisco Video Surveillance Safety and Security Desktop User Guide	Use the **Cisco Video Surveillance Safety and Security Desktop** (Cisco SASD) application to view cameras, video and alerts on a graphical map. You can also display a video grid on a separate monitor, view Video Walls on multiple workstations, or create unattended workstations.
Video clip player	Cisco Video Surveillance Review Player User Guide	Use the **Cisco VSM Review Player** desktop application for basic playback of multi-pane video clips.
Workstation requirements	Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification	Baseline performance specifications for a video surveillance monitoring workstation.
Workstation Profiler Tool	Using the Cisco Video Surveillance Monitoring Workstation Pofiler Tool	Describes how to use the Cisco Video Surveillance Workstation Profiler Tool to analyze the ability of a PC client to render video.
Restore or repair the server software	Cisco Video Surveillance Manager Flash Drive Recovery Guide	Instructions to repair or restore the Cisco VSM server software. • Repair: reinstalls the Operating System files and partitions without erasing video files stored on the server. You must backup the Cisco VSM database before using the recovery image, and then restore the database after the recovery process is complete. This action also preserves the RAID configuration. • Factory Restore: Restores the server to its factory default settings, reinstalls the operating system, and clears and reconfigures the RAID. This action deletes all data, configurations, software and video files from the appliance, and then reinstalls the operating system and Cisco VSM software. Perform this procedure only if necessary.

Topic	Related Document	Description
API Reference	• *Cisco Video Surveillance API Programming Guide* • *Cisco Video Surveillance API Reference Guide*	Describes the application programming interface (API) used to display video using third party applications. **Note** These documents are available on the Cisco Developer Network (CDN). See you Cisco support representative for more information.
Migrating a 6.3.2 system to release 7.0	*Cisco Video Surveillance Migration Guide, Release 6.3.2 to 7.0*	Describes how to migrate a release 6.3.2 Cisco Video Surveillance Manager (Cisco VSM) deployment to release 7.0. Migrating a Cisco Video Surveillance deployment from release 6.3.2 to release 7.0 is a one-time process that is performed using a special set of Cisco utilities. You can migrate the entire deployment, including all Media Servers at a single time, or migrate the Media Servers over an extended period of time. **Note** This document is available on the Cisco Developer Network (CDN). See you Cisco support representative for more information.